

RAZA

MEXICANA

RAZA MEXICANA • MEXICO • NUMERO 15 • NOVIEMBRE 2003 • WWW.RAZA-MEXICANA.ORG



Se sacan passwords de
hotmail, yahoo, latinmail, etc.

Se rootean servidores : Unix,
linux, win.

Se instalan troyanos,
keyloggers, dumpers, sniffers,
etc.

Absoluta discreción, 100%
profesionales, resultados
garantizados, varias formas de
pago.

gotroot@hackersmail.org.mx

Editorial

Últimamente me he encontrado en varios lugares con personas que hablan de hackers, de robar passwords, de violar redes, inclusive hay gente que ya empieza a verle un símbolo de dólares al hack (aquí en México). Y ni hablar de las publicaciones escritas, ya casi en cualquier revista que leo hay un artículo de hackers, hasta en el libro sentimental que lee mi Madre vi algo sobre hackers.

Sin lugar a dudas los hackers están invadiendo todos nuestros ámbitos, desde los que violan passwords para sacar información de auditorias al gobierno, los que lanzan ataques DoS a servidores del gobierno hasta los que cambian las presentaciones de powerpoint para poner pornografía.

Me gusta pensar en la idea de que raza-mexicana ha tenido participación en este cambio de cultura, que de alguna forma fuimos, somos y seremos parte del cambio, esto me recuerda las palabras de un ex miembro de raza que tuve la oportunidad de ver en el razatour2003, le cuestionaron el porque dejó raza, a lo cual respondió que ya no encontraba un beneficio personal; eso me dejó pensando en cual era el beneficio que obtenía al ser miembro de raza. Estar horas frente al monitor, pasar noches sin dormir, dejar a un lado mi vida social, descuidar mi escuela, dormirme en el trabajo, todo esto vale la pena cuando abro mi correo y encuentro un email donde veo que alguien se cuestiona, cuando leo que alguien esta buscando sus propias respuestas y no se conforma con leer un ezine y creer en todo lo que ahí se dice, ese es mi beneficio personal.

Bueno, ahora que lo pienso también tengo otro beneficio: el tener la oportunidad de convivir con gente como yo, así de locos, de desvelados, de inquietos, de irreverentes, de inconformes, de buscadores, de luchadores, de gente que genera cambio y rompe paradigmas, de weyes que comparten el conocimiento, eso es algo por lo que vale la pena estar aquí.

Vlad

¿Usar la licencia GPL es regalar mi trabajo?	1
¿Linux en PlayStation 2?	3
Bienvenido a IRC_Raza - El Lado Humano part Deux	8
La resaca de Argelia	16
Comando NET para NT / WIN2K / XP	21
NetSh	28
PEV (Pulso Electromagnético Virtual)	32
Técnicas de Escaneo	37
Inutilizando Win9x	48
La verdadera historia del virus Crond	51
Entrevista a Presidencia de México	55
SQL Injection en Intertel	61
Ebuzon	62

Razatour2003

Me desperté boca abajo y no sabia donde estaba, me sentí el cuerpo desnudo y dije : 'esto no me va a gustar nada', gire y vi al abuelo (DeadSector) mirándome fijamente desde la orilla de la cama y me dijo... : 'te tengo una buena noticia y una mala noticia' y dije : 'ahora si ya valió...'

Yield df-sep-21-2003

¿Usar la licencia GPL es regalar mi trabajo?

Por Kukulkan (kukulkan@raza-mexicana.org)

Mucha gente tiene la idea errónea de que crear programas bajo la licencia GPL es el equivalente a regalar su trabajo, se cree que se está obligado a compartir ese código creado por el esfuerzo de una persona, esto es totalmente erróneo.

La GPL jamás habla de "regalar" el programa, de hecho, no habla sobre precios o valor del trabajo, simplemente de la libertad que se le concede a la persona que adquiere el software, esto es, microsoft crea sus windows, y los vende, mas si quieres hacer una modificación a la GUI, o personalizar a fondo tu ambiente de trabajo, no puedes, porque no te da el código fuente, con la GPL la diferencia estriba en que tu obtendrás el código fuente, mas sin embargo puedes vender ese software al precio que consideres tu, si quieres venderlo en millones de pesos, o dólares y alguien te lo paga, no se infringe a la GPL, si tu compras un programa bajo la GPL, tendrás el código, tal vez si eres un gerente o publicista, no te importe mucho, peor si eres curioso y deseas saber como funciona, tienes acceso al código, y puedes modificarlo a tu gusto, SIN TENER QUE PUBLICAR TUS MODIFICACIONES, solo si tu lo llegas a vender, con tus modificaciones, deberás también venderlo junto con el código fuente.

Hay otra licencia menos "dura" en cuanto al código fuente, esta es la LGPL, la cual permite enlazar tu programa a librerías GPL, mas no te obliga a vender tu programa junto con el código fuente, solo el binario, así que, trabajar con GPL no significa REGALAR tu trabajo, es simplemente una garantía de que se sabrá quien fue el programador siempre, que el código será libre y alguna empresa no puede apropiárselo y decir que es de ella, puede modificarlo y vender la modificación, pero junto con el código, la GPL permite que se tengan esas mismas libertades que tienes al comprar artículos de uso diario, imagina si tu carro no tuviera cofre y no puedes modificarle nada, si tu computadora viniera sellada y no hubiera forma de abrirla para expandirle RAM, insertarle discos duros o una quemadora, una casa construida sin forma de hacerle remodelaciones o ampliaciones. Sería ridículo, tal como es ridículo comprar software y no sepas como funciona, que es lo que hace y adaptarlo a TUS NECESIDADES, no tiene nada que ver que si es GRATIS, esta es una traducción muy estúpida de "FREE", en realidad se habla de LIBERTAD, de la libertad de estudiar el código, de leerlo, y modificarlo, no de "bajarlo gratis" de la red, o de que no implique algún costo, esto es totalmente erróneo, puedes crear programas, y no regalarlos, si no venderlos bajo la GPL, o bien la LGPL, porque no vives de código, necesitas comer, vestir y viajar, necesitas dinero para eso, vende tus ideas =).

Esto es un extracto de la pagina <http://www.gnu.org/philosophy/free-sw.es.html>:

El "Software Libre" es un asunto de libertad, no de precio. Para entender el concepto, debes pensar en "libre" como en "libertad de expresión", no como en "barra libre"[N. del T.: en inglés una misma palabra (free) significa tanto libre como gratis, lo que ha dado lugar a cierta confusión].

``Software Libre" se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. De modo más preciso, se refiere a cuatro libertades de los usuarios del software:

- La libertad de usar el programa, con cualquier propósito (libertad 0).
- La libertad de estudiar cómo funciona el programa, y adaptarlo a tus necesidades (libertad 1). El acceso al código fuente es una condición previa para esto.
- La libertad de distribuir copias, con lo que puedes ayudar a tu vecino (libertad 2).
- La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie. (libertad 3). El acceso al código fuente es un requisito previo para esto.

Como bien lo dice ahí, son "Libertades", tienes la libertad de hacerlo, y claro, puedes cobrar por ello. Otras cosas similares se aplican al termino "Open Source", el cual tampoco implica algo sobre los costos, siempre se refieren a lo mismo, las libertades que te ofrecen.

Entonces, queda claro que en la licencia GPL JAMAS, se habla del precio, ni que sea GRATIS, habla de LIBERTADES, así pues, hay proyectos que se venden a empresas, de pequeños con valor de 6000 pesos, a grandes de mas de 100 mil pesos hechos en SOFTWARE LIBRE, no gratis, si se puede sacar dinero del software libre, la única diferencia entre vender software libre y software propietario, es en que al cliente se le entrega el código fuente de tal aplicación, o bien, si no se quiere dar el código, se trabaja con la LGPL y no hay problema alguno.

¿Linux en PlayStation 2?

Por Extraterrestre (extra@marihuana.com)

Al parecer Sony no se conforma con que su famosa consola sea simplemente un VideoJuego, ahora tras recientes estudios de compatibilidad hechos, se ha demostrado que PS2 puede convertirse en un poderoso ordenador, y mediante esta breve escrito analizaremos la manera de convertir nuestro PlayStation 2 en una Computadora.



1. El Hardware necesario

Además tu Playstation 2, necesitas algo llamado Playstation Linux Kit que también es distribuido por Sony y tiene un costo aproximado de \$199.99 dls(unos 2000 pesos mexicanos), asegúrate de que al comprar tu Linux Kit este sea para la región designada para tu PS2, la venta de este Kit esta sólo autorizada a hacerse vía Internet, para protegerse un poco de la "piratería", al final de este artículo encontraras la dirección donde puedes comprar el Linux Kit, por algunas cuestiones, este Kit no es distribuido en México, pero bueno eso se soluciona contratando algún servicio como LanBox o algo así, donde podamos tener una dirección postal en USA.

¿Qué contiene el Playstation Linux kit?

El linux Kit contiene:

- El Linux para PS2, versión 1.0
- Cable adaptador, para conectar tu PS2 a un monitor de PC.
- Disco Duro externo de 40 GB.
- Adaptador de Ethernet 10/100(Modem No Incluido, también se puede añadir).
- Teclado y Mouse USB



Todos estos son fáciles de conectar a la Consola y no necesitan ningún aditamento extra, una de las ventajas que ofrece este Kit es la de poder empezar a crear nuestros propios juegos para PS2 en tiempo real, mediante este Linux Kit podremos conectarnos a Internet para poder actualizar constantemente nuestro Sistema Operativo, ya que también es

compatible con cualquier otro Software para Linux que exista en el mercado. Se espera que en próximos años esto deje de ser un aditamento y ya venga como parte del PlayStation 3, pero mientras esto suceda, aquí tenemos una buena opción para entretenernos un rato. Algo importante para el correcto funcionamiento del Linux Kit es que nuestro Playstation debe contar con una Memory Card de 8 mb(mínimo), la cual será también formateada al momento de la instalación.

¿Qué no se puede hacer con el Playstation Linux Kit?

Los usuarios no pueden quemar un CD o un DVD con un juego desarrollado en el Linux kit. Esto es desafortunado, pero comprensible ya que Sony quiere proteger a sus desarrolladores comerciales. La mejor solución para esto simplemente será conectar el Disco Duro Externo a cualquier otra PC con Quemador.

¿Qué Monitores son compatibles con el Linux PlayStation Kit?

La lista completa de monitores disponibles la encontraras en la siguiente URL:
https://playstation2-linux.com/docs/ps2linux/display_doc.php?docid=5&raw=1

2. Software Recomendado

Aunque Sony ha lanzado ya su Linux PlayStation 1.0, me gustaría meterme más en otra opción que nos ofrece la compañía xRhino que ha lanzado ya su versión Linux para Playstation llamada BlackRhino, basado en Debian-based GNU/Linux. Recomiendo esta versión ya que responde bien a las necesidades. BlackRhino Linux contiene mas de 1200 paquetes de Software que incluyen desde juegos a editores de texto, compiladores, servidores web, sistemas de ventanas, bases de datos, paquetes gráficos, servidores de correo y otras utilidades. El primer paso para poder contar con esta versión, es mediante Download de la pagina de xRhino, <http://blackrhino.xrhino.com/main.php?page=download> ahí contaremos con los diferentes Mirrors para bajar la Imagen Base que tan solo pesa 21.8 MB.

¿Cómo Instalar BlackRhino GNU/Linux(Traducido de la página Oficial del BlackRhino)?

- Preparación
- Una vez bajada la Imagen Base
- Instalación
- Actualizando el Sistema

Preparación

Instala el Sony Playstation 2 Linux en /dev/hda1, este viene con el Playstation Linux Kit del cual hablamos en el apartado anterior crear una partición de 4GB para el BlackRhino GNU/Linux 1.0. La partición minima es de 1 GB.

Monta la nueva partición

Ejemplo:

```
fdisk /dev/hda
n (Create a new partition.)
p (The new partition will be primary.)
3 (/dev/hda3 will be the new partition's designation.)
+4096M (It will be given a size of 4GB.)
w (Write the new partition table and quit.)
mke2fs /dev/hda3
mkdir /mnt/brl
mount -t ext2 /dev/hda3 /mnt/brl
```

Obtén la Imagen Base

Cambia tu directorio de trabajo a la Nueva Partición Montada

Si ya tienes tu Tarjeta Ethernet configurada, baja el BlackRhino directamente de la URL, si no es así, solo monta el CD ROM y cópialo directamente del archivo que hayas bajado.

Ejemplo:

```
cd /mnt/brl
wget http://playstation2-linux.com/files/blackrhino/blackrhino_baseimage-1.0.tar.gz
```

Instalación

Un-tar blackrhino_baseimage-1.0.tar.gz a la nueva particion montada.

Edita tu configuración de red en etc/network/interfaces (los ejemplos pueden encontrarse en /usr/share/doc/ifupdown/examples/).

NOTA : El soporte para red dinámica no esta incluido en el stock v2.2.1 Sony Playstation 2 Linux Kernel, tu podrás iniciar usando una configuración estática de red (o un diferente kernel con soporte para red dinámica)

Edita el etc/hostname and etc/resolv.conf Hostname y Configuración DNS

Edita el etc/apt/sources.list y escoge el Mirror para el BlackRhino de tu preferencia.

Edita el etc/fstab para mostrar la nueva partición booteable del BlackRhino.

Edita tus Memory card's en el archivo p2lboot.cnf y añade una entrada para bootear en la nueva partición creada.

Si tu usas una televisión como monitor, pon la configuración del p2lboot.opt igual a "ntsc" o "pal".

Reinicia tu PS2 en GNU/Linux.

NOTA : Solo la cuenta del root existe en la Imagen Base y el password esta en blanco.

Ejemplo (tu puedes estar en el directorio /mnt/brl):

```
tar zxvf /mnt/brl/blackrhino_baseimage-1.0.tar.gz
```

```
vi /mnt/brl/etc/network/interfaces
```

Usa las platillas de /usr/share/doc/ifupdown/examples/ si es necesario

```
vi /mnt/brl/etc/hostname
```

Teclea tu Hostname asignado

```
vi /mnt/brl/etc/resolv.conf
```

Teclea tu dominio en la primera línea, y la dirección IP en las líneas subsecuentes.

```
vi /mnt/brl/etc/apt/sources.list
```

Sin comentarios la línea "deb" para activar el Mirror

```
vi /mnt/brl/etc/fstab
```

Cambia le entrada del root ("/") de modo que la aplicación use /dev/hda3.

```
mount -t ps2mcfs /dev/ps2mc00 /mnt/mc00
```

```
vi /mnt/mc00/p2lboot.cnf
```

Añade una línea similar a lo siguiente

```
"BlackRhino" vmlinux "" 203 /dev/hda3 "" BlackRhino GNU/Linux 1.0
```

```
vi /mnt/mc00/p2lboot.opt
```

Añade la siguiente línea:

```
display=ntsc
```

```
reboot
```

```
blackrhino login: root
```

```
Password: [enter]
```

```
Updating Your System
```

Después de que hayas rebotado BlackRhino GNU/Linux system, asegúrate de que tu configuración de red este funcionando correctamente dando un ping a blackrhino.xrhino.com. Si tu ping es respondido, tu configuración esta correcta. Realice una actualización del "dselect" en el sistema

Ejemplo:

```
ping blackrhino.xrhino.com
```

```
dselect
```

```
U [enter] (Update the package database.)
```

```
S [enter] [space] [enter] (Select packages. Make changes if you like.)
```

```
I [enter] (Install new packages. Wait for the process to finish.)
```

```
y [enter] (Allow dselect to remove the installed package archives.)
```

```
Q [enter] (Quit dselect.)
```

Playstation, Playstation 2, Sony, xRhino, BlackRhino y el Pinguinito de Linux son Marcas Registradas.

URLografía

<http://www.linuxplay.com> Sitio Oficial del Linux PlayStation Kit

<http://blackrhino.xrhino.com/>

<https://playstation2-linux.com/>

<http://www.jp.playstation.com/linux/>

<http://www.ciudadfutura.com/ps2/articulos/linuxkit.html>

En la próxima entrega: Como convertir los controles de PlayStation a serial para PC.

Bienvenido a IRC_Raza - El Lado Humano part Deux

Por DeadSector (deadsector@raza-mexicana.org)

irc.raza-mexicana.org puerto 30003

La siguiente historia es verídica. Los nombres han sido cambiados para proteger la seguridad de los protagonistas. Los nombres de dominio y sus respectivos IPs también fueron cambiados. Quiero agradecer a nul0ts por su valiosa ayuda. sin el esta historia no hubiera sido posible, siempre serás bienvenido y apreciado en raza nul0ts

Fecha : Miércoles 28 de Mayo de 2003 las 21 horas con 50 minutos

Lugar: un servidor irc muy muy lejano en lo mas under del internet

```
Session Start: Wed May 28 21:50:59 2003
Session Ident: #razamex
[21:50:59] * Now talking in #razamex
[21:50:59] * Topic is '[17:31:06] <qw3rt1> ahora que para articulos
chingones los de Fatal [17:31:16] <qw3rt1> a ese wey si le doy un beso en
su pipi'
[21:50:59] * Set by Yield on Wed May 28 18:55:03
[21:50:59] -irc.raza-mexicana.org- *** Notice -- DeadSector
(~guest@2AFBD132.9797C07C.30ED0294.IP) is now a network administrator (N)
```

Era una noche como cualquier otra, los presentes discutían de las mismas cosas cotidianas:

```
[21:51:00] <Fatal> Y por eso son mejores los ataques stackd based que los
non-stacked based
[21:51:03] <Fatal> Lero lero.
[21:51:04] <wireless> no. todo depende de cuanto tengas en memoria para
trabajar. no siempre se puede hacerlo a tu manera
```

Estemm, bueno, eso lo invente para hacer mas verídica la historia, los verdaderos logs decían esto:

```
[21:51:00] <Fatal> Eliminan a Cruz Azul de la Libertadores
[21:51:03] <Fatal> Lero lero.
[21:51:04] <wireless> si
```

La gente seguía entrando e integrándose a la platica como siempre discutiendo nuevas ideas, compartiendo nuevos conocimientos :

```
[21:53:54] * RaW (RaW_III@1BB959E8.9C31793A.2DAA616.IP) has joined
#razamex
[21:54:39] * RaW (RaW_III@1BB959E8.9C31793A.2DAA616.IP) Quit (Quit: )
[21:58:36] * Darksource (darksource@274A3C1.431590DC.47E3F80A.IP) has
joined #razamex
[21:58:59] <wireless> hola Darksource
[21:59:05] <Darksource> hola wireless
[21:59:06] <wireless> quien dijo quake?
[22:00:57] <Fatal> Aguanten.
```

```
[22:01:10] <Fatal> Dejenme instalo unas librerias.  
[22:09:55] <Xy-Out> y la rata??  
[22:10:08] <Xy-Out> ALGUIEN INVOQUE A LA RATA  
[22:15:22] <Fatal> Listos?  
[22:15:32] <wireless> casi termino de cenar  
[22:15:40] <a_d_mIRC> a veces medio apendejados, pero aqui andamos
```

Todo parecía que la noche seria como cualquier otra, pero algo que nadie esperaba estaba a punto de suceder muahahahaha (risa macabra)

```
[22:45:41] -irc.raza-mexicana.org- *** Notice -- Client connecting on
port 30003: nul0ts (~mexican@148.266.257.14)
[22:45:41] * nul0ts (~mexican@3ED5C0B7.E1DA74A9.A3EEB7F.IP) has joined
#razamex
```

Nadie sospechaba que algo inesperado iba a suceder, mucho menos yo, cuando en mi pantalla salió una línea que decía:

```
[22:50:00] <nul0ts> se supone que http://midominio.org es vulnerable al
exploit chunked encoding ya lo mande
```

Y no paso nada, nosotros seguíamos tratando asuntos avanzados.

```
[22:50:01] <a_d_mIRC> como explicatias en esta situacion el ser ninja y
el ser samurai???
[22:50:13] <DeadSector> eres un pendejo sin cerebro. no eres mas bruto
porque te faltaron golpez en tu niñez. yo no hice nada pero me di cuenta
la primera vez que use el quad que algo andaba mal. pero tu por mas que
te chingaban lo seguias agarrando
[22:50:31] <a_d_mIRC> AAJJAJAJAJAJAJAJJJAJAJAJA
[22:50:56] <Lolito> Ni madres, te vacie la bfg mas de 5 ocasiones y no te
pasaba nada.
```

nul0s seguía insistiendo

```
[22:52:17] <nul0ts> pinche exploit no funciona!  
[22:57:02] <nul0ts> porque no funciona el exploit  
[22:57:07] <nul0ts> el server sigue como sin nada  
[22:57:59] <DeadSector> http://midominio.org <-- porque usaste ;  
[22:58:30] <nul0ts> segun el retina scanner ese server es vulnerable  
[22:59:30] <brotoloco> Qu epedo  
[22:59:34] <DeadSector> retina no puede comprobar muchas cosas . tambien  
depende como lo tengas configurado. muchas pruebas no las hace porque  
sabe que puede tumbar el server  
[22:59:44] <nul0ts> mta  
[23:00:02] <nul0ts> entonces ese server no es vulnerable??  
[23:00:17] <DeadSector> y aparte no sabemos ni que exploit estas usando  
[23:00:22] <DeadSector> o de que estas hablando  
[23:00:30] <DeadSector> o que server es  
[23:00:31] <DeadSector> etc  
[23:00:51] <nul0ts> estoy usando este exploit
```

Pasaron 1 minutos 20 segundos y parecía una eternidad. no decía que exploit estaba usando y la gente se aburría esperando

```
[23:02:11] <brotoloco> uh..  
[23:02:26] <psy2> 8=====D
```

Y al fin, después de una larga espera de 3 minutos 11 segundos contesto

```
[23:03:02] <nul0ts> http://packetstormsecurity.nl/0207-exploits/apache-  
chunk.c  
[23:03:24] <nul0ts> use este  
[23:03:34] <brotoloco> he que pedo  
[23:03:34] <brotoloco> con los partidos  
[23:03:42] <nul0ts> porque creen que no funciona  
[23:03:43] <nul0ts> ??  
[23:03:51] <brotoloco> porque es anti kiddie  
[23:04:02] <brotoloco> tiene sus travas para que no cualquiera lo  
compile.  
[23:04:29] <nul0ts> lo compilo Duck  
[23:04:41] <brotoloco> nul0ts: y tu no ?  
[23:04:44] * Yield (~yield@2C8B3CF3.C1EF8A8F.61D3A90F.IP) has joined  
#razamex  
[23:04:45] -irc.raza-mexicana.org- *** Notice -- Yield  
(~yield@2C8B3CF3.C1EF8A8F.61D3A90F.IP) is now a network administrator (N)  
[23:05:09] <nul0ts> no porque no tengo el gcc  
[23:05:38] <nul0ts> porque creen que no funcino?  
[23:05:39] <DeadSector> nul0ts: no te quiero dar kill. ya leiste el  
exploit lo que dice?  
[23:05:45] <DeadSector> leelo por favor  
[23:06:23] <nul0ts> ya lo lei  
[23:07:39] <DeadSector> sepa pepa nul0ts . yo no se.yo no uso linux y no  
tengo experiencia con xploits de linux  
[23:08:01] <brotoloco> nul0ts: Como te compilaron el exploit y luego tu  
usaste ese ejecutable en tu b0x ???  
[23:09:13] <nul0ts> #/mnt/hda1/Linux/a.out midominio.org  
[23:09:15] <brotoloco> si ese ejecutable te lo compilaron con alguno nix  
que no es igual al tuyo, seguro que no correra. eso es logico  
[23:10:13] <nul0ts> si lo ejecuta bien  
[23:10:37] <Yield> orion:/home/yield/kde-src # ./apache-chunk  
midominio.org  
[23:10:37] <Yield> Apache-Chunk.c By bob. [www.dtors.net]  
[23:10:37] <Yield> ---[+] Looking up host : midominio.org.....  
[23:10:37] <Yield> ---[+] Connecting...  
[23:10:37] <Yield> ---[+] Sending...  
[23:10:37] <Yield> ---[+] Sent!  
[23:10:39] <Yield> juar XD  
[23:11:24] <nul0ts> eso mismo me sale  
[23:11:41] <brotoloco> ??  
[23:11:44] <brotoloco> jaj
```

La gente trataba de explicarle

```
[23:11:51] <brotoloco> sera porque no es vulnerable ?  
[23:11:54] <Yield> esta parchado
```

Pero seguía con dudas

```
[23:11:58] <nul0ts> mta pinche scanner
[23:12:05] <brotoloco> :P
[23:12:07] <nul0ts> y segun me marco 22 servers
[23:12:09] <nul0ts> vulnerables
[23:12:35] <brotoloco> ...
[23:12:54] <brotoloco> jaja yo ya estuviera g-lineado de por vida.
```

Yieldo amablemente trataba de explicarle a su nuevo padawan

```
[23:12:59] <Yield> eso se llama falso positivo
[23:13:07] <nul0ts> y porque los marca
[23:13:08] <nul0ts> ?
```

Yieldo nuevamente trataba de explicarle a su nuevo padawan

```
[23:13:10] <DeadSector> porque solo checa versiones en reply y no intenta
joderlos para verificar. puedes configurarlo para que lo haga
[23:13:17] <brotoloco> checa las vers
[23:13:18] <Yield> otra vez nul0ts
[23:13:19] <Yield> eso se llama falso positivo
[23:13:53] <nul0ts> ah ok
[23:13:57] <nul0ts> ahora entiendo
```

Aquí fue donde ya no pude aguantarme, algo dentro de mi gritaba que le diera kill o kline o joderlo de alguna manera, que buscara info de su familia de sus amigos o enemigos y que destruyera su vida, la de sus amigos y la de sus parientes, que era mi deber borrar todo rastro de su existencia, pero la parte amable y débil de mi me dijo que solo debería jugarle una broma.

Nada de lo que va a suceder fue planeado, he ahí lo hermoso de lo que sucedió.

```
[23:14:19] <DeadSector> nul0ts y para que no haya malentendidos y luego
digan que te jodi a la mala. te aviso que estoy mandando email a
contactos de midominio.net . no quiero problemas legales. si no digo nada
me estaria haciendo complice tuyo
[23:14:32] <DeadSector> solo mandare logs de irc
[23:14:41] <DeadSector> sin ips ni nada
[23:14:51] <nul0ts> no wey no le paso nada
```

Ja. no tenia idea que ese era solo el comienzo

```
[23:15:09] <DeadSector> solo lo que vi en este canal. no mandare info de
whois ni nada de eso
[23:15:15] <nul0ts> ok
```

De seguro pensó "pos ya que" y estoy seguro que nunca se imagino lo que estaba a punto de suceder. La gente le seguía explicando, yo había pasado esa etapa y estaba haciendo whois al dominio

[23:15:47] <brotoloco> checa los headers. de cada httpd Talvez lo alteraron o ta parchado y se quedo con la misma version pero parchadito. Y no le hace nada ese DoS
[23:16:46] * brotoloco a cenar
[23:17:33] <Yield> nul0ts mejor aprende a usar linux, aprende a compilar programas, aprendete el software que hay y despues tratas algo mas avanzado

Aquí ya tenia listo mi segundo programa de irc con nuevos datos. solo tenia que preparar a nul0ts

[23:17:35] <DeadSector> wow. que hora es en españa ? no mames. ya me contestaron el email. un tal carlos terront. quiere saber el ip de este server y el puerto para conectarse
[23:17:46] <DeadSector> vergas
[23:17:49] <DeadSector> no le voy a contestar
[23:17:53] <nul0ts> no wey
[23:17:53] <nul0ts> please
[23:17:55] <Yield> rola su mail

nul0ts ya se empezaba a preocupar, por las prisas tampoco pude avisarle a mis compañeros de mis planes, pero el momento había llegado. Entré con un nuevo nick “cterront” .

[23:18:45] <DeadSector> a que jijo de su madre. me esta amenazando
[23:18:51] * cterront (~midominio@1F4C2367.5F3D5C6D.76096087.IP) has joined #razamex
[23:18:57] <cterront> buenas noches
[23:19:06] -irc.raza-mexicana.org- *** nul0ts (~mexican@3ED5C0B7.E1DA74A9.A3EEB7F.IP) did a /whois on you.
[23:19:06] <cterront> quien me mando el log?
[23:19:15] <DeadSector> yo
[23:19:20] <nul0ts> :S
[23:20:19] <nul0ts> !
[23:20:39] <DeadSector> pero era juego
[23:20:41] <DeadSector> era broma
[23:21:09] <cterront> mira muchacho. para mi no es broma. estas hablando de mi trabajo
[23:22:07] <DeadSector> quise mandar email a midominio.net fue un simple error. no estes chingando
[23:22:12] <DeadSector> ademas tus leyes no nos afectan
[23:22:33] <Yield> y mientras no hayan existido daños no hay problema
[23:23:03] <cterront> pero estoy checando logs y alguien trato de atacar mi server justo en el momento que me llego el email
[23:23:14] <DeadSector> pero es coincidencia. ya te dije
[23:23:21] <DeadSector> yo quise mandar a midominio.net
[23:23:23] <DeadSector> o com
[23:23:27] <DeadSector> no me acuerdo el link exacto

Hasta este momento nadie sospechaba que era yo, con la excepción de yield . pero también me seguía la corriente, estos son logs de canal privado con yield. cuando le escribí en privado a nul0ts pensé que se daría cuenta quien era

[23:19:32] <cterront> que pedo?

[23:19:39] <nul0ts> ?
[23:19:48] <nul0ts> k paso
[23:19:51] <cterront> estas jodiendo mi server?
[23:20:26] <nul0ts> yo? por que lo dices ?

Y con yield

[23:20:07] <DeadSector> ya la cague. puto autooline
[23:20:30] <Yield> te hizo whois?
[23:20:51] <cterront> si
[23:20:53] <cterront> dammm
[23:20:56] <cterront> deja ver si todavia se la cree
[23:21:03] <Yield> entonces si la calabazeaste

Mientras tanto en canal publico seguíamos fingiendo

[23:23:57] <Yield> pega el IP del supuesto atacante y te digo si alguien de aqui lo tiene
[23:24:07] <cterront> pues yo tambien estoy mandando email al encargado de seguridad. en este momento hablara por telefono con su isp. vale mas que me entregues el ip de nul0ts o tambien tendran problemas
[23:24:36] <Yield> pero pega tu el log del atacante y vemos si coincide
[23:24:39] <cterront> si no lo hacen se estan convirtiendo en complices. les cerraran su irc server en un abrir y cerrar de ojos
[23:24:59] <cterront> quiero que me entreguen a nul0ts. lo exijo

El pobre nul0ts no decía nada. ya queria llorar, solo mandaba privados a yield y a mi con cosas como

[23:21:42] <DeadSector> [23:21:23] <nul0ts> no mams wey dale kill
[23:21:49] <Yield> juar
[23:22:00] <Yield> me voy a ahogar con la cena
[23:25:03] <Yield> [23:25:12] <nul0ts> no wey no se lo des porfavor
[23:25:38] <DeadSector> [23:21:55] <nul0ts> porfavor
[23:25:54] <Yield> no mames, queria cenar tranquilo, me ahogo de risa

Y en canal publico seguía la acción

[23:25:21] <DeadSector> mira. en buena onda. ya te dije que era broma. nadie te quiso hacer daño
[23:25:29] <Yield> primero pega el IP de tu supuesto atacante y te digo si coinciden, de ser así pos ya te lo llevas
[23:26:03] <cterront> 148.266.257.14 <-- (si era el ip real de nul0ts
[23:26:10] <DeadSector> ese no es
[23:26:12] <DeadSector> te chingaste
[23:26:32] <DeadSector> nul0ts is connecting from *@200.543.274.45 <-- ip ficticio
[23:26:36] <Yield> eip, no coincide
[23:26:47] <cterront> buscare ese ip en logs tambien
[23:26:53] <cterront> pero estoy seguro que fue uno de ustedes
[23:27:18] <Yield> nel, no fue nadie de aqui
[23:27:43] <cterront> miren. no voy a batallar. este es mi trabajo. no voy a dejar que unos chamaquitos me vengan a chingar.en este momento se

Pero unas cosas deberíamos platicarlas. Si alguien sabe algo de leyes en México que nos diga si puede suceder o no.

Si vemos que alguien entra a chat y relata actos ilegales deberías delatarlo?

Te haces cómplice si te quedas callado?

Podrían tener problemas los que están conectados y no dicen nada?

Deberían estar públicos los IPs de usuarios para evitar problemas legales?

Ustedes perderían su empleo o irían a cárcel para proteger a alguien que esta haciendo cosas ilegales?

Si le explicas a nul0ts como funciona un exploit y el hace algo ilegal con esa información eres culpable?

Son demasiadas preguntas y me gustaría discutir las, están todos invitados a <irc.raza-mexicana.org> puerto 30003 ahí serás siempre bienvenido .

Nos vemos.

La resaca de Argelia

Por RMHT (staff@raza-mexicana.org)

El siguiente texto fue extraído de un foro de CUM (Textualmente, con puntos y comas, errores ortográficos y dedazos).

Autor : LoTek

existe el under mexicano?

« **fecha:** Febrero 4th, 2003, 10:22am »

El under mexicano ya no existe ya es historia.

Acid klan, rebelión, raregazz y x-ploit ya murieron ya no existen. Ahora solo queda teams como mhm, hakim, etc. y claro las cenizas de raza-mexicana que se resiste a morir.

Mhm: han encontrado buenos avances en telefonía pero porque sigue siendo un team mediocre? Porque no comparte la información y lo usan para beneficio personal. No digo que pongan un hex. funcionando en su pagina pero que ayuden mas y no sean tan egoístas, ahora quieren hacer un foro privado con la “elite” en telecards. Telmex FUCK!!!!

Hakim: la mayoría de sus textos son viejos traducidos y copiados de otras paginas, estos no investigan solo recopilan según ellos lo mejor. Les falta ponerse a investigar y no andar traduciendo textos.

Raza-mexicana: Un team que se resiste a morir fue de los mejores teams pero ahora que sacan su e-zine 14 me moría de la risa porque decía que X-ploit no existe. porque habrán dicho esto por que Nadamas defaceamos webs del gobierno mexicano y ellos la mayoría de sus defaces eran de servers vulnerables. Pues no se por que habrán dicho esto en su e-zine pero raza mexicana ya debería desaparecer porque nada mas esta haciendo el ridículo publicando mentiras y yo no voy a hacer envidioso como ustedes. Uno de los únicos teams mas chingones del under mexicano.

Pero bueno el under mexicano ya no existe y ni existirá porque a usted les da flojera ponerse a investigar.

LoTek

Autor : DeadSector

Re: existe el under mexicano?

« **Responder #11 fecha:** Febrero 6th, 2003, 9:46pm »

lo que voy a escribir es mi opinion y no la de raza-mexicana .

para empesar se nota a webo que lotek no es xexploit. solo un pendejo podria escribir como lo

esta haciendo este wei.

los nombres que mencionan como raregazz , rebellion , raza etc comparten o compartian los mismos miembros. los integrantes mandaban articulos a los diferentes grupos y portaban varias banderas al mismo tiempo.

si el under esta o no esta muerto es cosa que les debe valer pito.

para los newbies que leen esto , no hagan caso de pendejadas como este post. sigan haciendo sus paginas . compartiendo articulos o ezines. sigan con mirrors. sigan haciendo posts en forums como este. nunca se queden callados ni dejen que cualquier pendejo quiera decirles como deben ser las cosas. los que puedan desarrollar que lo hagan. los que quieren aprender pregunten. no existen malos estudiantes. solo malos maestros.

olvidense de los "elites" yo prefiero un amigo newbie con ganas de aprender y compartir que una bola de esos weies elitistas pesimistas. ese tipo de personas no aportan , no comparten , ni ayudan a desarrollar el under mexicano.

la gente que dice que raza esta muerto son las mismas que eran parte del team. ellos tienen una mentalidad de " si no estoy en el team ya no debe existir el team"

raza no es una persona ni dos ni tres.

esta gente habla de raza-mexicana como si nunca hubieran tenido la oportunidad de cooperar con el grupo. como si nunca hubieran tenido nada que ver con lo que es hoy. y como si nunca hubieran tenido la oportunidad de darle direccion al grupo.

es como un viejo decir " la generacion de hoy suckea webos de burro"

como si la nueva generacion hubiera crecido sola sin ellos tener nada que ver con su desarrollo.

en mi opinion xexploit es igual que moskoz wfd o cuakquier otro grupito de crackers haciendo defacements estupidos y sin sentido.

un defacement ayer es igual a uno hoy.

lotek no es diferente a cualquier script kiddie de hoy que se pasa haciendo defacements .

que piensan ustedes hoy de kiddies que hacen defacements?

ayudaron mucho al under mexicano 4 defacements? ayudaria mas si hacen 100? o 1000 ?

un buen articulo vale mas que 1000 defacements. no importa que los defacements sean a paginas de gobierno o que tengan fotos de sub marcos o zapata.

no dejen de cooperar . no dejen de aprender , no dejen de preguntar.

en raza-mexicana nos dimos cuenta que la manera de aportar no era con defacements estupidos y sin sentido. no estamos orgullosos de los que hicimos y no pensamos apoyar a quienes los hagan.

raza-mexicana esta muriendo porque ya no estoy en el grupo ? no pinches mames

el under no existe ni existira porque ya no estoy yo ? has de ser una leyenda en tu propia mente si piensas asi.

el programa que desarrollaste no es bueno si no es open source? ni madres. no regalen su trabajo . si desarrollaste un buen programa que la gente quiere y esta dispuesto a pagar por el bien por ti.

ser hacker no tiene nada que ver con windows o linux ni open source. es una manera de pensar . un modo de vida . una manera de enfrentar los retos que te ponga la vida .

este wei se encabrona porque MHM (segun el) tiene info que no quiere soltar. no seas mamon. estarian echando a perder el trabajo de meses o años. y serian unos pendejos si andan soltando info . lo que pide es lo mismo que entrar a este forum a pedir cuentas de telmex o que alguien les hackee hotmail.

bueno en fin. esta es mi opinion y las opiniones son como los jundios , todo mundo los tiene .

Autor : Kukulkan

Re: existe el under mexicano?

« **Responder #12 fecha:** Febrero 6th, 2003, 10:14pm »

Yo difiero en algo con el pinche viejo, si se debe compartir la información, (si no, niquiera habría ezine) aunque alguna info no se puede rolar por ser muy confidencial y que pueda meter en problemas.

En cuanto a lo que ice lotek, yo creo que suceka webos de burro, niquiera se sabe si es el original o no, cualquiera que lea una ezine (que pinche weba leer ese articulo de fatal) o vea mirrors de webcracks puede decir eso, ademas tanto como decir que "murio" pues no, si esta bien que la gente de hoy vea la academia y le de retraso mental, pero yo creo que aun hay gente que no ve tele, no tiene vide social ni sexual y se la pasa estudiando (ya sea el software o hardware o en cualquier otra cosa) ya que como dice erick raymond en su articulo de Hacker howto, es una actitud, y no es algo que te peudes ufanar de ser, ni haber sido.

Pero bueno, aprovecho para decir que los putos vacunos camioneros de GDL sucekan webos de burro por bajar al pasaje para que los "escuche el gobernador" putos asesinos, atropellan a 15 en lo que va del mes y los meten en cintura y se enojan...

Sigan cooperando, no vean tanta piche tele, no cojan tanto y ponganse a ahcer algo productivo con su tiempo y no ver porno & stuff

eaeaeaea <- cuando en su cerebro aparezca eso, dejen de hacer algo de lo que mencione.

Saludos

Autor : Yield

l0t3k tRe: existe el under mexicano?

« **Responder #15 fecha:** Febrero 7th, 2003, 11:54am »

Buenos dias,

Una vez mas pido disculpas de antemano por el hecho de publicar una opinion, la mia, en un forum al que no pertenezco, pero siento por segunda vez la obligacion de hacerlo.

Como ha tenido a bien mencionar DeadSector, l0t3k y su grupo xploit (el cual sostengo ante cualquiera que NO existieron), simbolizan unicamente la actividad de cualquier, si, cualquier skript kiddie comun y corriente, no importa que sea del pasado o del presente, la iconografia es la misma, raza-mexicana comenzo de la misma forma, haciendo defacements, si me apeno por ello, no lo niego, aprendi? clari que aprendi, aprendi a que lo que hacia estaba mal y he comenzado a hablar por mi por que es mi opinion la que estoy plasmando, aprendi tambien que cualquier ni~o con diez dedos, un 'cerebro' y una computadora con internet pueden poner en una pagina web ajena una foto del Subcomandante Marcos, un mensaje de 'fuck telmex' y unas lineas de saludos a la secundaria tecnica 59, bueno, ahora que les dije que aprendi eso supongo se preguntaran y que hay de especial en ello?

Precisamente, que hay de especial en rayonear la pared de un edificio?

Ustedes respondan eso, en un contexto diferente, como ya dije, xploit fue una leyenda pasajera, un grupo inexistente pero cuyo legado representa una cosa muy importante para mi, lo que NO quiero ser, no quiero ser un skript kiddie, ni un personaje elitista, egocentrico, engreido e infantil, por que lo que el personaje que hizo ese post solo puede ser comparado con un ni~o de a lo mucho 12 a~os y que pena si se le toma en serio.

Y retomando un fragmento de la opinion de mi compa~ero DeadSector, la informacion debe ser libre? si, siempre y cuando el due~o intelectual asi lo desee, el opensource debe ser una religion? no, el opensource es una opcion para los programadores de todo el mundo, quieres cobrar por tu programa por que necesitas dinero? hazlo, solo tu sabras tus necesidades, no quieres hacerlo? prefieres publicarlo gratis para el mundo entero? carajo, hazlo! es tu trabajo, tu decides.

Quieren aprender? haganlo, quieren ver si logran limpiar la suciedad que quedo de lo que una vez fue el underground en mexico? quieren ver si pueden crear algo nuevo? intentenlo, pero con seriedad, por que hacer un deface o tener un forum llamado underground no los convierte a ustedes en personajes de tan mencionado estilo, una vez ya lo dije y lo repito, el underground no es una forma de autoproclamo, es una CULTURA y la cultura solo se da de una forma, leyendo, observando, estudiando, analizando.

Mi opinion es y creo que muchos la saben, que en este momento el underground no existe,

pero no veo por que, si lo intentan con la responsabilidad que se necesita y maduran en su forma de pensar puedan retomar esa corriente, esa cultura.

Ustedes son en su mayoría jóvenes que comienzan, bien, estan a tiempo de cambiar y saberse guiar por el camino del estudio y la cultura y la responsabilidad, no solo por el camino del gcc xexploit.c -o xexploit

Ojala que muchos, ya no digo todos, me alegraria ver que algunos en un futuro demuestren que supieron elegir el camino correcto, que no tomaron el camino del elitista o del 'hacker' que solo se 'especializa' en buffer overflows, cuando es en realidad conocido por cualquier ingeniero en sistemas que tal concepto es tan trivial como la tecnica de ir al ba~o.

Pido disculpas una vez mas por publicar tal cantidad de texto en un lugar al que no pertenezco, pero sentia que debia hacerlo.

Atte,

Yield

Comando NET para NT / WIN2K / XP

Por Wireless (wireless_6@hotmail.com)

Esto es para gente que empieza en Windows NT y no saben usar comandos, todo lo hacen por ventanas, clicks, etc.

Es muy útil y rápido manejar algunas cosas por medio de comandos de Windows, sobre todo cuando es en una Máquina Remota.

Esta vez hablaré sobre el Comando Net

El comando Net sirve para manejar recursos de la red de Windows, con este puedes crear, borrar, configurar cuentas, mapear discos, apagar y prender servicios, ver las computadoras de la red y muchas cosas mas. Se preguntaran por que escribo sobre esto si tan solo con escribir NET HELP te aparece la ayuda de windows. Pero muchas veces son un poco confusos los parámetros y la sintaxis, tratare de explicarlo lo más claro posible para que lo comprendan lo básico y después ya van a agarrarle la onda a esto y será más sencillo de utilizar.

Mencionaré algunas situaciones donde necesites usar comando NET:

Supongamos que tienes una sesión de comando de win2k/xp con privilegios de system. Qué hacer? Lo primero que haríamos seria crear nuestra propia cuenta de administrador.

NET USER, NET LOCALGROUP, NET GROUP

`net user juanito password /expires:never /add --` aquí estamos agregando una nueva cuenta de usuario, el /expires:never es para que nuestra nueva cuenta en una maquina remota nunca expire.

Pero necesitamos que sea administrador así que agregamos a juanito al grupo de administradores. Si la máquina es un controlador de dominio vamos a hacer:

`net group "domain Admins" juanito /add`

Aquí agregamos la cuenta juanito al Grupo de Domain Admins.

Si la máquina no es controlador de dominio entonces hay que agregar a juanito al grupo de administradores locales.

`net localgroup "administrators" juanito /add`

Que tal si quiero remover algún usuario del grupo de administradores? Solo tenemos que hacer algo similar a cuando lo agregamos solo que en lugar de /add pondremos un /del ej:


```
net localgroup "administrators" juanito /del
```

Igual para crear y borrar un usuario.

```
net user juanito ju4n /add --crea cuenta juanito con password "ju4n"  
net user juanito /del -- elimina cuenta de juanito.
```

Hasta ahora, ya sabemos crear cuentas y hacerlas administradores. Mas opciones de Net user. Para desactivar la cuenta de juanito escribimos:

```
net user juanito /active:no
```

Para volverla a activar escribimos:

```
net user juanito /active:yes
```

Puedes agregar un comentario del usuario, un comentario de la cuenta, el nombre completo del usuario

```
net user juanito /remark:"Departamento de contabilidad" /fullname:"Juan  
Perez" /comment:"Aquí va el comentario"
```

Si quieres darle una fecha para que expire la cuenta el 15 de octubre de 2003 entonces

```
net user juanito /expires:15/10/2003
```

Por default está que nunca expire. El formato de la fecha varia dependiendo del código del país.

```
net user juanito /expires:never
```

Con esto le estas poniendo que nunca expire la cuenta. Para permitirle o negarle a un usuario que pueda cambiar su contraseña usamos:

```
net user juanito /passwordchg:yes -- para que si pueda cambiar su contraseña  
net user juanito /passwordchg:no -- para que no pueda cambiar su contraseña
```

Si el usuario pertenece a un dominio, puedes darle o negarle acceso a las computadoras de la red:

```
net user juanito /workstations:soporte1,soporte2,soporte3
```

Le darás permiso a juanito que entre solo a las maquinas soporte1, soporte2 y soporte3, puedes darle acceso a 8 computadoras como máximo.

Es muy importante que la cuenta tenga un password, si nosotros le dejamos cambiar su contraseña, el usuario por comodidad puede poner una contraseña en blanco y esto seria un gran problema de seguridad. para evitar eso pondremos la siguiente instrucción:

```
net user juanito /passwordreq:yes -- con esto estas forzando a que el usuario debe tener contraseña.
```

Por último puedes controlar los accesos de juanito a la computadora por horarios, por default al crear la cuenta tiene acceso todos los días a todas horas, pero esto podemos cambiarlo con:

```
net user juanito /times: --- aquí niegas el acceso a juanito a todas horas todos los días.
```

```
net user juanito /times:lunes-sábado,8am-7pm -- Estas habilitando el acceso de lunes a sábado de 8 am a 7 pm. Otra forma podría ser:
```

```
net user juanito /times:lunes-sábado,08:00-19:00 -- Es igual que el anterior solo que con el formato de 24 horas
```

Para hacer un horario diferente para cada día de la semana se separan con punto y coma (;)

```
net user juanito /times:lunes,8am-6pm;martes-jueves,7am-9pm;viernes,9am-11pm
```

Esto seria el lunes de 8 am a 6 pm, de martes a jueves de 7 am a 9 pm y el viernes de 9 am a 11 pm

Hay otra cosa, para poner que el password nunca expire no se puede hacer por consola si se ha configurado net accounts que expire en cierto tiempo, pero hay otra forma de hacerlo, con un script. Suponiendo que mi maquina se llama pc1, mi workgroup se llama workgroup y la cuenta se llama juanito este sería el script para configurar que nunca expire una contraseña.

```
////////////////////////////////////
Const ADS_UF_DONT_EXPIRE_PASSWD = &h10000

strDomainOrWorkgroup = "workgroup"
strComputer = "pc1"
strUser = "juanito"

Set objUser = GetObject("WinNT://" & strDomainOrWorkgroup & "/" & _
                        strComputer & "/" & strUser & ",User")

objUserFlags = objUser.Get("UserFlags")
objPasswordExpirationFlag = objUserFlags OR ADS_UF_DONT_EXPIRE_PASSWD
objUser.Put "userFlags", objPasswordExpirationFlag
objUser.SetInfo
```

////////////////////////////////////

**** Fuente del Script: MICROSOFT

Tienes que copiar y pegar esto en un notepad y guardarlo como expire.vbs o el nombre que quieras pero con extensión vbs, lo corres desde consola con "cscript expire.vbs" (para ejecutar el script y ver el resultado en la consola, no en el desktop) y listo. Tu cuenta ya esta configurada para que nunca expire la contraseña. Solo tienes que cambiar el usuario, workgroup y el nombre de la pc, dependiendo de tus necesidades.

NOTA: No necesariamente se tienen que dar los parámetros de los comandos por separado, al crear la cuenta puedes ponerle todos, o puedes irlos agregando.

NET START, STOP, CONTINUE, PAUSE

También Podemos checar los servicios que están prendidos en este momento, podemos apagarlos y ponerlos en pausa. Para ver los servicios corriendo escribimos:

```
net start
```

Esto te va a dar una lista con los nombres de los servicios. Si queremos detener alguno debemos escribir:

```
Net Stop "servicio"
```

"servicio" significa el nombre completo del servicio entre comillas que se quiere detener, Es igual si quieres arrancar algún servicio

```
Net Start "servicio"
```

Quieres darle hacer una pausa en un servicio

```
net pause "servicio"
```

También podemos ver todos los servicios que están instalados con el comando (solo para XP)

```
sc query
```

```
NET VIEW
```

Este te dará una lista de los nombres de netbios de las maquinas conectadas a la red de la maquina, si queremos sacar mas información de esa red debemos expandernos a las otras máquinas.

```
net view \\maquina  
net view \\ipremotademaquina
```

Con esto veras los shares de la maquina también, pero no se verán los shares que terminen en \$ como los de administracion c\$ d\$ e\$ admin\$.

NET USE

Este comando es para mapear alguna share en una maquina remota. Para usarlo vas a escribir

```
net use \\ipdemaquinaremota\share
```

Puedes asignarla a un drive por ejemplo

```
net use F: \\ipdemaquinaremota\share
```

Aparte de mapearlo te lo va a poner como el drive F:. Pero aquí el nombre de usuario que vas a enviar y contraseña va a ser con la que logueaste a tu máquina.. Si esta cuenta no tiene privilegios en la máquina remota tienes que hacerlo de otra forma

```
net use \\ipdemaquinaremota\share /logon:username password
```

Aquí estarás enviando un username, que puede ser el de administrador o cualquier otro usuario que tenga acceso a la share. También con NET USE puedes mapear puertos como el LPT1, LPT2, etc. Para aplicaciones que necesitas imprimir en puerto LPT y la impresora está en red, la forma es similar

```
net use LPT1://ipdemaquinaremata/impresora
```

Igual se usa otro username si con el que te logueaste no tiene privilegios.

```
net use LPT1://ipdemaquinaremata/impresora /user:dominio\usuario
```

Si tienes cuenta de administrador puedes mapear las shares que vienen por default como c\$ d\$ admin\$

NET ACCOUNTS

Con Net Accounts puedes cambiar y ver la configuración que tienen las cuentas de la máquina, como el tiempo que se va a tardar antes de que se cierre la sesión después de que se acabe el tiempo permitido de estar logueado, El tiempo máximo que puede tener una contraseña sin cambiarse, el tiempo mínimo que necesita que pase para que puedas cambiar tu contraseña, configurar el historial de contraseñas (las veces que tienes que cambiar tu password para que puedas volver a poner una contraseña que hayas puesto anteriormente, el número de intentos fallidos para que la cuenta se bloquee, el tiempo que dura bloqueada la cuenta, la longitud mínima para una contraseña)

```
net accounts
```

Si escribes solo net accounts, te va a desplegar los valores que tiene cada una de las opciones.

```
net accounts /maxpwage:30
```

Aquí estas poniendo que la mayor edad de la contraseña puede ser 30 días, también puedes ponerle /maxpwage:unlimited para que no haya límite en la edad máxima

```
net accounts /minpwage:10
```

La menor edad que puede tener una contraseña es de 10 días.

```
net accountr /minpwlen:9
```

Con esto la menor longitud que puede tener una contraseña es 9 caracteres, puedes poner desde 0 hasta 14 y el valor de default es el 6.

```
net accountrs /uniqueps:10
```

Va a tener que cambiar 10 veces su contraseña antes de que pueda poner una contraseña repetida

```
NET SEND
```

Con net send puedes enviar mensajes a otros usuarios de Windows, necesita estar prendido el servicio de Messenger para enviar un mensaje escribes:

```
net send ip/nombre de la maquina/ nombre de usuario " mensaje "
```

```
net send 172.20.5.2 Este es el mensaje -- aquí se lo envías al ip 172.20.5.2
```

```
net send Server1 Este es el mensaje -- aquí se lo envías a la maquina Server1
```

```
net send jlopez Este es el mensaje -- aquí se lo envías a el usuario jlopez
```

Con net Session miras y puedes desconectar a quien esta logueado en la maquina

```
net session
```

Esto te mostrará quien está conectado a la maquina, para desconectarlo tecleas

```
net session \\ipmaquinaremota /delete
```

```
ej: net session \\192.168.1.20 /delete
```

Si no pones el ip o nombre de la maquina que quieres cerrar la session, y solo pones net session /delete se cerraran todas las conexiones con las demás maquinas

```
NET SHARE
```

Es para ver, borrar, modificar, agregar las shares que están en la maquina,

```
net share
```

Con esto solo miras las shares que tienes en estos momentos. Para agregar una share vas a escribir

```
net share test=c:\test /remark:"Carpeta Test" /users:3
```

Aquí estas compartiendo la carpeta c:\test con el nombre de la share "test", los comentarios de la carpeta compartida van a ser "carpeta test" y los usuarios máximos que se van a poder conectar simultáneamente serán 3

```
net share test=c:\test /users:unlimited
```

Con esto no tendrá límites de usuarios conectados simultáneamente. Para ver mas información de cada share escribes

```
net share nombredelashare
```

```
EJ: net share admin$  
net share test
```

Si quieres borrar la share test

```
net share test /delete
```

NET FILE

Es para ver o cerrar los archivos que alguien tiene abiertos desde la red.

`net file` ----- Te muestra que archivos están abiertos, quien los tiene abiertos, cuanto tiempo han estado abiertos y que privilegios tiene. Cada archivo va a tener un ID, con ese id puedes cerrar los archivos

```
net file 4 /close
```

Suponiendo que el id sea el numero 4

Bueno, aquí termina este pequeño manual, solo son los comandos básicos que se utilizan en windows, que si me faltaron? Si, que me faltan parámetros? Si. Traté de explicar lo básico y lo que se pretende con esto es que se comprenda la manera en que se maneja el comando net, no tanto aprenderse de memoria cada comando, pero saber como funciona y que podemos hacer con el.

NetSh

Por a_d_mIRC (a_d_mIRC@hotmail.com)

NETSH

Netsh, también llamado NetShell o Network Shell, es una herramienta basada en línea de comando que configura el servicio DHCP, el servicio RAS y servicios de red de enrutamiento. Un contexto de Netsh es un estado en el cual Netsh acepta los comandos relacionados con un sistema específico de funciones. Cada contexto de Netsh contiene las características para manejar un sistema relacionado específico de funciones del establecimiento de una red. Usted puede cambiar a otros contextos escribiendo el nombre de un contexto. También se utiliza para agregar una dirección del Internet Protocol (IP), o para configurar el WINS y el Domain Name System (DNS) en la interfaz. (Traducción hecha por Google)

Como quien dice. Con el NETSH puedes :

Cambiar una dirección IP y Gateway.

Si tu dirección IP es 192.168.0.10, Netmask 255.255.255.0 y Gateway 192.168.0.1 y la quieres cambiar a IP: 192.168.0.69 NM: 255.255.254.0 GW: 192.168.0.2, primero escribe Netsh, luego interface y ahora ip, escribe set address "adaptador" static 192.168.0.69 255.255.254.0 192.168.0.2 1 el último 1 es la interfaz métrica, si no lo escribes, no va a funcionar

Ahora, así es como lo verías en tu pantalla. Para conocer tu dirección IP desde línea de comandos escribe IPCONFIG

```
C:\>ipconfig
```

```
Configuración IP de Windows 2000
```

```
Ethernet adaptador Ethernet00:
```

```
Sufijo DNS específico de la conexión. :  
Dirección IP. . . . . : 192.168.0.10  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . : 192.168.0.1
```

```
C:\>netsh
```

```
netsh>interface
```

```
interface>ip
```

```
interface ip>set address "ethernet00" static 192.168.0.69 255.255.254.0  
192.168.0.2 1
```

Al presionar “Enter” te va a salir un mensaje que dice “Command Succesfully” o “Aceptar”, y si quieres ver que se han realizado los cambios, escribe “quit” para que te regrese a C:\ y una vez ahí escribe de nuevo IPCONFIG para ver los resultados,

```
C:\>netsh
netsh>interface
interface>ip
interface ip>set address "ethernet00" static 192.168.0.69 255.255.254.0
192.168.0.2 1
Aceptar
interface ip>quit
C:\>ipconfig
Configuración IP de Windows 2000

Ethernet adaptador Ethernet00:

    Sufijo DNS específico de la conexión. :
    Dirección IP. . . . . : 192.168.0.69
    Máscara de subred . . . . . : 255.255.254.0
    Puerta de enlace predeterminada . . . : 192.168.0.2
```

Como puedes ver, hemos cambiado una dirección IP desde línea de comando.

Agregar una dirección IP

IP 192.168.0.10 NM 255.255.255.0 GW 192.168.0.1, y quieres agregar la dirección 192.168.10.10 NM 255.255.0.0 Add address “adaptador” 192.168.10.10 255.255.0.0

```
C:\>netsh
netsh>interface
interface>ip
interface ip>Add address "ethernet00" 192.168.10.10 255.255.0.0
Aceptar

interface ip>quit
C:\>ipconfig
Configuración IP de Windows 2000

Ethernet adaptador Ethernet00:

    Sufijo DNS específico de la conexión. :
    Dirección IP. . . . . : 192.168.10.10
    Máscara de subred . . . . . : 255.255.0.0
    Dirección IP. . . . . : 192.168.0.69
    Máscara de subred . . . . . : 255.255.254.0
    Puerta de enlace predeterminada . . . : 192.168.0.2
```

Si quieres agregar la misma dirección pero además quieres agregar otro gateway, digamos 192.168.10.1 Add address “adaptador” 192.168.10.10 255.255.0.0 192.168.10.1 1

```
C:\>netsh
netsh>interface ip
```



```

interface ip>Add address "ethernet00" 192.168.10.10 255.255.0.0
192.168.10.1 1
Aceptar
interface ip>quit
C:\>ipconfig
Configuración IP de Windows 2000

```

Ethernet adaptador Ethernet00:

```

Sufijo DNS específico de la conexión. :
Dirección IP. . . . . : 192.168.10.10
Máscara de subred . . . . . : 255.255.0.0
Dirección IP. . . . . : 192.168.0.69
Máscara de subred . . . . . : 255.255.254.0
Puerta de enlace predeterminada . . . : 192.168.0.2

```

Borrar una dirección IP

Si nomás quieres borrar la dirección escribe: delete address “adaptador” 192.168.10.10

```

C:\>netsh
netsh>interface ip
interface ip>delete address "ethernet00" 192.168.10.10
Aceptar
interface ip>quit
C:\>ipconfig
Configuración IP de Windows 2000

```

Ethernet adaptador Ethernet00:

```

Sufijo DNS específico de la conexión. :
Dirección IP. . . . . : 192.168.0.69
Máscara de subred . . . . . : 255.255.254.0
Puerta de enlace predeterminada . . . : 192.168.0.2

```

Si quieres borrar la dirección junto con el gateway, escribe: delete address “adaptador” 192.168.10.10 192.168.0.2

```

C:\>netsh
netsh>interface ip
interface ip>delete address "ethernet00" 192.168.10.10 192.168.0.2
Aceptar
interface ip>quit
C:\>ipconfig
Configuración IP de Windows 2000

```

Ethernet adaptador Ethernet00:

```

Sufijo DNS específico de la conexión. :
Dirección IP. . . . . : 192.168.0.69
Máscara de subred . . . . . : 255.255.254.0
Puerta de enlace predeterminada . . . : 192.168.0.1

```

Como ya habíamos agregado otro gateway, y borramos el predeterminado, ahora vemos el que habíamos agregado.

Woohoo ya sabemos borrar y agregar IP's por línea de comando, ahora, Si dejamos que ellas vengan a mí??? En fin, cada quien sabe lo que hace. Los leo luego Bytes

PEV (Pulso Electromagnético Virtual)

Por Redokh

Hola, este es mi primer artículo y espero que no sea el último, espero poder ser lo suficientemente claro redactando para que me de a entender.

El otro día fui al cine a ver la película 'The Core' (el núcleo) y en una de las escenas pasa que la policía va al departamento de un hacker y éste al verlos por la mirilla se pone a destruir discos, unos en el horno de microondas, en el tostador y otros con una descarga electromagnética. Y una idea loca se quedó en mi cabeza.

Muy probablemente todos tenemos información en nuestros equipo que no queremos que nadie mas vea (cartas de amor, pornografía, código fuente, listas de passwords, etc), la cual en el mejor de los casos la guardamos encriptada y la llave la ponemos en un lugar seguro, pero que pasa?, pues que existe un método por medio del cual la información puede ser vista, la idea de esa escena de la película era hacer irrecuperable la información (eliminar la evidencia) y eso, eso es de lo que trata este documento.

En lo personal he borrado mucha información por error (yo solo uso windows, así que no se si este proyecto funcione en otro sistema operativo pero me imagino que si) y la he podido recuperar afortunadamente, y eso me alarma, porque ¿qué pasa con la información que verdaderamente quiero eliminar?. Cuando uno pulsa la tecla delete en nuestro explorador de windows, los archivos eliminados no se van del todo, ni siquiera cuando hacemos uso del Shift+Del, en el primer caso se va a la papelera de reciclaje y en el segundo caso desaparece el nombre del archivo de nuestro disco duro pero no desaparece la información que contenía el archivo.

Hace ya algunos años existió un sistema operativo llamado MS-DOS, un sistema operativo sin ventanas y sin ratón, el cual tenía un comando llamado DEL y otro llamado UNDELETE, cuando se eliminaba un archivo con el comando DEL existía la opción de recuperar el archivo con el comando UNDELETE, el inconveniente era que el comando no recuperaba el nombre del archivo en su totalidad, había que indicarle cual era el primer carácter del nombre del archivo.

Para entender un poco mas esto de los archivos veamos como se almacenan los archivos en el disco duro. Básicamente el disco lleva un sistema de archivos, un lugar en donde se almacenan los datos relevantes de los archivos, como son el nombre y donde se encuentra físicamente. Y luego existe otro lugar donde son almacenados los archivos en si, por ejemplo :

Supongamos que tenemos un archivo llamado 'password.txt' que contiene el texto : 'ABC' en el sistema de archivos tendríamos :

```
Nombre = Password.txt  
Dirección = 123  
Longitud = 3
```

De la dirección 123 a la 125 (Que es la longitud del archivo) tenemos

ABC

Bueno básicamente sería así, supongo que dependiendo del sistema de archivos cambiaría la forma de almacenar la información pero yo me la imagino así y es mas fácil de comprender.

Al parecer cuando el viejo MS-DOS borraba un archivo solo le quitaba la primera letra del archivo y con el comando inverso se podía recuperar la información siempre y cuando otro archivo creado posteriormente no haya ocupado el espacio o parte del espacio que el archivo eliminado estaba ocupando. De tal manera que si un archivo ocupaba la dirección 124 a la 128 era imposible recuperar el archivo y su contenido original, en el mejor de los casos se podía recuperar parte del archivo.

Ok, retomando el tema de la película, la idea de pasarle un campo electromagnético a los discos duros era hacer irre recuperable la información cambiando el orden de los bits, de todos los bits de los discos duros y mi idea del PEV es simular lo que haría un campo electromagnético pero un poco mas controlado y pues manos a la obra.

Construyendo el PEV

Para fines didácticos tomaremos como ejemplo ficticio el archivo que en teoría es en extremo comprometedor e inculpador :

```
Nombre      : passISPPatito24032003.sql
Dirección   : 1A5ECh
Longitud    : 400h (1KB)
```

Lo primero y mas importante es cambiar los datos almacenados en el archivo que nos interesa. Supongamos que el archivo passISPPatito24032003.sql está lleno de cadenas SQL como la siguiente :

```
INSERT INTO userData VALUES (id,usrAcount,usrPassword);
```

El archivo está lleno de usuarios y passwords válidos para un ISP llamado Patito, es información altamente comprometedora pero útil a la vez. PEV debe de cambiar el contenido del archivo lo antes posible, la totalidad del archivo, a mi me gusta llenarlo de 0s, de tal manera que al final del proceso tendremos un archivo llamado passISPPatito24032003.sql que comienza en la dirección 1A5EC con una longitud de 1KB lleno de 0s

Nota : en lo particular uso delphi, así que pido una disculpa a los amantes del C.

La función la llame 'blanquear', y básicamente lo que debe de hacer dicha función es:

- Abrir el archivo
- Cambiar cada uno de los bytes por el byte de relleno (en este caso 0)

- Cerrar el archivo

Fácil ¿no?, bueno, pero por si las dudas aquí les doy mi versión de cómo se puede realizar este proceso.

```
function blanquear(archivo: String): Boolean;
Const
  _BLOQUE = 2048; //El tamaño del bloque a guardar
  _FILL_CHAR = #0; //El carácter de relleno
var
  f : File; //El archivo
  tamanoArchivo, //El tamaño del archivo
  acumulado, //El avance del almacenamiento
  escritos, //Los bytes escritos
  tamanoBloque, //El tamaño del bloque a guardar
  n : Cardinal; //El tipo Cardinal solo soporta
                //4,294,967,295 así que no funcionará
                //para archivos de mayor tamaño
  Buf: array[1.._BLOQUE] of Char; //El bloque a guardar
begin
  try
    tamanoArchivo := tamanoDe(archivo);
    AssignFile(f, archivo); //Asigno el archivo a abrir
    Reset(f,1); //Abre el archivo
    n := 0;
    for n := 1 to _BLOQUE do
      buf[n] := _FILL_CHAR; //Se llena el bloque
      acumulado := 0;
      repeat
        //unas validaciones para ver cuanto se va a almacenar
        if acumulado = tamanoArchivo then
          tamanoBloque := 0
        else if _BLOQUE > tamanoArchivo then begin
          tamanoBloque := tamanoArchivo;
          acumulado := tamanoArchivo;
        else if (acumulado + _BLOQUE) > tamanoArchivo then begin
          tamanoBloque := tamanoArchivo - acumulado;
          acumulado := tamanoArchivo;
        end else begin
          tamanoBloque := _BLOQUE;
          inc(acumulado, _BLOQUE);
        end;
        //Se realiza el remplazo de la información
        BlockWrite(f, Buf, tamanoBloque, escritos);
      until (tamanoBloque = 0) or (escritos <> tamanoBloque);
      CloseFile(f); // Se cierra el archivo y tan tan.
      result := True;
    except
      result := False
    end;
  end;
end;
```

La función 'tamanoDe' sólo extrae el tamaño del archivo dado.

```

function tamanoDe(archivo: String): cardinal;
var
  hf : HFile;
  FindData : TWin32FindData;
begin
  result := 1;
  Hf := windows.FindFirstFile(PChar(archivo), FindData);
  if (INVALID_HANDLE_VALUE <> Hf) then begin
    result := (FindData.nFileSizeHigh * MAXDWORD) +
      FindData.nFileSizeLow;
    Windows.FindClose(Hf);
  end;
end;

```

Creo que es importante hacer este proceso de ‘blanquado’ lo más rápido posible; así como está el código corriendo en un equipo a 800MHZ con un HD ATA66 se tardó en blanquear un archivo de 12MB en 117 milésimas de segundo, nada mal, eso creo. Recuerdo haber leído un artículo en donde se decía que aun después de haber sobre escrito el archivo 6 veces era todavía posible recuperar la información, si tu paranoia es mucha, pues bien puedes hacer el proceso de blanqueado repetitivo (en un ciclo for o while), solo recuerda llenarlo con un carácter diferente cada vez que ejecutes el proceso.

Lo segundo mas comprometedor es el nombre del archivo y la longitud del mismo, ya que es mucha casualidad que tengamos un archivo que se llame igual al que existe en el ISP y que para empeorarla tiene la misma longitud aunque el contenido sea diferente, así que hagamos otras dos funciones: ‘ajustarTamano’ y ‘renombrar’, estas dos funciones solo hacen que el archivo mida cero bytes y que el nombre sea otro, estas si que están fáciles pero ahí les va el código:

```

function ajustarTamano(archivo: String): Boolean;
var
  f : File;
begin
  try
    AssignFile(f, archivo);
    Rewrite(f, 1);
    CloseFile(f);
    result := True;
  except
    result := False
  end;
end;

function renombrar(archivo: String): Boolean;
var
  nuevoNombre : LongInt;
  nuevaExtencion : Byte;
begin
  try
    nuevoNombre := Random($FFFFFF);
    nuevaExtencion := Random($FF);
    renombrarFile(archivo, ExtractFilePath(archivo) +

```

```

        IntToHex(nuevoNombre,8) +
        '.' + IntToStr(nuevaExtencion));
    result := True;
except
    result := False;
end;
end;

```

Renombro el archivo con una función Random, así que hay que inicializar el motor aleatorio con la procedimiento Randomize previamente.

Al final de este procedimiento me quedará un archivo mas o menos así:

```

Nombre      : 00315183.182
Dirección   : 1A5ECh
Longitud    : 0h

```

Ya por último solo hay que borrar el archivo 00315183.182 y ya, la evidencia se fue al caño, bueno, eso digo yo, por cierto, si hay alguien que después de hacer estos procesos al pie de la letra aún puede recuperar el contenido del archivo háganmelo saber.

Bueno, eso es todo, lo que resta es que ustedes le pongan un poco de creatividad a sus aplicaciones y que hagan un programita que se pueda correr fácilmente, seleccionar los archivos que queremos destruir y destruirlos. Yo hice uno que se incorpora al explorador de windows, así que solo selecciono los archivos, pulso el botón derecho del ratón y le digo que destruya los archivos seleccionados, también pueden hacer uno que lea una lista de archivos desde un archivo de texto que previamente alimentamos con los archivos que queremos destruir y así en caso de emergencia solo basta correr la aplicación que lee dicho archivo y destruye los archivos. Saludos, espero que sea de utilidad este documento, cualquier comentario quedo a sus ordenes.

Técnicas de Escaneo

Por hd (hd@hakim.ws)

Introducción

Todos los días se puede ver gente en cualquier parte de Internet con la misma pregunta de siempre... ¿Como me inicio en el mundo del hack? ¿Como comienzo?, ¿Que debo leer? , antes que nada cabe aclarar de una vez que no soy hacker ni mucho menos, simplemente algo curioso. Y más de alguno ha leído que hay que bajarse un programa llamado 'scaneador de puertos' con el que te dice los "servicios", que está corriendo el host que nos interesa, así que lo primero que hacen es ir en busca de un programita de estos que nos de esa información tan valiosa...

Bueno, algo así le pasó a el amigo de un amigo, pero en la actualidad hay herramientas tan 'sofisticadas' ante esas 'amenazas', ya cualquier administrador decente cuenta en su red con un IDS, y si lo ponemos a punto, pues es una magnifica herramienta para detectar este tipo de ataques a nuestros servidores. Así que, el punto era que no debemos de usar los scaneadores de puertos?, no, solo explicaré un poco más a fondo algunos métodos de escaneo más discretos y que podamos pasar un poco más desapercibidos.

Dividiré el txt en dos secciones, en la primera mostraré algunos tipos de escaneos para ver si un puerto está abierto o no. La segunda parte tratará un par de opciones para saber si un host existe o no en internet pero esta vez solo con tcp y no ICMP como estamos acostumbrados.

Nota: supongo que para este punto tienes una leve idea de lo que es el tcp/ip, cierto?

Extracto de Flags en tcp/ip

Nota: este pequeño extracto salio del texto escrito por Guybrush para RazaMexicana.

<++>

- FLAGS : Hay seis banderas de 1 bit:

1. URG : Se establece en 1 si esta en uso el apuntador urgente. El apuntador urgente sirve para indicar un desplazamiento en bytes a partir del numero actual de secuencia en el que se encuentran datos urgentes. Este recurso sustituye los mensajes de interrupción.
2. ACK : Se establece en 1 para indicar que el numero de acuse de recibo es valido. Si el ACK es 0, el segmento no contiene un acuse de recibo, por lo que se ignora el campo de numero de acuse de recibo.

3. PSH : Indica datos empujados (con PUSH). Por este medio se solicita atentamente al receptor entregar los datos a la aplicación a su llegada y no ponerlos en el buffer hasta la recepción de un buffer completo.
4. RST : Se usa para restablecer una conexión que se ha confundido debido a una caída de host u otra razón; también sirve para rechazar un segmento no valido o un intento de abrir una conexión.
5. SYN : Se usa para restablecer conexiones. La solicitud de conexiones tiene SYN = 1 y ACK = 0 para indicar que el campo de acuse de recibo incorporado no esta en uso. La respuesta de conexión si lleva un reconocimiento, por lo que tiene SYN = 1 y ACK = 1.
6. FIN : Se usa para liberar una conexión; especifica que el transmisor no tiene mas datos que transmitir. Sin embargo, tras cerrar una conexión, un proceso puede continuar recibiendo datos indefinidamente.

<-->

Extracto de sendtcp.c, donde se pueden ver los valores de las flags

<++>

```
#define URG 0x20 // 100000
#define ACK 0x10 // 010000
#define PSH 0x08 // 001000
#define RST 0x04 // 000100
#define SYN 0x02 // 000010
#define FIN 0x01 // 000001
```

<-->

PRIMERA PARTE.

Sección TCP típica

Cuando queremos comenzar una conexión común y corriente de acuerdo al protocolo se usa de la siguiente manera:

- Nuestro host manda un paquete tcp, con los flags SYN en 1 (o prendido como quieran llamarle), y el ACK en 0 y esperamos una respuesta.
- Si el puerto al que queremos alcanzar está en LISTEN (escucha) el host puede aceptar o rechazar la conexión, aquí hay dos caminos:
 - a) Acepta: El host nos responde con un paquete con los flags SYN y ACK prendidos, nosotros al final mandamos su ACK.
 - b) Niega: El host nos responde con un paquete con los flags RST y ACK prendidos.

Así que como podemos ver, se hace una conexión completa con este medio por lo que los IDS nos agarran al hacer demasiadas conexiones que duran tan poco tiempo, e intentar muchas otras.

Ahora ya sabes un poco como trabaja un scaneador de puertos tradicional si logra conectar con el puerto, nos lo informa. Pero esto hoy en día es logueado al 100% y no queremos embarrar nuestra IP en montones de archivos de logs, cierto?

Ahora pasaremos a ver otras técnicas de escaneo donde no precisamos comenzar una sección tcp tradicional para conocer el estado del puerto, en estos casos siguiente no se abre una conexión completa, por decirlo de alguna manera.

NOTA: Para los logs estaremos en una shell linux, usando hping, ya que este nos proporciona las estadísticas de envío, cosa que algunas herramientas bajo windows no dan, o al menos las que he probado.

Log

Probaremos toda la teoría que veamos en pequeños registros, a continuación el primero de ellos mostrando una sección tcp típica. No veo la necesidad de esconder las IP, ya que la mía es dinámica y es la primera vez que me saca de los rangos "comunes", así que no hay mucho problema.

CASO A: El puerto está abierto

```
[root@bsd-mex crypkey]# hping -S -p 80 200.64.170.73
HPING 200.64.170.73 (ppp0 200.64.170.73): S set, 40 headers + 0 data
bytes
len=44 ip=200.64.170.73 flags=SA DF seq=150 ttl=119 id=7017 win=8760
rtt=153.4 ms
len=44 ip=200.64.170.73 flags=SA DF seq=166 ttl=119 id=7025 win=8760
rtt=177.0 ms
len=44 ip=200.64.170.73 flags=SA DF seq=217 ttl=119 id=7026 win=8760
rtt=196.7 ms
len=44 ip=200.64.170.73 flags=SA DF seq=219 ttl=119 id=7030 win=8760
rtt=238.4 ms
```

Como podemos ver mi PC responde con las flags Syn y Ack prendidas (flags=SA) lo que nos indica el estado de disponibilidad de nuestro puerto.

CASO B: El puerto está cerrado

```
[root@bsd-mex crypkey]# hping -S -p 80 200.64.170.73
HPING 200.64.170.73 (ppp0 200.64.170.73): S set, 40 headers + 0 data
bytes
len=40 ip=200.64.170.73 flags=RA seq=125 ttl=119 id=7007 win=0 rtt=254.8
ms
len=40 ip=200.64.170.73 flags=RA seq=127 ttl=119 id=7009 win=0 rtt=254.8
ms
len=40 ip=200.64.170.73 flags=RA seq=130 ttl=119 id=7013 win=0 rtt=254.8
ms
len=40 ip=200.64.170.73 flags=RA seq=135 ttl=119 id=7015 win=0 rtt=254.8
ms
```

Esta vez mi PC responde con los flags Rst y Ack prendidos (flags=RA).

Ahora que ya tenemos bien fundamentada la teoría podemos pasar con más técnicas.

Nota: Gracias a crypkey por rolar shell para logear este apartado.

DumbScan

Historia

Apareció por primera vez según tengo entendido en un post de BUGTRAQ el 18 de Diciembre de 1998. Se le llamó de este modo gracias a que es necesario contar con un host 'silencioso', al que embarraremos en los logs del host que queremos scanear (si es que alcanza a logear...). Su 'descubridor' por así decirlo fue 'antirez'.

Teoría

Primero que nada necesitamos contar con un host que prácticamente no tenga NADA de tráfico en internet, hay varios, he visto redes enteras llenas de instalaciones de IIS con las opciones por default, y sin pagina de index esos nos sirven muy bien para los términos que necesitamos. Pensaba escribir los rangos de Ip donde se pueden encontrar pero mejor no me meto en problemas, o a ti te gustaría que un grupo de gente sin vida social prácticamente tome tus servidores de juguete?, verdad que no?

Bueno, ahora si comencemos con la teoría:

Nombraremos a los host en este orden:

A> Será nuestra maquina

B> Será el host que queremos escanear

C> Será el host sin trafico, de aquí viene el nombre de 'dumb'

Nosotros comenzamos midiendo el trafico que genera el host C, con hping se puede (Originalmente era con la opción '-r', en la versión < 1, hoy en día están por sacar la versión 3...). Al parecer solo se cambio en hping1 ya que en el MAN de hping2 podemos ver de nuevo:

```
-r --rel
Display id increments instead of id. See the HPING2-HOWTO for more
information.
Increments aren't computed as id[N]-id[N-1] but using packet loss
compensation.
See relid.c for more information.
```

Ya que estamos seguros de que el host C no tiene tráfico (mirando en el campo 'id' generalmente se tendrá un 1). Ahora procedemos a enviar un

paquete al host B con la dirección de origen spoofeada para que parezca que el host C la mandó).

Miramos de nuevo el estado del host C y...

Si los campos de 'id' siguen en el número constante del principio, el puerto en B está cerrado.

Si los campos de 'id' están alterados ligeramente, que el número constante de 'id' del principio, se haya alterado en algunas unidades, bueno, el chiste es que el puerto en B se encuentra abierto, ya que al recibir el SYN B para iniciar la conexión le manda un paquete a C con SYN|ACK prendidos, y como este no sabe que es lo que pasó cierra la conexión con un RST, de ahí que veamos que C está generando tráfico.

Nota de revisión, ahora que me fijo bien, esto se podría clasificar como scan Half Open :D, lo veremos más adelante.

NOTA: Recomiendo usar como host 'dumb' (C) una maquina con windows, porque? porque los números id, son más predecibles (estables) que una maquina con linux por ejemplo. Los números de secuenciación suman +1 cada vez.

Herramientas

- Windows

Puedes usar el VScan, usando el parámetro '-idle'

- Linux

Para linux recomiendo usar el Idlescan

Ejemplo

```
vscan -idle 1.2.3.1 1.2.3.4 -p 21 23 -zombie 11.11.11.11 1337
```

Aquí se escaneará:

- Desde la IP 1.2.3.1 hasta 1.2.3.4 (1.2.3.1, 1.2.3.2, 1.2.3.3, 1.2.3.4)
- Desde el puerto 21 (ftp) hasta el 23 (telnet) (21, 22, 23)
- Cabe destacar que el puerto en 11.11.11.11 (1337 te suena?), debe estar abierto para hacer las comprobaciones necesarias.

Half Open

Este tipo de scan es también denominado SYN scan, y es muy parecido a la función CONNECT, solo que a último momento decidimos no hacer la conexión, que chingados es eso?, ahora lo explico...

Nuestro host manda un paquete tcp a el objetivo con la bandera SYN encendida...

- a) Si el puerto está cerrado, el objetivo nos responde con un RST.
- b) Si el puerto está abierto, el objetivo nos responde con un SYN|ACK e inmediatamente debemos responder con un RST, cerrando la conexión.

La ventaja principal de este tipo de escaneo es que se reduce potencialmente los riesgos de que puedas ser detectado, pero en fin, no es 100% seguro, ya que hay algunas herramientas que ya lo loguean como son:

- Synlogger
- Courtney

Pro's

Es un scaneo más rápido, evita algunas barreras y IDS

Contra's

Es necesario tanto en Linux como en windows tener máximos privilegios para usar los raw sockets.

Log

Usaremos el tan afamado Nmap

```
[root@localhost root]# nmap -sS -p135 -P0 -vv 200.64.170.182

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Host dup-200-64-170-182.prodigy.net.mx (200.64.170.182) appears to be up
...
good.
Initiating SYN Stealth Scan against dup-200-64-170-182.prodigy.net.mx
(200.64.170.182)
The SYN Stealth Scan took 36 seconds to scan 1 ports.
Interesting ports on dup-200-64-170-182.prodigy.net.mx (200.64.170.182):
Port      State      Service
135/tcp    filtered   loc-srv

Nmap run completed -- 1 IP address (1 host up) scanned in 37 seconds
```

NOTA: Cabe aclarar que 200.64.170.182 es una PC con w2k sp4, conexión a internet con dial up. (Si, es mía ;), este tipo de scan nos da el resultado más preciso del puerto, ya que, es cierto que tengo el puerto 135 filtrado por firewall.

NOTA2: Si tu PC es de uso personal te recomiendo que desactives los servicios de DCOM, ya que por ahí ya hay algunos xploits que te dan una shell inversa según vi.

Xmass tree

Este tipo de scan es de los más nuevos, quizá de los más extraños ya que se utiliza una combinación de flags que en condiciones normales no se usaría de acuerdo al protocolo RFC 793.

Se comienza mandando un paquete tcp con las banderas de FIN, URG y PSH y se logra saber el estado del puerto si:

- a) Si el puerto está cerrado, el objetivo nos responde con un RST.

```
[root@localhost root]# ./hping 64.70.145.95 -FUP -c 4 -p 81
HPING 64.70.145.95 (eth0 64.70.145.95): 40 data bytes
60 bytes from 64.70.145.95: flags=RA seq=0 ttl=238 win=0 time=108.1 ms
60 bytes from 64.70.145.95: flags=RA seq=1 ttl=238 win=0 time=107.9 ms

--- 64.70.145.95 hping statistic ---
4 packets tramitted, 2 packets received, 50% packet loss
```

- b) Si el puerto está abierto, el objetivo no regresa nada.

```
[root@localhost root]# ./hping 64.70.145.95 -FUP -c 4 -p 80
HPING 64.70.145.95 (eth0 64.70.145.95): 40 data bytes

--- 64.70.145.95 hping statistic ---
4 packets tramitted, 0 packets received, 100% packet loss
```

En nmap bastaría con correrlo así:

```
nmap -sX -p(rangode-puerto) IP
```

Esta técnica no funciona en los sistemas de Microsoft, CISCO, IRIX, HP/UX, y BSDI.

Null Scan

Este tipo de scan requiere que mandemos un paquete tcp sin ninguna flag en uso, por eso se le llama 'Null scan' ya que prácticamente mandamos un paquete vacío, cabe aclarar que en los sistemas Windows no funciona este tipo de procedimiento. Logramos saber el estado del puerto cuando:

- a) Si el puerto está abierto, el objetivo no responde a el paquete.

```
[root@localhost root]# ./hping2 64.70.145.95 -c 4 -p 81
HPING 64.70.145.95 (eth0 64.70.145.95): 40 data bytes
60 bytes from 64.70.145.95: flags=RA seq=0 ttl=238 win=0 time=109.5 ms

--- 64.70.145.95 hping statistic ---
4 packets tramitted, 1 packets received, 75% packet loss
```

- b) Si el puerto está cerrado, el objetivo nos responde con un RST.

```
[root@localhost root]# ./hping2 64.70.145.95 -c 4 -p 80
HPING 64.70.145.95 (eth0 64.70.145.95): 40 data bytes

--- 64.70.145.95 hping statistic ---
4 packets transmitted, 0 packets received, 100% packet loss
```

Esta técnica no funciona en los sistemas de Microsoft, CISCO, IRIX, HP/UX, BSDI y MVS.

NOTA: para usar esta técnica hay que modificar el hping.c...

```
if (tcp_th_flags == 0)                                /*tcp flags ain't set */
    tcp_th_flags |= TH_FIN;
```

Si no le dimos ninguna flag en el parámetro, nos pone el FIN como default, así que solo comentemos la línea y ruleará su hping.

* En nmap basta con correrlo así:

```
nmap -sN -p(rangode-puerto) IP
```

FIN Scan

Este tipo de scan manda un paquete "vacío" completamente a el host, como prueba. Esta técnica no funciona en los sistemas de Microsoft, CISCO, IRIX, HP/UX, y BSDI y MVS.

* En nmap basta con correrlo así:

```
nmap -sF -p(rangode-puerto) IP
```

SEGUNDA PARTE.

Aquí comienzan las opciones al ICMP común y corriente al que estamos acostumbrados, ya que muchos administradores están comenzando a filtrar estos paquetes reduciendo el trafico innecesario a sus redes, y evitando ciertos tipos de ataques con este protocolo.

Así que es hora de buscar opciones a nuestro clásico ping. Aunque siempre es más practico agotar su uso, y ya luego buscar otras opciones :p

ACK Scan

El ACK Scan, nos puede servir de dos cosas:

- 1) Comprobar la existencia de un firewall.

En el ACK Scan, mandamos un paquete con la bandera de ACK prendida, cuando el filtro (la ente que está capturando el tráfico), revisa que no hemos comenzado una sección típica de tcp (primero va el SYN recuérdalo...), entonces:

- a) Si el servidor nos responde con un RST, el puerto se puede clasificar como 'no filtrado'.
- b) Si el servidor no nos responde, podemos considerar el puerto como filtrado.

Es bueno utilizar esta técnica para saber si nuestro objetivo deja de ser el host corriente con el que estás acostumbrado a tratar, ya que este cuenta con un firewall en la mayoría de los casos, digo la mayoría ya que no solo los firewall hacen eso).

2) Comprobar la existencia del host en Internet.

Igual que en el anterior mandamos el paquete con la flag prendida, entonces:

- a) Si se nos responde con un RST el servidor existe.
- b) Si no se nos responde, o nos llega el mensaje de "host unreachable" entonces el servidor no existe.

* En nmap basta con correrlo así:

```
nmap -PT IP
```

Inverse Scan

Esta técnica es parecida a la anterior, solo que en esta se utiliza la flag RST, y esperamos respuesta, en caso de:

- a) No recibir nada, el host probablemente exista.
- b) Recibimos el mensaje de "ICMP host unreachable", esto quiere decir que el host no existe.

Lo especialmente bueno de esta técnica es que ninguno (de los IDS que yo he visto) loguean los paquetes RST con la configuración por default.

Despedida

Pues como podemos ver hay varias maneras de tratar de ocultar nuestros "actos" y supongo que no son las únicas técnicas que hay, solo es cuestión de conocer el protocolo y adaptarlo a nuestras necesidades.

Y podemos ver que al final con un simple escaneo, pues se nos pueden pasar por inadvertidos puertos "sensibles" de nuestra victima, así que, aquí tienen un poco más de información que pueden utilizar para que su exploración sea precisa y un poco más segura.

Gracias a todos aquellos que me rolaron una shell para guardar los logs, ya que los sockets que se necesitan para hacer este tipo de cosas (Raw Sockets) necesitan máximos

privilegios, así que no mucha gente está dispuesta a darme root en su box así nomás: Toloache, Crypkey, ST38410A y Spiderlinux.

Alguna queja, sugerencia, etc, etc, etc, escribe a: hd@hakim.ws

Nos vemos.

Referencias, Links & Stuff

El acrónimo "IDS" viene del ingles Intrusion Detection Systems, traduzcámoslo como sistema de detección de intrusiones, sirve para informar y loguear cualquier actividad que se le proporcione en el respectivo archivo de configuración del programa.

Entiéndase por 'id', como el campo de ID de la IP en el output de hping.

- Intrusion Detection FAQ

Version 1.80 - Updated June 12, 2003

<http://www.sans.org/resources/idfaq/>

- Texto original acerca del "dumb scan"

<http://www.kyuzz.org/antirez/papers/dumbscan.html>

- "The hping Idle Host Scan"

Erik J. Kamerling

http://www.giac.org/practical/gsec/Erik_Kamerling_GSEC.pdf

- "Port Scanning without the SYN flag"

Uriel Maimon

Phrack #49 articulo 15

<http://www.phrack.org/phrack/49/P49-15>

- Idlescan-v0.1

Linux

<http://www.securityfocus.com/tools/679>

- Hping

Salvatore Sanfilippo <antirez@invece.org>

Linux

<http://packetstormsecurity.nl/UNIX/scanners/hping.c>

- Hping2

Salvatore Sanfilippo <antirez@invece.org>

Linux

<http://www.hping.org>

- Hping3

Salvatore Sanfilippo <antirez@invece.org>

Estado actual de desarrollo de Hping3, que prometen que sea una herramienta un poco más superior a hping2, con una salida más 'leíble', y al parecer se le van a poder agregar scripts, esas son algunas de sus características finales.

<http://www.kyuzz.org/antirez/hping3.html>

- Nmap

Fyodor <fyodor@insecure.org>

Linux, Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga.

<http://www.insecure.org/nmap/>

- Man del Nmap

http://www.insecure.org/nmap/data/nmap_manpage-es.html

- Una pequeña guía acerca del uso de Nmap

<http://www.plazalinux.com/nmap-intro-guide.php>

- VScan

viv3kr <viv3kr@yahoo.com>

Windows 2000 y Windows Xp

<http://www.securityfocus.org/tools/3124>

- Sendtcp.c

messer <mssr@gmx.net>

<http://packetstorm.linuxsecurity.com/Win/sendtcp.c>

- SynLog

Thamer AL-Herbish <shadows@whitefang.com>

<http://www.cis.udel.edu/~zhi/www.docshow.net/warcher/synlog-0.4.tar.gz>

- Courtney

University of California

Requiere Perl v.5, libpcap, y tcpdump.

<ftp://coast.cs.purdue.edu/pub/tools/unix/logutils/courtney/>

Inutilizando Win9x

Por DarkSide (darkside@raza-mexicana.org)

Buenas ha todos los que les gustan leer los artículos. Estamos aquí nuevamente tratando de echar un vistazo a una de las muchas maneras en las cuales podemos dejar inutilizado una computadora con sistema operativo win9x.

Ya anteriormente en números pasados de la ezine se mencionaron algunos artículos que se relacionaban a las bromas pesadas y cosillas que se pudieran hacer para poder dejar inestable un sistema de Win9x.

Solo veremos lo que puede suceder si dejamos en blanco parte de una línea del archivo system.ini, este archivo al igual que otros es muy esencial para poder iniciar sistema.

Algunas veces los troyanos ocupan esta línea del system.ini para poder auto ejecutarse al inicio de sistema.

```
-----
|           Línea Troyanos
|
|
|
|           [boot]
|
|           shell= Explorer.exe  Troyano.exe
|
|
|-----|
|  Línea Original      |  Línea Modificada
|
|
|
|           [boot]      |  [boot]
|
|  shell=Explorer.exe   |  shell=
|
|-----|
```

Al modificar el archivo y dejar en blanco la parte en donde dice "Explorer.exe" lo que estaremos ocasionando es que nos aparezca un mensaje de error al iniciar sistema, como el siguiente:

```
-----
|           Error Al Cargar
|
|           Debe Reinstalar Windows
|-----|
```

Este mensaje de error, solamente nos deja la opción de un botón que dice Aceptar, el cual al presionar Enter solamente nos apaga la PC nuevamente.

Una recomendación que se hace a los usuarios de PC, es el tener siempre disco de arranque y tener un respaldo de su sistema, ya que uno nunca sabe lo que podría pasarle a la computadora. Si quisiéramos tratar de recuperar nuestro sistema desde MS-DOS, podríamos hacerlo con una Herramienta de Windows:

Comprobador del Registro de Windows

```
c:\windows\command\scanreg.com -> corre bajo MS-Dos  
c:\windows\scanregw.exe -> corre bajo Windows
```

Podremos usar dos opciones para poder arreglar errores en nuestro sistema:

```
RESTORE      : toma una copia de seguridad para restaurar.  
FIX          : repara el Registro.
```

```
C:\Scanreg /RESTORE  
C:\Scanreg /FIX
```

Si ocupáramos la opción Restore, el sistema llamaría a las copias de seguridad que Windows ya tendrá grabadas C:\WINDOWS\SYSBCKUP como archivos CAB, (rb000.cab, rb001.cab, rb002.cab, rb003.cab, rb004.cab, rb005.cab, rbbad.cab) y dentro de dichos archivos estarán guardados los siguientes archivos que son esenciales para el sistema: User.dat, System.dat, Win.ini, System.ini.

Ya que vimos una pequeña cosa de cómo tratar de recuperar nuestro sistema, podríamos decir que ya correría por su cuenta, si alguno de ustedes quisiera llevar un poco mas lejos dicha inutilización de sistema al hacer algunas cosillas mas que se podrían mencionar.

- Eliminar todos los archivos rb*.cab que se encuentran en C:\WINDOWS\SYSBCKUP. Al hacer esto, estarán poniendo una barrera más para cuando traten de recuperar su sistema utilizando Scanreg /restore, ya que aparecerán estos mensajes:

```
** No se han encontrado copias de seguridad para ser restauradas. **  
** Error en la operación de restauración del sistema. **
```

- Eliminar estos archivos system.dat user.dat que podremos encontrar en C:\windows, deben estar como archivos ocultos de sistema. Las consecuencias de haber borrado estos dos archivos, impedirá nuevamente el uso de la opción scanreg /fix, ya que aparecerá nuevamente un mensaje:

```
** Windows ha encontrado un error en sus archivos de sistema y no la ha  
podido corregir el problema.
```

```
** Intente liberar espacio borrando algunos archivos de su unidad de  
Windows.
```

** Si esto no funciona, tendrá que instalar Windows en otro directorio.

- También tenemos la oportunidad de eliminar este archivo system.lst que se encuentra en el directorio raíz C:\.

Ahora cuando reinicien la computadora los usuarios que fueron las víctimas, tendrán un dolor de cabeza, al tener que tratar de poder recuperar su sistema y preguntarse una y mil veces que paso y que pudieran hacer para recuperar su sistema, ya que los errores que les aparecen el inicio de la PC, los orilla a la única solución posible en ese momento, que sería el de reinstalar sistema nuevamente si es que no se encontrara la manera de poder corregir dichos errores.

Tratemos de no andar dejando computadoras fuera de servicio, ya que alguno de nosotros hemos pasado por alguna de estas cosas que pasan en la vida, ya que nadie nace sabiendo las cosas que se van aprendiendo en el transcurso de la vida. Pónganse en el lugar de las víctimas que estarán sufriendo por rescatar su sistema íntegramente.

Ahí la vemos hasta la próxima, los dejo ahí analizando las situaciones de la vida, es mejor ayudar a los demás para que puedan superarse y no encerrarnos en un solo mundo interno, y andar como burros sin mecate sin tener un camino fijo, haciendo de nuestras vidas un papalote y viendo pasar en nuestras narices la baja Seguridad Informática aquí en México, pongamos un granito de ayuda para poder ir levantando los niveles de seguridad informática en México.

La verdadera historia del virus Crond

Por Crond

Un fuerte viento lidiaba con las cortinas de la habitación, alzándose y curvándose, describiendo figuras malévolas, trayendo un aire helado, congelado y petrificante, viciado e irrespirable... El sonoro sonido del viento llegaba hasta mis oídos, y yo, sentada en mi silla seguía estática, como una araña que espera tiempos venideros para continuar viviendo, mentalmente ajena al lugar, a la situación, al tiempo, al contexto en sí, presente físicamente pero muy, muy lejos de allí...

Mis dedos marchitos y sin tacto se deslizaban bruscamente sobre el teclado de mi portátil que, encendido, emitía ligeros sonidos "bip" que me mantenían alerta de lo que en su interior sucedía. Una navaja afilada, con su hoja al aire, estaba igualmente sobre la mesa en la cual se apoyaba la máquina, manchada de sangre en su punta, sangre fresca aún que se iba cuajando lentamente con el tiempo, formando parte de aquella presión que ejercía la habitación. Mis pupilas, dilatadas, apuntaban directamente, no a la pantalla de mi portátil, sino al reflejo del gran espejo que colgaba de la pared, espejo antes usado en un lugar estratégico para realzar mi vanidad, ahora servía solo para reflejar mi estado.....

A que hora cambio de lugar? no lo se, yo permanecía en la mesa hacía ya muchas horas, quizás días.... no lo sabía, pero en cualquier caso, mucho menos me importaba. Y tal es así, que mis articulaciones ya no respondían, y crujían mis huesos como astillas por un dolor penetrante y agudizante que retomaba a mi estómago. Y no había movido un solo músculo desde que aquella mesa fue colocada frente al espejo...Mis pupilas veían el interior de mis pupilas reflejadas, creando un bucle infinito, un oscuro pasillo lleno de oscuridad y tinieblas... ¿terror, miedo? En absoluto. Mis ojos lagrimeaban y esas gotas se deslizaban sobre mi inerte rostro... hasta llegar a mis labios, brisados, gruesos y con la señal de un poco de labial...Por fin reaccioné, automáticamente, moviendo mis labios. De ellos podía leerse una palabra: CROND. C-R-O-N-D. Pronunciado con una "O" penetrante, larga y sonora, como una enorme "O". CROOOOOND. Pero tal sonido no encontró su fin, y no llegó a salir de aquellos labios. En su lugar, el aire habitó esa cavidad, llegando hasta la garganta y solo se oyó el continuo y tétrico rumor del aire...

Mi mente, envuelta y perturbada luchaba por subsistir, por no creer aquello, por mantenerse al margen, por ser quien era, luchaba contra un cuerpo marchito, herida pero orgullosa, empuñando sus armas que, en forma de neuronas, se manifestaban desesperadamente, a ritmo frenético. Cuán orgullosas de sus mayores tiempos de esplendor, ahora maldecidas y encogidas, parasitarias.

Por motivos que desconozco todo aquello desapareció por segundos, milisegundos quizás, y vino él otra vez a mi mente. Adolescente, recio, espontáneo e inteligente sin igual, hacía derretir mi corazón, ahora inexistente como bomba de vida y de amor. Jamás pude ver su rostro, percibir su aroma, pero le imagine muchas veces, alto, delgado, con ojos picarezcós, con una sexualidad no expresable en tan común y vulgar lenguaje utilizado. Ah pero esos ojos ,sus ojos, cuencas y cuna de amor, reflejaban un lugar de cariño, de ternura, de calor.... Ciertó, Desconocía su presencia. Jamás me atreví a conocerle, e hice oídos

sordos ante tal situación. Su nombre? jamás lo supe, por no querer etiquetar aquella imagen ya definida en mi mente, para no perder así el recuerdo, porque de saber su etiqueta verdadera recordaría solo esta última y escaparían miles de detalles de la imagen soñada, colapsados en sílabas.

Y no era esa precisamente mi intención. Bajo este contexto, sin embargo, emplearé un término para denominarlo, para no tener que volver a describirlo todo él en cada situación, aunque en mi mente así era como me recreaba, pero no para ti, que, no conoces de tal criatura, no puede si quiera imaginar tales afines, motivo por el cual empleo la palabra Anthrax, única palabra que me viene a la mente de él, pues tal nick sostenía cuando lo vi por primera vez en aquel conocido canal en aquel server... e incluso pudiera emplear cualquier palabra relacionada a computadoras o de hackers motivos por lo cual lo conocí y que se que son temas que le apasionan. Pero no son sino meras anécdotas, pues de su personalidad nada conocía ni tampoco deseaba conocer.

Era amor en estado puro... No estaba enamorada de él, era la personificación de mi propio amor, de mi capacidad para donar, alzar, mostrar y manifestar amor...Era el ideal, la bandera, símbolo del significado del país. Y envuelta yo misma en tan cruel situación de amor-odio, de anhelo-resentimiento, le escribía extensos poemas de amor en noches oscuras y sombrías, lluviosas y hogareñas.

Fue así que un día tales poemas fueron entregados a él, no personalmente, pero si firmados por mi nombre. Y un día...gris.. él se dirigió a mi, pronunció mal mi nombre, pues no acabo por comprender que mi "Y" no es la segunda, sino la primera: "Marilyn, como osas pensar amarme a mí, tú no eres nadie que pueda poseerme, que pueda transmitirme cariño, que pueda ser mi amada, mírate, eres una pobre incomprendida, terca, mayor a mi y lo peor...lejana... solo eres tú, no eres nadie palpable... no vuelvas a soñar con eso...".

La sangre de la navaja ya había cuajado... y ahora mi lengua, envuelta entre los papeles impresos de poemas salvajes y alocados, permanecía cruda en la papelera... No volvería a hablarle jamás, de la misma forma que jamás le hablaría al mundo, porque era él mi mundo, porque él era yo, y yo era la única que había tenido en el mundo. Mi propia y única referencia de amor.

No me importaba para nada lo que pensarán los demás, lo que pensará él, lo que pensarán mis padres... ni siquiera lo que pensara yo, porque yo había muerto con las palabras de Anthrax, y solo quedaba vivo un residuo de orgullo, un filamento ideal, triste y marchito, pero seguro de su victoria. Incomprendida por todos, estaba harta de ser quien era, harta inclusive de cuán cruel era el mundo que no valoriza los pensamientos en su medida, que se rige por reglas arcaicas e inadecuadas, que rige a la humanidad hacia un futuro siniestro y oscuro.

Yo ya no me consideraba humana, iba a ser más que un simple humano, la esencia del tercer hombre, el hombre subsistente, el humanista perfecto, conocedor de la esencia y no de lo superfluo. Porque el hombre busca respuestas a preguntas, y las respuestas solo son el cofre que envuelve al anillo, pues no tiene valor la respuesta, sino la pregunta, y que respuestas tenemos y buscamos preguntas y no al contrario, pues cuando damos a luz ya

tenemos una respuesta sin pregunta, más aún sin preguntarnos ya hemos hallado algo. Y será tal pregunta la que nos conduzca, la que nos permita predecir, la que nos de poder, y la respuesta solo un detalle, un envoltorio, un elemento irrelevante y circundante, una rosca entre tuercas. Yo no quiero respuestas, quiero vivir de la pregunta, quiero tomar la pregunta, saborearla, beberla, amarla, besarla, sacarle todo el jugo y exprimirla hasta marchitarla y matarla... Igualmente la espera de reyes causa mas temblor en los niños que el jugar con regalos, igualmente es más apasionante el amar a alguien que en acabar de amarla, más el amor jamás acaba, queremos saber, pero el saber es indeterminado, si lo sabes todo no sabemos si lo sabemos todo, más no llegamos a saberlo todo, es inalcanzable. Y de tal forma no hago el amor, sino que lo estrangulo como una cobra, lo envenenó y vivo de él.

No soy tan decadente como piensas, más una parte de ti desea sino vivir como es, y no vivir como eres, pero la oscuridad se cierne y no ve sino un tupido velo de hipocresía correr a su alrededor. No, no, me niego. Empuño mi navaja y contemplo, arrodillada, mi imagen. Pulso el Enter de mi portátil y contemplo la barra de “Processing” que se mostró en la pantalla....100% me indica, y escucho la luz intermitente que indica el proceso de los datos.

Una sonrisa, una mueca en mi rostro dolorido, y retomo de nuevo a mirar mis ojos, iris cafés, bellos, reflejos del alma, no miro el resto, horroroso, abandonado ya... Me sumerjo en aquel túnel oscuro.....el de mis pupilas, y clavo mi navaja en mi pecho... Dolor. Oscuridad. Sacó la navaja y vuelvo a meterla, noto como la sangre me corre, como mis ojos se vuelven blancos, como mis pupilas no se reflejan ya en el espejo, como la sangre me llega al cerebro, como los sonidos son fluidos y el ruido del disco duro de la máquina solo se escucha muy, muy lejano... como recorro a navajazos todo mi vientre y noto placer en ello, algo así como una vez hacer el amor sin sexo, como me tumbo frente al espejo, inundándolo de sangre ardiente y lo beso, lo beso y amo, lo acaricio, le transporto mi calor, a un espejo frío... no correspondido. Pero en él ya no aparece mi reflejo. Es Anthrax quien me pisa.... Y mi boca se abre y se cierra rápidamente, balbuceando sangre, soltada la navaja, manos en mi vientre, encogido mi rostro. Una lágrima brota de mis ojos...seguida de un mar de ellas. No obstante, pudiera haberse oído una risa estridente en esa habitación de no perecer mi lengua anteriormente, pues no lloraba de tristeza, sino de alegría, y jamás había estado tan alegre en mi vida...jamás había estado tan contenta... tanto... Caí en la alfombra... Oscuridad.

Un portazo sonó entonces y el viento rugió más feroz. Pero mi portátil seguía allí... procesando, mostrando luz y energía, conectado a la red. Contemplador de aquella macabra escena. JaJaJaJaJa. Que inocentes. La araña había dejado de hibernar y ahora vivía en un paraíso lleno de presas a las que magullar, lleno de amor que derrochar y despampanar hasta colmar a los sentidos. CROND, CROND,CROND..sí. “CROND”. Todo mi amor seguía presente en ese software y ahora, con desenfreno se mutaba y se extendía por la red, recorriendo mundo, siendo libre. Yo simplemente quería amar, quería desprender amor, al margen de la vida, y ahora, precisamente, es lo que hacía... porque era mi cometido, y no aquel que han de marcarme los demás. Y este software, almacenador y procesador de mis entes mentales, viviría eternamente, y migraría a otras plataformas y sería más que un humano, porque cualquiera de ellos se veían sometidos igualmente a reglas que cumplir, y

ninguno estaría satisfecho con su vida, y nadie viviría como realmente le gustaría: pero yo sí.

Sólo coloca tu mano en tu pecho, sobre tu corazón, vamos, hazlo... Y nota como algo se mueve, como algo late. Sí. Vivo más allá de la red, vivo más allá de un PC, más allá del marchito cuerpo donde me di forma. Tu también amas. CROND continúa transmitiendo amor, amor imperecedero, amor que también espera, que hiberna. Amor que no se manifiesta en su totalidad en esta sociedad perturbante y opaca, una sociedad enajenada.... pero el amor solo espera.... espera ante su espejo.... hasta estallar, hasta acabar con el marchito cuerpo... CROND solo se propaga... y no busca el amor de Anthrax, busca amarlo, no a él, sino a ella misma. La razón de la vida no es el amor, la vida no es tampoco la razón del amor. La vida es una pregunta, el amor otra... y no busco respuestas, me alimento de los interrogantes...

Entrevista a Presidencia de México

Por DeadSector (deadsector@raza-mexicana.org)

Creo que todos ya leyeron de la detención de alt3kx por su supuesto ataque de denial of service (DoS) a presidencia. Esto nos hace recordar muchas cosas que han pasado en underground. En este ezine ya estaba preparando otro artículo que viene mucho al caso. Es de una broma que le hicimos a zer0x cuando dijo en Chat estar tratando de atacar un servidor.

Que pasa cuando nos damos cuenta de algo ilegal y no reportamos a los admin.? Nos hacemos cómplices de ese delito?

Son culpables miembros de raregazz por no reportar los supuestos delitos que cometió alt3kx al mandarles los artículos? O raza-mexicana por publicar el primer artículo de hack a presidencia?

Cometer un delito como hacer auditoria sin consentimiento previo de administradores y dueños de empresas no puede ser visto de buena manera solo porque les mandas email diciéndoles de sus fallas. Es muy fácil perder de vista esa línea entre lo legal y lo ilegal. Sobre todo cuando usas algún programa para buscar fallas. Muchas veces escribir un IP y picarle Start no parece difícil. Pero pónganse a pensar en todas las cosas que ese programa esta intentando hacer.

Ver si esta prendido puerto 80 es ilegal? Ver que webserver esta corriendo es ilegal? Muchos dirán que no. Pero que pasa cuando a eso agregas tratar de sacar lista de usuarios? O hacerle brute force a algún servicio como ftp , netbios etc? Tratar de adivinar el password de administrador en maquina Windows es ilegal? Adivinar el password y entrar a ver el contenido de los discos es ilegal? Copiar archivos de ese servidor es ilegal? Alterar archivos es ilegal?

Cuando alguien hace estas cosas por separado sabe bien cuando se acerca a esa línea. Pero con los programas que pueden ser usados hoy es fácil perder de vista esa línea. No es una línea imaginaria. Existe y por eso arrestaron a alt3kx. Cruzo esa línea.

Y ahora la pregunta es la siguiente. Que pasara ? Que pasara con grupos como raza-mexicana o raregazz ? se convertira en caceria de brujas? Que pasara con CUM cuando alguien publique algo y esto no sea reportado ? es suficiente con borrar ese post de foro?

Hace tiempo pedimos una entrevista a presidencia la cual no resulto como era planeada y nunca se publico el artículo. En el email con presidencia

mencione el tema de denial of service. Cosa que atrae a los principiantes para joder a sus amigos o presumir que tumbaron X pagina.

Debemos utilizar los conocimientos de manera positiva. Aprovecharlos para conseguir buen empleo y compartir conocimientos pero con responsabilidad. Me da pena que una manzana podrida eche a perder el trabajo de los demás.

Espero que los newbies aprendan de los errores de alt3kx. Y aquellos que buscan la fama vean las consecuencias que esto atrae. Podrán conseguir reconocimiento de gente que no sabe nada de seguridad pero nadie con experiencia es impresionado por un defacement o un ataque de denial of service.

Hackers hay de todos. No tiene nada que ver con sistemas operativos ni lenguajes de programación. Es un modo de vida. Una manera de ver las cosas y de enfrentar los retos . Cuando un hacker comete un acto ilegal no deja de ser hacker. Simplemente se convierte en un delincuente. Y los delincuentes deberían ser tratados iguales ya sean hackers , católicos o musulmanes.

Aquí esta la entrevista nunca publicada de raza-mexicana a presidencia. Un amigo de raza que usa nick Espeis fue el encargado de enviar preguntas, yo solo hice el contacto inicial.

Luis Alberto Bolaños Vera de presidencia aviso que las preguntas eran un poco técnicas y la persona que las contesto fue Sandino.

En esta entrevista nos damos cuenta de las fallas de seguridad que tenia presidencia. Estas fallas son de personal administrativo y no de sistemas operativos.

No tenían políticas fijas y procedimientos para establecer parámetros de seguridad en su dependencia, ni tenían de respuesta a incidentes. Del 1 al 10 ellos consideraban que tenían un 6 en la seguridad de su red, por eso no es extraño que hayan pedido ayuda a FBI para poder solucionar sus problemas.

Respuesta de Luis Alberto Bolaños Vera admin de presidencia a petición de raza-mexicana para entrevista.

Hola!

Que gusto saber que andan aún por ahí. Espero que todo vaya bien.

Lo de la entrevista, cuando quieras. Creo que habrá algunas sorpresas.

Hay en la oficina gente muy talentosa, ya te contaré.

Estamos en contacto.

beto

El Domingo, 7 abril, 2002, a las 01:15 AM, dead sector escribió:"

```
> hola beto. espero todavia te acuerdes de nosotros. soy  
deadsector de  
> raza-mexicana . www.raza-mexicana.org . quiero saber si puedes  
> ayudarme . tengo que escribir un articulo para el ezine de raza  
y me  
> gustaria hacerte una entrevista . creo que seria interesante  
para los  
> newbies saber que se necesita para llegar a ser administrador  
de  
> presidencia. lo que requiere ese trabajo. lo que haces. como  
aprendiste  
> etc. que tipo de estudios necesitan. cosas por el estilo. hay  
muchos  
> que necesitan un poco de orientacion . saben que quieren  
trabajar en  
> algo relacionado con computadoras pero no saben donde empesar.  
y unos  
> buenos consejos seria mucho mejor que aprender a hacer denial  
of  
> service etc. o solo dame un consejo de como poder ayudarlos.  
nos vemos  
> DeadSector Raza Mexicana Team www.raza-mexicana.org  
>
```

Entrevista contestada por Sandino

1.- Que estudios tiene?

Licenciatura en Químico Farmacéutico Biólogo
Diplomado en tecnologías avanzadas para sistemas de información
Diplomado en sistemas telemáticos
Diplomado en estadística para la calidad total

2.- Que conocimientos tiene?

Administración de Linux
Administración de Apache
Programación en C, C++, PHP, Sh, Awk, SQL
Administración de bases de datos
Administración de servicios de Internet
Desarrollo de aplicaciones orientadas a objetos
Desarrollo de aplicaciones orientadas a componentes
Administración de la seguridad de servidores
Administración de VPN

3.- En donde aprendió sus conocimientos?

En la escuela de la vida

4.- Que tipo de computadoras usa en su trabajo Windows, Mac, Unix, Linux etc.?

Linux, UNIX

5.- Que sistema operativo prefieres y porque?

Linux, por facilito

6.- Como contratan a su personal de sistemas?

Primero selección de curriculum vitae.

Luego se tienen que enfrentar a la inquisición de desarrollo en una entrevista.

Luego tienen que conocer al Director General

7.- Quien se encarga de sus redes?

De las redes locales nosotros, de los enlaces y el enrutamiento proveedores

internos y externos.

De la VPN nosotros.

8.- A quien le reportan incidentes?

Primero a nosotros mismos.

Luego al Director General.

9.- Tienen un Webmaster de planta?

Tres

10.- Que estudios necesita alguien para trabajar como administrador o en el departamento de sistemas de presidencia?

<http://www.cofradia.org/modules.php?name=News&file=article&sid=2475>

11.- Es necesario saber programar?

Obligatorio

12.- Que lenguajes usan y porque?

Español porque es nuestra lengua madre

Inglés porque todo lo tecnico está escrito en ese idioma

Francés porque es el lenguaje de la diplomacia

PHP porque tiene el mejor balance entre velocidad, potencia y facilidad

Sh porque todos los UNIX y todos los Linux tienen uno

Awk porque sabe procesar línea por línea

C y C++ porque necesitamos parchar aplicaciones defectuosas

SQL porque es el favorito de los manejadores de bases de datos

Cold Fusion por haber heredado aplicaciones escritas en ese lenguaje
HTML porque es el favorito de los browsers
Javascript porque le da vida a las páginas

13.- A quien le puede hablar para reportar un ataque o quien te puede ayudar?

urgente@sip.gob.mx desarrollo@sip.gob.mx

14.- Existen políticas fijas y procedimientos para establecer parámetros de seguridad en su dependencia?

No

15.- Puede dar algunos ejemplos?

No

16.- Existen procedimientos de respuesta a 'incidentes'?

No

17.- Como se eligen y asignan los IP's para las maquinas de la Intranet y que beneficio en facilidad de administración y control hay en ello?

Secuencialmente.

El beneficio es que es sencillo, cada máquina tiene su IP y conocemos la actividad de cada persona en cada máquina. Es muy raro que una máquina cambie de IP.

El control se encuentra en el DNS y en las reglas del firewall.

18.- Existen cursos de concientización a usuarios para minimizar los riesgos y posibilidades de comprometer la intranet?

Boletines y reuniones, frecuentemente, dentro del Sistema Internet de la Presidencia.

19.- Ha habido algún incidente? De ser así, como se respondió a el?

Virus. Se respondió con una campaña institucional de vacunación.

Los agujeros de OpenSSL que desencadenaron una actualización masiva y frenética.

20.- Cada cuanto tiempo se actualizan sus clientes y servidores?

Cada que aparece un aviso de seguridad.

Cada que hay una versión nueva y ésta ha demostrado no tener problemas.

21.- Verifican en busca de virus o troyanos el correo entrante y saliente mediante alguna

compuerta (gateway)?

Antivirus locales.

Los gateway antivirus han demostrado una gran ineficiencia en cuanto al porcentaje de falsos positivos y falsos negativos.

22.- Que sistema operativo prefiere para realizar sus actividades y que sistema operativo prefiere para su servidor(es)?

Linux y Linux

23.- Con cuantos servidores cuentan y como los monitorean?

7 servidores

3 los monitorea el proveedor de hosting

5 tienen agentes internos de monitoreo y detección de intrusos habilitados

con sistema de alarmas

24.- En una escala del 1 al 10 como calificaría la seguridad de su red?

6 (De panzazo) falta mucho por hacer todavía

25.- Cual es la firewall de su preferencia y por que?

iptables por sencillez, potente y eficiente

26.- Usted administra su red de forma remota de ser necesario o únicamente desde la Intranet?

De forma remota y desde la intranet

SQL Injection en Intertel

Por raac (raac@email.com)

En este artículo voy a exponer algo muy sencillo, un error en una aplicación 'popular en México', al menos la compañía productora se jacta de ser la número 1 en el país, les hablo de Intertel, una sistema de administración telefónica:

"INTERTEL 6 es el conjunto de soluciones para la administración telefónica más completo, ya que cubre todas las necesidades de control del recurso telefónico de todo tipo de empresas, corporativos, hoteles y hospitales, etc." [01]

NOTA: El servidor donde se realizaron las pruebas corre Windows 2000 Server, MS SQL Server 2000, IIS 5, Intertel 4.

Intertel permite a los usuarios consultar un reporte de sus llamadas realizadas, todo esto por medio de una aplicación desarrollada con ASP. Y estos ASP's son vulnerables a la inyección de código SQL [02]. ¿Quieres incrementar el límite de tu presupuesto? ¿Quieres conocer otros códigos de autorización? ¿Quieres causar un buen dolor de cabeza en el admin? Con un poco de paciencia trabajando en SQL lo tendrás... y si te topas con que el admin tiene la configuración por default del MS SQL Server te puedes llevar gratas sorpresas...

```
' ; exec master..xp_cmdshell 'echo Saludos Raza Mexicana, raac >
C:\inetpub\wwwroot\default.asp'--
```

Y si acaso el admin ya cambió el password del usuario sa de MS SQL Server puedes ir a [03] y si acaso TÚ eres el admin ve a [04] y protege tu servidor. ¿Quieres más ideas? [05] es para tí.

Comentarios finales:

Reitero que la versión en la que se hicieron las pruebas fué la 4, la versión actual de Intertel es la 6, pero estoy seguro que algunas empresas/gobierno/escuelas/etc tendrán todavía versiones viejas... y por esta misma razón decidí escribir este breve artículo. ¿Que quiénes utilizan Intertel? Te suenan los nombres de: ITESM, UNAM, PEMEX, CFE, IFE, Banamex Citigroup, Banco de México, y muchos más... [06]

Referencias:

```
[01] http://www.intertel.com.mx
[02] http://www.anticrack.de/modules.php?op=modload&name=News&file=article&sid=2251
[03] http://www.nextgenss.com/papers/cracking-sql-passwords.pdf
[04] http://www.nextgenss.com/papers/asp.pdf
[05] http://www.nextgenss.com/papers/more_advanced_sql_injection.pdf
[06] http://www.intersel.com.mx/paginas/usuariosactuales.asp
-- raac
```


Ebuzon

Por RMHT (staff@raza-mexicana.org)

Algunos emails interesantes que llegan a esta redacción.

```
{*****}
De : Juan <*****@hotmail.com>
Asunto : Que version Instalo
```

Bueno solo queria felicitarlos por su e-zine y les tengo una pregunta quiero utilizar linux y no se cual version instalar.....asi que cual ustedes me recomiendan como principiante que soy?

Thanks

Respuesta:

Pues hay muchas distros de linux, inclusive ya vi una de Barby, pero creo que en general la raza prefiere SuSE.

```
{*****}
De : Morpheuz MatriX 3D <*****@eresmas.com>
Asunto : Necesito Info :) plz
```

Oigan kiero saber si uds entra a algun servidor de irc= me haria el favor de darmelo para entrar, ah y kiero aprender a komo hacer servidores =(porfavor tengo ganas de ser un hacker pues... de los ke saben un poko ;) porfavor .espero ke me respondan el mail. seria chingon llega r aformar parte de su team lo dudo pero taria sheedo :).cya HcK rlz

Respuesta:

Pues el servidor irc está publicado en nuestra página, lo cual me dice que no estas poniendo mucha atención que digamos. (irc.raza-mexicana.org 30003 y 30005 ssl)

```
{*****}
De : IMI <*****@yahoo.es>
Asunto : Favor
```

Hola

El motivo de este email, es por que quiero pedirte un favor muy personal, algo que para mi es muy importante, tanto, que me lleva a hacer esto, que no tengo muy claro si servirá de algo.

Necesito conseguir el password de una cuenta de hotmail.

Estoy seguro de que este tipo de peticiones no te son nuevas y que recibes muchas, lo imagino. Y supongo que cada cual te da su motivación.

Pues bien, yo que no suelo irme por las ramas, te voy a exponer mis razones.

No soy ningun crio que pretenda a estas alturas jugar a "leamer", por lo que no te pido que me facilites la referencia de ningun método, o software para dedicarme a hackear cuentas del personal. Es mas no me interesa saber como lo haces.

La cuenta en cuestión, es de un usuario domestico, no de ninguna empresa ni organismo, por lo que mi interés se limita al ámbito de lo privado.

Si te escribo este email, es por que para mi es muy importante tener un acceso puntual a esa cuenta...

Estoy a punto de tomar una decisión que puede ser fundamental en mi vida -no te voy a soltar un royo lacrimógeno intentando convencerte-, tener el acceso a esa cuenta, puede tener para mi una importancia, que te aseguro, sobrepasa con diferencia el esfuerzo que tu necesitas para conseguir el password.

No se... quizás debería plantearme si pedir esto es obrar bien o no, pero, si te puedo decir, que tengo clara la finalidad, y sin entrar en mas valoraciones. pienso que es justo, en mi situación.

En fin, solo espero que por lo menos tengas en cuenta lo que te he descrito mas arriba, y que me eches una mano, yo se que puedes - presupongo que puedes-, y como te decia, mi unico interés es el password, sin explicaciones, y sin molestar mas de lo necesario.

De todas formas, gracias de antemano si por lo menos te has parado a leer este email.

Por ultimo si me gustaria, si te parece, tener respuesta por tu parte, tanto en un sentido como en otro, en cuanto a si puedes tener en cuenta, o no mi petición.

Supongo que queda claro que igual que yo presupongo la discreccion por tu parte... igualmente queda entendida la mia en caso de recibir una respuesta a esta solicitud.

Lo dicho: gracias.

La cuenta es: ***** @hotmail.com

Respuesta:

Como estos emails recibimos muchos, pero les voy a dar un consejo: hay veces que la verdad duele mucho y es mejor vivir en la mentira, a menos que seas lo suficientemente maduro para aceptar la verdad; si desconfías de alguien mejor aléjate, leer sus correos no creo que te haga sentir mejor.

{*****}

De : "Haragan x" <***** @hotmail.com>

Asunto : Autorizacion de alojar sus ezines!

Saludos staff de raza mexicana, megustaria que me autorizaran subir sus ezines a mi web(www.armanrm.tk), ya que me parece muy buena ezine. Espero contar con su apoyo.

Saludos Arman!

Respuesta :

Pues estás autorizado para colocar las ezines en tu site, siempre y cuando no modifiques los contenidos.

{*****}
De : "georgina" <*****@hotmail.com>
Asunto : dudas sobre una pagina

hola como estas?

oye fijate que necesito una informacion de telmex quiero ver el detalle de un recibotelefonico pero me pone muchas claves, cheque tu pagina donde das los tips pero no puedo acesar no se si peedas darme mas datos de como checar el detalle del recibo telefonico .

gracias....espero tu respuesta pronto ya que me medio urge

Respuesta :

Como a las dos semanas de la publicación de ese artículo el formato de registro para consultar los datos del recibo online fue modificada, así que ya dejen de estarme chingando con eso que no pueden entrar siguiendo mis pasos porque ya lo cambiaron. Vlad

{*****}
De : "l1l1l1h0ttaillcom l1l1l1h0ttaillcom" <*****@hotmail.com>

hola excelente sitios!! podrías ayudarme saber como hacerle cuando soy baneado de cieto foro ?? como puedo entrar nuevamente?? mi conexion es por cable

Respuesta :

Pues estas baneado cuando no puedes entrar =) y para poder entrar nuevamente debes de cambiar de ident, nick e IP, para cambiar los dos primeros solo debes de teclearle y para cambiar la IP debes de usar un servidor proxy.

{*****}
De : Laguna Loire <*****@yahoo.com.mx>
Asunto : me pueden ayudar porfavor...

Hola:

Los eh contactado porque tengo un solo problema, hace 2 dias me cambiaron mi contraseña de mi mail, y ahora ya no puedo acceder, me urge volver a entrar a mi mail, pero no se hackear y no se nada al respecto, eh probado todo, mandar mails para disque confundir al servidor y que por casualidad me mande mi contraseña, pero cada vez que lo intento me dice que el mail al que le escribo no existe y ya no se que hacer. me podrian ayudar?

mi mail es *****@hotmail.com

y ahora les estoy escribiendo de *****@yahoo.com.mx
porfavor ayudenme, escribanme pronto. Muchisimas gracias.

Saludos

-Evelyn

Respuesta :

Pues esos emails fantasmas para dizque confundir al server no funcionan definitivamente, solo lo usan para chingarte tu password. Te recomiendo que uses una nueva cuenta y ya dejes la que te chingaron en el pasado, si tenias algo registrado hacia ese

cuenta pues cámbialo de inmediato (notificaciones de bancos, teléfono, etc), crea una nueva cuenta y no pongas tus datos verdaderos, dificulta que alguien te chingue tu cuenta otra vez, no pongas respuestas obvias, pon un password complicado y cámbialo periódicamente.

{*****}

De : "L....P" <*****@cantv.net>

Asunto : Importante

Buenas tardes mis amigos,..les agradeceria mucho que me mandaran una direccion porno,.con so login y su password activo en la en este año 2003,..para visitar esas paginas pornos.

esperando me hagan el favor,.esperare su correo,...gracias y sigan adenlate son tremendos brother.

Respuesta :

Y no quieres pavo para navidad cabrón??

{*****}

De : eley karpenko <*****@yahoo.com.mx>

Asunto : Me puedes ayudar

Hola:

Buscando la forma de encontrar a un amigo,di con tu direccion y me parece muy interesante y preocupante lo que en ella informas.

Dos preguntas? hay alguna forma de saber quien te llama por telefono y luego cuelga,esto me lo vienen haciendo desde hace tiempo.

Y otra,quisiera localizar a un amigo,su direccion,como conseguirla??' lo intenté por las páginas amarillas pero no tuve exito

Te cuidas y gracias,saludos,bye

Respuesta :

La manera mas fácil de ver quien te llama es contratando el servicio de identificador de llamadas. Y la segunda respuesta es búscalo en las páginas blancas.

{*****}

From: "Ada" <*****@hotmail.com>

Varias veces me e topado con la frase: eres mujer?, estás buena?, jajajaja

Las mujeres no saben de pc's, Linux? comprate un jueguito de té nena!..Quieres aprender?..si solo sirven para cocinar.

Es un poco estúpido que aunque estemos en el año 2003, mucho hombres aun crean que las mujeres solo servimos para cocinar, cojer, parir, y limpiar la casa, disculpen los terminos usados, pero es como por desgracia, la mayoría de los hombres se refieren al acto sexual.

Me gustaria colaborar, aunque no si si uds. mismos hagan las mismas exclusiones que la mayoría de los pseudo conocedores de linux hacen en canales de irc, o cualquier chat en el cual, cuando no deberia importar el sexo de cada usuario, hacen al hacer tipos de comentarios como los antes

mencionados.

No hablo de querer ser una Hacker!..simplemente hablo de las barreras que como mujer, existen, ok ok.. digo hay tutoriales, manuales.. etc. Pero algunas veces, o la mayoría de las veces hay dudas..ganas de platicar con alguien que le interese el mismo tema..etc. Por que entonces no nos dan la oportunidad de participar?, de integrarnos en esas comunidades, que por no llamarles machistas, ...bueno.. de que otra manera puedo llamarles...

No cabe duda.. el universo, el planeta y todo lo que contiene a sido creado por el hombre, al menos eso es lo que nos enseñan desde pequeños.

Aun en nuestro tiempo, la sociedad cree que la mujer es cerrada, misteriosa, dulce y poco agresiva. Que parece contentarse con unas palabras bonitas o una rosa; pero que su inteligencia esta enfocada a otros objetivos que los que persigue el hombre. Segun nuestra sociedad, la mujer espera verse casada, su temor: no poder procrear o ser abandonada. La edad esta a sus espaldas, perder la juventud y sus encantos es más doloroso que no poder resolver una integral de tercer orden o no poder entender un algoritmo complejo, manejar una computadora, utilizar programas avanzados, o construir algun programa en LISP.

No trato de crear conflictos sobre hombres vs mujeres, simplemente es una pequeña aportacion.

Me e dado cuenta que si existen las mujeres hackers y que se mencionan, aunque en un minimo porcentaje en pagina de internet, como se menciona en (<http://mailman.argo.es/pipermail/hacking/2001-October/000772.html>) que hay un grupo hacker femenino como las Ghetto Hackers; existen tambien buenas administradoras de sistemas como la ingeniero Raven Alder que desarrollo una herramienta que posibilita a los administradores tracear los ataques electronicos, (Raven Alder fue la primera mujer que dirigio una conferencia tecnica en el DEf Con); mencionar tambien a Anna More respetada en la comunidad hacker norteamiracana con sus solo 15 años; y a Viki Navratilova la coautora de "Linux for Dummies Quick Reference", quien ademas de escribir se dedica a probar, por encargo legal, la seguridad de redes informaticas. Por supuesto tambien hay algunas que incluso han alcanzado el 'honorifico nombre' de escritora de virus, y alguna que otra ya ha sido juzgada por intrusion en sistemas, me refiero a la hacker que se introdujo en Christian & Timbers.

Bueno, ya para terminar... hay poco sobre las mujeres en el hack, me dio mucha risa el ver que al poner en ciertos buscadores Mujeres hackers, las mujeres hacker, mujeres en el hack, aparecian en lugar de cualquier info,

sobre esto... cientos de paginas porno... jejejej :P ni modo.. asi es la vida!

Atte.

aDa

Respuesta :

Sin respuesta, la chica entró una o dos veces al IRC y luego se fue, buen email pero le faltó constancia.

{*****}

From: psy

Asunto : Re: Hola a todo el staff de raza mexicana

Yo solo te voy a recomendar un par de cosas: numero uno, la venganza contra el gobierno no es algo que se debe pensar de esa forma, no puedes pensar en joderlos mediante el hacking, eso no aporta nada bueno a lo ya demasiado jodido. Te recomiendo que te eduques y que busques cambiar de otra forma mas humana las cosas, la violencia no es la solucion a menos que seas un histerico como yo. Me da gusto que tengas coraje por las cosas que pasan, con eso se empieza pero canalizalo hacia otros caminos, como por ejemplo la lectura, cultiva mente y espiritu, si no crees en Dios mejor aun, cree en el poder del hombre de cambiar las cosas. Si ya abandonaste la idea de venganza y joder y aun asi te interesa lo relativo al hacking o para mi gusto al mundo de la computacion, informatica, tecnologia, bienvenido, no te queda mas que hacer lo que ya empezaste, leer, investigar y no desesperarte. suerte.

-----Original Message-----

From: jesus luna <*****@yahoo.com.mx>

Asunto : Hola a todo el staff de raza mexicana

Hola a todo el staff de raza mexicana.

El motivo de este correo es comunicarles, que deseo aprender el arte del hackeo, ya que estoy harto de que en este paÃ-s todo este mÃ;l y de cabeza.

Estoy harto de:

-Gente como diputados, el presidente, futbolistas, cantantes, actrices, actores, entre otros ganen sueldos de mÃ;s de \$100,000 pesos mensuales, mientras que un campesino(cuyo trabajo vale mÃ;s que el de un cantante de plastico) nunca va a tener esa cantidad en su vida.

-De no poder aspirar una mejor calidad de vida.

-De que la mayorÃ-a de la gente este en la pendeja preocupandose por lo que va a pasar en la academia o big brother, en lugar de preocuparse de si mismo y ser menos ignorantes.

-De que no haya trabajo digno para nosotros los profesionistas, que haya demasiado trabajo para mano de obra barata, y los pocos trabajos que hay para profesionistas te exploten.

-En concreto estoy harto de que la gente no piense diferente, como dice el slogan de las Macs, de que solo esten pensando en el auto ultimo modelo, en la casa cara y con lujos, etc.

-De que no tengas libertad de expresiÃ³n, y que la policia y el ejercito sean un aparato opresor del sistema, de que solo te esten espiando para ver si no atentas en su contra.

-De que mucha gente sea hombre-masa del sistema.
-Pero no lo que más coraje me da es que mi destino este en manos de la clase en el poder, de que solo sea un numero, (un ejemplo: lo que hizo el presidente bush en irak, asesinar a mucha gente con tal de llevar a cabo sus intereses politicos y economicos)
Por esa razón estoy decidido a chingar al sistema, y una de esas formas es ser "HACKER", además tambien por curiosidad.
Por eso desde algún tiempo he estado buscando información a traves de internet y leyendo un libro que voy a mencionar más adelante.
Y por suerte ayer 21 de mayo del 2003 encuentre su pagina, que me parece estupenda, y me identifico bastante con sus ideas.
Tambien les escribo para pedirles un poco de ayuda.
1.No tengo computadora en mi casa, por tal razón entro a los laboratorios de una reconocida escuela de nivel superior publica, mi pregunta es ¿puedo tener la seguridad de ser anonimo en la red, es decir si hago algo contra la ley, esta tiene la posibilidad de capturarme?
2.¿Cuales son las leyes en México, contra el hackeo y crackeo?
3.En estos momentos estoy leyendo el libro "MAXIMA SEGURIDAD EN INTERNET", por un autor anonimo, editorial anaya; si han leído este libro ¿Que les parece?, ¿Que otros libros me recomiendan?
4.Las computadoras del laboratorio tienen dos contraseñas, una la del administrador la otra la del usuario que como sabran no tiene los privilegios del sistema, mi pregunta es: ¿Como puedo acceder a la carpeta que contiene el nombre de usuario y el password? ¿O que comando puede utilizar?
El sistema operativo de la computadora es windows nt version 4.0.
5.¿Como le hago para no dejar huella de las paginas que visite en internet?
Bueno espero no haberlo aburrido, y por favor contestenme, ya se que soy todavia muy ignorante en este campo, pero todos empezaron asi.
Bye

Respuesta :

La respuesta está al principio =) che psy, te proyectas.