NETWORK INSTALLATION AND ADMINISTRATION I

(420-635-AB)

PROJECT PART1

Teacher: Antoine Tohme
Student: Houman Sharifian alborzi

APRIL 21, 2025

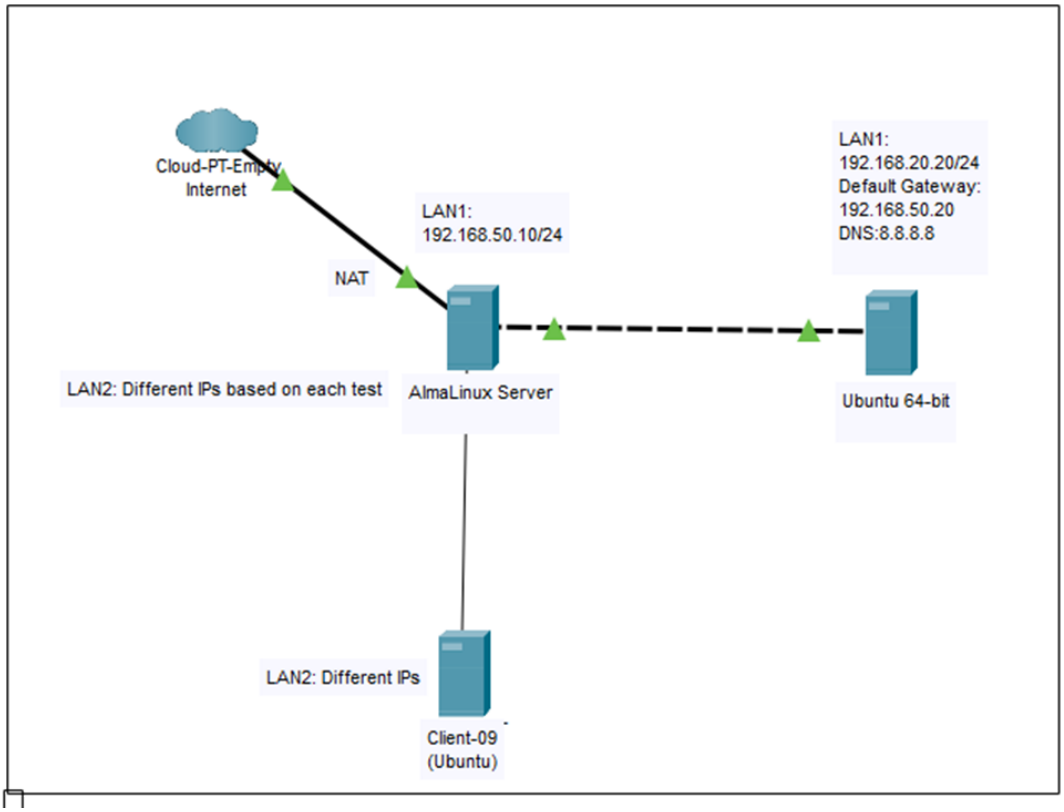
COLLEGE JOHNABBOTTE

Contents

NETWORK CONFIGURATION

Topology:

The following image shows the network topology.



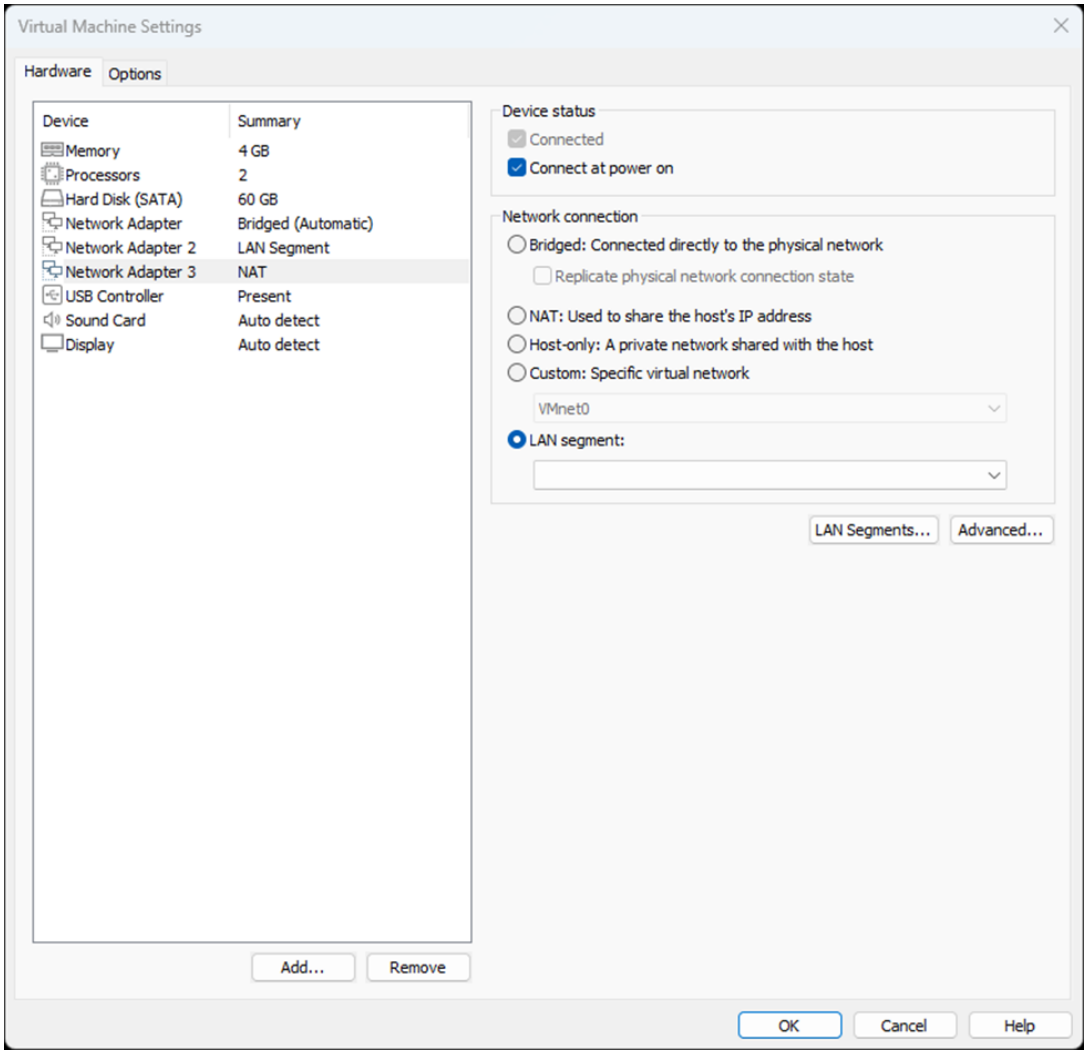
Picture 1) Topology

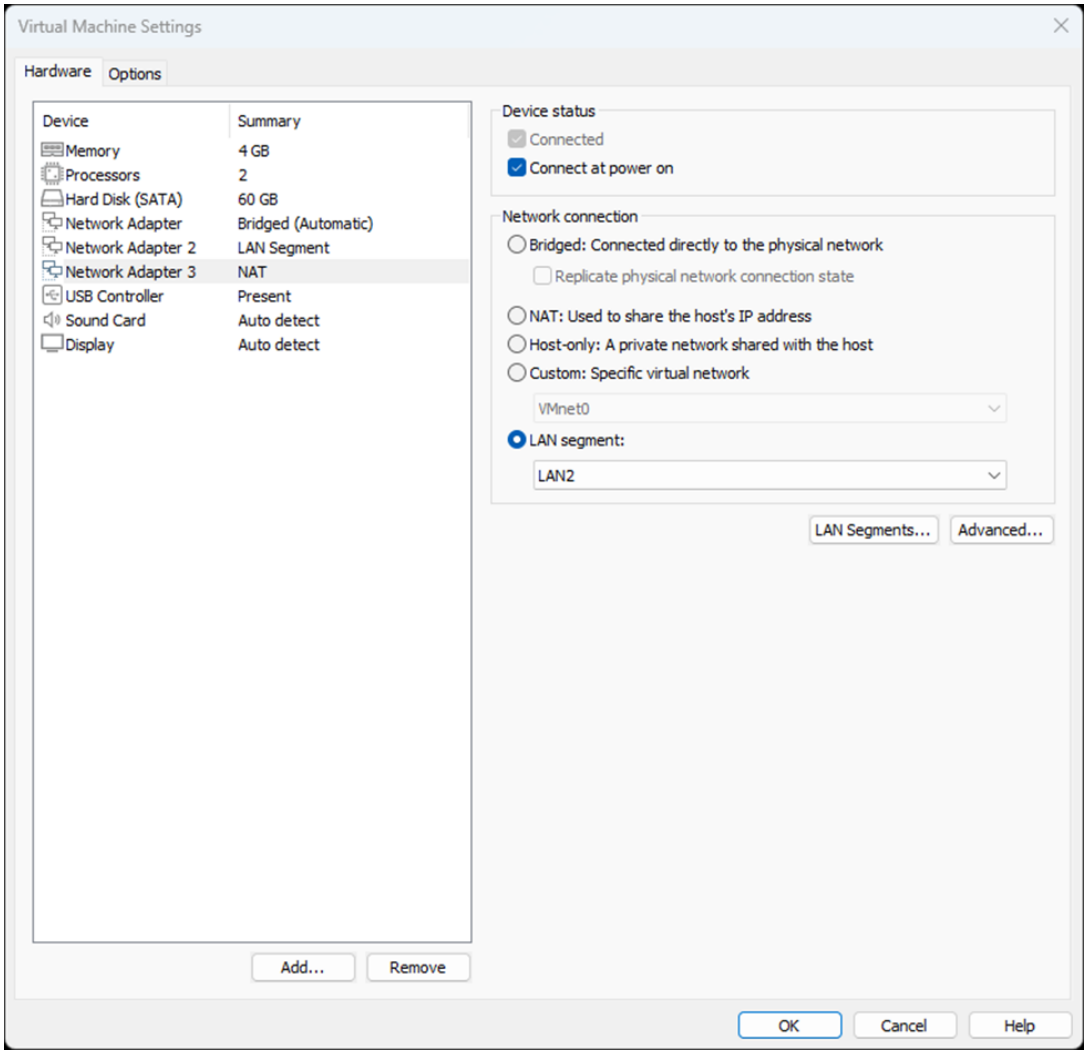
Comprehensive IP Address Table:

For testing, it is added a computer to the previous topology that was used in last practice, this client has different IPs based on Test type. It is added third network card to server for connecting second client because in this project is not used the switch.

Addressing Table

Device	Interface	Connection	IP Address	Subnet Mask	Default Gateway	DNS
Client-09 (UBUNTU)	ens33	LAN2	*	255.255.255.0	*	8.8.8.8
Ubuntu 64-bit	Ens33	LAN1	192.168.50.20	255.255.255.0	192.168.50.10	8.8.8.8
Alma Linux Server	ens192	LAN1	192.168.50.10	255.255.255.0		8.8.8.8
	Ens224	LAN2	*	255.255.255.0	*	8.8.8.8
	ens160	NAT	DHCP			


Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
4 GB
Processors
2
Hard Disk (SATA)
60 GB
Network Adapter
Bridged (Automatic)
Network Adapter 2
LAN Segment
Network Adapter 3
NAT
USB Controller
Present
Sound Card
Auto detect
Display
Auto detect
Add...
Remove
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
LAN Segments...
Advanced...
OK
Cancel
Help




```
[root@server09 ~]# nmcli con add type ethernet ifname ens224 con-name LAN2 ip4 1
92.168.1.2/24
Connection 'LAN2' (97c98b30-717a-48f1-8548-68e1a8693c68) successfully added.
[root@server09 ~]# nmcli con up LAN2
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkMa
nager/ActiveConnection/5)
[root@server09 ~]#
```

IP 192.168.20.10 and the other numbers in the following of project will be used in this machine for doing different tests.

OBJECTIVES

In this 1st part of the project, I will install and configure an Apache web server and create my first website by applying the necessary security rules.

In the following all questions of this project with screen shot of run commands will come.

TASK 1 – CREATING A WEBSITE

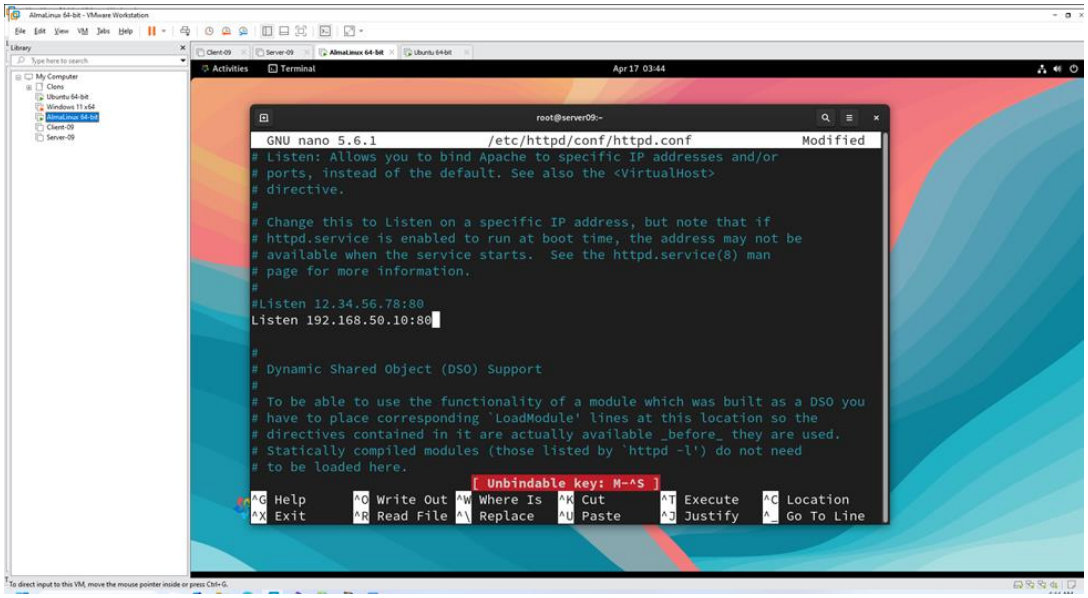
Install and configure the Apache server to read web pages from the directory "/var/www/html_project1".

```
[root@server09 ~]# sudo dnf install httpd -y
```

➢ You must copy the httpd.conf file to httpd.conf.original.

```
root@server09:~
[root@server09 ~]# cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.orig
inal
```

➢ Configure the server to be accessible via the IP address 192.168.50.10.

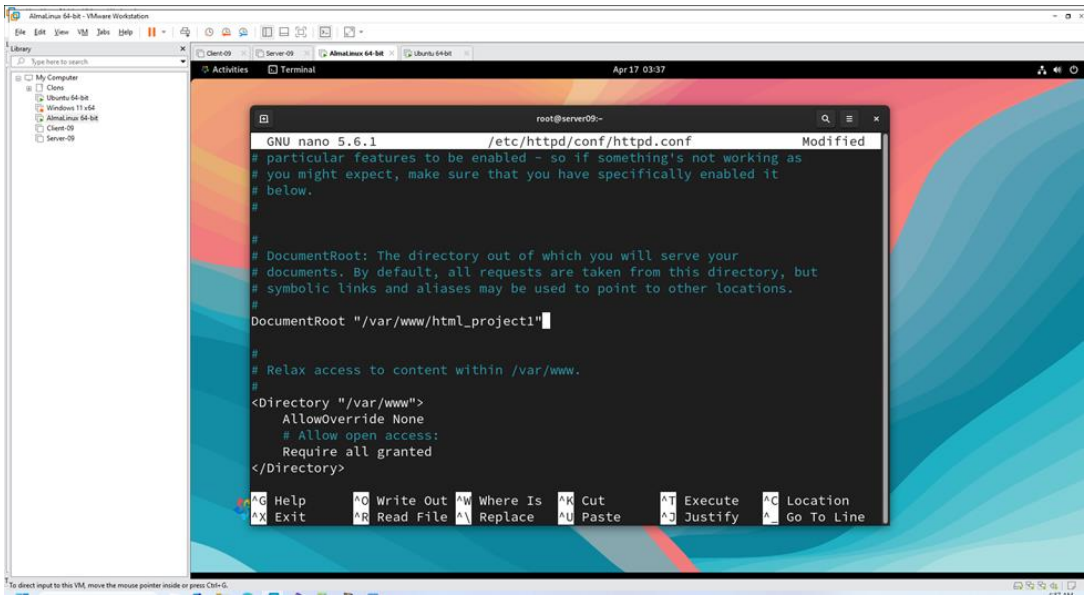


➢ Ensure the httpd service is started and enabled to run at boot.

```
root@server09:~
[root@server09 ~]# systemctl start httpd
[root@server09 ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr
/lib/systemd/system/httpd.service.
[root@server09 ~]#
```

```
[root@server09 ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr
/lib/systemd/system/httpd.service.
[root@server09 ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: di>
     Active: active (running) since Thu 2025-04-17 03:53:15 CDT; 1min 35s ago
       Docs: man:httpd.service(8)
   Main PID: 35755 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes>
      Tasks: 177 (limit: 22829)
     Memory: 28.1M
        CPU: 90ms
     CGroup: /system.slice/httpd.service
             ├─35755 /usr/sbin/httpd -DFOREGROUND
             ├─35756 /usr/sbin/httpd -DFOREGROUND
             ├─35757 /usr/sbin/httpd -DFOREGROUND
             ├─35758 /usr/sbin/httpd -DFOREGROUND
             └─35759 /usr/sbin/httpd -DFOREGROUND
```

```
root@server09:~
[root@server09 ~]# sudo mkdir -p /var/www/html_project1
[root@server09 ~]#
```



2. Create a new homepage named index.html in the/var/www/html_ project1 directory.

```
root@server09:~
[root@server09 ~]# nano /var/www/html_project1/index.html
```

3. The page must include all of the following HTML tags (each used at least once):

<html>, <head>, <title>, <body>, <p>, <hr>, <a href>, <img>,
, <b>, <i>, and <u>.

➢ The page title must be Project Part I - Homepage

➢ You must add a link to each web page of this project inside the index.html page.

➢ Add a hyperlink to each web page created for this project inside the index.html page. Each link should open the corresponding web page of each question, allowing you to test its functionality. See the example provided on the last page of this document.

```
root@server09:~
  GNU nano 5.6.1          /var/www/html_project1/index.html          Modified
<!DOCTYPE html>
<html>
<head>
    <title>Project Part I - Homepage</title>
</head>
<body>
    <h1><b><u>Project Part 1</u></b></h1>

    <p><b>Task 2 - Secure directories:</b></p>
    <a href="secure1.html">secure1 (user01 - accessible)</a><br>
    <a href="secure2a.html">secure2 (user01 and 192.168.50.0/24 - accessible)</
    <a href="secure2b.html">secure2 (user01 and 10.35.16.1/24 - Not accessible)
    <a href="secure3a.html">secure3 (user01 or 192.168.0.0/24 - accessible)</a>
    <a href="secure3b.html">secure3 (user01 or 192.168.50.0/24 - accessible)</a
    <a href="secure4.html">secure4 (user02 - accessible)</a><br>
    <a href="secure5.html">secure5 (user01 with .htaccess - accessible)</a><br>
    <a href="secure6a.html">secure6 (user01 and 192.168.50 with .htaccess - Acc
    <a href="secure6b.html">secure6 (user01 and 10.35.16.1/24 with .htaccess - 
    <a href="secure7a.html">secure7 (user01 or 192.168.50 with .htaccess - Acce
    <a href="secure7b.html">secure7 (user01 or 192.168.50 with .htaccess - Acce

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

HTML Code for this page based on last pages of this document should be like this:

<!DOCTYPE html>

<html>

<head>

<title>Project Part I - Homepage</title>

</head>

```
<body>
   <h1><b><u>Project Part 1</u></b></h1>

   <p><b>Task 2 - Secure directories:</b></p>
   <a href="secure1.html">secure1 (user01 - accessible)</a><br>
   <a href="secure2a.html">secure2 (user01 and 192.168.50.0/24 - accessible)</a><br>
   <a href="secure2b.html">secure2 (user01 and 10.35.16.1/24 - Not accessible)</a><br>
   <a href="secure3a.html">secure3 (user01 or 192.168.0.0/24 - accessible)</a><br>
   <a href="secure3b.html">secure3 (user01 or 192.168.50.0/24 - accessible)</a><br>
   <a href="secure4.html">secure4 (user02 - accessible)</a><br>
   <a href="secure5.html">secure5 (user01 with .htaccess - accessible)</a><br>
   <a href="secure6a.html">secure6 (user01 and 192.168.50 with .htaccess -
Accessible)</a><br>
   <a href="secure6b.html">secure6 (user01 and 10.35.16.1/24 with .htaccess - Not
accessible)</a><br>
   <a href="secure7a.html">secure7 (user01 or 192.168.50 with .htaccess -
Accessible)</a><br>
   <a href="secure7b.html">secure7 (user01 or 192.168.50 with .htaccess -
Accessible)</a><br>

   <hr>

   <p><b>Task 3 - Project 1:</b></p>
   <a href="project1a.html">Project1 (192.168.50.10 - All is accessible)</a><br>
   <a href="project1b.html">Project1 (10.35.16.1 accessible except secret.* and
*.txt)</a><br>
   <a href="project1c.html">Project1 (10.35.17.1 accessible except secret.* and
*.txt)</a><br>
   <a href="project1d.html">Project1 (192.168.100.1 Not accessible)</a><br>

   <hr>
```

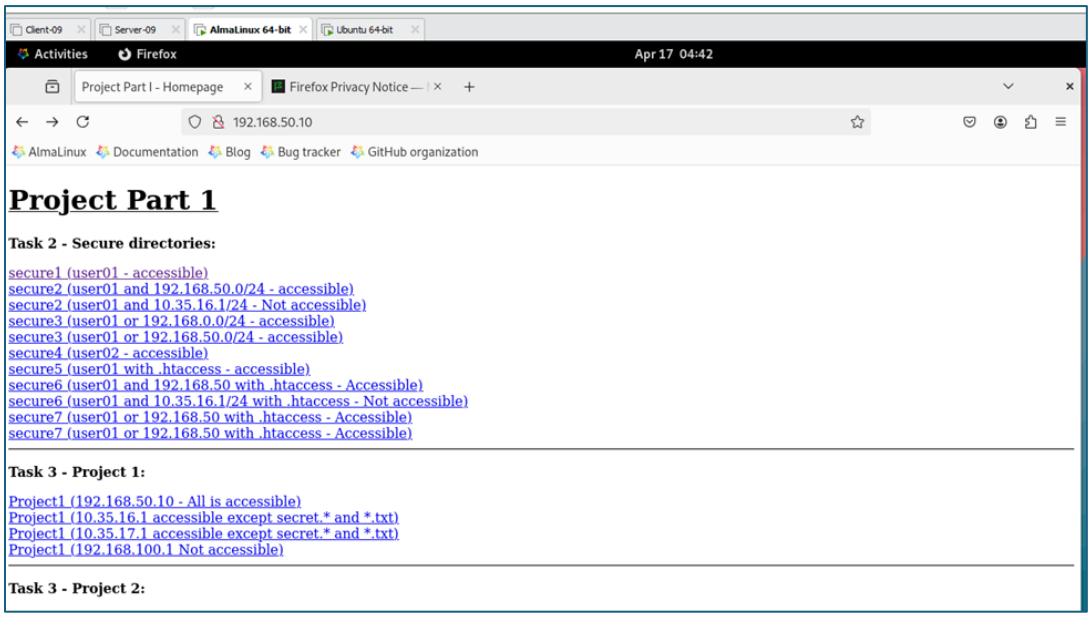
```
<p><b>Task 3 - Project 2:</b></p>
<a href="project2a.html">Project2 (192.168.50.10 - All is accessible)</a><br>
<a href="project2b.html">Project2 (10.35.16.1 Not accessible)</a><br>
<a href="project2c.html">Project2 (10.35.17.1 accessible except *.txt)</a><br>
<a href="project2d.html">Project2 (192.168.100.1 accessible except *.txt)</a><br>

<hr>
<p><b>Task 3 - Project 3:</b></p>
<a href="project3a.html">Project3 (192.168.50.10 - All is accessible)</a><br>
<a href="project3b.html">Project3 (10.35.16.1 Not accessible)</a><br>
<a href="project3c.html">Project3 (10.35.17.1 Not accessible)</a><br>
<a href="project3d.html">Project3 (192.168.100.1 accessible except files *.gif and
*.txt)</a><br>

<hr>

<p><b>Task 3 - Project 4:</b></p>
<a href="project4a.html">Project4 (192.168.50.10 - All is accessible)</a><br>
<a href="project4b.html">Project4 (10.35.16.1 accessible except files test.html)</a><br>
<a href="project4c.html">Project4 (10.35.17.1 Not accessible)</a><br>
<a href="project4d.html">Project4 (192.168.100.1 accessible except files
test.html)</a><br>

<hr>

<p><b>Task 4 - Vendors website:</b></p>
<a href="vendors1.html">Accessible to Vendors (10.50.1.0/24)</a><br>
<a href="vendors2.html">Not accessible to Accountants (10.51.0.0/24)</a><br>
<a href="vendors3.html">Accessible to Administrators (10.52.1.0/24)</a><br>
```

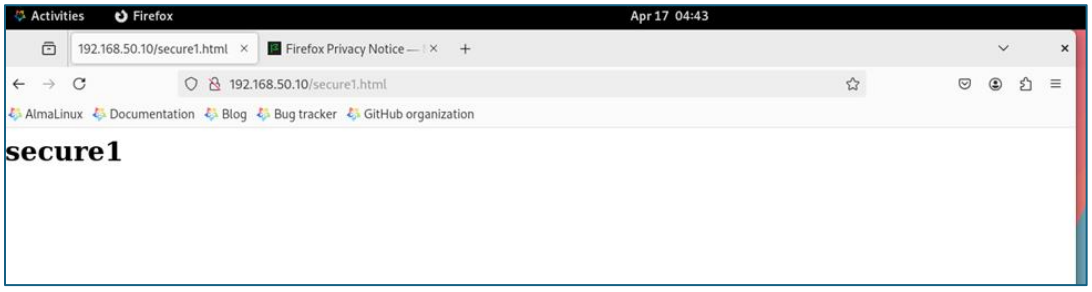
```
   <a href="vendors4.html">Accessible to Programmers (10.53.1.0/24) but not *.gif and
*.jpg files</a><br>


   <hr>


   <p><b>Task 4 - Accountants website:</b></p>

   <a href="accountants1.html">Not accessible to Vendors (10.50.1.0/24) but not *.html
files</a><br>

   <a href="accountants2.html">Accessible to Accountants (10.51.0.0/24)</a><br>

   <a href="accountants3.html">Accessible to Administrators (10.52.1.0/24)</a><br>

   <a href="accountants4.html">Accessible to Programmers (10.53.1.0/24) but not *.gif
and *.jpg files</a><br>


   <hr>


   <p><b>Task 4 - Programmers website:</b></p>

   <a href="programmers1.html">Not accessible to Vendors (10.50.1.0/24)</a><br>

   <a href="programmers2.html">Not accessible to Accountants (10.51.0.0/24)</a><br>

   <a href="programmers3.html">Accessible to Administrators (10.52.1.0/24)</a><br>

   <a href="programmers4.html">Accessible to Programmers (10.53.1.0/24)</a><br>


   <hr>


   <p><b>Task 4 - Administrators website:</b></p>

   <a href="admins1.html">Not accessible to Vendors (10.50.1.0/24)</a><br>

   <a href="admins2.html">Not accessible to Accountants (10.51.0.0/24)</a><br>

   <a href="admins3.html">Accessible to Administrators (10.52.1.0/24)</a><br>

   <a href="admins4.html">Accessible to Programmers (10.53.1.0/24) but not *.gif and
*.jpg files</a><br>


</body>
```

</html>

```
root@server09:~
[root@server09 ~]# nano /var/www/html_project1/index.html
[root@server09 ~]# echo "<html><body><h1>secure1</h1></body></html>" | sudo tee
/var/www/html_project1/secure1.html
<html><body><h1>secure1</h1></body></html>
[root@server09 ~]#
```

Based on the Main menu should be created a page for each link, by a command like this.





TASK 2 – AUTHENTICATION

All files for this section should be created within the /var/www/html_project1 directory.

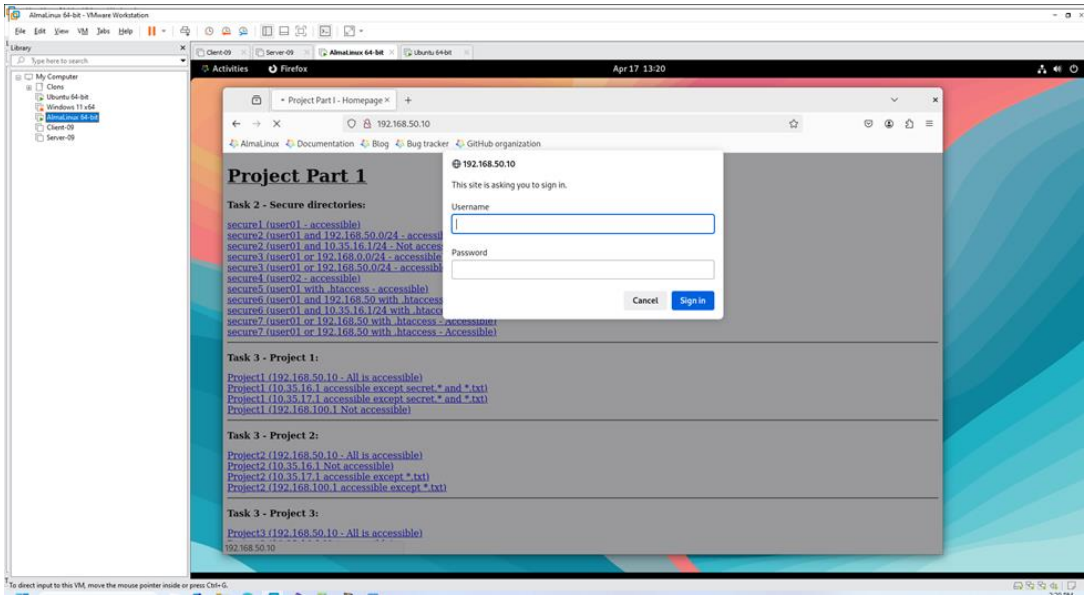
1. Create a secure1 directory and configure Apache using the directive so that only the user user01 with the password “secret” can access it from any subnet. No other users should have access.

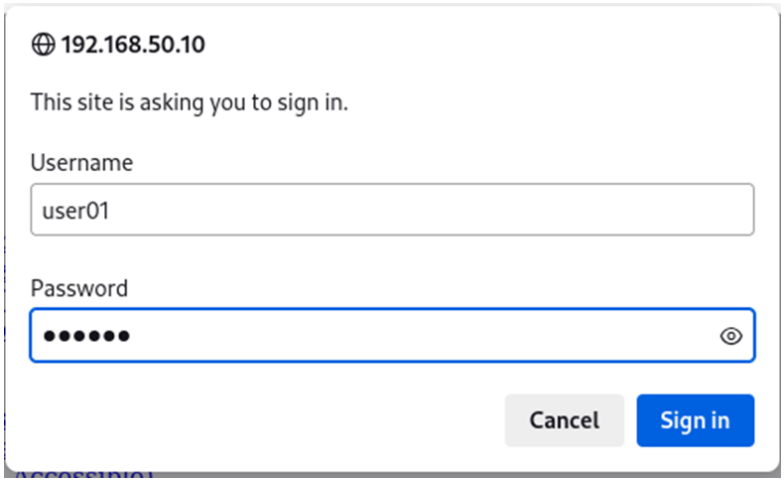
```
[root@server09 ~]# mkdir -p /var/www/html_project1/secure1
[root@server09 ~]# cd /var/www/html1_project1
-bash: cd: /var/www/html1_project1: No such file or directory
[root@server09 ~]# cd /var/www/html_project1
[root@server09 html_project1]# mv secure1.html secure1
[root@server09 html_project1]# htpasswd -c /etc/httpd/.htpasswd user01
New password:
Re-type new password:
Adding password for user user01
[root@server09 html_project1]#
```

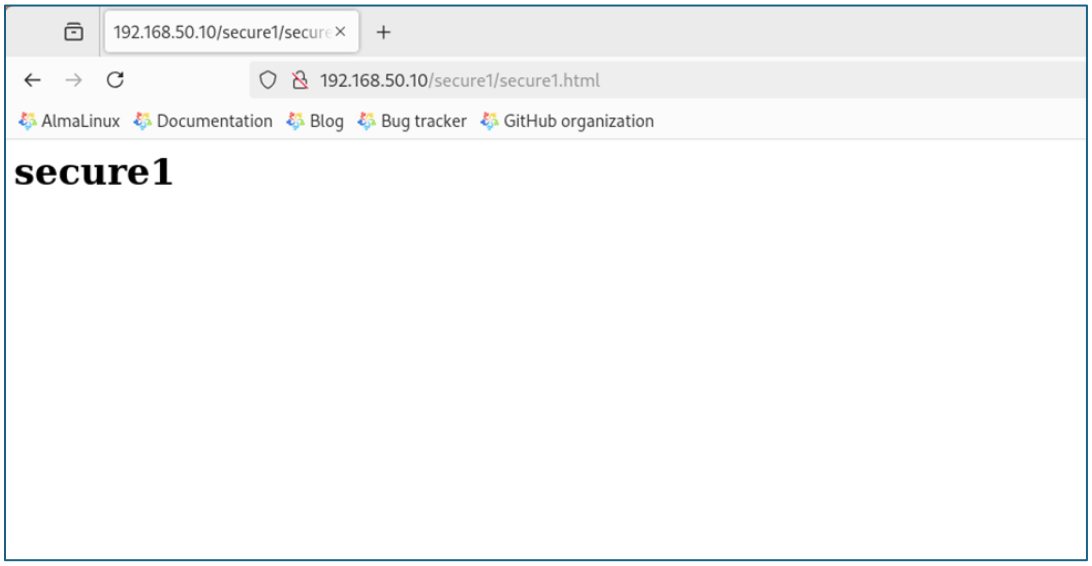
```
[root@server09 html_project1]# sudo nano /etc/httpd/conf.d/secure.conf
```

```
  GNU nano 5.6.1                /etc/httpd/conf.d/secur
<Directory "/var/www/html_project1/secure1">
        AuthType Basic
        AuthName "Restricted Area - Secure1"
        AuthUserFile /etc/httpd/.htpasswd
        Require user user01
</Directory>
```

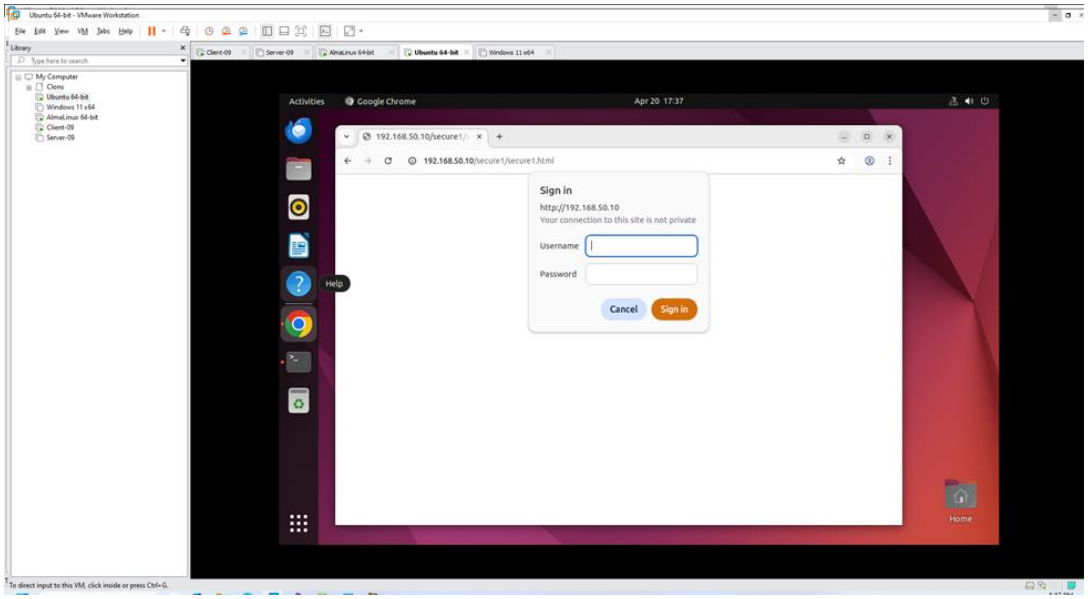
```
[root@server09 html_project1]# chown -R apache:apache /var/www/html_project1
[root@server09 html_project1]# chmod -R 755 /var/www/html_project1
[root@server09 html_project1]# chcon -R -t httpd_sys_content_t /var/www/html_pro
ject1
[root@server09 html_project1]# systemctl restart httpd
[root@server09 html_project1]#
```

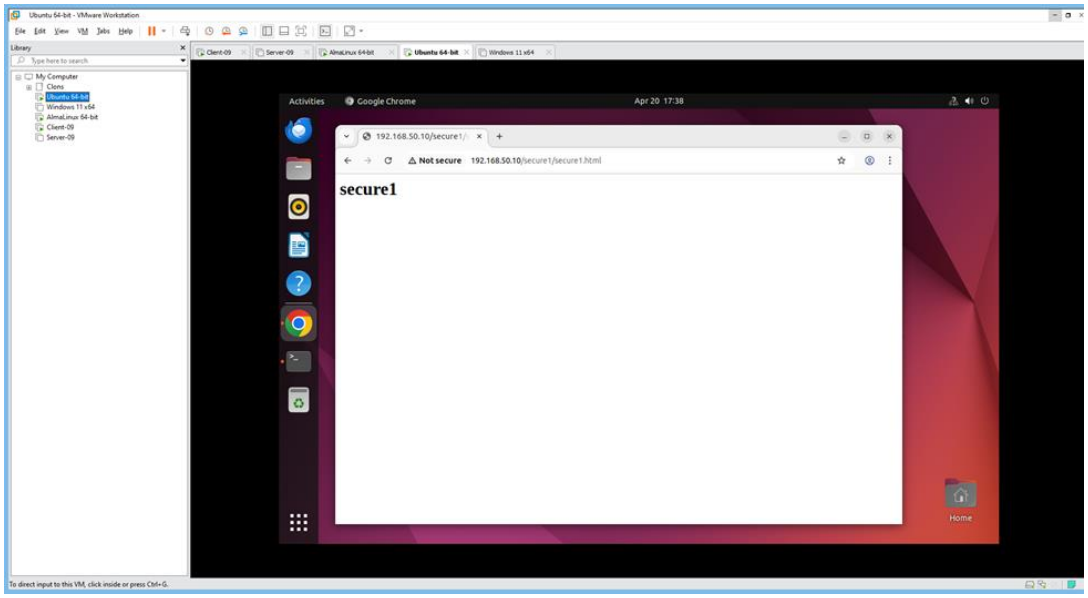

Project Part 1
Task 2 - Secure directories:
secure1 (user01 - accessible)
Task 3 - Project 1:
Project1 (192.168.50.10 - All is accessible)
Project1 (10.35.16.1 accessible except secret.* and *.txt)
Project1 (10.35.17.1 accessible except secret.* and *.txt)
Project1 (192.168.100.1 Not accessible)
Task 3 - Project 2:
Project2 (192.168.50.10 - All is accessible)
Project2 (10.35.16.1 Not accessible)
Project2 (10.35.17.1 accessible except *.txt)
Project2 (192.168.100.1 accessible except *.txt)
Task 3 - Project 3:
Project3 (192.168.50.10 - All is accessible)
192.168.50.10
This site is asking you to sign in.
Username
Password
Cancel
Sign in


192.168.50.10
This site is asking you to sign in.
Username
user01
Password
Cancel
Sign in

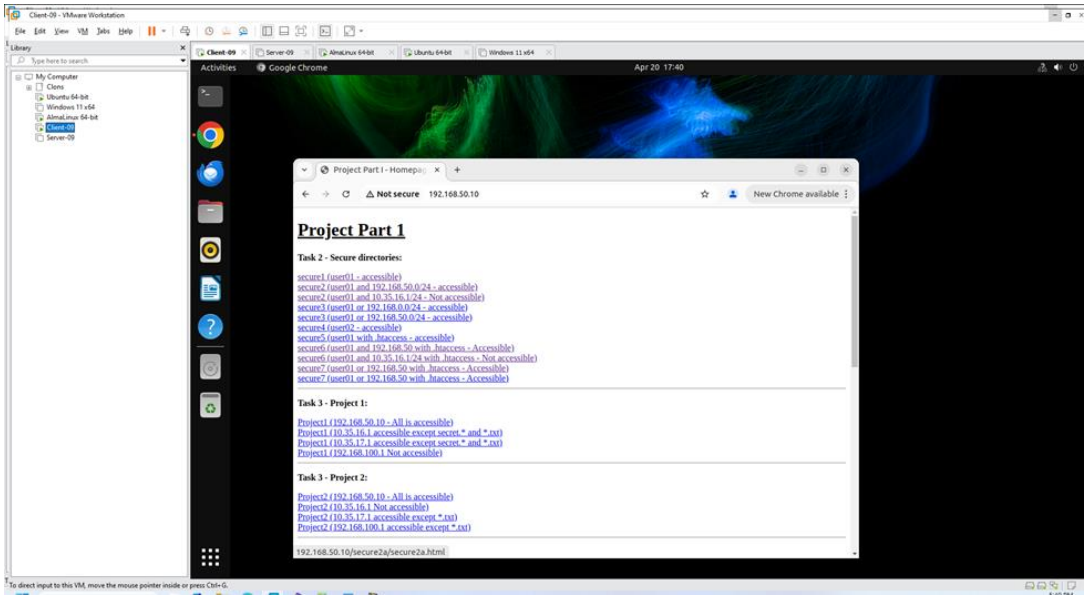

192.168.50.10/secure1/secure
192.168.50.10/secure1/secure1.html
AlmaLinux
Documentation
Blog
Bug tracker
GitHub organization
secure1

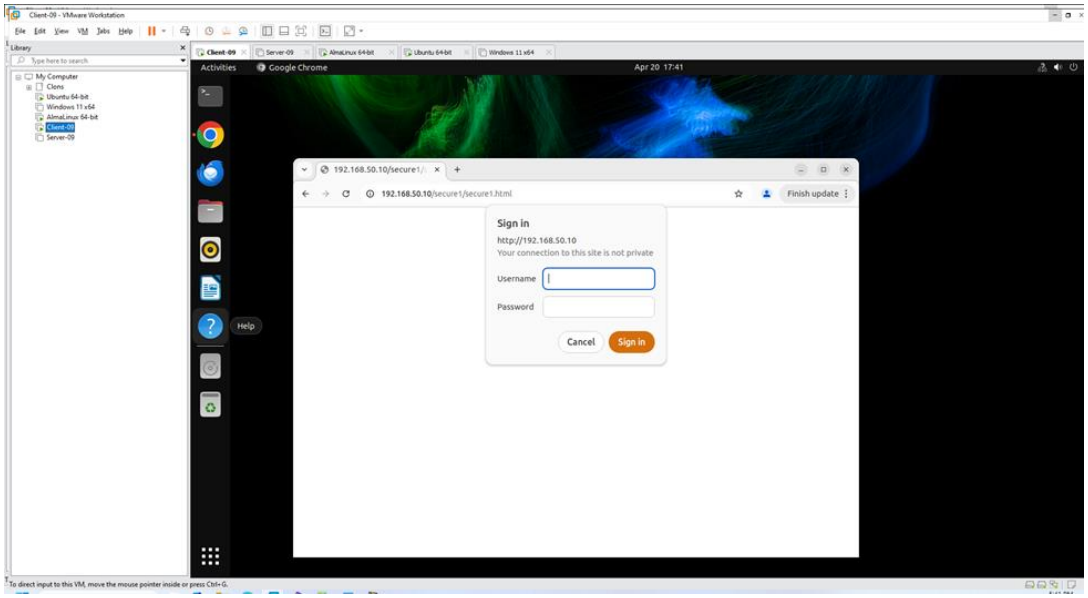
Test from Ubuntu 64-bit(192.168.50.20/24)

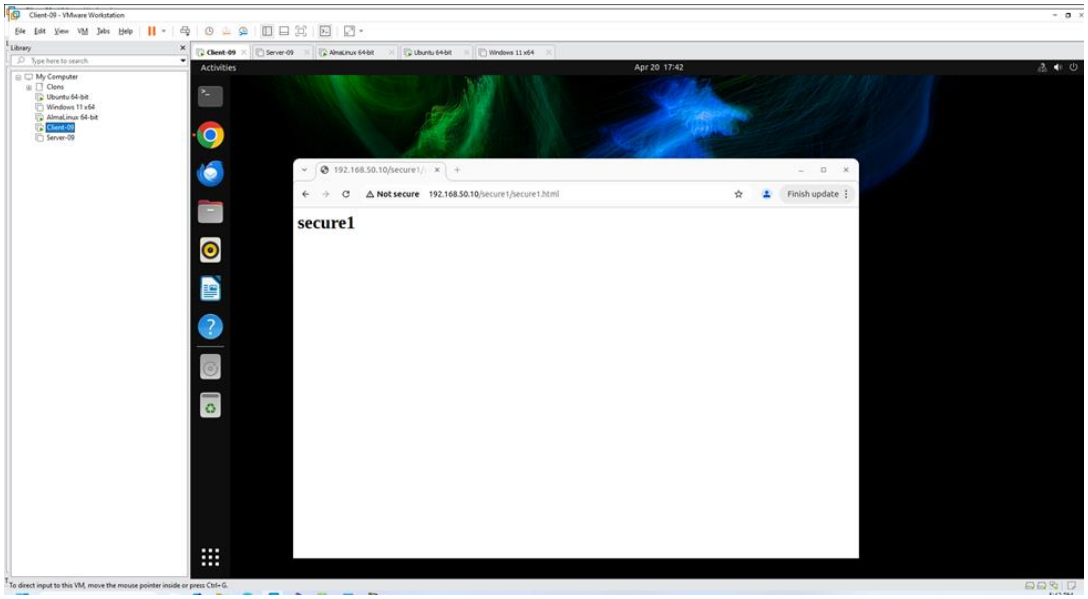




Test from Client-09 (192.168.20.20)







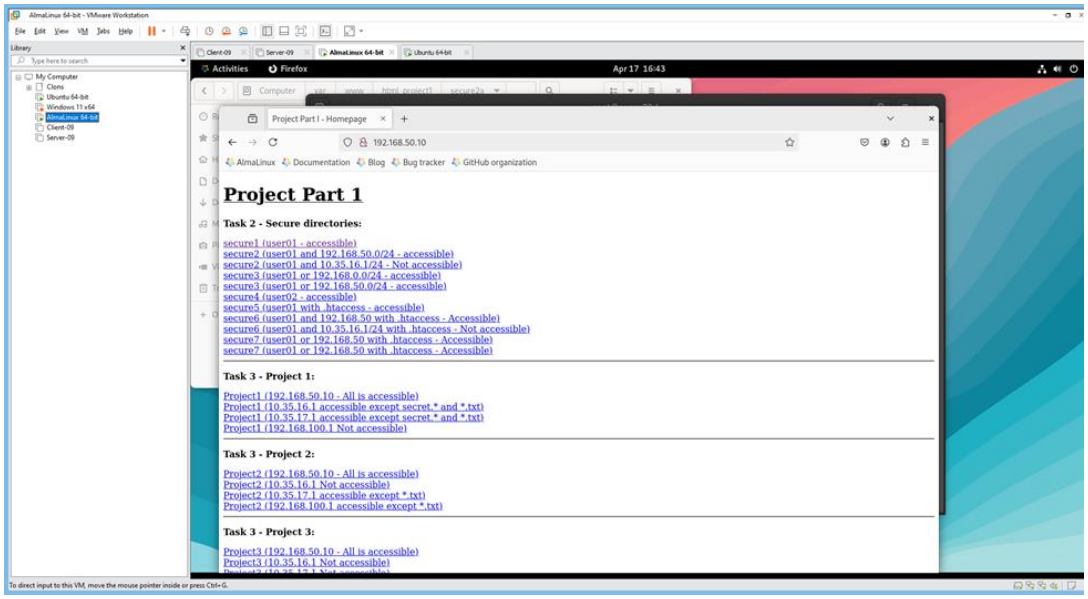
2. Create a secure2 directory and configure Apache so that only user01 can access it when connecting from the subnet 192.168.50.0/24.

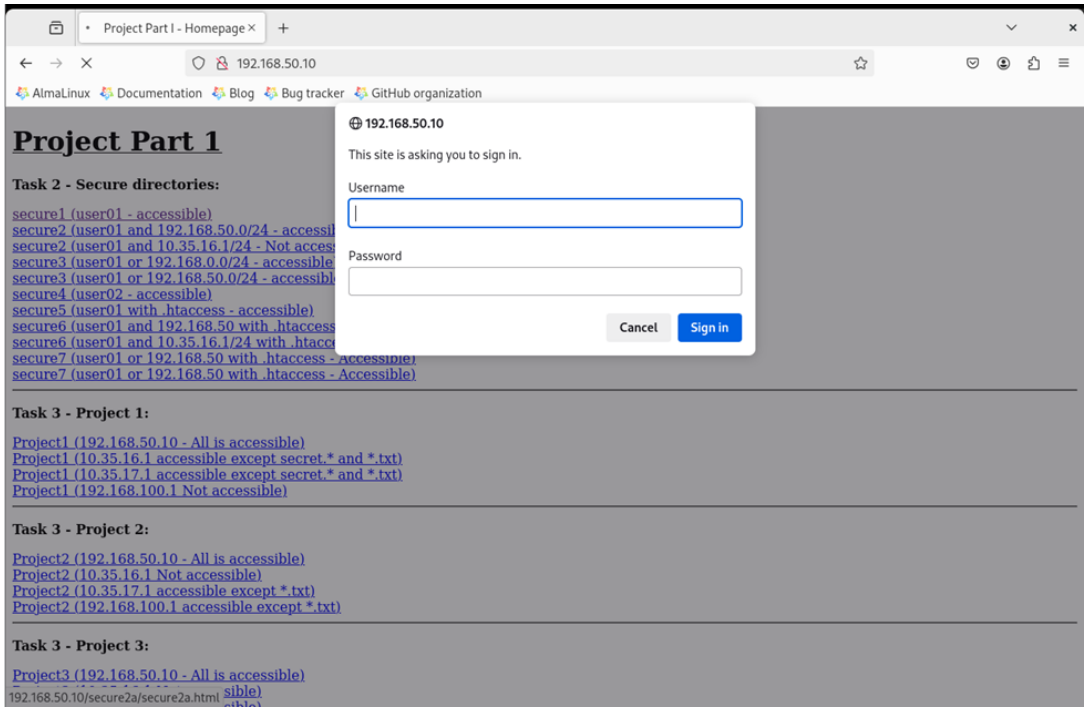
there were 2 parts for secure2 folder so I created secure2a and secure2b in previous steps.

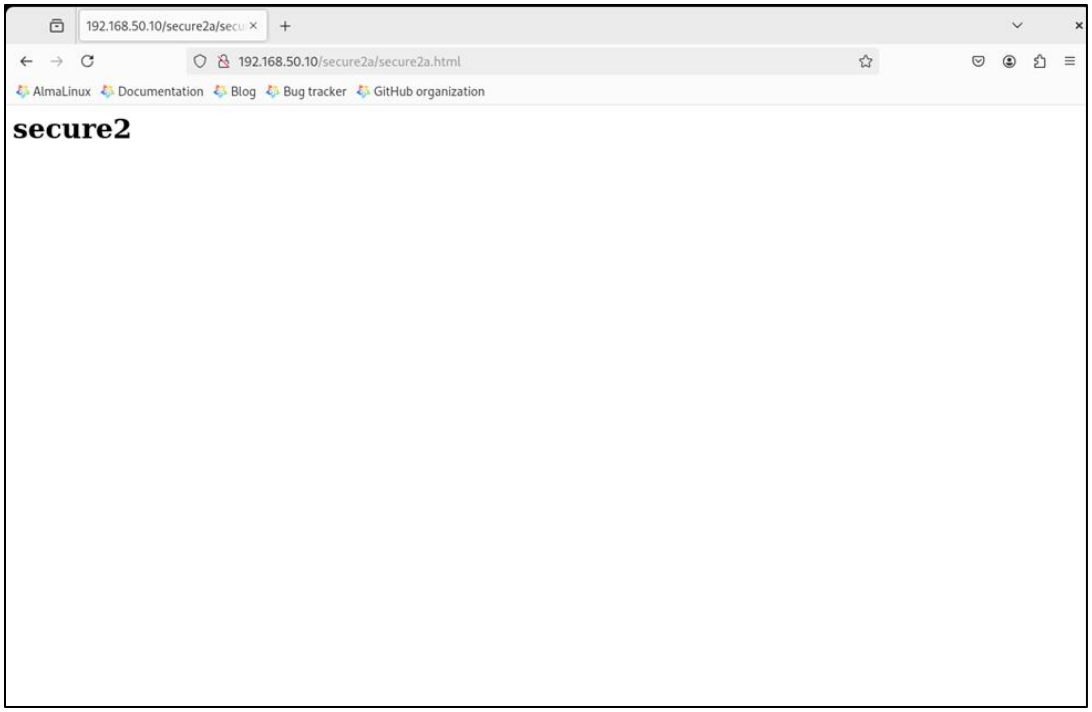
```
[root@server09 /]# mkdir /var/www/html_project1/secure2a
```

```
  GNU nano 5.6.1                /etc/httpd/conf.d/secure.conf
<Directory "/var/www/html_project1/secure1">
        AuthType Basic
        AuthName "Restricted Area - Secure1"
        AuthUserFile /etc/httpd/.htpasswd
        Require user user01
</Directory>
<Directory "/var/www/html_project1/secure2a">
        AuthType Basic
        AuthName "Restricted Area - Secure2a"
        AuthUserFile /etc/httpd/.htpasswd
        <RequireAll>
                Require user user01
                Require ip 192.168.50.0/24
        </RequireAll>
</Directory>
```

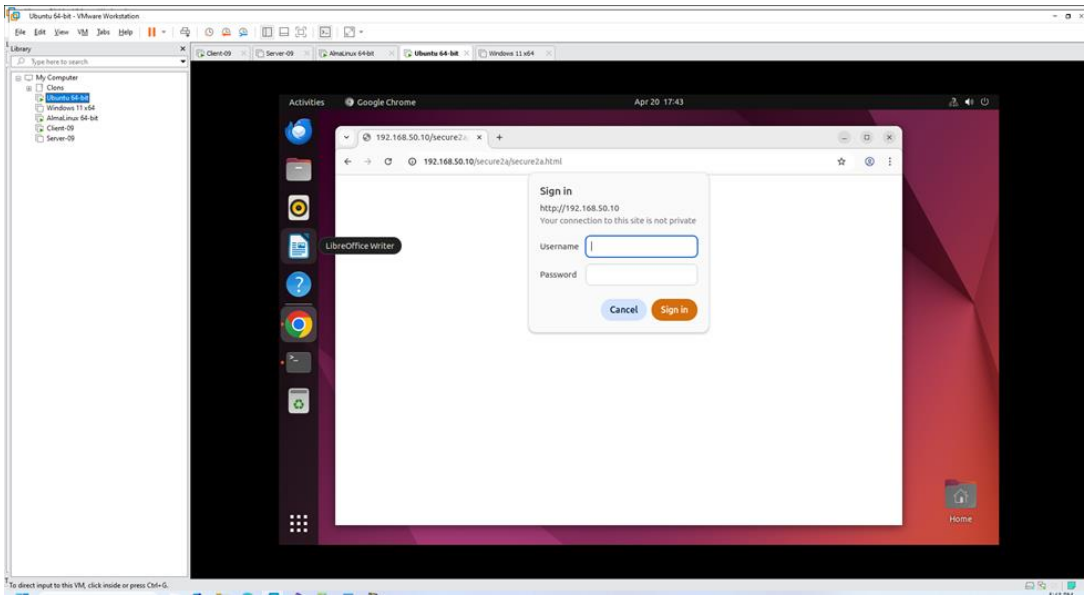
```
root@server09:/
[root@server09 /]# nano /etc/httpd/conf.d/secure.conf
[root@server09 /]# nano /etc/httpd/conf.d/secure.conf
[root@server09 /]# systemctl restart httpd
```


Project Part I - Homepage
192.168.50.10
AlmaLinux Documentation Blog Bug tracker GitHub organization
Project Part 1
Task 2 - Secure directories:
secure1 (user01 - accessible)
secure2 (user01 and 192.168.50.0/24 - accessible)
secure2 (user01 and 10.35.16.1/24 - Not accessible)
secure3 (user01 or 192.168.0.0/24 - accessible)
secure3 (user01 or 192.168.50.0/24 - accessible)
secure4 (user02 - accessible)
secure5 (user01 with .htaccess - accessible)
secure6 (user01 and 192.168.50 with .htaccess - Accessible)
secure6 (user01 and 10.35.16.1/24 with .htaccess - Not accessible)
secure7 (user01 or 192.168.50 with .htaccess - Accessible)
secure7 (user01 or 192.168.50 with .htaccess - Accessible)
Task 3 - Project 1:
Project1 (192.168.50.10 - All is accessible)
Project1 (10.35.16.1 accessible except secret.* and *.txt)
Project1 (10.35.17.1 accessible except secret.* and *.txt)
Project1 (192.168.100.1 Not accessible)
Task 3 - Project 2:
Project2 (192.168.50.10 - All is accessible)
Project2 (10.35.16.1 Not accessible)
Project2 (10.35.17.1 accessible except *.txt)
Project2 (192.168.100.1 accessible except *.txt)
Task 3 - Project 3:
Project3 (192.168.50.10 - All is accessible)
Project3 (10.35.16.1 Not accessible)

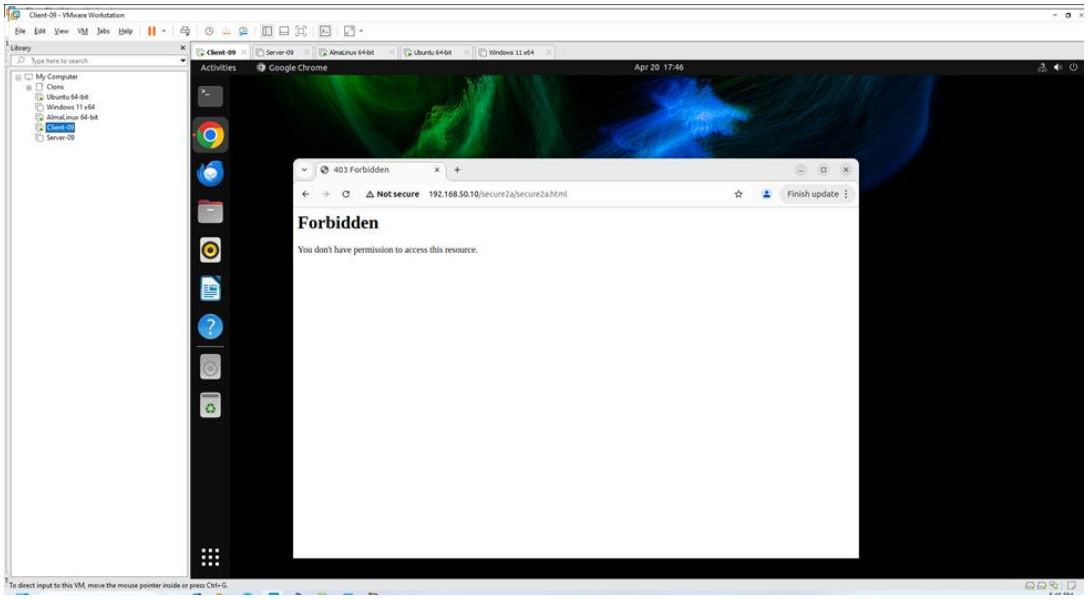

Project Part I - Homepage
192.168.50.10
AlmaLinux Documentation Blog Bug tracker GitHub organization
192.168.50.10
This site is asking you to sign in.
Username
Password
Cancel
Sign in
Project Part 1
Task 2 - Secure directories:
secure1 (user01 - accessible)
secure2 (user01 and 192.168.50.0/24 - accessible)
secure2 (user01 and 10.35.16.1/24 - Not accessible)
secure3 (user01 or 192.168.0.0/24 - accessible)
secure3 (user01 or 192.168.50.0/24 - accessible)
secure4 (user02 - accessible)
secure5 (user01 with .htaccess - accessible)
secure6 (user01 and 192.168.50 with .htaccess - Accessible)
secure6 (user01 and 10.35.16.1/24 with .htaccess - Not accessible)
secure7 (user01 or 192.168.50 with .htaccess - Accessible)
secure7 (user01 or 192.168.50 with .htaccess - Accessible)
Task 3 - Project 1:
Project1 (192.168.50.10 - All is accessible)
Project1 (10.35.16.1 accessible except secret.* and *.txt)
Project1 (10.35.17.1 accessible except secret.* and *.txt)
Project1 (192.168.100.1 Not accessible)
Task 3 - Project 2:
Project2 (192.168.50.10 - All is accessible)
Project2 (10.35.16.1 Not accessible)
Project2 (10.35.17.1 accessible except *.txt)
Project2 (192.168.100.1 accessible except *.txt)
Task 3 - Project 3:
Project3 (192.168.50.10 - All is accessible)
192.168.50.10/secure2a/secure2a.html



test from Ubuntu 64-bit(192.168.50.20)



Test from Client-09 (192.168.20.20)



3. Create a secure3 directory and configure Apache so that either user01 or any user from the 192.168.50.0/24 subnet can access it.

```
[root@server09 ~]# mkdir -p /var/www/html_project1/secure3
[root@server09 ~]# mv /var/www/html_project1/secure2b /var/www/html_project1/sec
ure3
mv: cannot stat '/var/www/html_project1/secure2b': No such file or directory
[root@server09 ~]# mv /var/www/html_project1/secure2b.html /var/www/html_project
1/secure3
[root@server09 ~]#
```

```
  GNU nano 5.6.1                /etc/httpd/conf.d/secure.conf

<Directory "/var/www/html_project1/secure2a">
        AuthType Basic
        AuthName "Restricted"
        AuthUserFile /etc/httpd/.htpasswd
        <RequireAll>
           Require user user01
           Require ip 192.168.50.0/24
        </RequireAll>
</Directory>
<Directory "/var/www/html_project1/secure3">
        AuthType Basic
        AuthName "Restricted..."
        AuthUserFile /etc/httpd/.htpasswd
        <RequireAny>
                Require user user01
                Require ip 192.168.50.0/24
        </RequireAny>
</Directory>
```

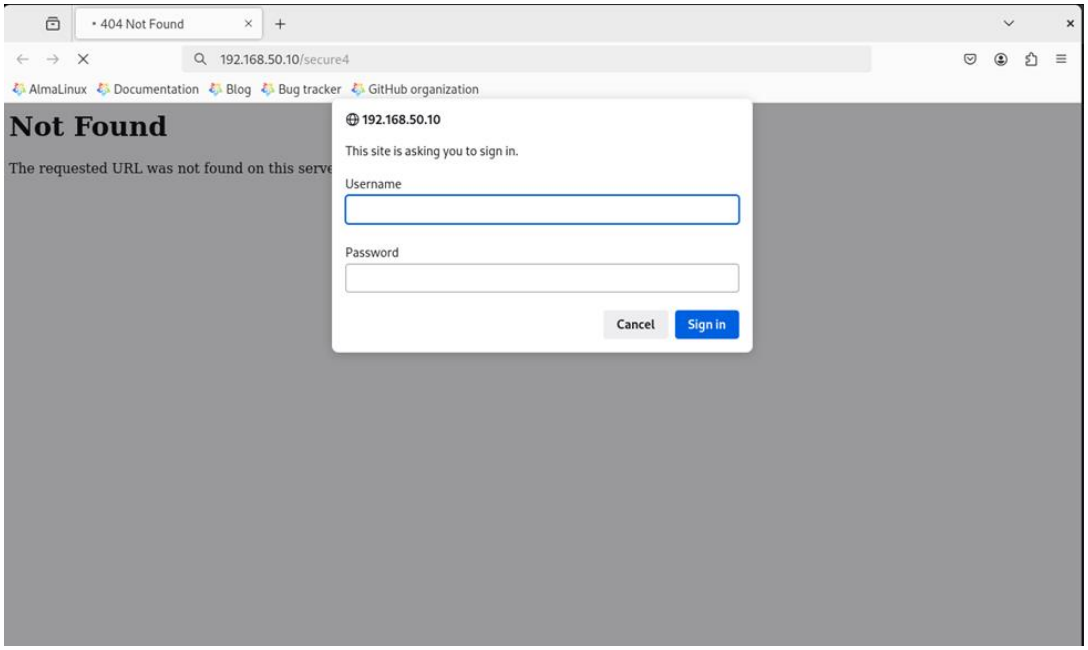
```
root@server09:~
<!DOCTYPE html>
<html>
<head>
    <title>Project Part I - Homepage</title>
</head>
<body>
    <h1><b><u>Project Part 1</u></b></h1>

    <p><b>Task 2 - Secure directories:</b></p>
    <a href="/secure1/secure1.html">secure1 (user01 - accessible)</a><br>
    <a href="/secure2a/secure2a.html">secure2 (user01 and 192.168.50.0/24 -
ssible)</a><br>
    <a href="/secure3/secure2b.html">secure2 (user01 and 10.35.16.1/24 - No
essible)</a><br>
    <a href="secure3a.html">secure3 (user01 or 192.168.0.0/24 - accessible)
br>
    <a href="secure3b.html">secure3 (user01 or 192.168.50.0/24 - accessible
<br>
    <a href="secure4.html">secure4 (user02 - accessible)</a><br>
    <a href="secure5.html">secure5 (user01 with .htaccess - accessible)</a>
    <a href="secure6a.html">secure6 (user01 and 192.168.50 with .htaccess -
ssible)</a><br>
@@
```

4. Create a secure4 directory and configure it similarly to secure1 but grant access only to the user user02 (password “secret”).

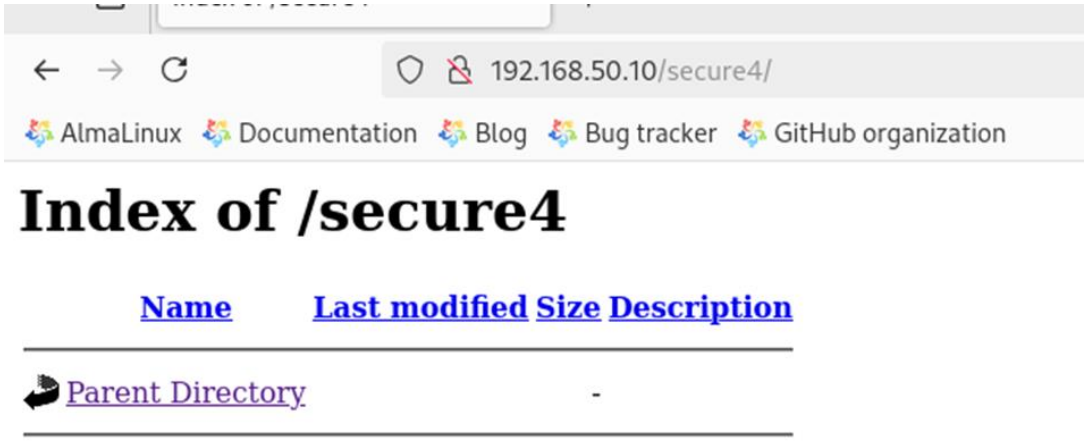
```
[root@server09 ~]# sudo mkdir -p /var/www/html_project1/secure4
[root@server09 ~]# htpasswd /etc/httpd/.htpasswd user02
New password:
Re-type new password:
Adding password for user user02
[root@server09 ~]# nano /etc/httpd/conf.d/secure.conf
```

```
<Directory "/var/www/html_project1/secure4">
        AuthType Basic
        AuthName "Restricted"
        AuthUserFile /etc/httpd/.htpasswd
        Require user user02
</Directory>
```

```
[root@server09 ~]# systemctl restart httpd
[root@server09 ~]#
```



User02 +secret



5. Create a secure5 directory and place an .htaccess file inside it to restrict access to only user01 from any subnet.

```
[root@server09 ~]# sudo mkdir -p /var/www/html_project1/secure5
[root@server09 ~]#
```

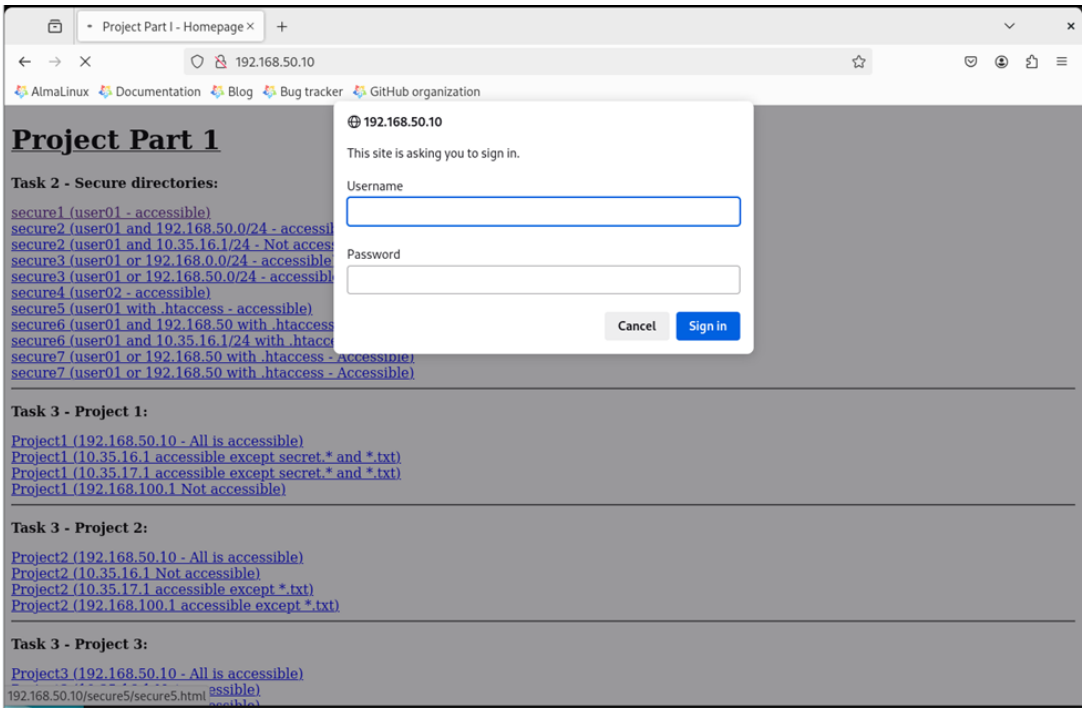
```
<Directory "/var/www/html_project1/secure5">
        AllowOverride All
</Directory>
```

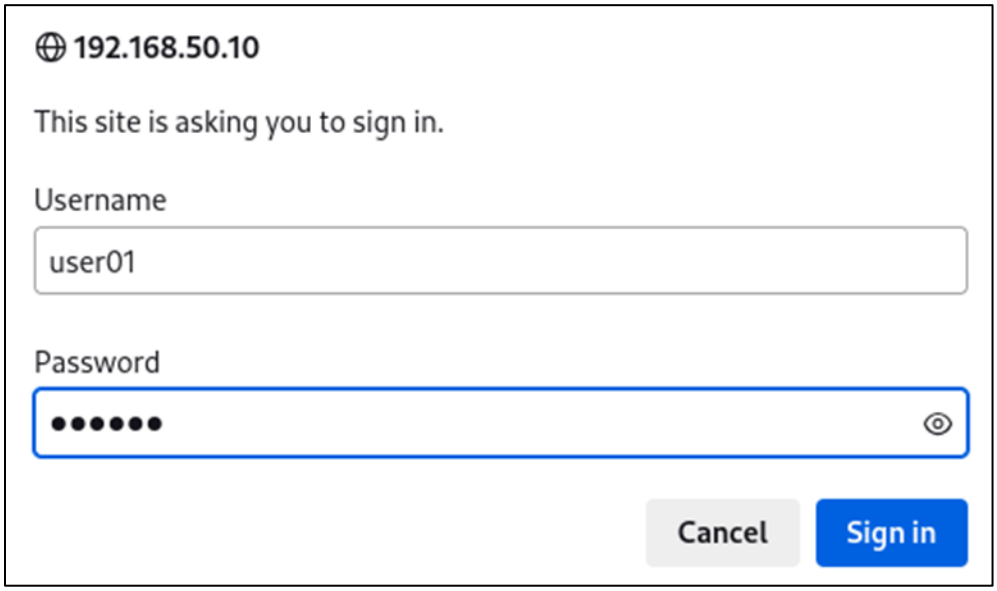
```
[root@server09 ~]# nano /var/www/html_project1/secure5/.htaccess
```

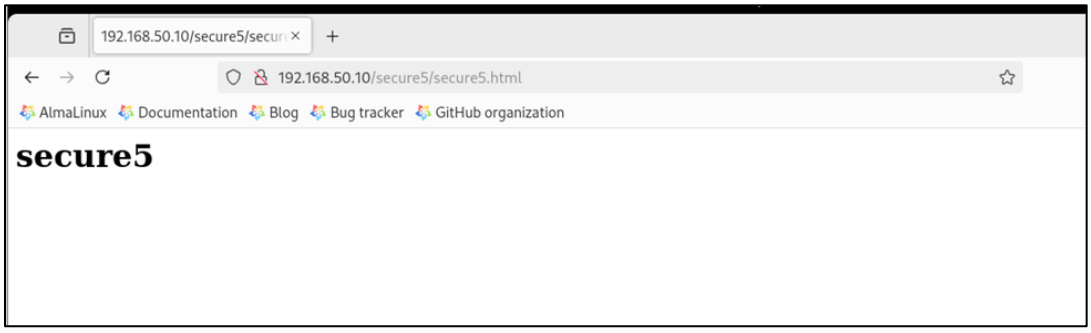
```
  GNU nano 5.6.1       /var/www/html_project1/secure5/.htaccess       Modified
AuthType Basic
AuthName "Secure5"
AuthUserFile /etc/httpd/.htpasswd
Require user user01
```

```
[root@server09 ~]# sudo mkdir -p /var/www/html_project1/secure5
[root@server09 ~]# nano /etc/httpd/conf.d/secure.conf
[root@server09 ~]# systemctl restart httpd
[root@server09 ~]# nano /var/www/html_project1/secure5/.htaccess
[root@server09 ~]# htpasswd -c /etc/httpd/.htpasswd user01
New password:
Re-type new password:
Adding password for user user01
[root@server09 ~]# mv /var/www/html_project1/secure5.html /var/www/html_project1
/secure5
[root@server09 ~]# nano /var/www/html_project1/index.html
```

```
  GNU nano 5.6.1          /var/www/html_project1/index.html          Modified
<!DOCTYPE html>
<html>
<head>
    <title>Project Part I - Homepage</title>
</head>
<body>
    <h1><b><u>Project Part 1</u></b></h1>

    <p><b>Task 2 - Secure directories:</b></p>
    <a href="/secure1/secure1.html">secure1 (user01 - accessible)</a><br>
    <a href="/secure2a/secure2a.html">secure2 (user01 and 192.168.50.0/24 - ac
    <a href="/secure3/secure2b.html">secure2 (user01 and 10.35.16.1/24 - Not a
    <a href="secure3a.html">secure3 (user01 or 192.168.0.0/24 - accessible)</a
    <a href="secure3b.html">secure3 (user01 or 192.168.50.0/24 - accessible)</
    <a href="secure4.html">secure4 (user02 - accessible)</a><br>
    <a href="/secure5/secure5.html">secure5 (user01 with .htaccess - accessibl
    <a href="secure6a.html">secure6 (user01 and 192.168.50 with .htaccess - Ac
    <a href="secure6b.html">secure6 (user01 and 10.35.16.1/24 with .htaccess -
    <a href="secure7a.html">secure7 (user01 or 192.168.50 with .htaccess - Acc
    <a href="secure7b.html">secure7 (user01 or 192.168.50 with .htaccess - Acc
```


Project Part I - Homepage
192.168.50.10
AlmaLinux
Documentation
Blog
Bug tracker
GitHub organization
Project Part 1
Task 2 - Secure directories:
secure1 (user01 - accessible)
secure2 (user01 and 192.168.50.0/24 - accessi
secure2 (user01 and 10.35.16.1/24 - Not acces
secure3 (user01 or 192.168.0.0/24 - accessible
secure3 (user01 or 192.168.50.0/24 - accessibl
secure4 (user02 - accessible)
secure5 (user01 with .htaccess - accessible)
secure6 (user01 and 192.168.50 with .htaccess
secure6 (user01 and 10.35.16.1/24 with .htacc
secure7 (user01 or 192.168.50 with .htaccess - Accessible)
secure7 (user01 or 192.168.50 with .htaccess - Accessible)
192.168.50.10
This site is asking you to sign in.
Username
Password
Cancel
Sign in
Task 3 - Project 1:
Project1 (192.168.50.10 - All is accessible)
Project1 (10.35.16.1 accessible except secret.* and *.txt)
Project1 (10.35.17.1 accessible except secret.* and *.txt)
Project1 (192.168.100.1 Not accessible)
Task 3 - Project 2:
Project2 (192.168.50.10 - All is accessible)
Project2 (10.35.16.1 Not accessible)
Project2 (10.35.17.1 accessible except *.txt)
Project2 (192.168.100.1 accessible except *.txt)
Task 3 - Project 3:
Project3 (192.168.50.10 - All is accessible)
192.168.50.10/secure5/secure5.html


192.168.50.10
This site is asking you to sign in.
Username
user01
Password
Cancel
Sign in


192.168.50.10/secure5/secur
192.168.50.10/secure5/secure5.html
AlmaLinux
Documentation
Blog
Bug tracker
GitHub organization
secure5

6. Create a secure6 directory and use an .htaccess file to restrict access to user01, but only when connecting from the 192.168.50.0/24 subnet.

```
[root@server09 ~]# mkdir -p /var/www/html_project1/secure6
[root@server09 ~]#
```

```
[root@server09 ~]# nano /etc/httpd/conf.d/secure.conf
```

```
<Directory "/var/www/html_project1/secure6">
        AllowOverride All
</Directory>
```

```
  GNU nano 5.6.1                          .htaccess
AuthType Basic
AuthName "Secure6 Area"
AuthUserFile /etc/httpd/.htpasswd
Require user user01

Order deny ,allow
Deny from all
Allow from 192.168.50.0/24
```

```
[root@server09 html_project1]# ls secure6*
secure6a.html  secure6b.html

secure6:
[root@server09 html_project1]# mv secure6a.html secure6
[root@server09 html_project1]#
```

```
[root@server09 html_project1]# systemctl restart httpd
[root@server09 html_project1]#
```

7. Create a secure7 directory and use an .htaccess file to allow access to either the user01 or any user from the 192.168.50.0/24 subnet.

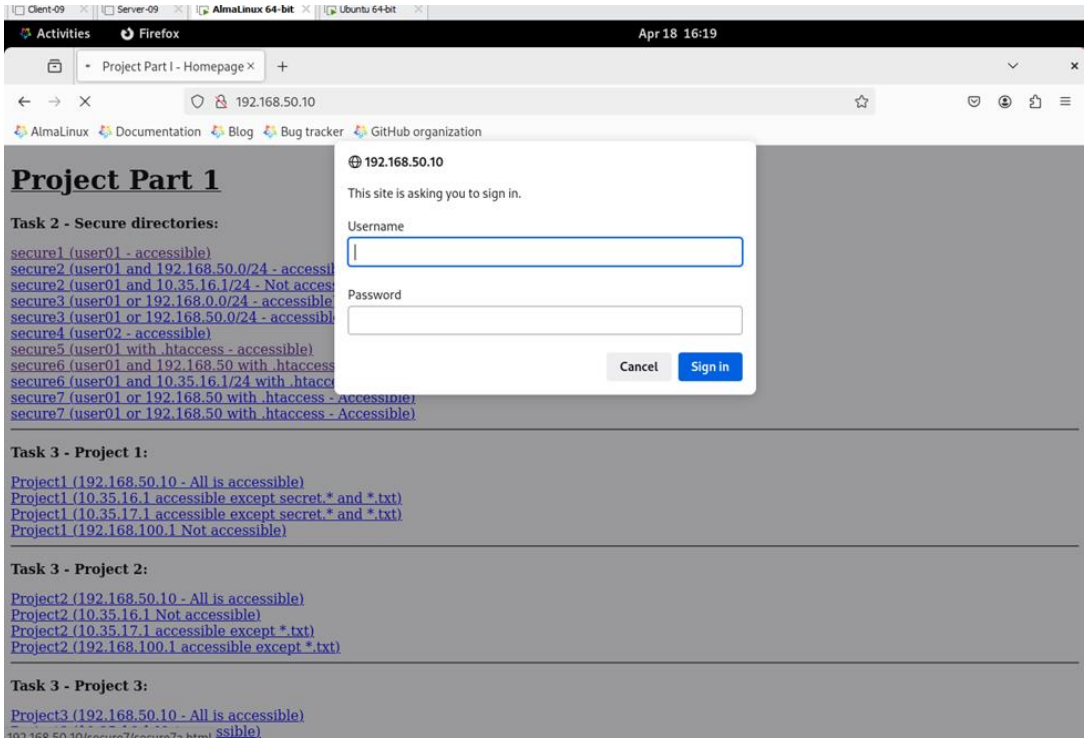
```
[root@server09 ~]# cd /var/
[root@server09 var]# cd www
[root@server09 www]# cd html_project1
[root@server09 html_project1]# ls
accountants1.html  programmers2.html  project2d.html  secure2a       secure7a.html
accountants2.html  programmers3.html  project3a.html  secure2a.html  secure7b.html
accountants3.html  programmers4.html  project3b.html  secure3        vendors1.html
accountants4.html  project1a.html     project3c.html  secure3a.html  vendors2.html
admin1.html        project1b.html     project3d.html  secure3b.html  vendors3.html
admin2.html        project1c.html     project4a.html  secure4        vendors4.html
admin3.html        project1d.html     project4b.html  secure4.html
admin4.html        project2a.html     project4c.html  secure5
index.html         project2b.html     project4d.html  secure6
programmers1.html  project2c.html     secure1         secure6b.html
```

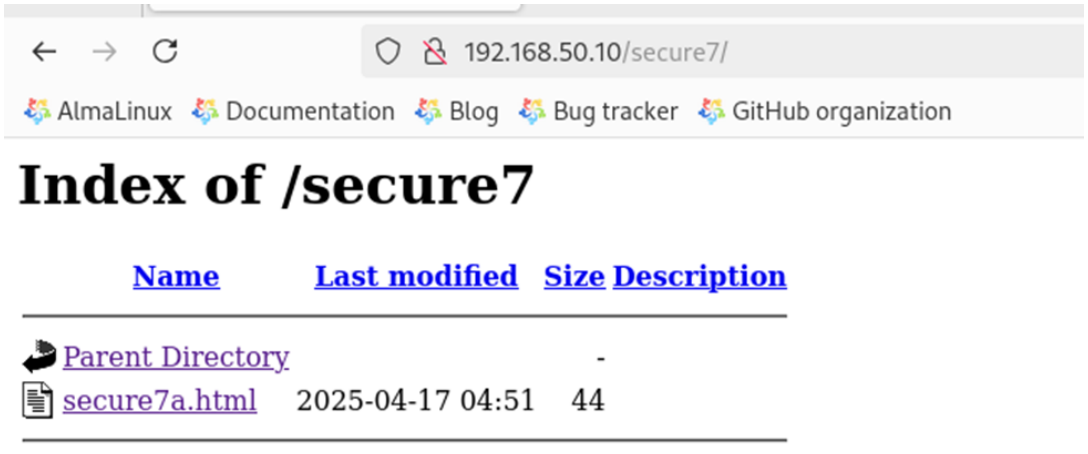
```
[root@server09 html_project1]# mkdir secure7
[root@server09 html_project1]# mv secure6b.html secure7
[root@server09 html_project1]# ls
accountants1.html  programmers2.html  project2d.html  secure2a       secure7a.html
accountants2.html  programmers3.html  project3a.html  secure2a.html  secure7b.html
accountants3.html  programmers4.html  project3b.html  secure3        vendors1.html
accountants4.html  project1a.html     project3c.html  secure3a.html  vendors2.html
admin1.html        project1b.html     project3d.html  secure3b.html  vendors3.html
admin2.html        project1c.html     project4a.html  secure4        vendors4.html
admin3.html        project1d.html     project4b.html  secure4.html
admin4.html        project2a.html     project4c.html  secure5
index.html         project2b.html     project4d.html  secure6
programmers1.html  project2c.html     secure1         secure7
[root@server09 html_project1]#
```

```
<Directory "/var/www/html_project1/secure7">
        AllowOverride All
</Directory>
```

```
AuthType Basic
AuthName "Secure6 Area"
AuthUserFile /etc/httpd/.htpasswd
Require user user01

Order Deny,Allow
Deny from all
Allow from 192.168.50.0/24
Satisfy all
~
```

```
[root@server09 secure7]# systemctl restart httpd
```


Client-09
Server-09
AlmaLinux 64-bit
Ubuntu 64-bit
Activities
Firefox
Apr 18 16:19
Project Part I - Homepage
192.168.50.10
AlmaLinux
Documentation
Blog
Bug tracker
GitHub organization
Project Part 1
Task 2 - Secure directories:
secure1 (user01 - accessible)
secure2 (user01 and 192.168.50.0/24 - accessi
secure2 (user01 and 10.35.16.1/24 - Not acces
secure3 (user01 or 192.168.0.0/24 - accessible
secure3 (user01 or 192.168.50.0/24 - accessibl
secure4 (user02 - accessible)
secure5 (user01 with .htaccess - accessible)
secure6 (user01 and 192.168.50 with .htaccess
secure6 (user01 and 10.35.16.1/24 with .htacc
secure7 (user01 or 192.168.50 with .htaccess - Accessible)
secure7 (user01 or 192.168.50 with .htaccess - Accessible)
Task 3 - Project 1:
Project1 (192.168.50.10 - All is accessible)
Project1 (10.35.16.1 accessible except secret.* and *.txt)
Project1 (10.35.17.1 accessible except secret.* and *.txt)
Project1 (192.168.100.1 Not accessible)
Task 3 - Project 2:
Project2 (192.168.50.10 - All is accessible)
Project2 (10.35.16.1 Not accessible)
Project2 (10.35.17.1 accessible except *.txt)
Project2 (192.168.100.1 accessible except *.txt)
Task 3 - Project 3:
Project3 (192.168.50.10 - All is accessible)
192.168.50.10
This site is asking you to sign in.
Username
Password
Cancel
Sign in


192.168.50.10/secure7/
AlmaLinux
Documentation
Blog
Bug tracker
GitHub organization
Index of /secure7
Name
Last modified
Size
Description
Parent Directory
-
secure7a.html
2025-04-17 04:51
44

TASK 3 – ACCESSIBILITY

In the/var/www/html_project1 directory add the following subdirectories:

➢ Project1

➢ Project2

➢ Project3

➢ Project4

```
[root@server09 html_project1]# mkdir -p Project1 Project2 Project3 Project4
```

```
[root@server09 html_project1]# ls
accountants1.html  programmers1.html  Project2        project3d.html  secure3        secure7b.html
accountants2.html  programmers2.html  project2a.html  Project4        secure3a.html  vendors1.html
accountants3.html  programmers3.html  project2b.html  project4a.html  secure3b.html  vendors2.html
accountants4.html  programmers4.html  project2c.html  project4b.html  secure4        vendors3.html
admin1.html        Project1           project2d.html  project4c.html  secure4.html   vendors4.html
admin2.html        project1a.html     Project3        project4d.html  secure5
admin3.html        project1b.html     project3a.html  secure1         secure6
admin4.html        project1c.html     project3b.html  secure2a        secure6b.html
index.html         project1d.html     project3c.html  secure2a.html   secure7
```

2. In each of these directories, create a web page named after the directory itself. For example, Project1/project1.html, Project2/project2.html, etc.

```
[root@server09 html_project1]# echo "<h1>Welcome to Project1</h1>" | sudo tee Project1/project1.html
<h1>Welcome to Project1</h1>
[root@server09 html_project1]# echo "<h1>Welcome to Project2</h1>" | sudo tee Project2/project2.html
<h1>Welcome to Project2</h1>
[root@server09 html_project1]# echo "<h1>Welcome to Project3</h1>" | sudo tee Project3/project3.html
<h1>Welcome to Project3</h1>
[root@server09 html_project1]# echo "<h1>Welcome to Project4</h1>" | sudo tee Project4/project4.html
<h1>Welcome to Project4</h1>
[root@server09 html_project1]#
```

3. Do not place an index.html file in these directories. Instead, configure Apache to display a directory listing when accessed.

```
[root@server09 html_project1]# vim /etc/httpd/conf.d/secure.conf
```

```
<Directory "/var/www/html_project1/Project1">
    Options +Indexes
    AllowOverride All
</Directory>

<Directory "/var/www/html_project1/Project2">
    Options +Indexes
    AllowOverride All
</Directory>

<Directory "/var/www/html_project1/Project3">
    Options +Indexes
    AllowOverride All
</Directory>

<Directory "/var/www/html_project1/Project4">
    Options +Indexes
    AllowOverride All
</Directory>
```

4. Add and directives to implement the following access controls:

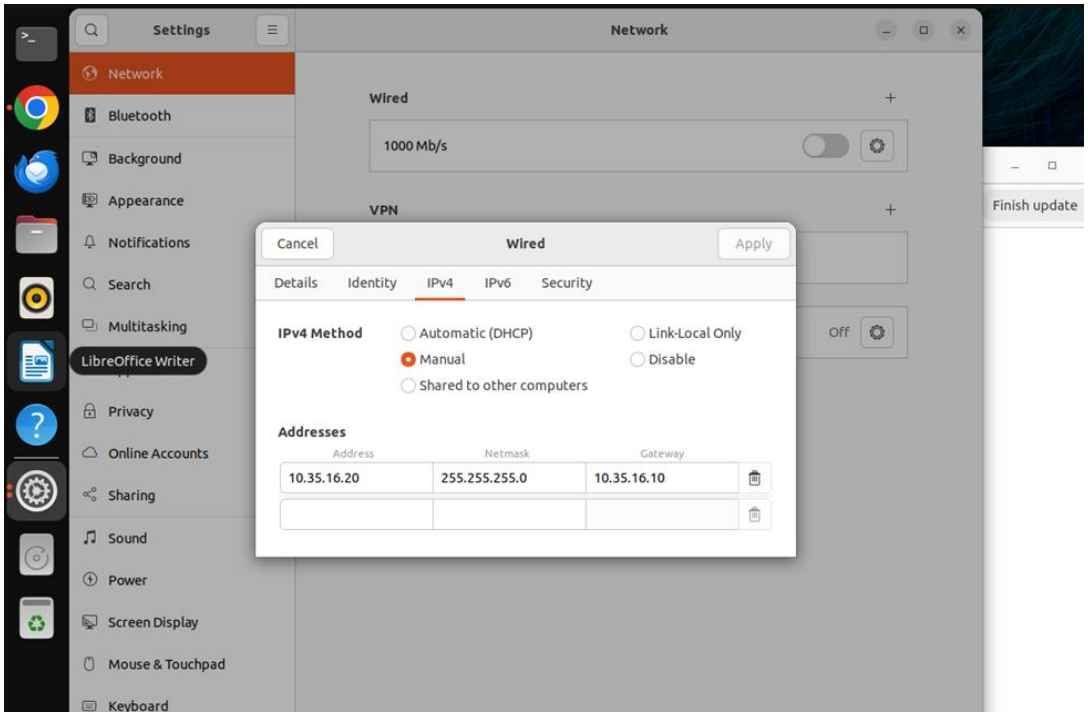
➢ All directories and their contents must be accessible from the 192.168.50.0/24 subnet.

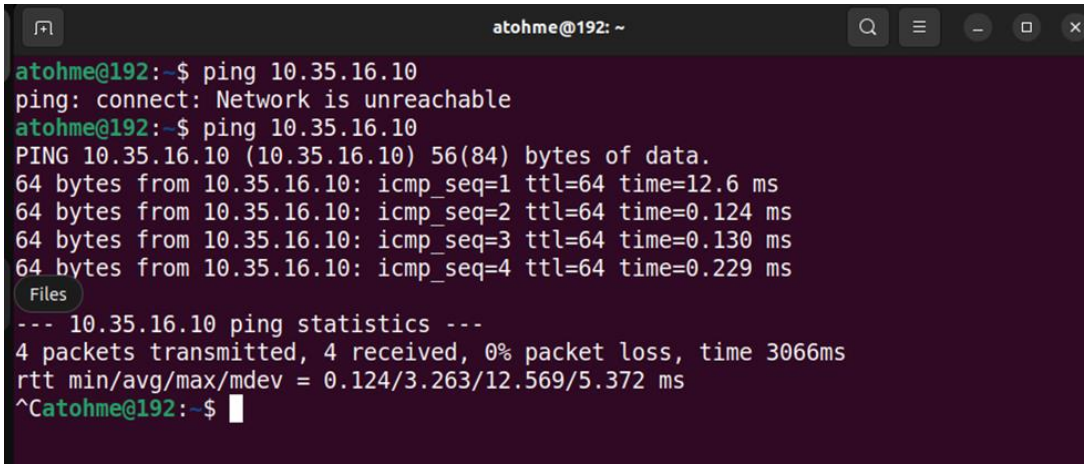
➢ Project1: Accessible only from the 10.35.16.0/24 and 10.35.17.0/24 subnets. Any files named secret.* must not be accessible.

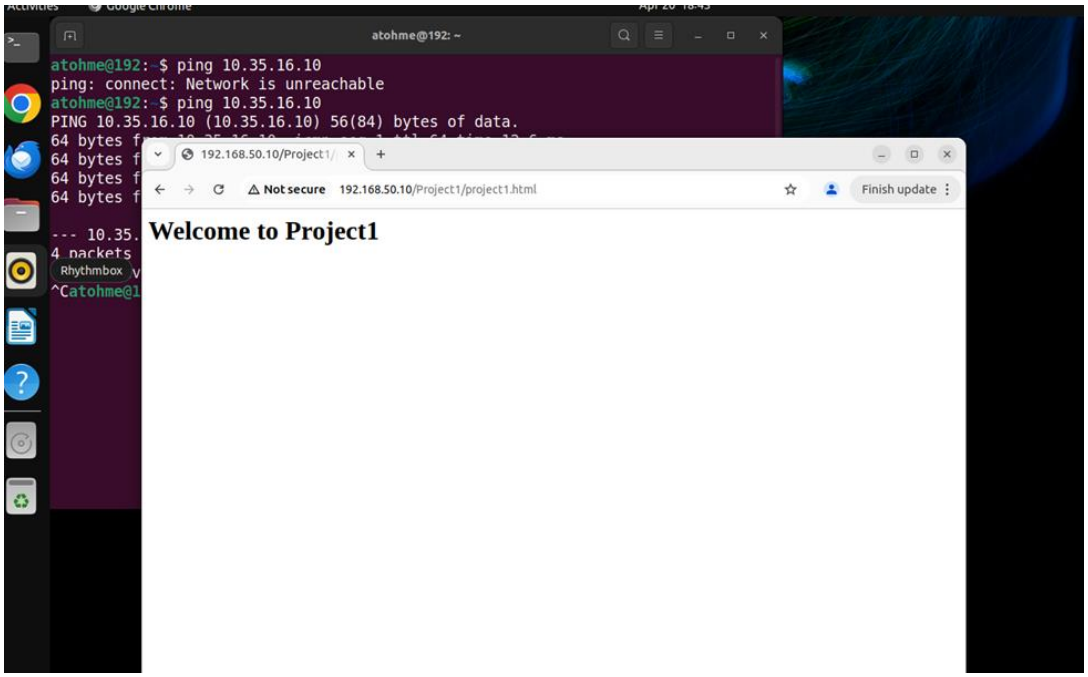
```
<Directory "/var/www/html_project1/Project1">
    Options +Indexes
    AllowOverride All
    Require ip 10.35.16.0/24 10.35.17.0/24
</Directory>

<Directory "/var/www/html_project1/Project1">
    <FilesMatch "^secret\..*">
        Require all denied
    </FilesMatch>
</Directory>
```

```
[root@server09 html_project1]# nmcli con delete LAN2
Connection 'LAN2' (681732f7-0619-40f2-870f-68f8d80258ff) successfully deleted.
[root@server09 html_project1]# nmcli con add type ethernet ifname ens224 con-nam
e LAN2 ipv4.method manual ipv4.addresses 10.35.16.10/24
Connection 'LAN2' (1a823e55-777d-4738-8319-506347be37d7) successfully added.
[root@server09 html_project1]#
```

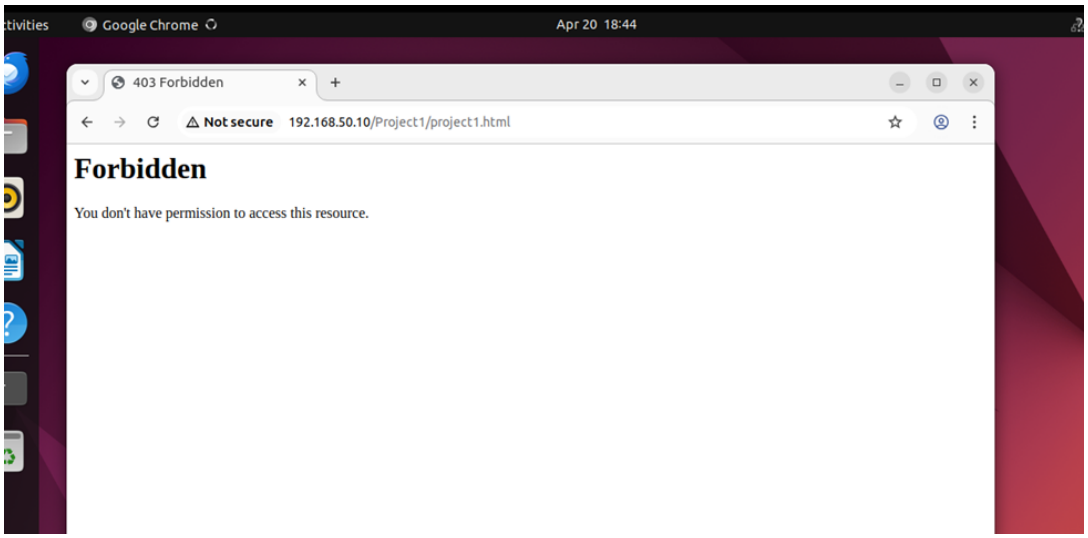
Connection IP in server changed.







From LAN1(192.168.50.0/24)



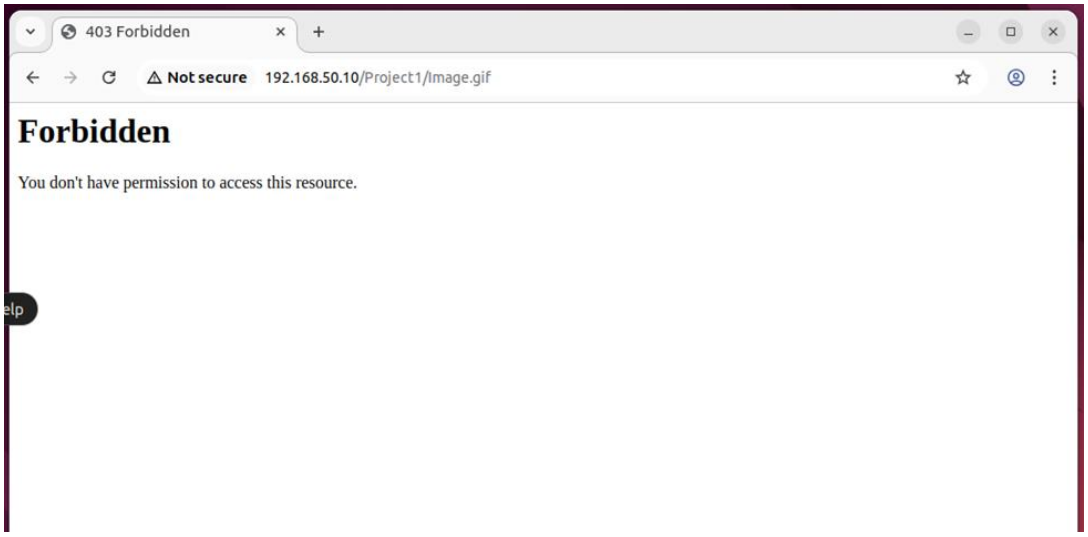
➢ Project2: Not accessible only from the 10.35.16.0/24 subnet. All files must be accessible to others.

```
<Directory "/var/www/html_project1/Project2">
    Options +Indexes
    AllowOverride All
    <RequireAll>
       Require all granted
       Require not ip 10.35.16.0/24
    </RequireAll>
</Directory>
```

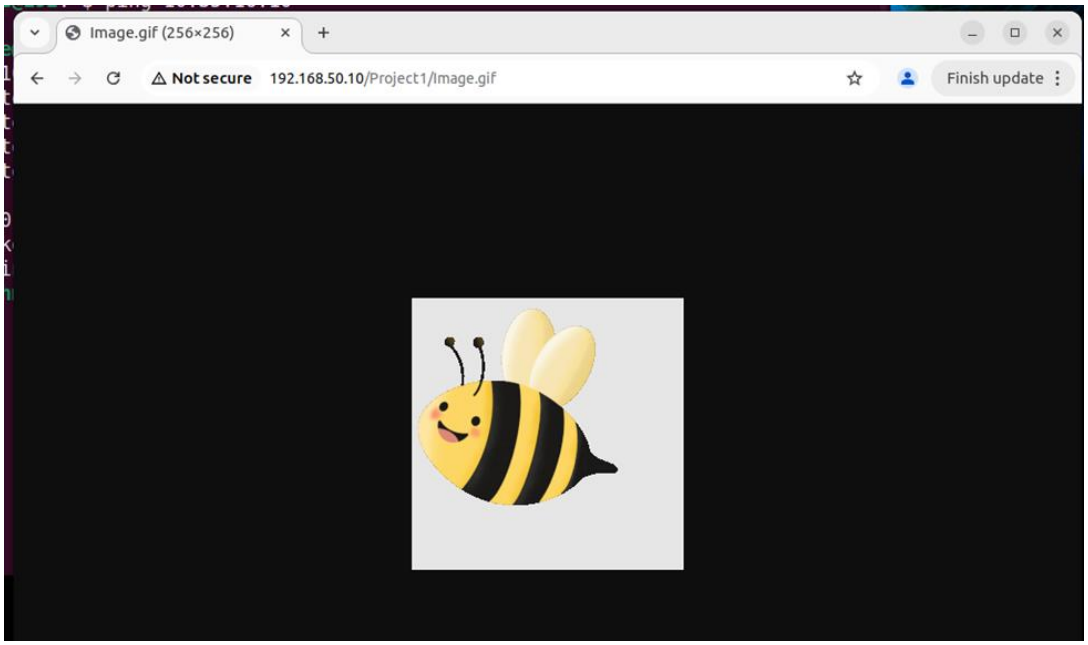
➢ Project3: Accessible only from the 192.168.100.0/24 subnet. All *.gif files must not be accessible.

```
<Directory "/var/www/html_project1/Project3">
    Options +Indexes
    AllowOverride All
    Require ip 192.168.100.0/24
</Directory>

<Directory "/var/www/html_project1/Project3">
    <FilesMatch "\.gif$">
        Require all denied
    </FilesMatch>
</Directory>
```

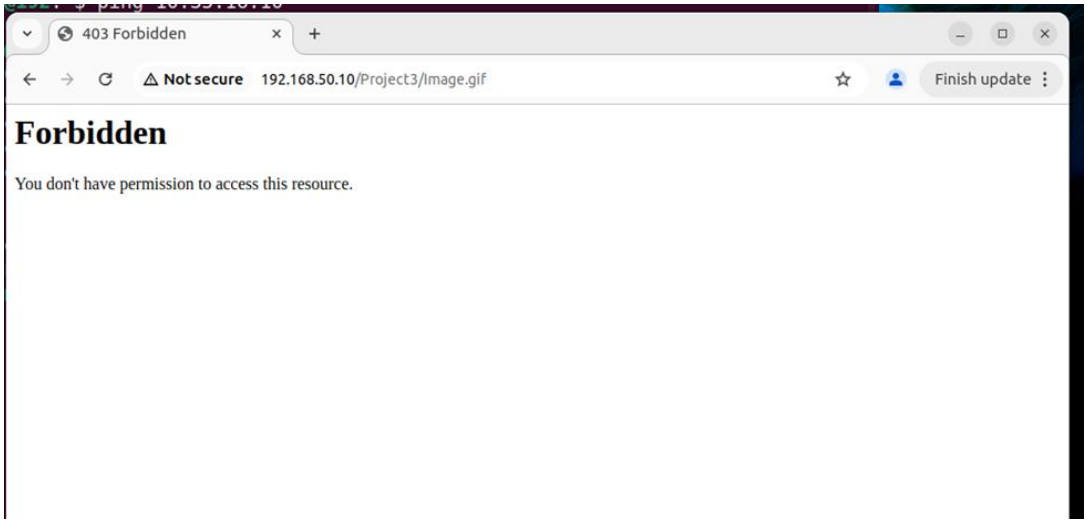
access to Image to Project1 folder by Computer Ubuntu(192.168.50.20)



In the folder Project1 from Client-9(10.35.16.20/24)



but from save computer but Image in Picture3



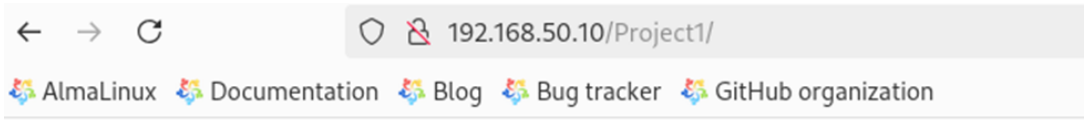
➢ Project4: Accessible only from 10.35.16.0/24 and 192.168.100.0/24. All test.html files must not be accessible.

```
<Directory "/var/www/html_project1/Project4">
    Options +Indexes
    AllowOverride All
    Require ip 10.35.16.0/24 192.168.100.0/24
</Directory>

<Directory "/var/www/html_project1/Project4">
    <Files "test.html">
        Require all denied
    </Files>
</Directory>
```

5. For all directories, *.txt files must not be accessible. Place the corresponding directive outside of any blocks.

```
<FilesMatch "\.txt$">
    Require all denied
</FilesMatch>
```

```
[root@server09 html_project1]# sudo systemctl restart httpd
[root@server09 html_project1]#
```



Forbidden

You don't have permission to access this resource.

TASK 4 – AUTHORIZATION

Identify the network subnet of each department:

➢ Vendors use the subnet 10.50.1.0/24

➢ Accountants use the subnet 10.51.1.0/24

➢ Administrators use the subnet 10.52.1.0/24

➢ Programmers use the subnet 10.53.1.0/24

2. Each department has its own dedicated web directory on the server.

```
[root@server09 www]# mkdir htdocs
[root@server09 www]# mkdir /var/www/htdocs/vendors
[root@server09 www]# mkdir /var/www/htdocs/accountants
[root@server09 www]# mkdir /var/www/htdocs/administrators
[root@server09 www]# mkdir /var/www/htdocs/programmers
[root@server09 www]#
```

3. Websites must be placed in the /var/www/htdocs/<group_name> directory. For example: /var/www/htdocs/vendors, /var/www/htdocs/accountants, etc.

```
[root@server09 www]# echo "<h1>Welcome Vendors</h1>" | sudo tee /var/www/htdocs/vendors/index.html
<h1>Welcome Vendors</h1>
[root@server09 www]# echo "<h1>Welcome Accountants</h1>" | sudo tee /var/www/htdocs/accountants/inde
x.html
<h1>Welcome Accountants</h1>
[root@server09 www]# echo "<h1>Welcome Administrators</h1>" | sudo tee /var/www/htdocs/administrator
s/index.html
<h1>Welcome Administrators</h1>
[root@server09 www]# echo "<h1>Welcome programmers</h1>" | sudo tee /var/www/htdocs/programmers/inde
x.html
<h1>Welcome programmers</h1>
[root@server09 www]#
```

4. You must use aliases to make these websites accessible. For example, to access the vendors' website, use: http://10.50.1.1/vendors

with command

vim /etc/httpd/conf.d/departments.conf

5. Configure the Apache server with the following access rules:

➢ Vendors can access only their own website.

```
Alias /vendors "/var/www/htdocs/vendors"
<Directory "/var/www/htdocs/vendors">
    Require ip 10.50.1.0/24
</Directory>
```

➢ Accountants can access only the accountants' website and must not be able to view any *.html files.

```
Alias /accountants "/var/www/htdocs/accountants"
<Directory "/var/www/htdocs/accountants">
    <RequireAll>
        Require ip 10.51.1.0/24
        Require not all denied
    </RequireAll>
    <FilesMatch "\.html$">
        Require all denied
    </FilesMatch>
</Directory>
```

➢ Administrators must be able to view all department websites.

```
Alias /administrators "/var/www/htdocs/administrators"
<Directory "/var/www/htdocs/administrators">
    Require ip 10.52.1.0/24
</Directory>
```

➢ Programmers must be able to access their own website and to view all department websites except their *.gif or *.jpg files.

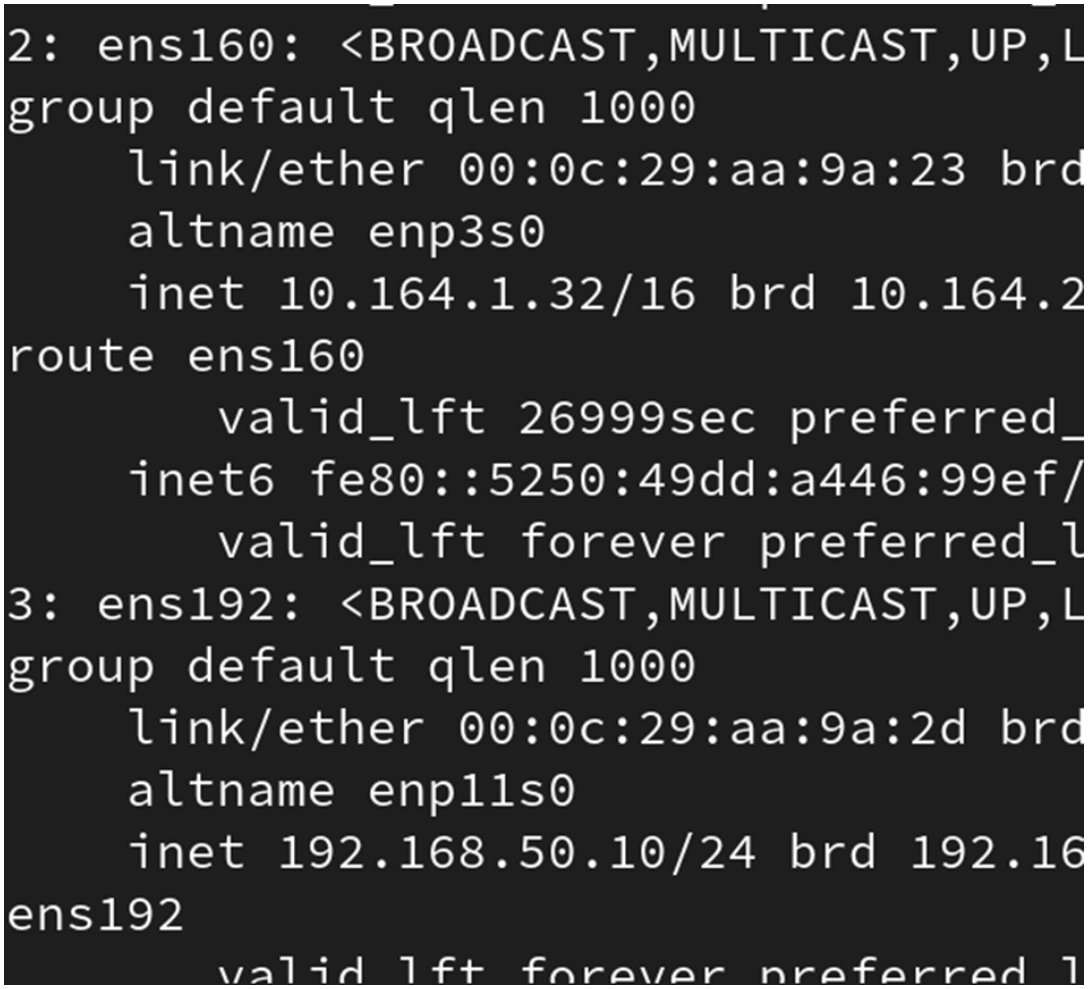
```
Alias /programmers "/var/www/htdocs/programmers"
<Directory "/var/www/htdocs/programmers">
    Require ip 10.53.1.0/24
</Directory>
```

```
# Shared access rules for Programmers to other depts
<Directory "/var/www/htdocs">
    <RequireAny>
        Require ip 10.52.1.0/24  # Admins can access all
        Require ip 10.53.1.0/24  # Programmers can access all EXCEPT *.gif, *.jpg
    </RequireAny>
</Directory>

# Restrict .gif and .jpg for programmers
<Directory "/var/www/htdocs">
    <FilesMatch "\.(gif|jpg)$">
        Require not ip 10.53.1.0/24
    </FilesMatch>
</Directory>
```

Note: Make sure to demonstrate the enforcement of each access control rule through appropriate tests and screenshots or logs as evidence.

For testing first is checked connections:

ip a



Connection ens160 and ens224 (LAN1 and LAN2) will change with 10.50.1.1 and 10.53.1.1 and in client 10.50.1.10 and 10.53.1.10. and after test responses.

```
Connection 'LAN1' (23a19d8a-d4d4-400f-a125-94a9dd67800e) successfully de
leted.
[root@server09 Pictures]# nmcli con delete LAN2
Connection 'LAN2' (1a823e55-777d-4738-8319-506347be37d7) successfully de
leted.
[root@server09 Pictures]#
```

```
[root@server09 Pictures]# nmcli con add type ethernet ifname end160 con-
name LAN1 ipv4.method manual ipv4.addresses 10.50.1.1/24
Connection 'LAN1' (e2fff7f0-d006-4190-bd22-295a7d49644f) successfully ad
ded.
[root@server09 Pictures]# nmcli con add type ethernet ifname end224 con-
name LAN2 ipv4.method manual ipv4.addresses 10.53.1.1/24
Connection 'LAN2' (e31d4f97-50cf-416d-95f7-7eb3718a4fd7) successfully ad
ded.
[root@server09 Pictures]#
```

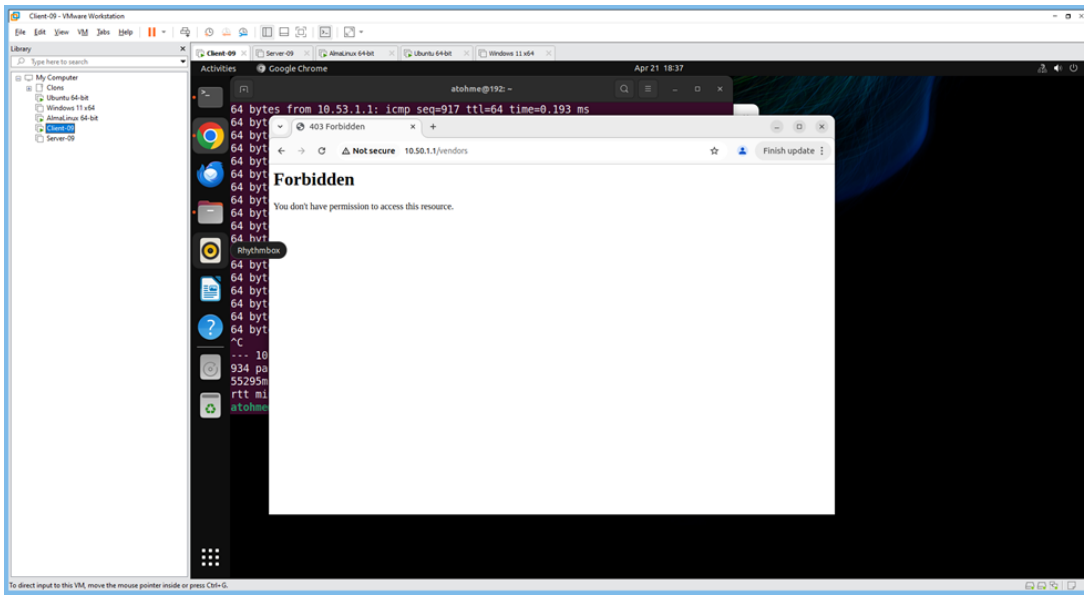
```
[root@server09 Pictures]# nmcli con sh
NAME  UUID                                  TYPE      DEVICE
NAT   ba7fe6c5-ef7b-4a1b-a039-53fa2a439968  ethernet  ens160
lo    2e728425-4216-4e45-bccd-ffa3e62445f8  loopback  lo
LAN1  e2fff7f0-d006-4190-bd22-295a7d49644f  ethernet  --
LAN2  e31d4f97-50cf-416d-95f7-7eb3718a4fd7  ethernet  --
[root@server09 Pictures]#
```

```
houman@client09:~$ sudo nmcli con delete LAN1
Connection 'LAN1' (1fe8c54d-4d5a-4027-b167-c1f18b2ee4a9) successfully deleted.
houman@client09:~$ sudo nmcli con add type ethernet ifname ens160 con-name LAN1
ipv4.method manual ipv4.addresses 10.50.1.10/24
Connection 'LAN1' (e326fb78-dddb-431d-96dd-6f6b5667575c) successfully added.
houman@client09:~$
```

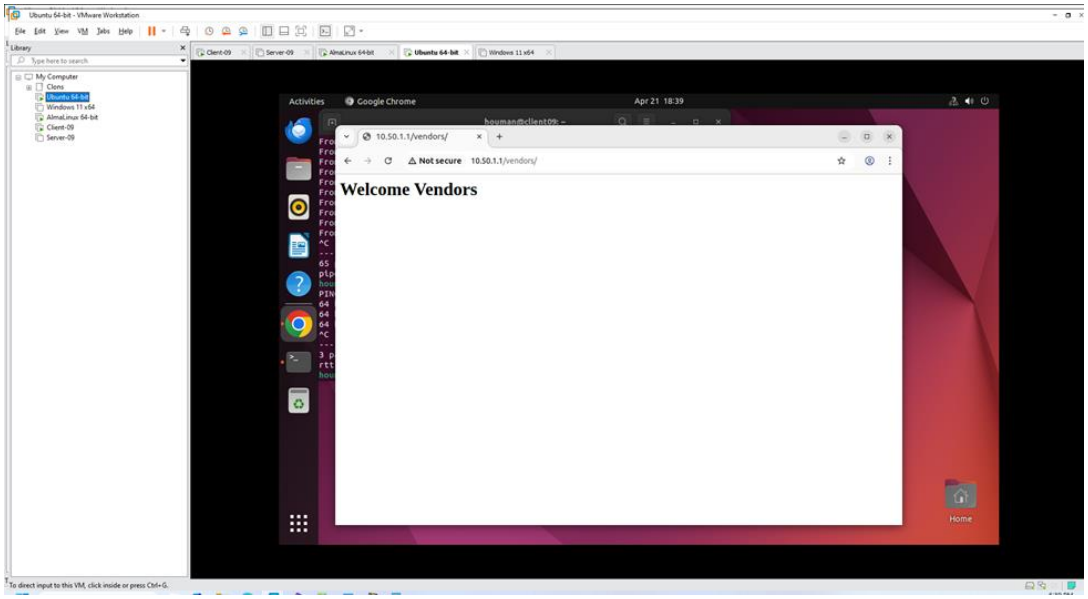
```
atohme@192:~$ sudo nmcli con add type ethernet ifname ens33 con-name LAN2 ipv4.m
ethod manual ipv4.addresses 10.53.1.10/24
Connection 'LAN2' (fc96450c-2c68-47be-9927-dc6d24c3f480) successfully added.
```

```
[root@server09 Project1]# ls
Image.gif  project1.html
[root@server09 Project1]# cp Image.gif /var/www/htdocs/vendors/
[root@server09 Project1]#
```

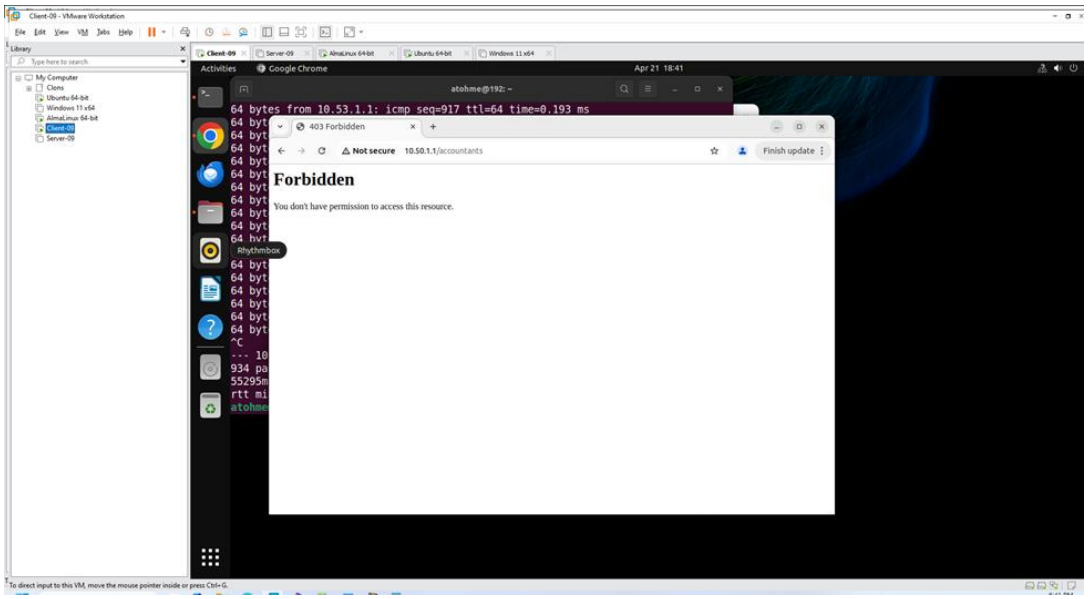
from ubunto (10.53.1.10) request for http://10.50.1.1/vendors



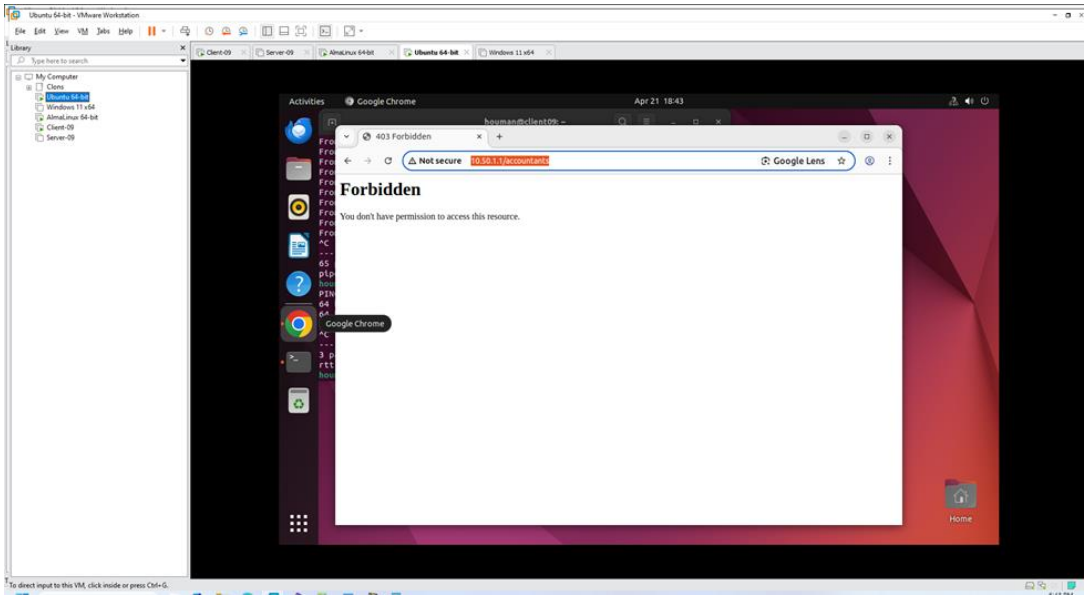
but from Ubuntu(10.50.1.10) when request for http://10.50.1.1/vendors



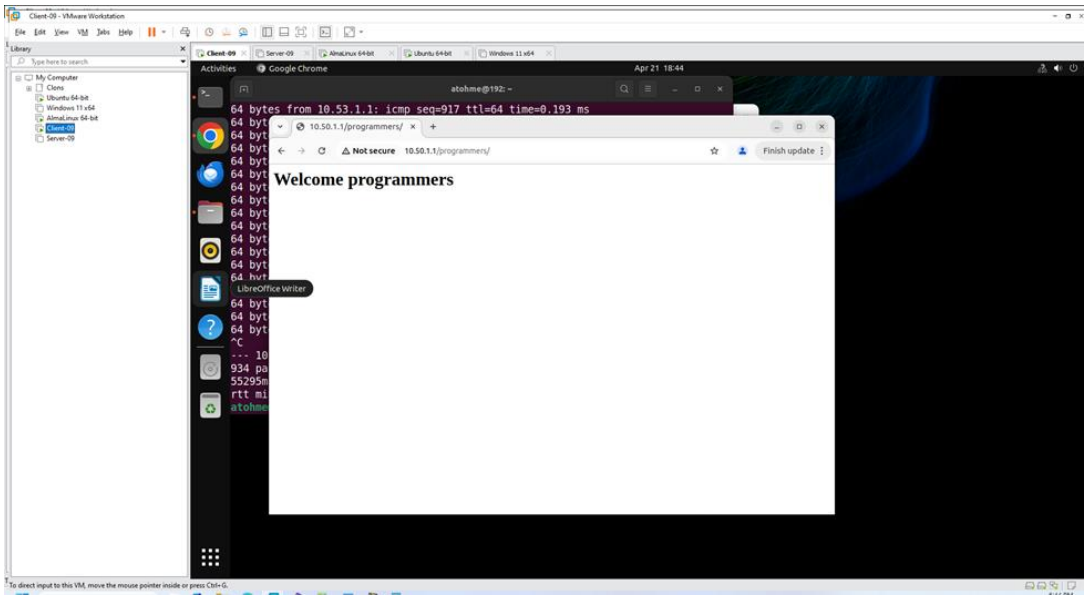
from 10.53.1.1 request http://10.50.1.1/accountants



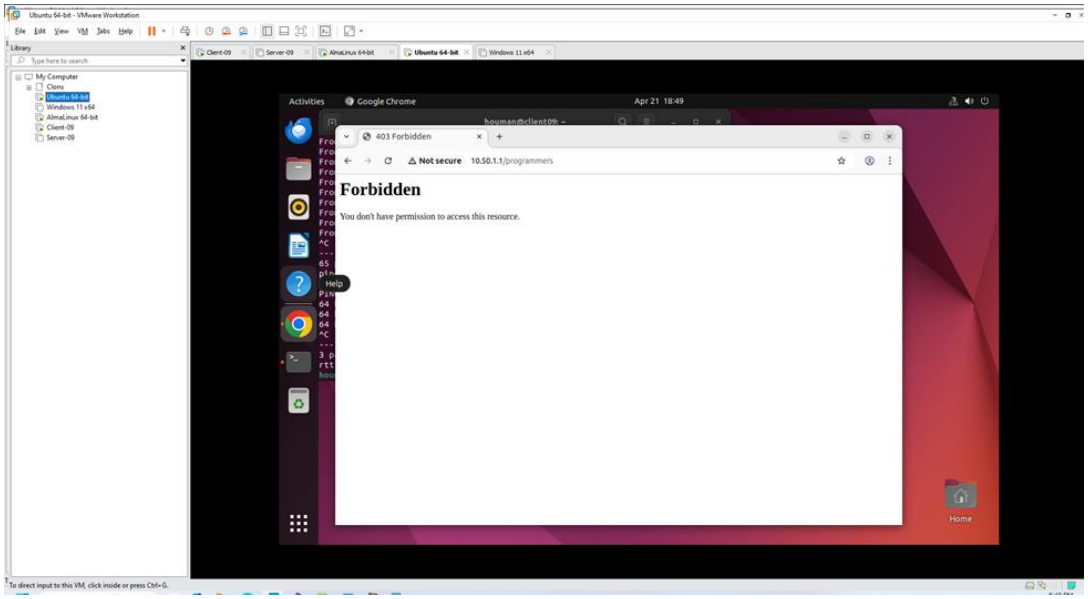
from 10.50.1.1 request http://10.50.1.1/accountants



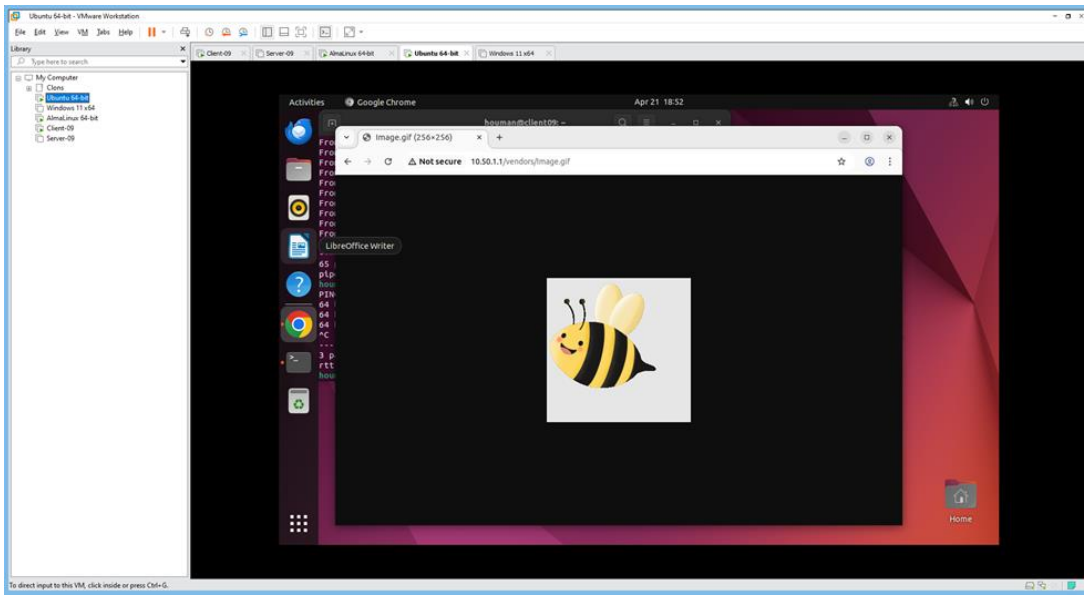
from 10.53.1.1 request http://10.50.1.1/programmers



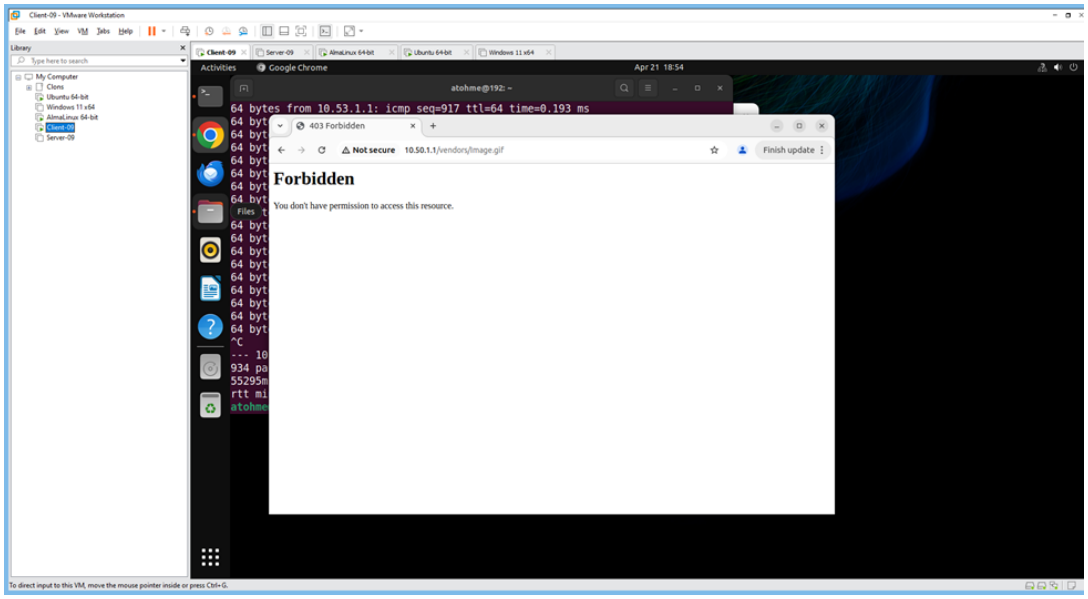
from 10.50.1.1 request http://10.50.1.1/programmers



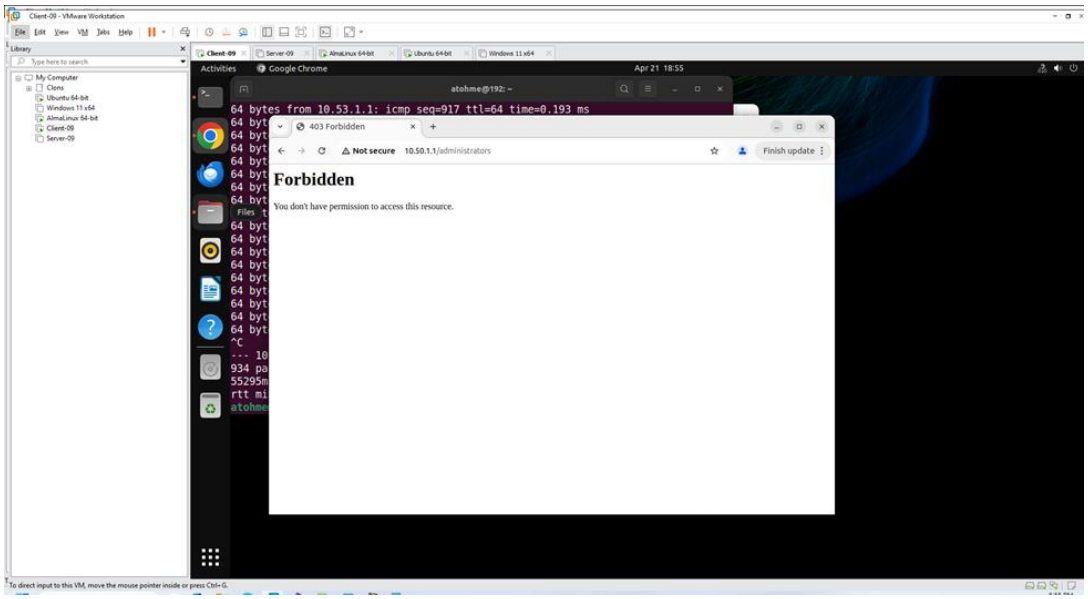
from 10.50.1.1 request http://10.50.1.1/vendors/Image.gif



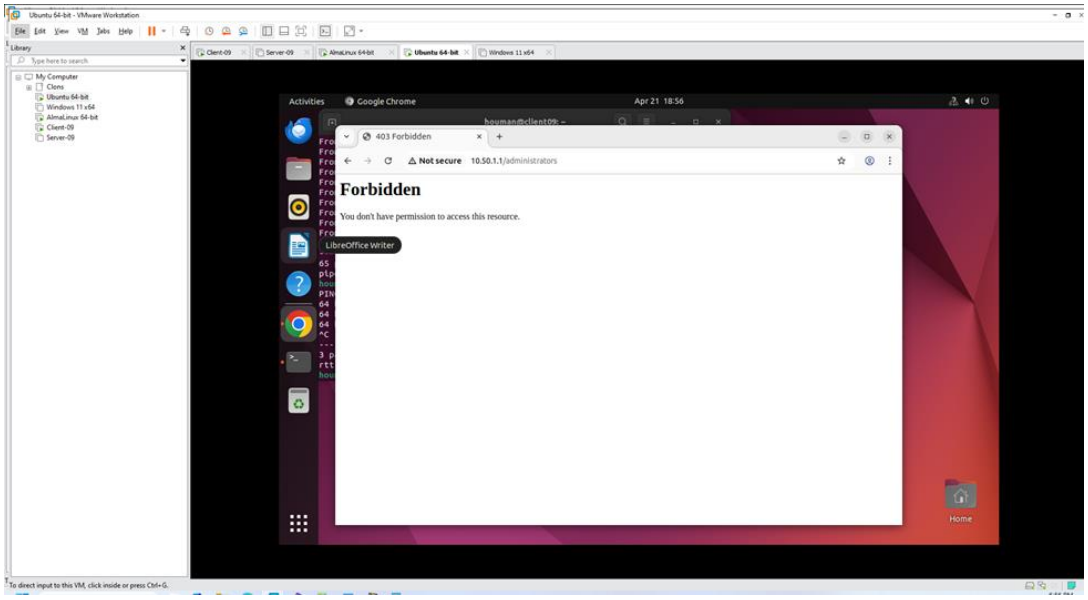
from 10.53.1.1 request http://10.53.1.1/Image.gif



from 10.53.1.1 request http://10.50.1.1/administrators



from 10.50.1.1 request http://10.50.1.1 /administrators



Example - index.html

Project Part 1

Task 2 - Secure directories:

- secure1 (user01 - accessible)
- secure2 (user01 and 192.168.50.0/24 - accessible)
- secure2 (user01 and 10.35.16.1/24- Not accessible)
- secure3 (user01 or 192.168.50.0/24 - accessible)
- secure3 (user01 or 192.168.50.0/24 - accessible)
- secure4 (user02 - accessible)
- secure5 (user01 with .htaccess - accessible)
- secure6 (user01 and 192.168.50 with .htaccess - Accessible))
- secure6 (user01 and 10.35.16.1/24 with .htaccess - Not accessible))
- secure7 (user01 or 192.168.50 with .htaccess - Accessible)
- secure7 (user01 or 192.168.50 with .htaccess- Accessible)

Task 3 - Project 1:

- Project1 (192.168.50.10 - All is accessible)
- Project1 (10.35.16.1 accessible except files secret.* and *.txt)
- Project1 (10.35.17.1 accessible except files secret.* and *.txt)
- Project1 (192.168.100.1 Not accessible)

Task 3 - Project 2:

- Project2 (192.168.50.10 - All is accessible)
- Project2 (10.35.16.1 Not accessible)
- Project2 (10.35.17.1 accessible except files *.txt)
- Project2 (192.168.100.1 accessible except files *.txt)

Task 3 - Project 3:

- Project3 (192.168.50.10 - All is accessible)
- Project3 (10.35.16.1 Not accessible)
- Project3 (10.35.17.1 Not accessible)
- Project3 (192.168.100.1 accessible except files *.gif and *.txt)

Task 3 - Project 4:

- Project4 (192.168.50.10 - All is accessible)
- Project4 (10.35.16.1 accessible except files test.html)
- Project4 (10.35.17.1 Not accessible)
- Project4 (192.168.100.1 accessible except files test.html)

Task 4 - Vendors website:

- Accessible to Vendors (10.50.1.0/24)
- Not accessible to Accountants (10.51.1.0/24)
- Accessible to Administrators (10.52.1.0/24)
- Accessible to Programmers (10.53.1.0/24) but not *.gif and *.jpg files

Task 4 - Accountants website:

- Not accessible to Vendors (10.50.1.0/24) but not *.html files
- Accessible to Accountants (10.51.1.0/24)
- Accessible to Administrators (10.52.1.0/24)
- Accessible to Programmers (10.53.1.0/24) but not *.gif and *.jpg files

Task 4 - Programmers website:

- Not accessible to Vendors (10.50.1.0/24)
- Not accessible to Accountants (10.51.1.0/24)
- Accessible to Administrators (10.52.1.0/24)
- Accessible to Programmers (10.53.1.0/24)

Task 4 - Administrators website:

- Not accessible to Vendors (10.50.1.0/24)
- Not accessible to Accountants (10.51.1.0/24)
- Accessible to Administrators (10.52.1.0/24)
- Accessible to Programmers (10.53.1.0/24) but not *.gif and *.jpg files