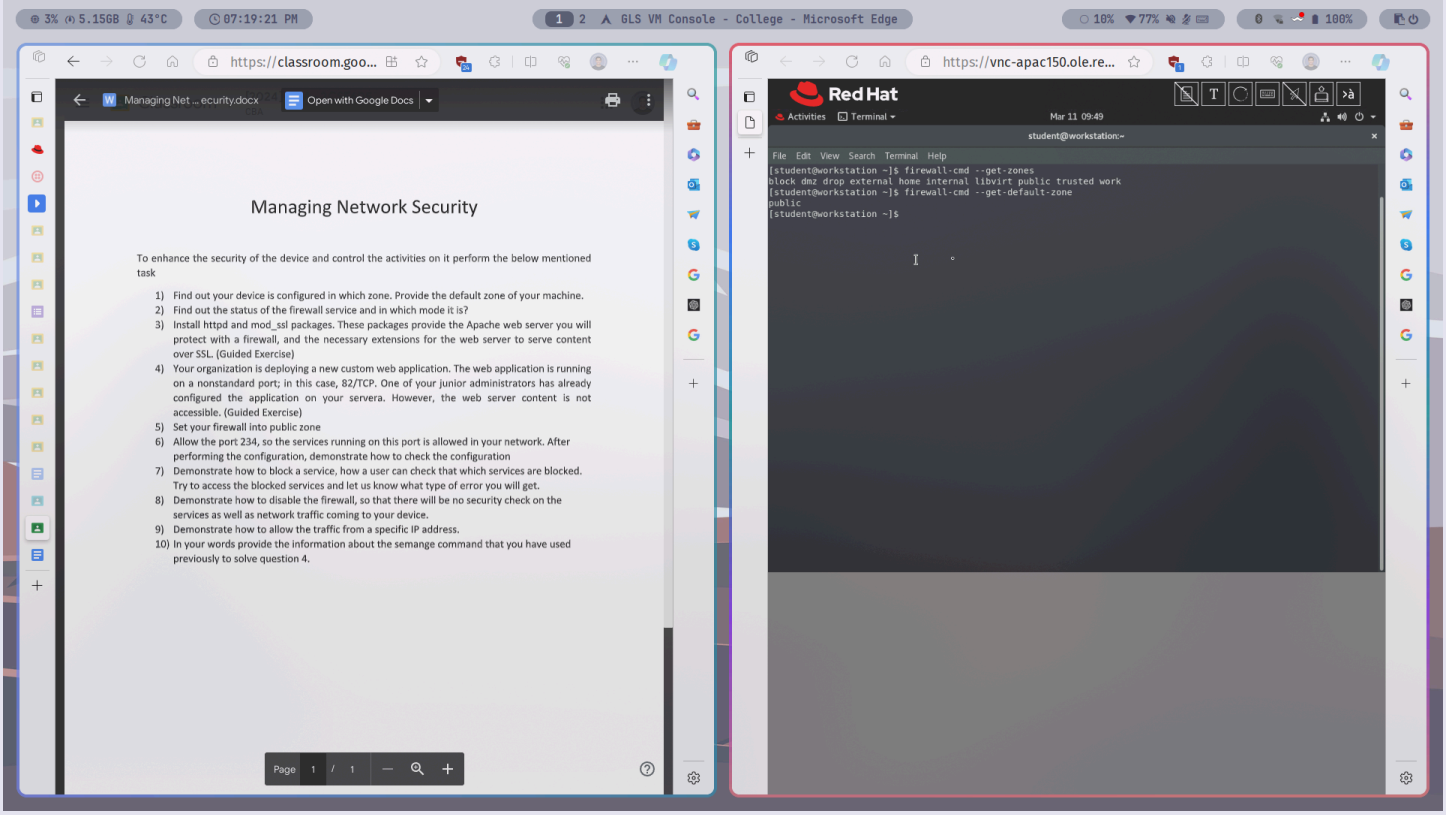
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

Aim : To enhance the security of the device and control the activities on it perform the below mentioned task

1) Find out your device is configured in which zone. Provide the default zone of your machine.

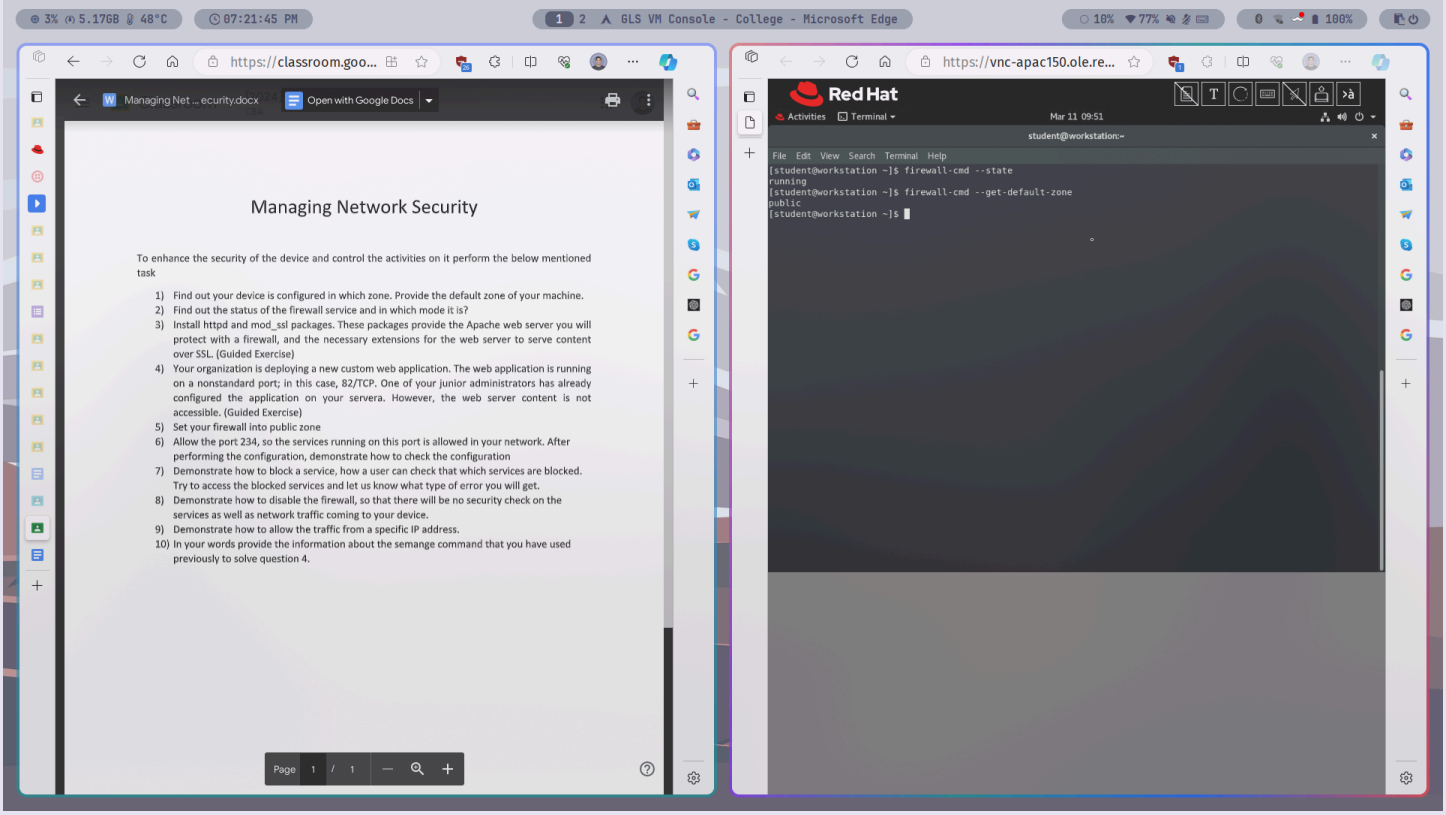


Commands :

- **firewall-cmd –get-zones** (to list all available zone options for firewall)
- **firewall-cmd –get-default-zone** (to get the default zone of device's firewall configuration)

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

2) Find out the status of the firewall service and in which mode it is?



Command : **firewall-cmd –state**

Currently, the firewall daemon is in ***running*** state/mode.

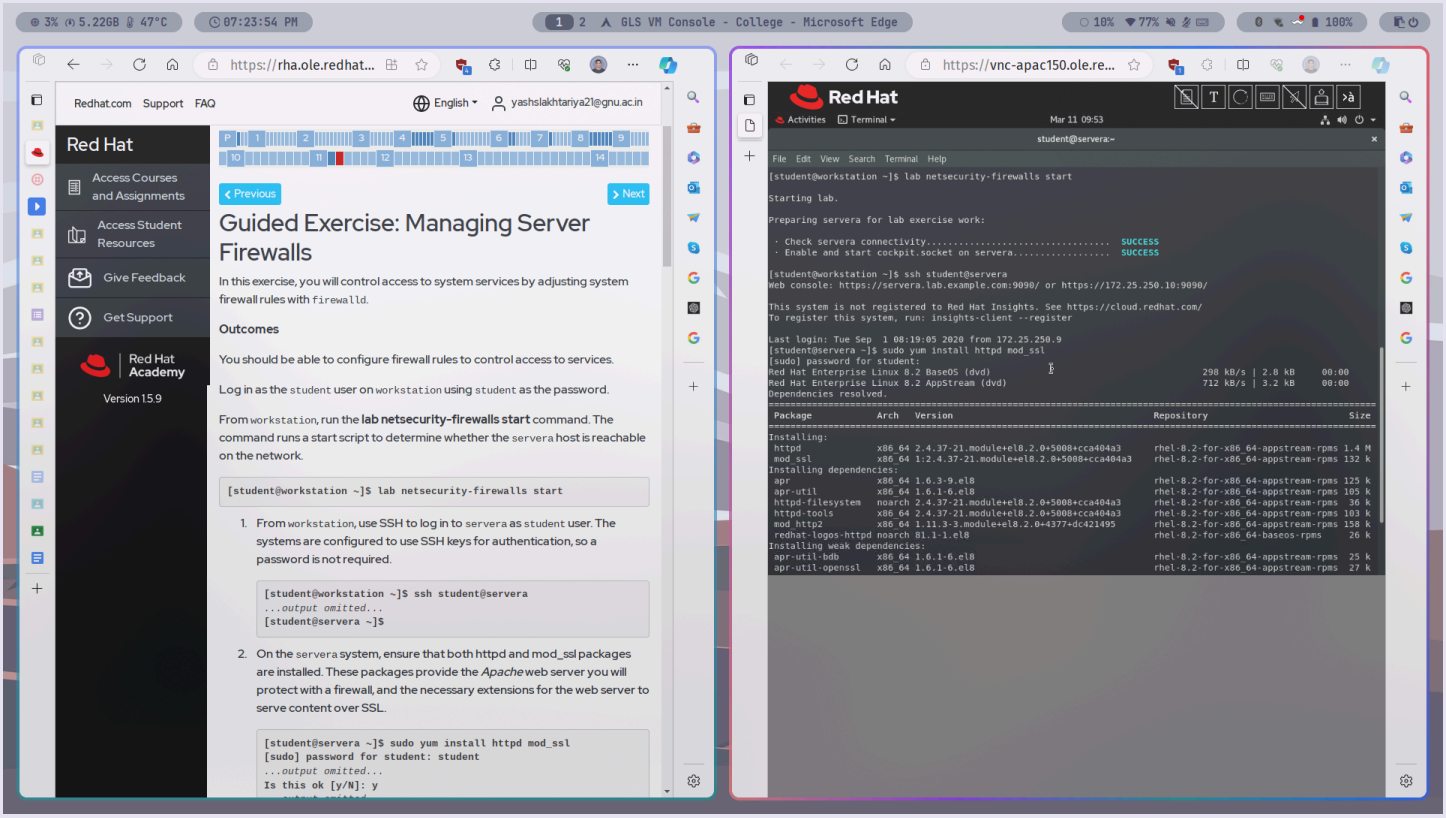
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

3) Install httpd and mod_ssl packages. These packages provide the Apache web server you will protect with a firewall, and the necessary extensions for the web server to serve content over SSL. (Guided Exercise)

Steps :

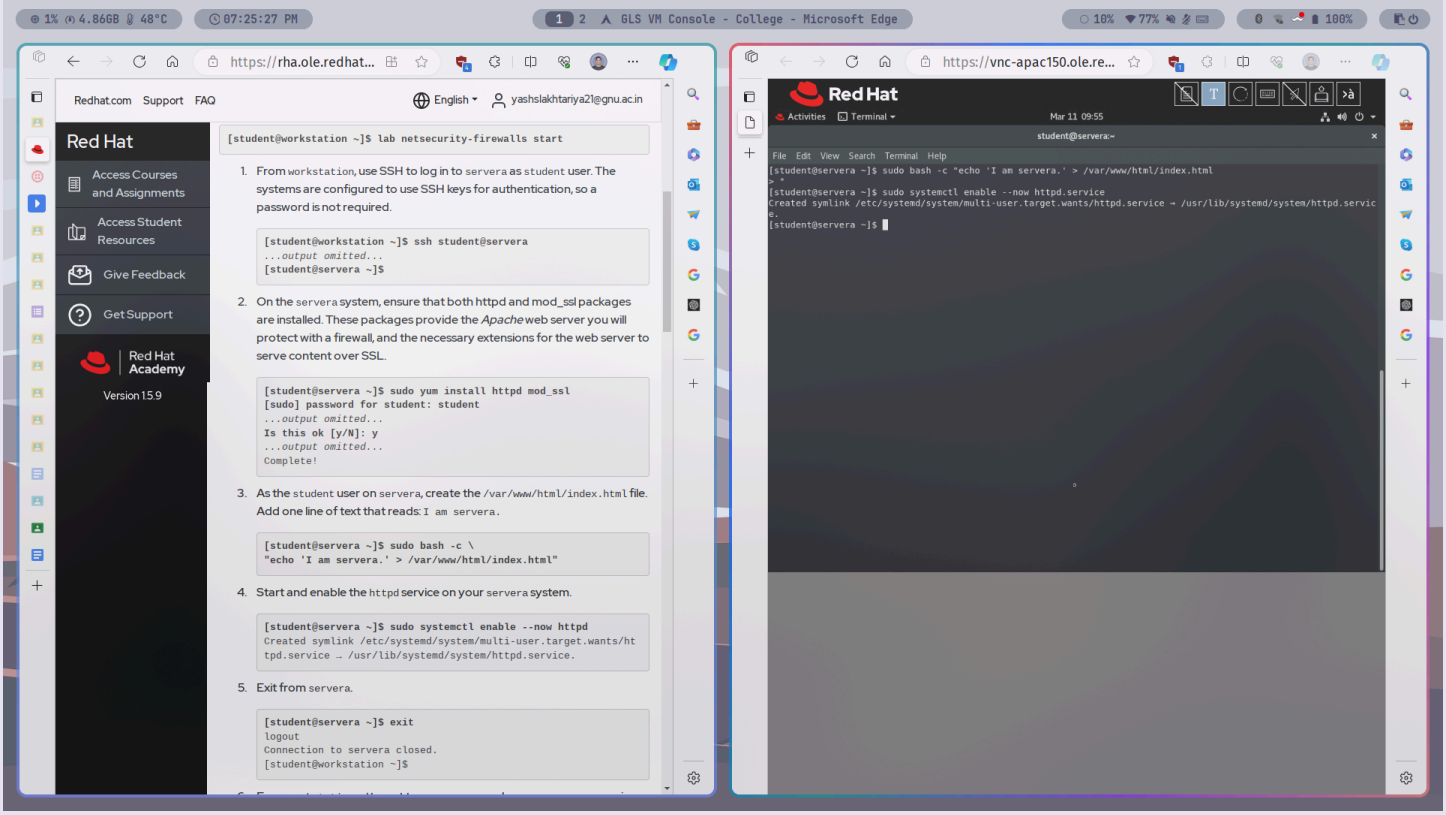
a. Run the lab setup script and login to servera via ssh. Thereafter, install httpd and mod_ssl



Command : **sudo yum install httpd mod_ssl** (to install the apache server and SSL modules packages using yum package manager with root privileges)

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

b. Create index.html file inside apache root and enable and start the http daemon

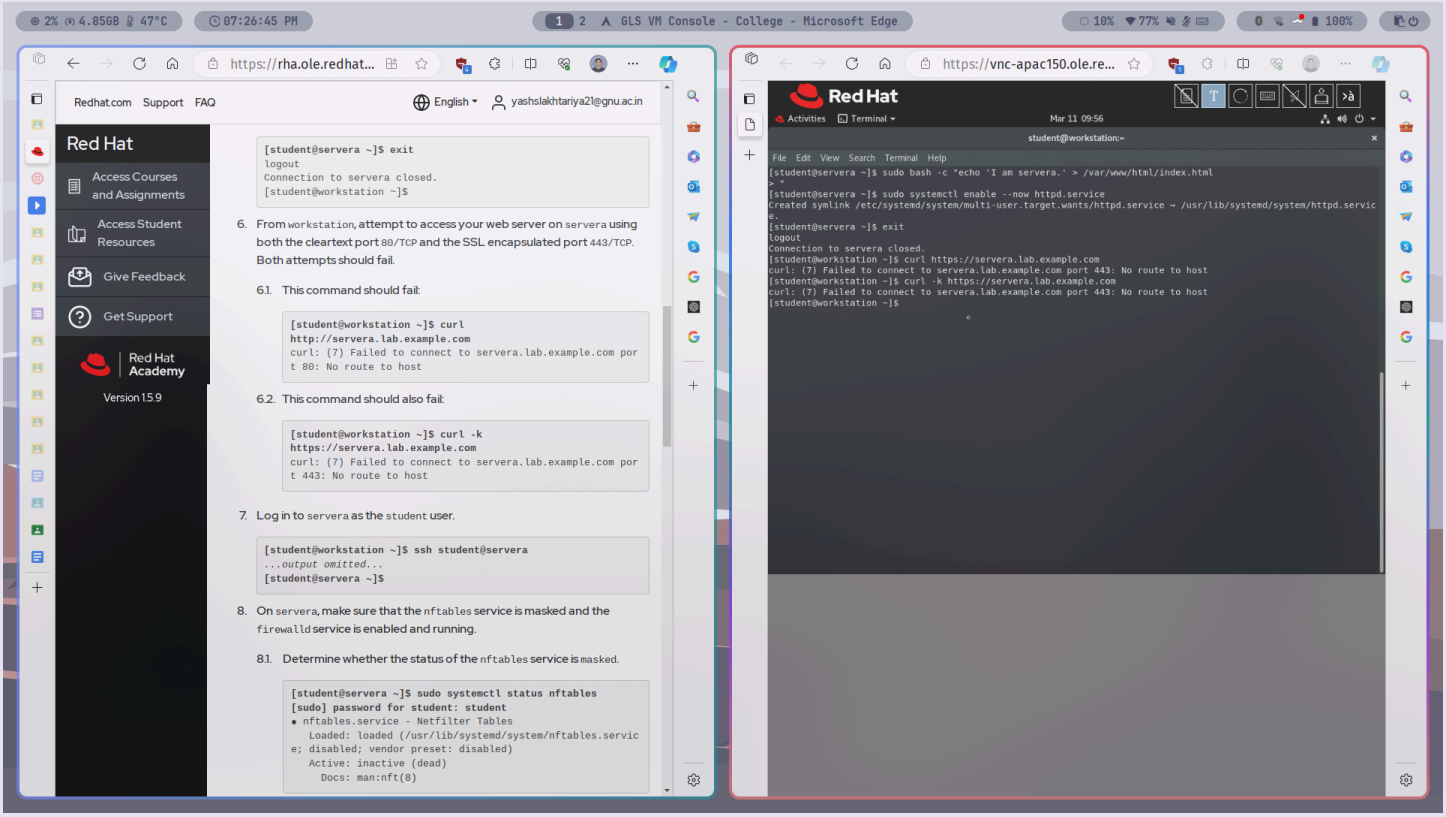


Commands :

- **sudo bash -c “echo ‘I am servera’ > /var/www/html/index.html”** (to append text to the index.html file (create if not exists) of path specified, this command echo is run via bash shell with -c option which specifies to accept the whole string as command)
- **sudo systemctl enable --now httpd.service** (to enable http daemon service and start now only)

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

c. Now, exit from servera and try to reach servera site from workstation via curl, it should give an error because it is not configured and firewall isn't allowing it



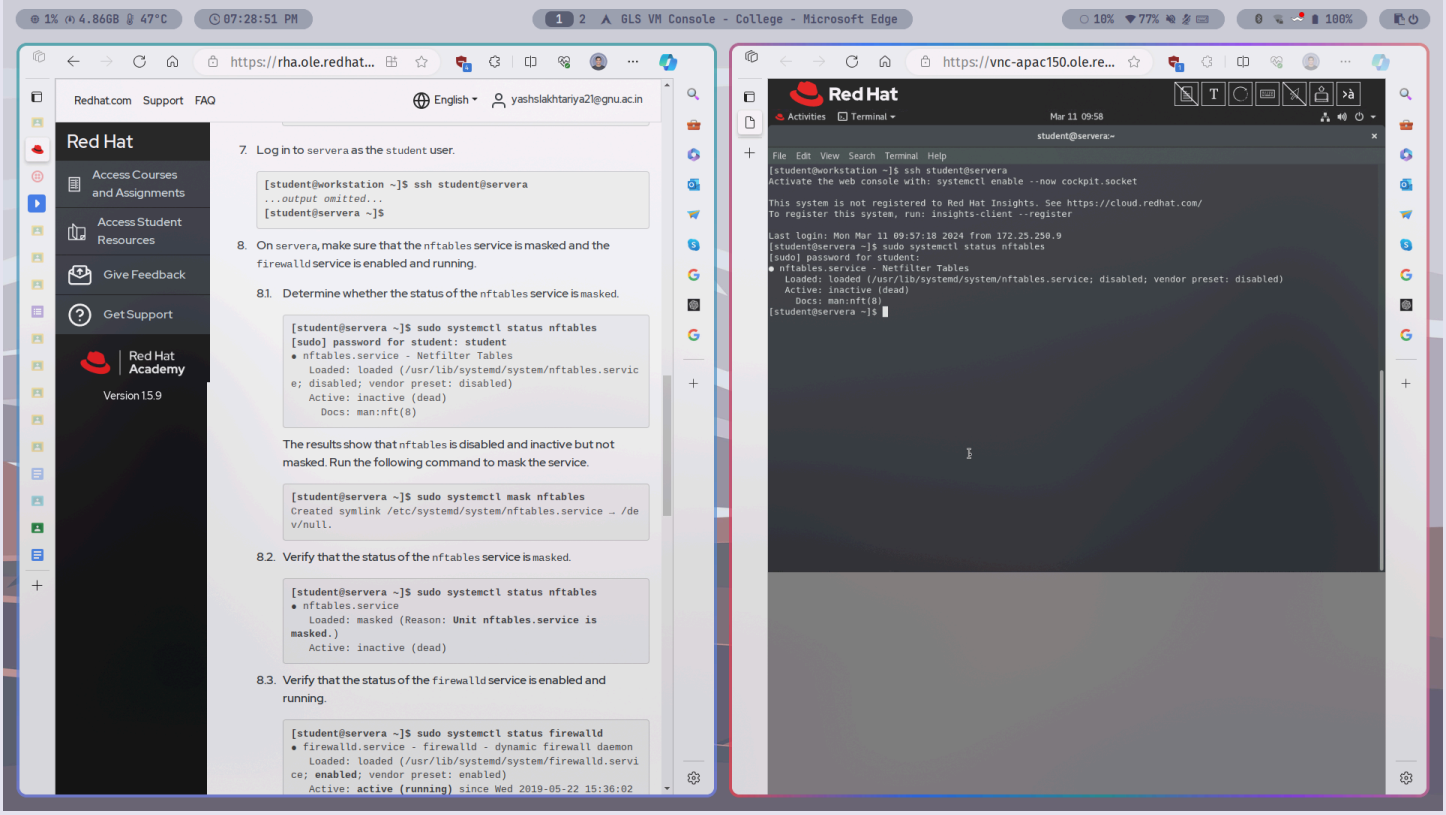
Commands :

- **curl http://servera.lab.example.com**
- **curl -k http://servera.lab.example.com**

(both for accessing the given URL via curl command, but -k for allowing insecure connections also)

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

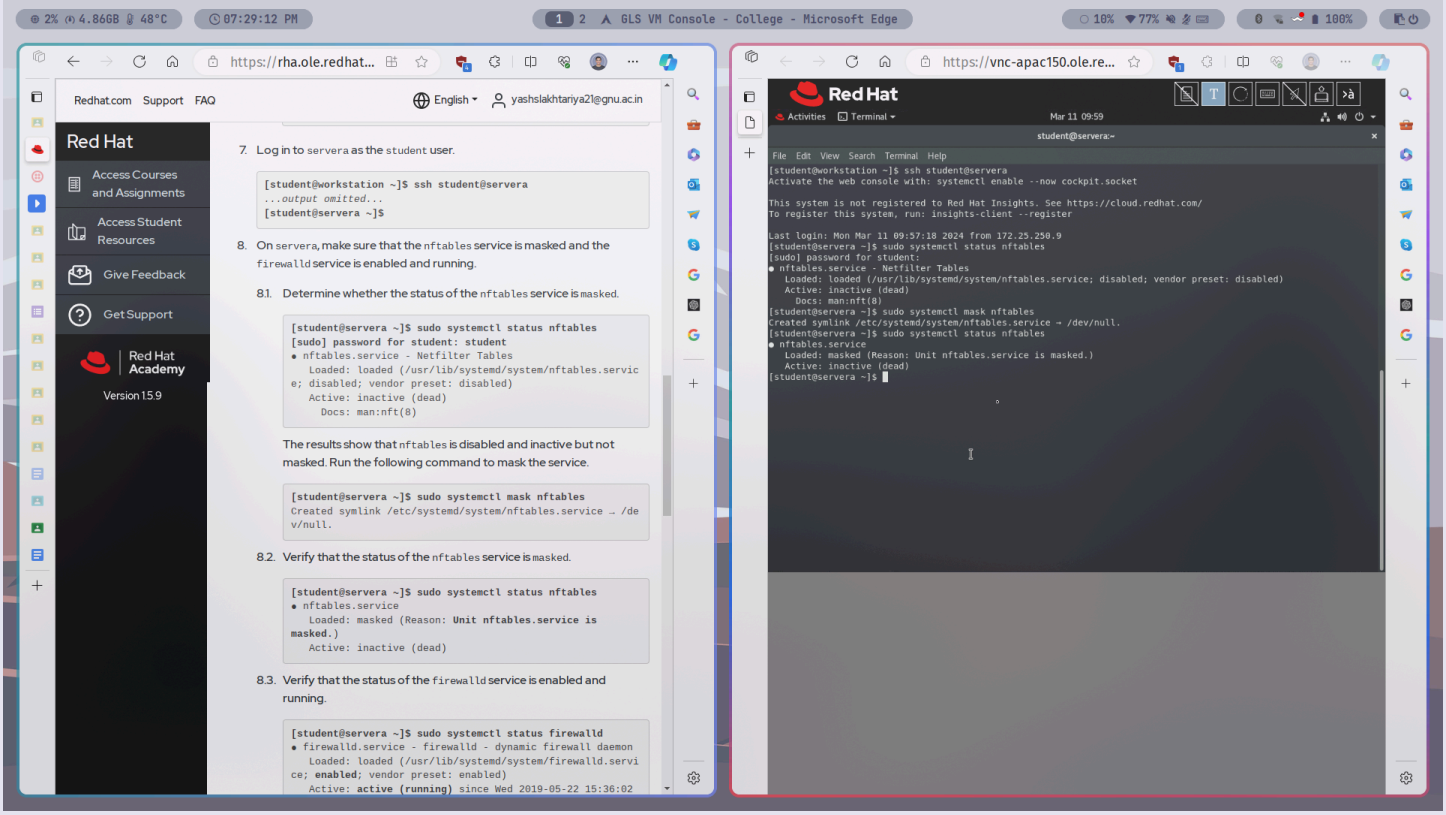
d. Now, login to servera and check the status of nftables service



Commmand : **sudo systemctl status nftables**

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

e. Mask the Netfliter tables service

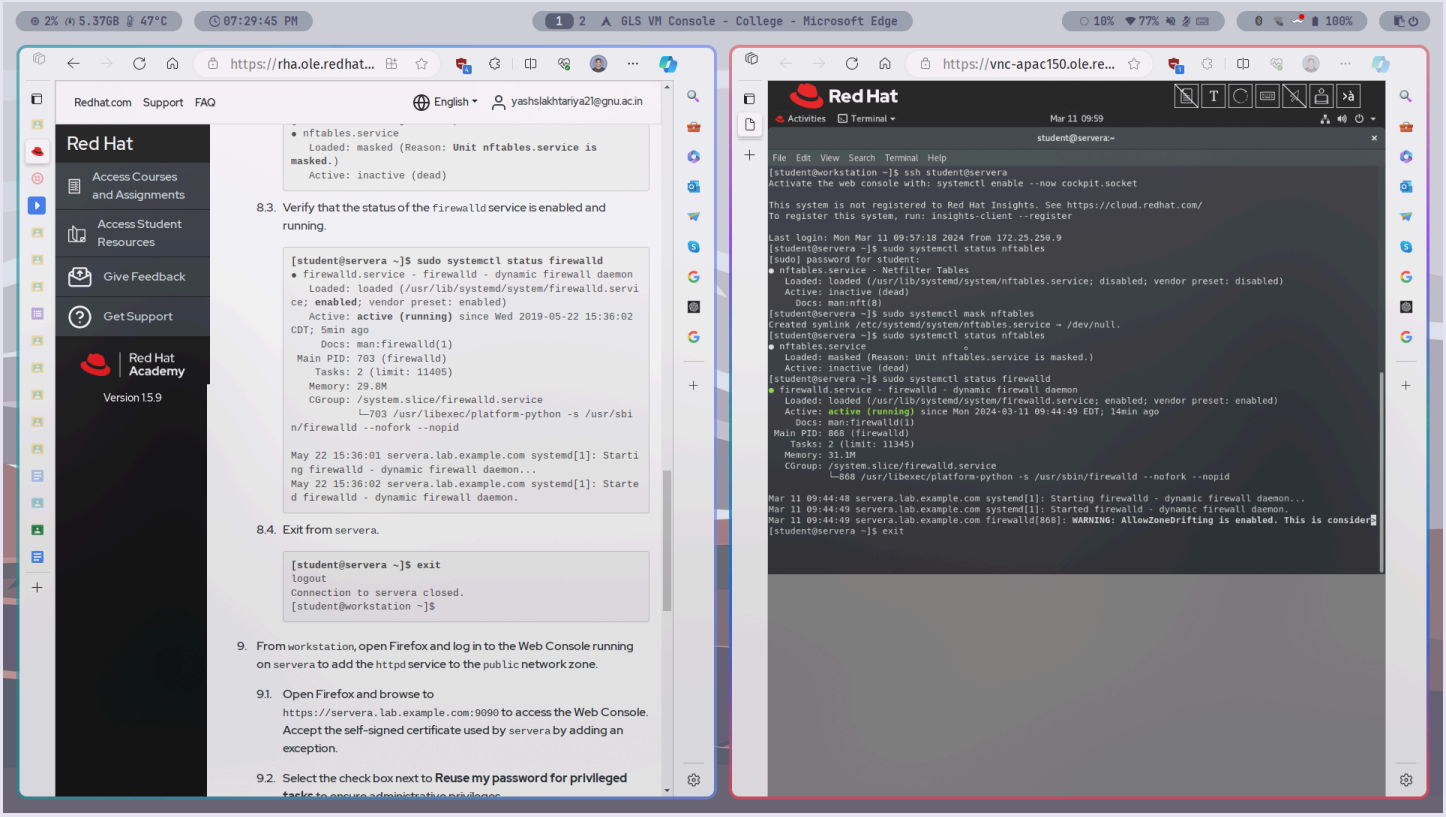


Commands :

- **sudo systemctl mask nftables** (to mask the service given)
- **sudo systemctl status nftables** (to check its status)

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

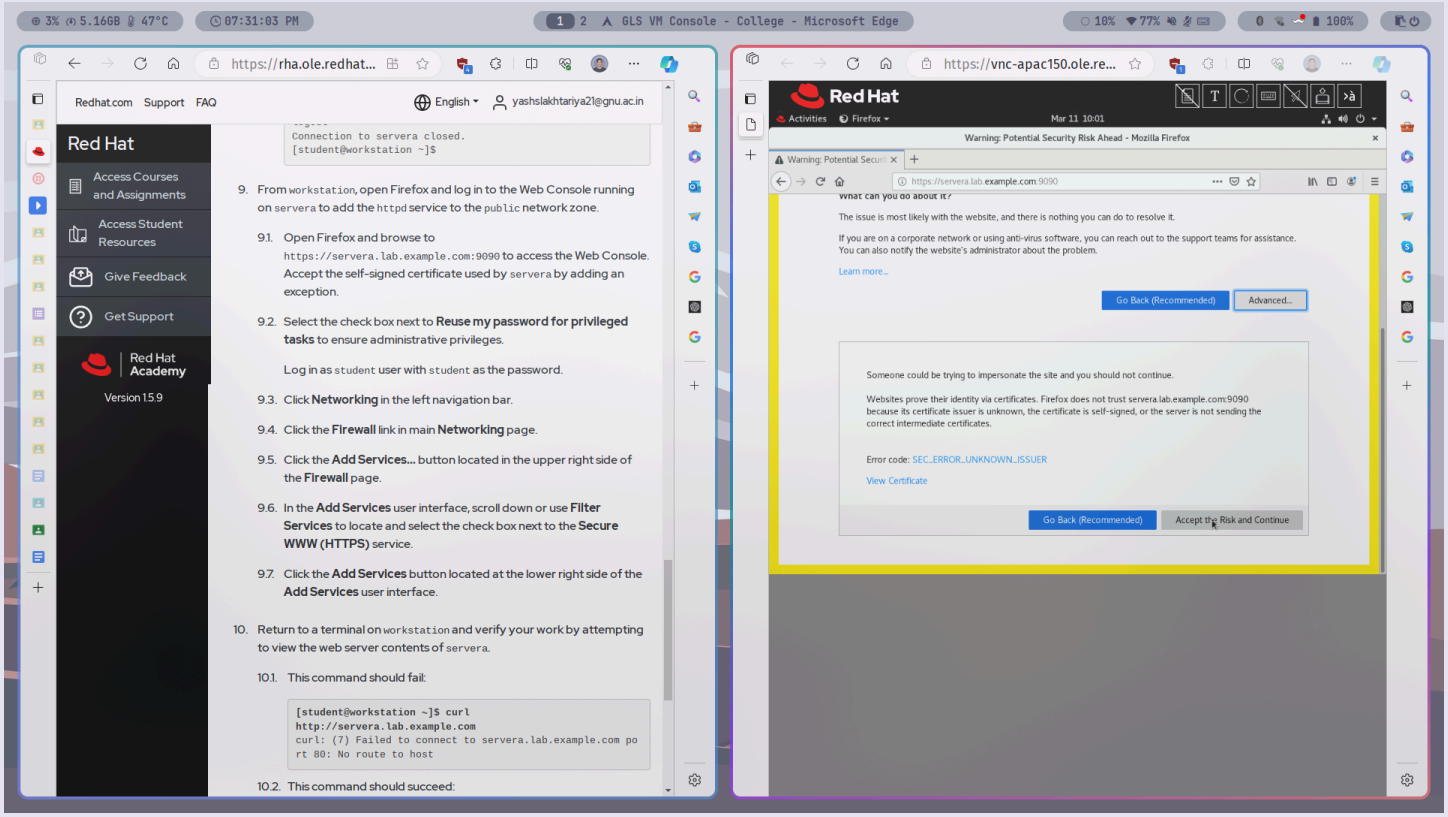
f. Now check the status of firewall daemon and it would be in running state and exit from ssh session



Command : **sudo systemctl status firewalld**

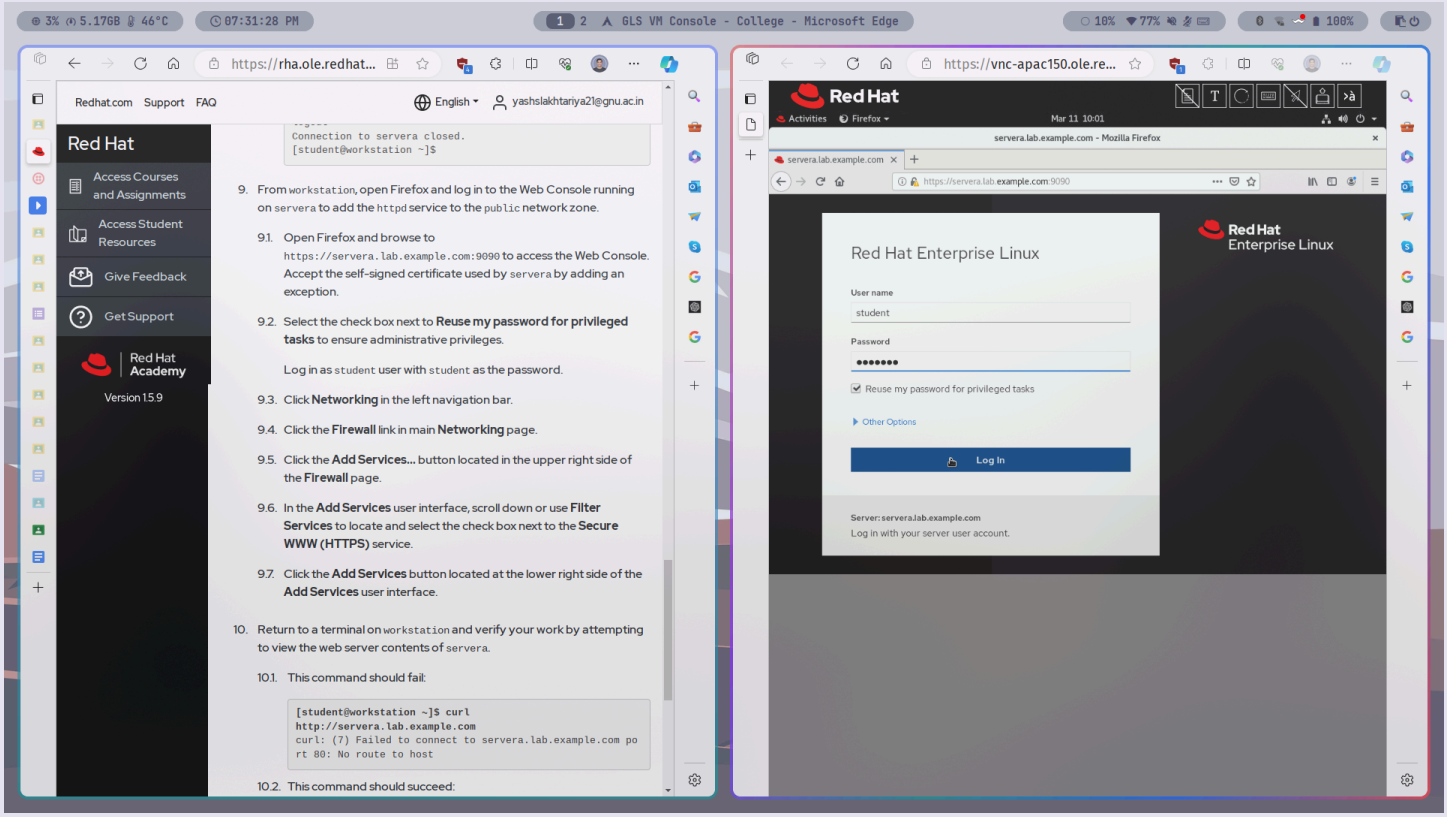
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

g. Now, go to browser and accepting the self-signed certificate, go to servera lab URL with port 9090



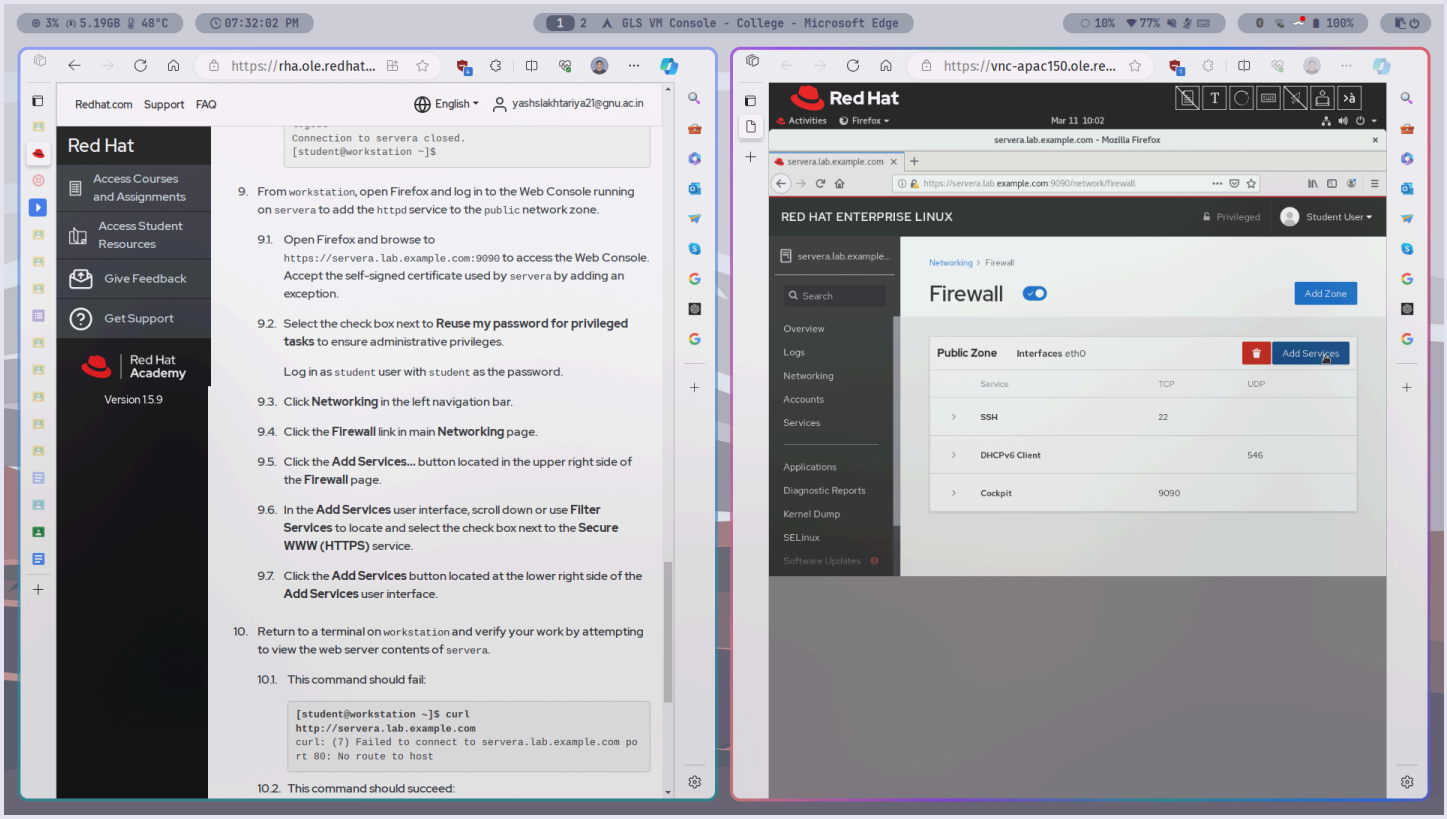
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

h. Login as student with password student and Reuse password forprivileged tasks option enabled



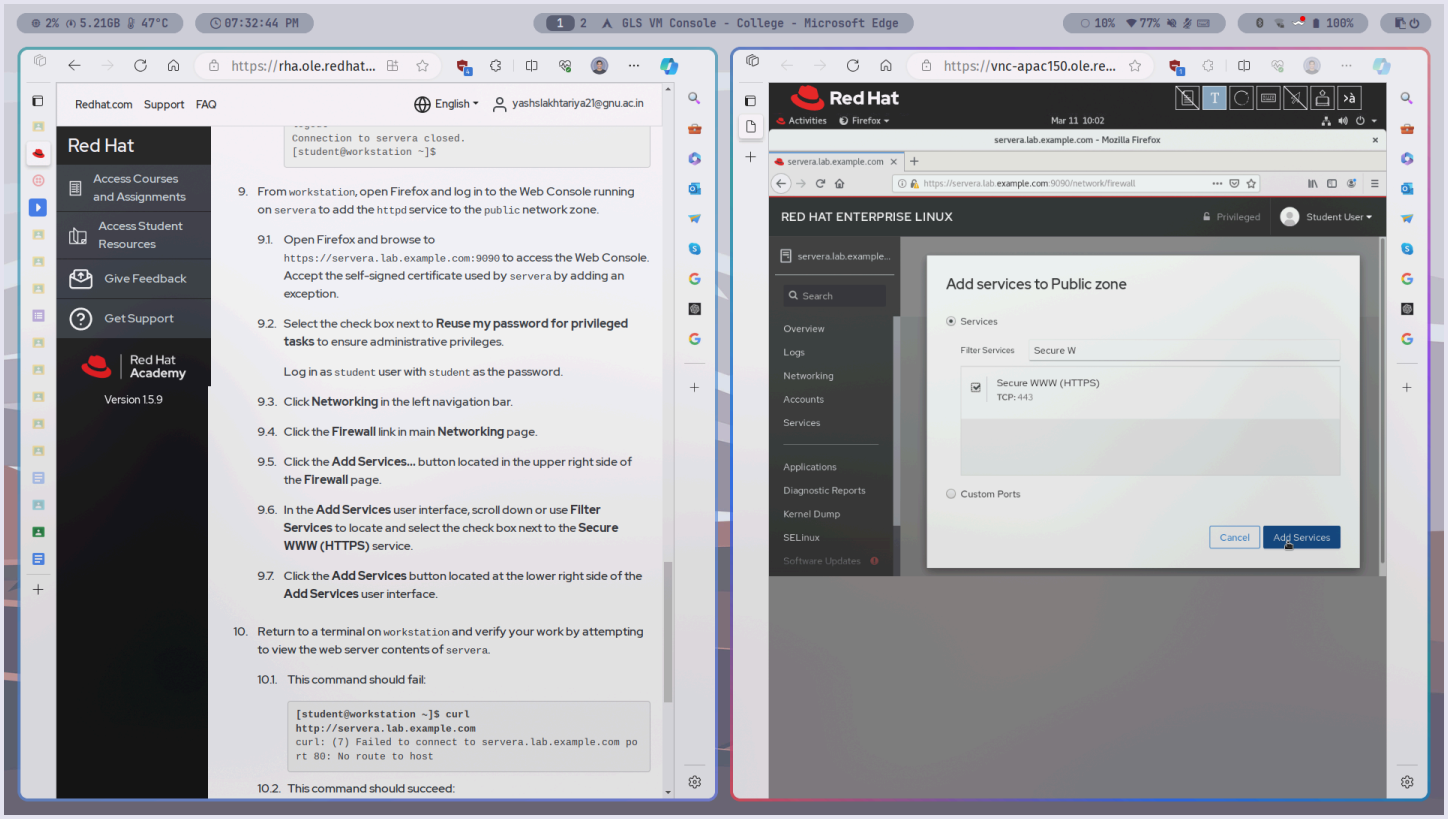
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

i. In Networking, tab go to Firewall and click Add service button



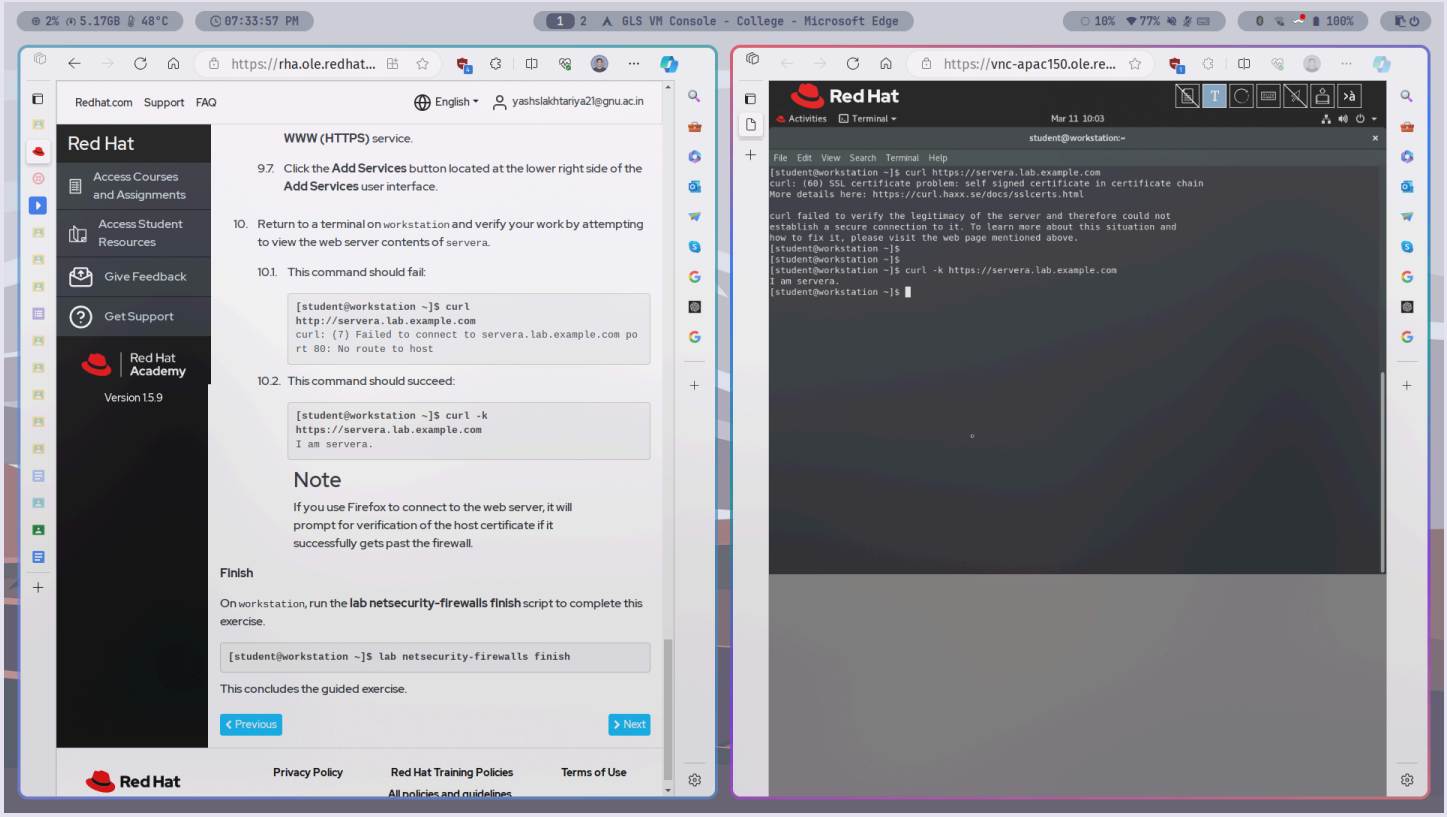
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

j. Search for and add Secure WWW service



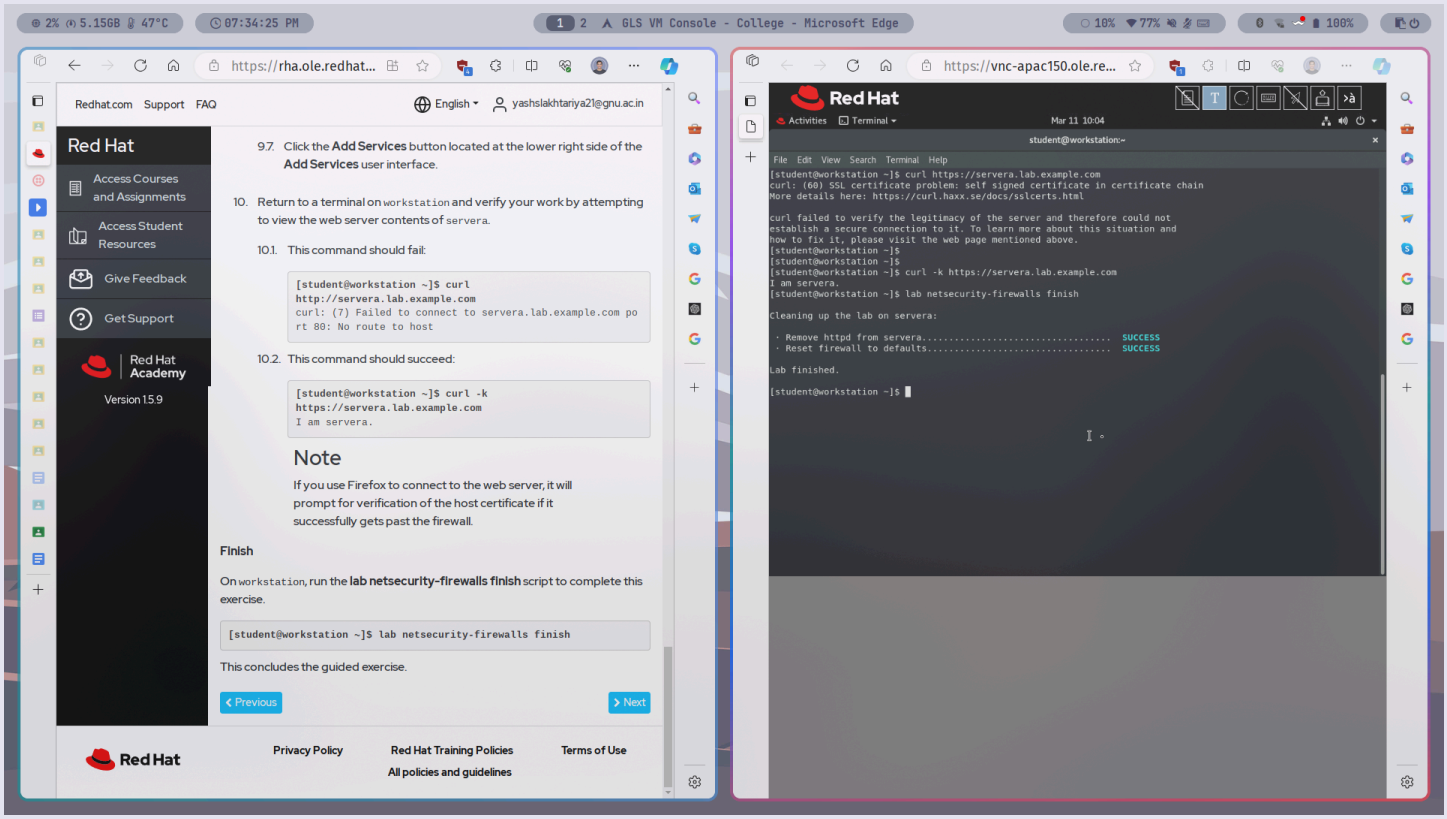
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

k. Now, curl command with secure connection will fail but -k (insecure) will succeed.



Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

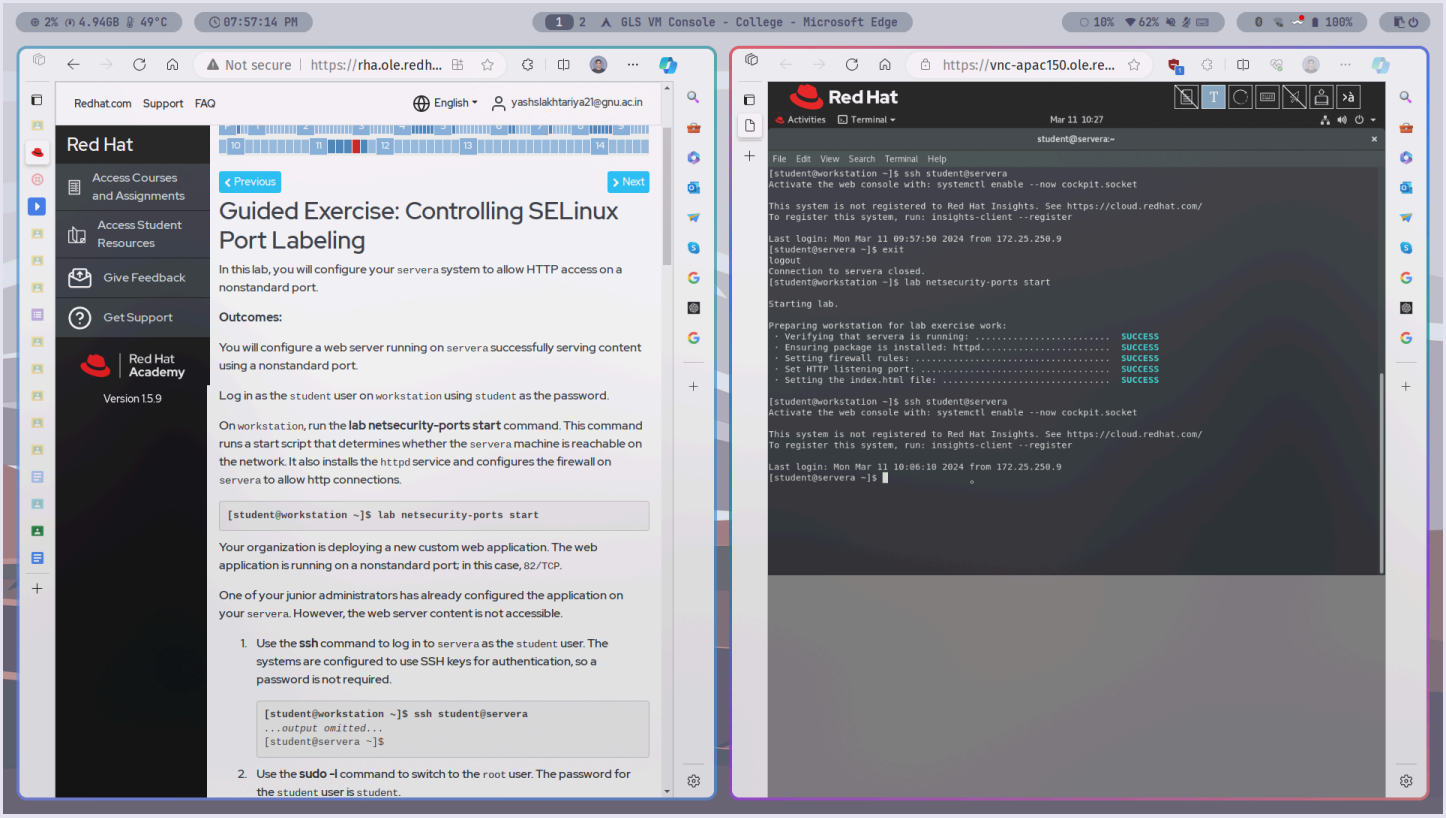
l. Finish the lab and exit from ssh



Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

4) Your organization is deploying a new custom web application. The web application is running on a nonstandard port; in this case, 82/TCP. One of your junior administrators has already configured the application on your servera. However, the web server content is not accessible. (Guided Exercise)

a. Start the lab and login to servera via ssh and switch to root user

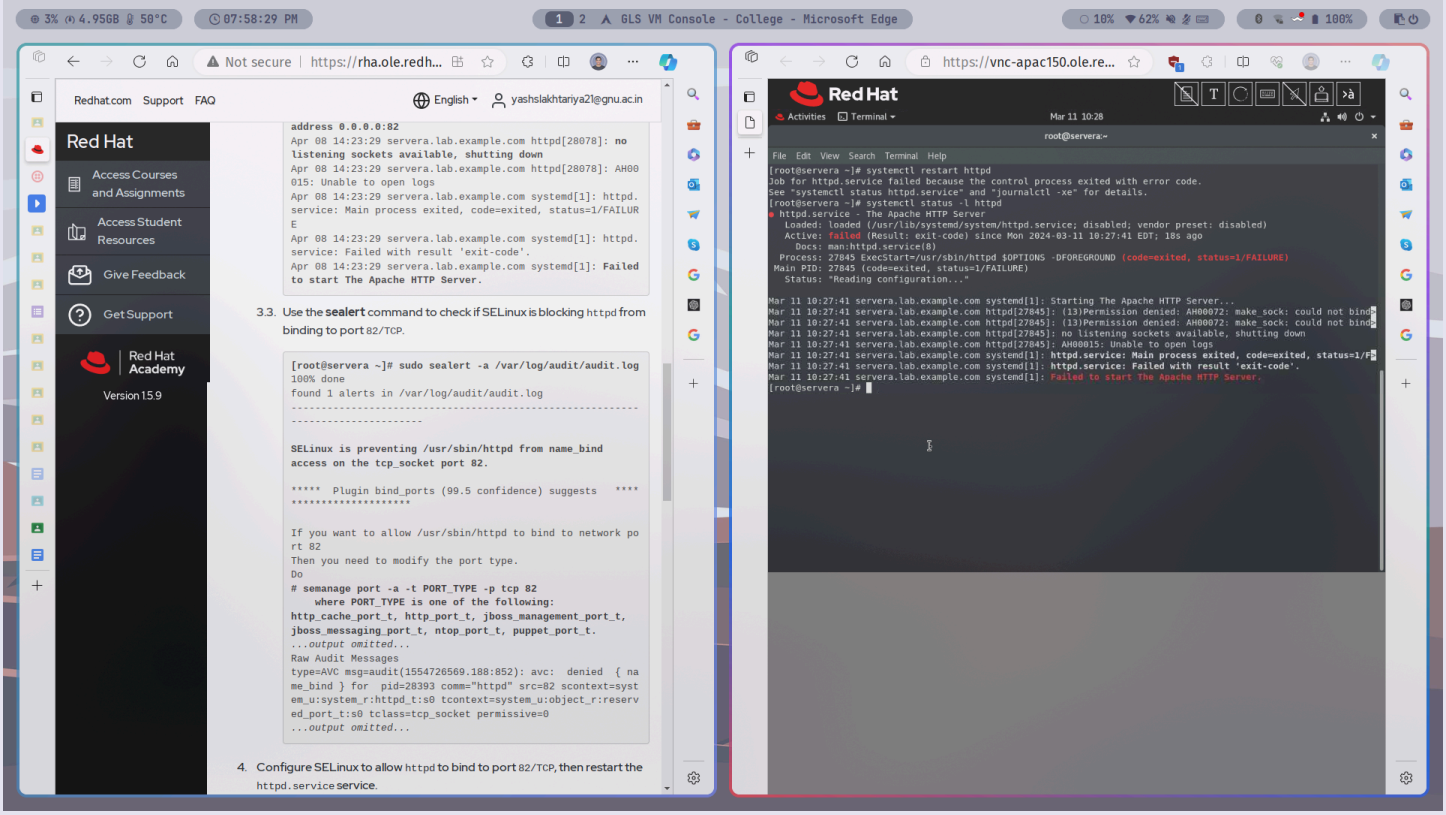


Commands :

- lab netsecurity-ports start
- ssh student@servera
- sudo -i

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

b. Restart httpd service and check the status, it should fail

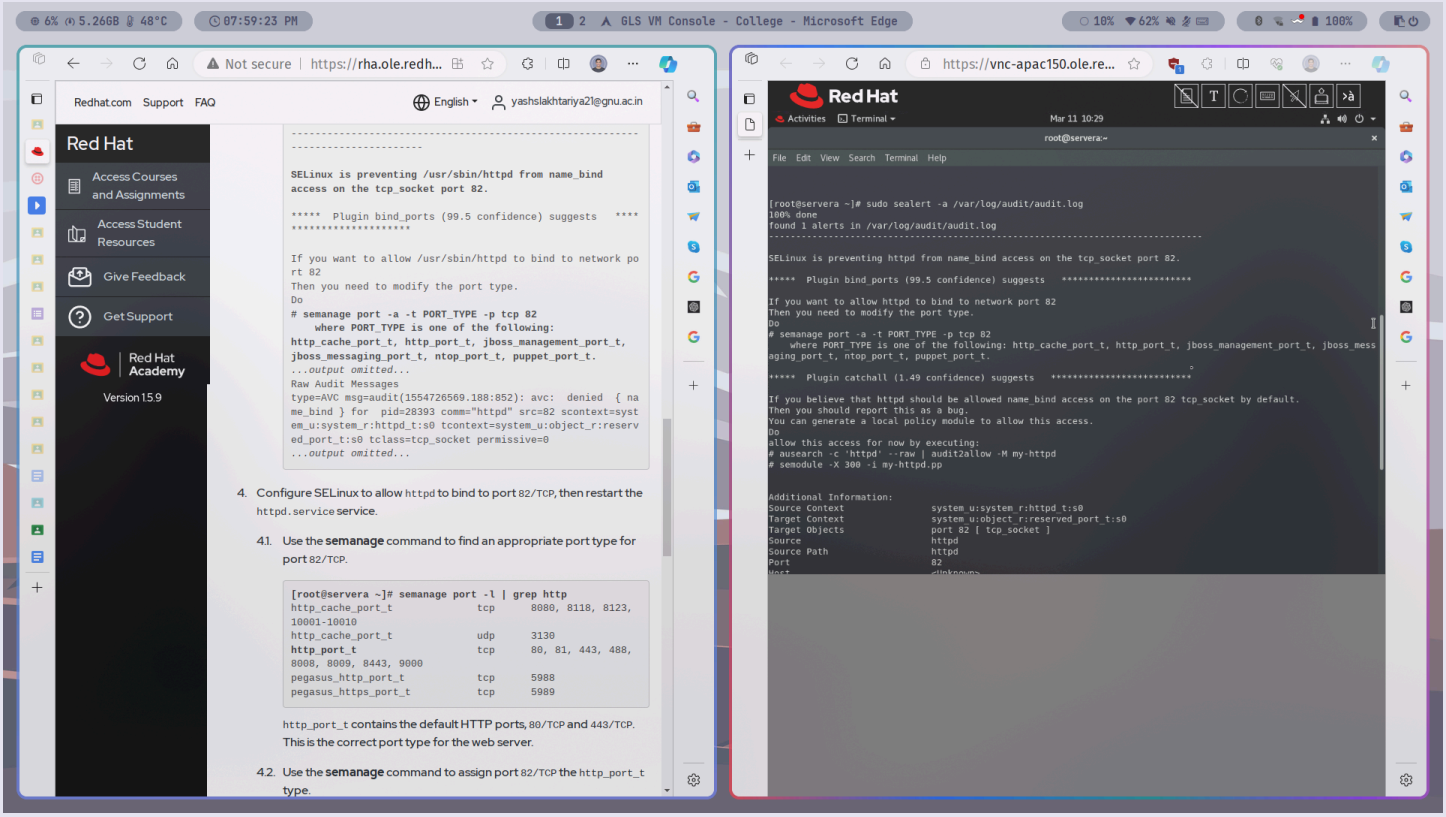


Commands :

- **systemctl restart httpd.service**
- **systemctl status -l httpd.service** (-l stands for giving full output, without elipsizing unit names)

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

c. Use the sealert command to check if SELinux is blocking httpd from binding to port 82/TCP.

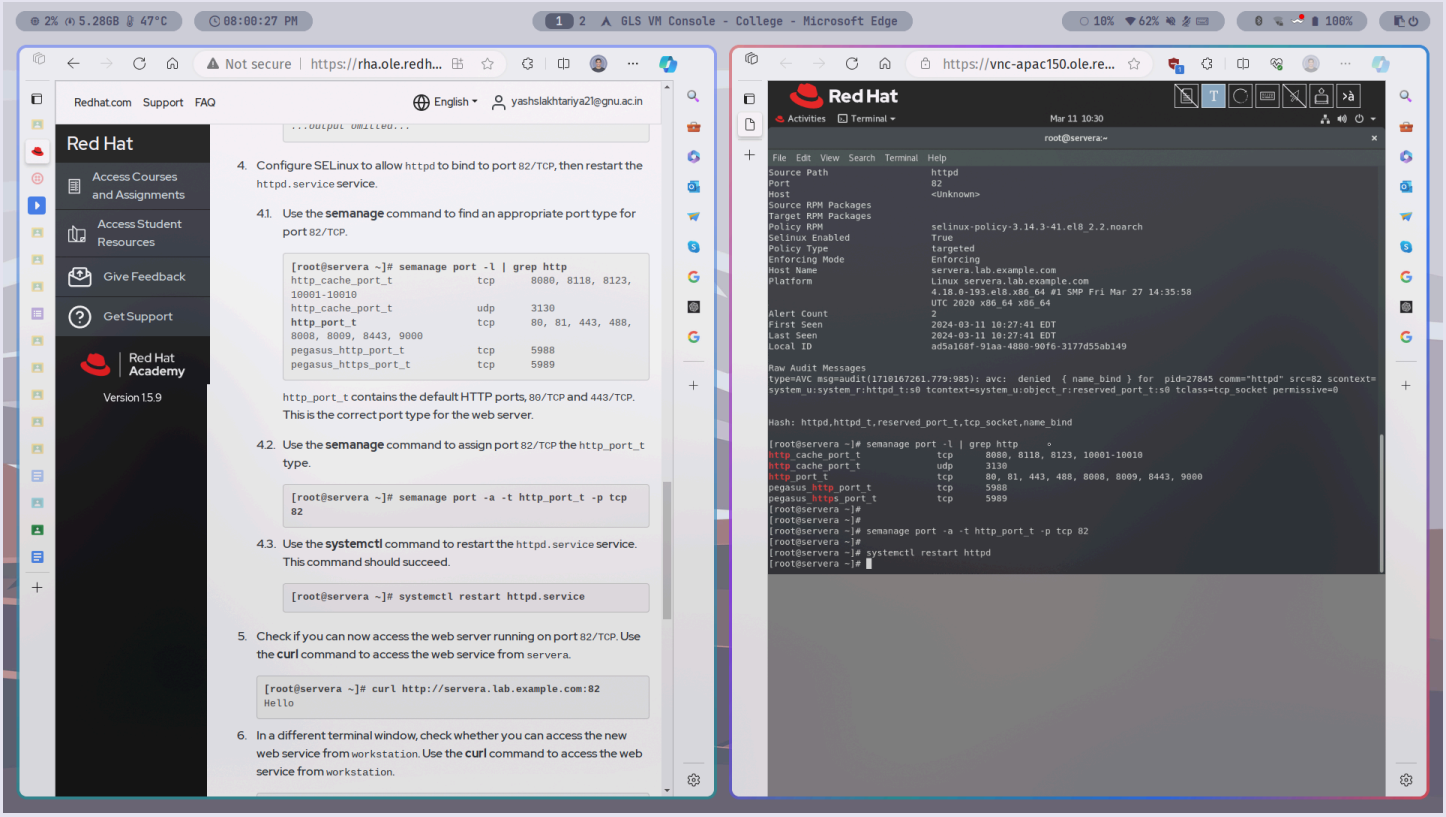


Command : **sudo sealert -a /var/log/audit/audit.log**

Explanation : It records the results of the analysis and signals any clients which have attached to the setroubleshootd daemon that a new alert has been seen. sealert can be run in either a GUI mode or a command line mode. In both instances sealert run as a user process with the privileges associated with the user. The option ***-a*** stands for scanning the log file and analyse it. (Only available for SELinux)

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

d. Use the semanage command to find an appropriate port type for port 82/TCP and restart http daemon

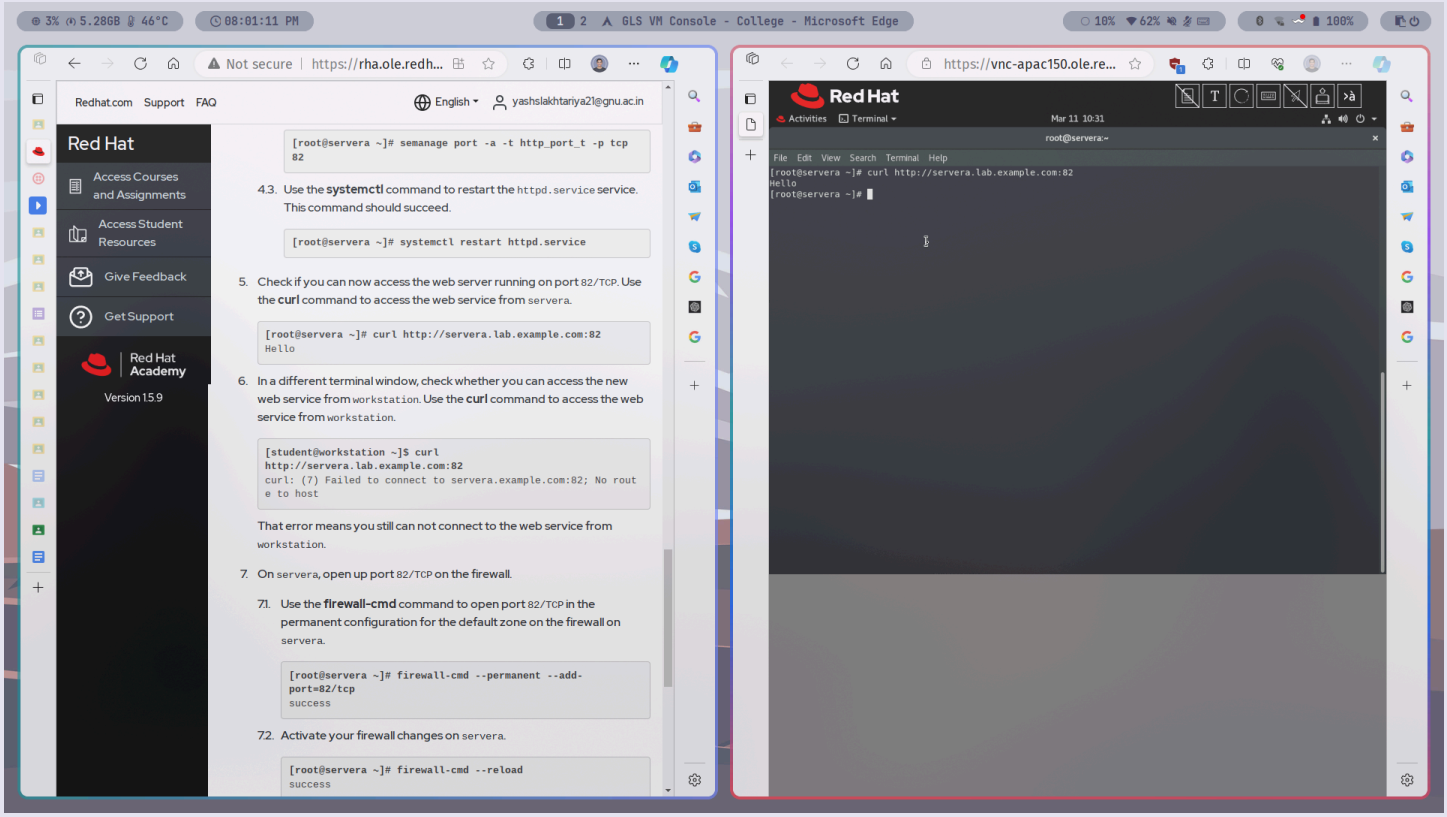


Commands :

- **semanage port -a -t http_port_t -p tcp 82** (SELinux manage command, port to manage port and ***-a*** stands for add object, ***-t*** for object type mentioned here (http_port_t) and ***-p*** for protocol of specified port, here tcp 82
- **systemctl restart httpd**

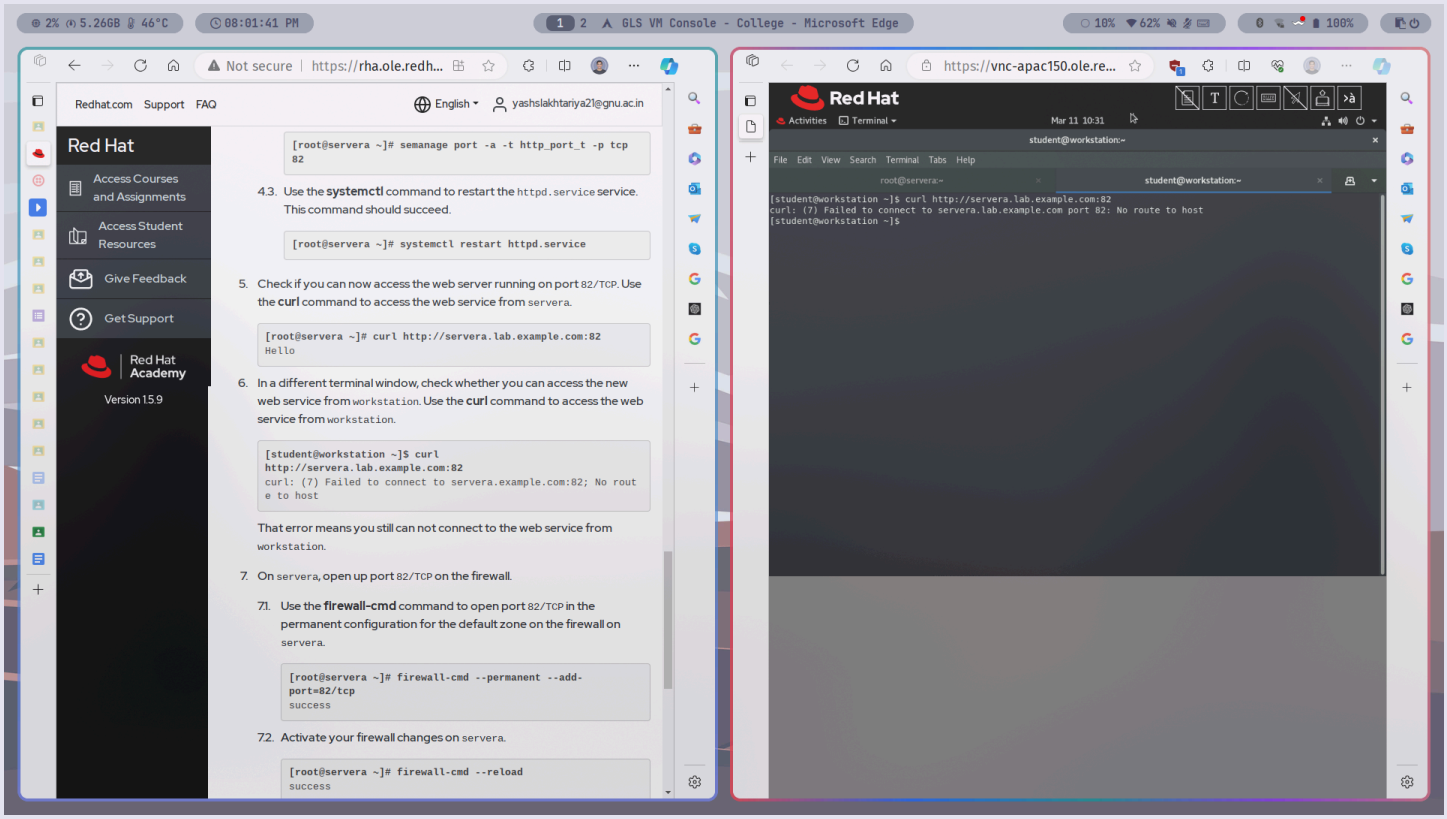
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

e. Now, use curl command to test connection with servera lab URL through port 82



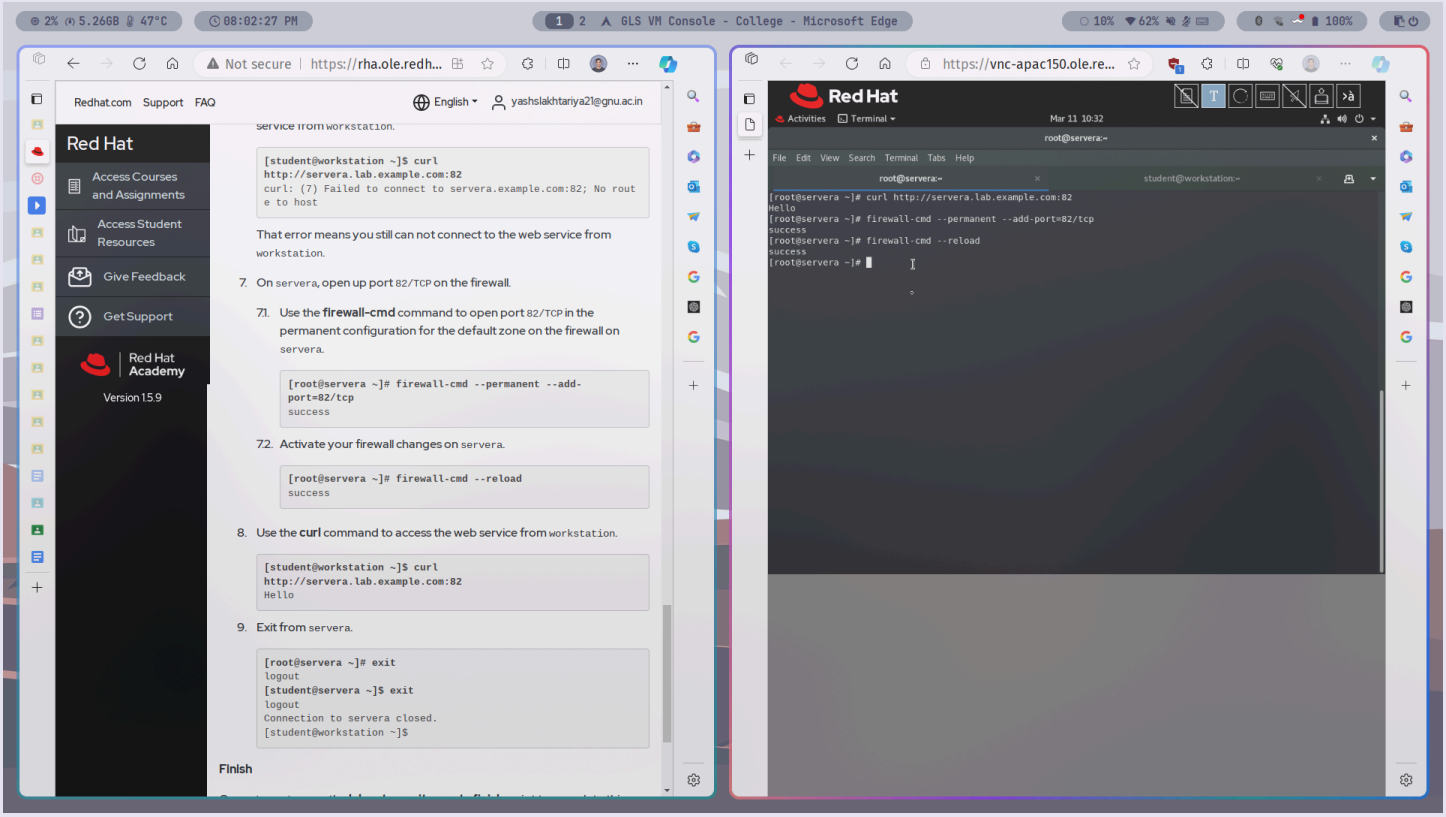
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

f. But, it would fail if tested from workstation



Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

g. Through firewall daemon allow permanently tcp connections over port 82 and reload firewall daemon

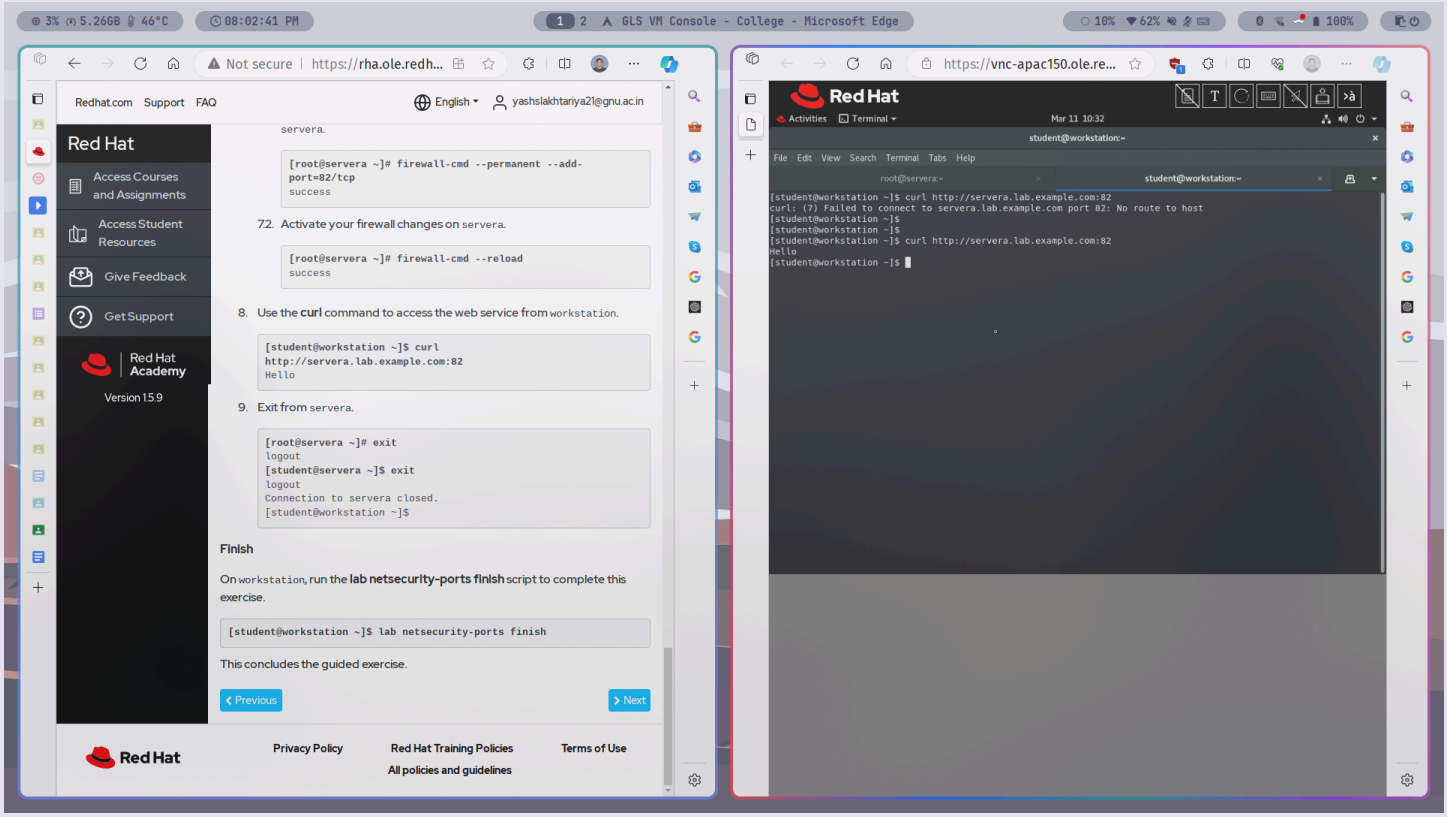


Commands :

- **firewall-cmd --permanent --add-port=82/tcp** (to add port 82 and allow tcp connections permanently)
- **firewall-cmd --reload** (to reload the firewall daemon)

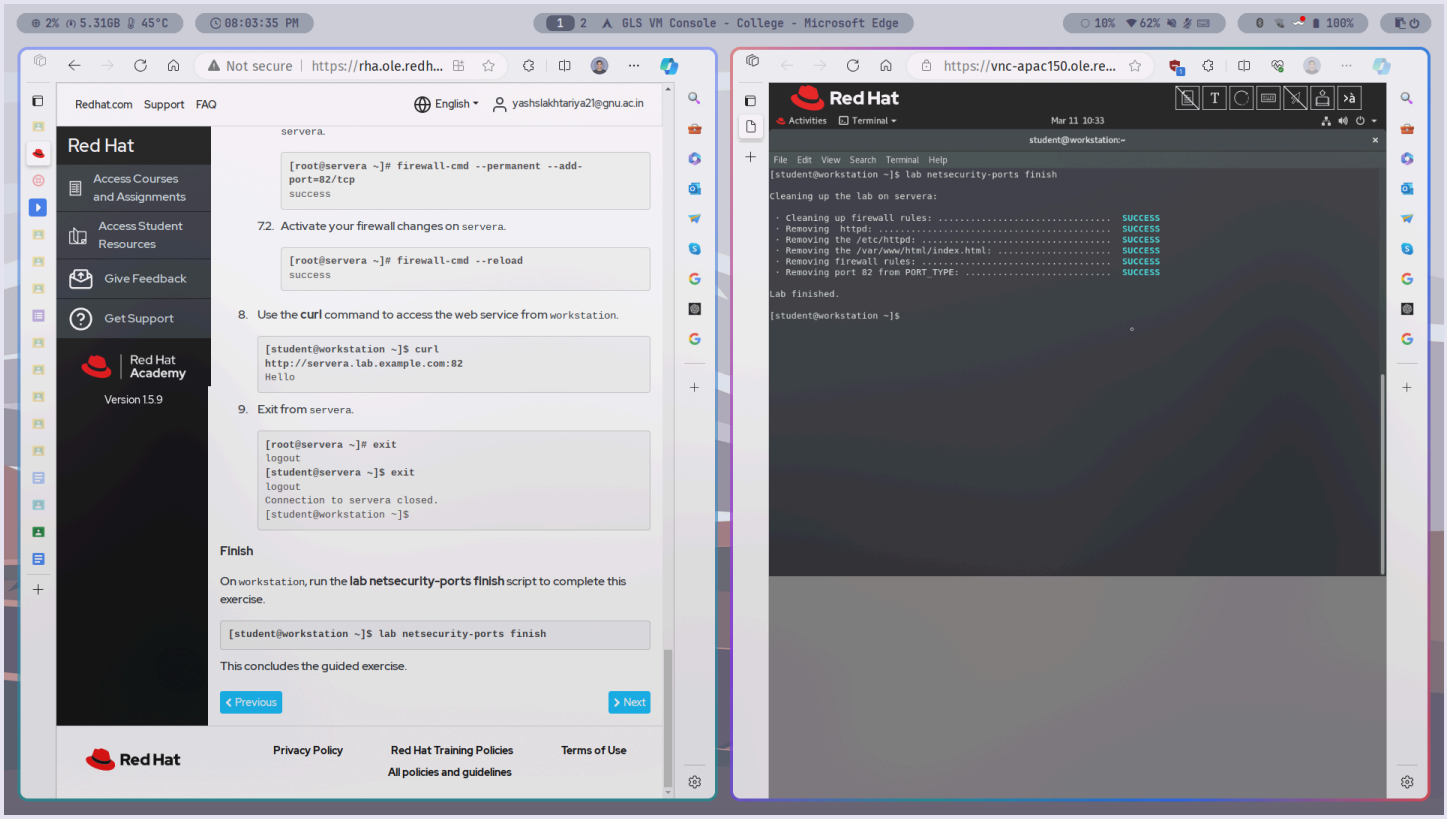
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

h. Now, from workstation also curl command will work for testing connection over tcp port 82



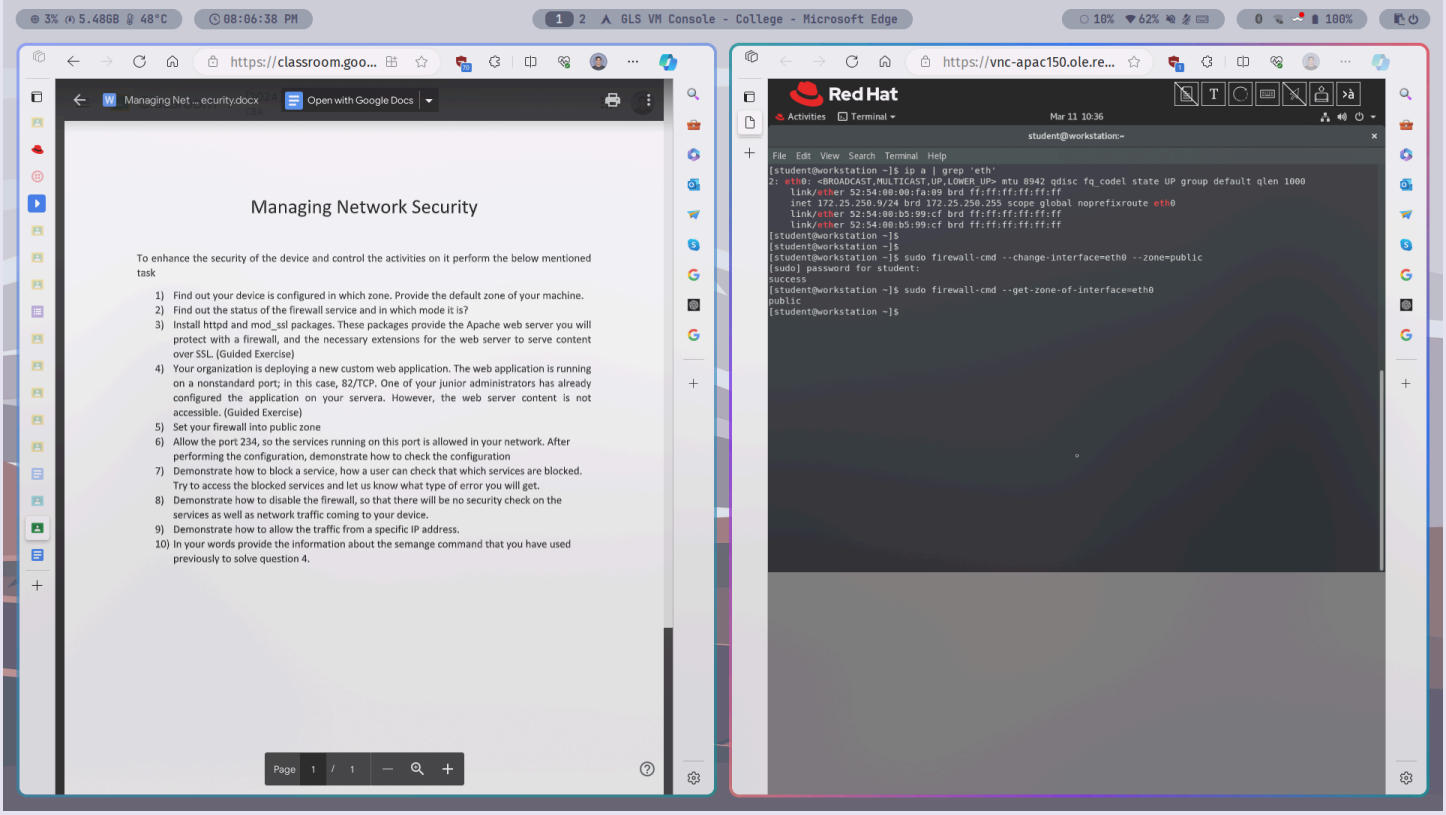
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

i. Finish the lab and exit from ssh



Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

5) Set your firewall into public zone

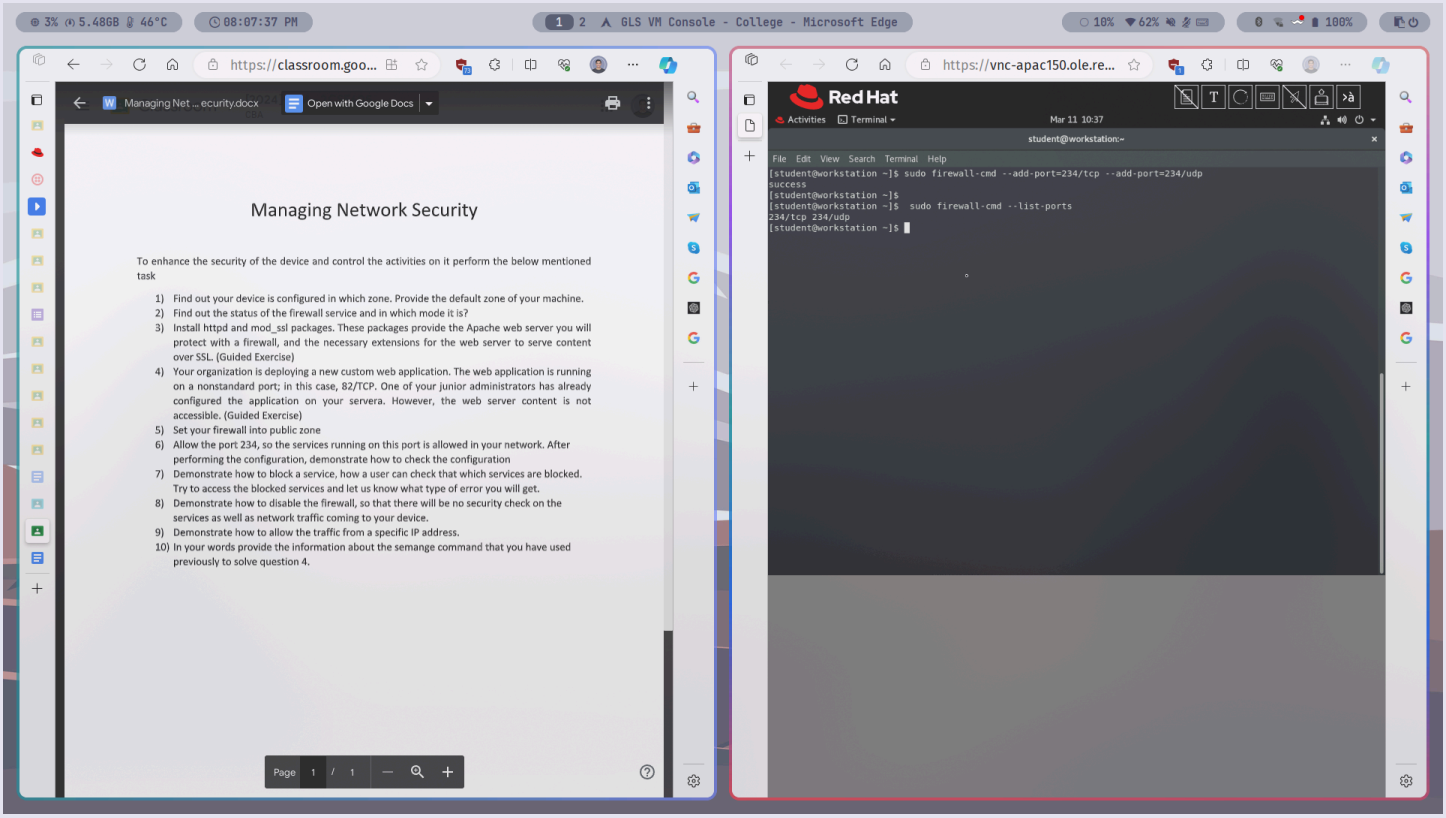


Commands :

- **ip a | grep 'eth'** (to get lines containing eth in output of ip a, which is similar to ifconfig, for showing interface configurations)
- **sudo firewall-cmd --change-interface=eth0 --zone=public** (to change firewall on eth0 interface to public zone)
- **sudo firewall-cmd --get-zone-of-interface=eth0** (to check the zone of specified (eth0) interface)

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

6) Allow the port 234, so the services running on this port is allowed in your network. After performing the configuration, demonstrate how to check the configuration

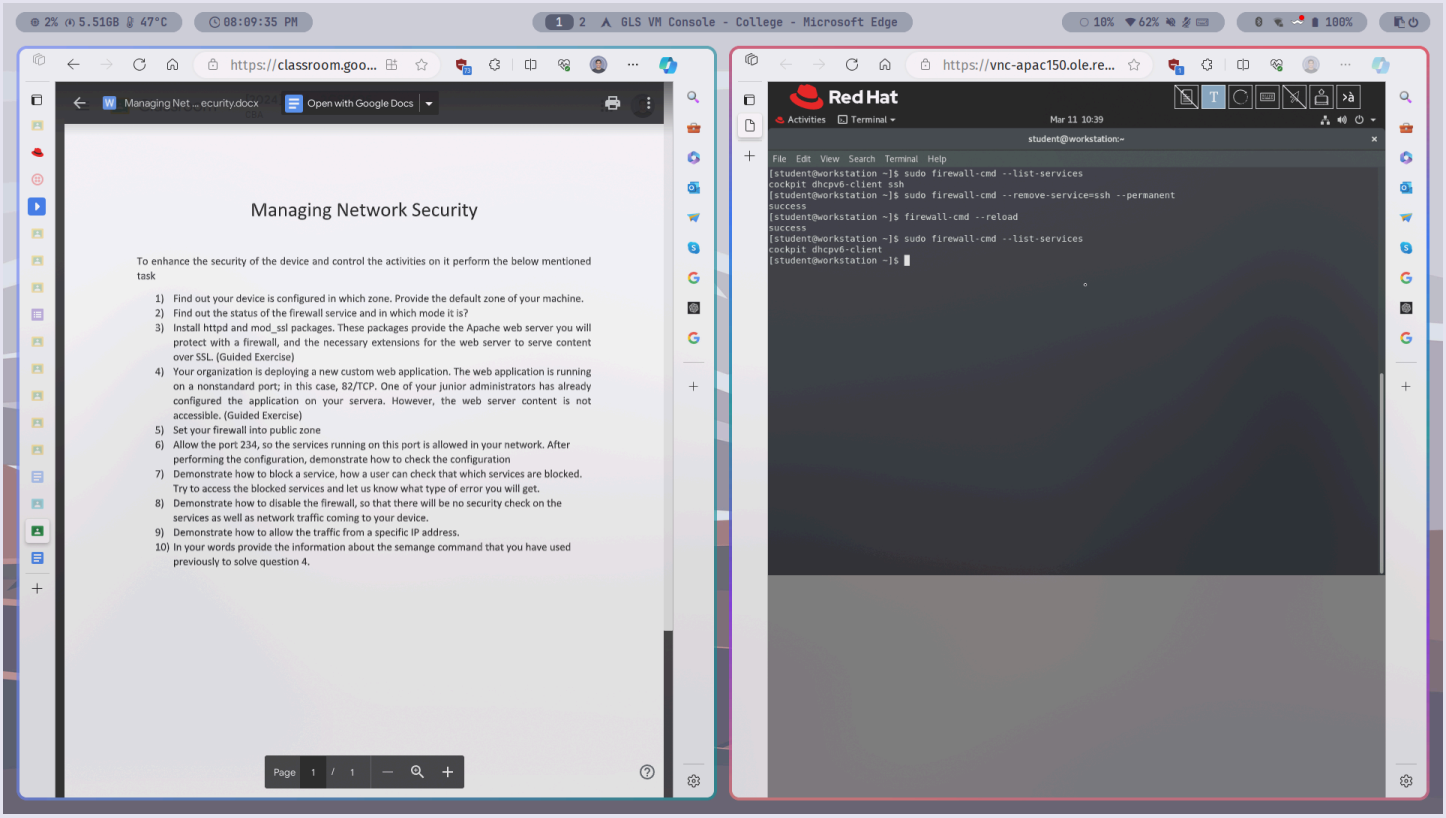


Commands :

- **sudo firewall-cmd --add-port=234/tcp --add-port=234/udp** (to add port 234 for tcp and udp connections)
- **sudo firewall-cmd --list-ports** (to check list of added ports)

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

7) Demonstrate how to block a service, how a user can check that which services are blocked. Try to access the blocked services and let us know what type of error you will get.

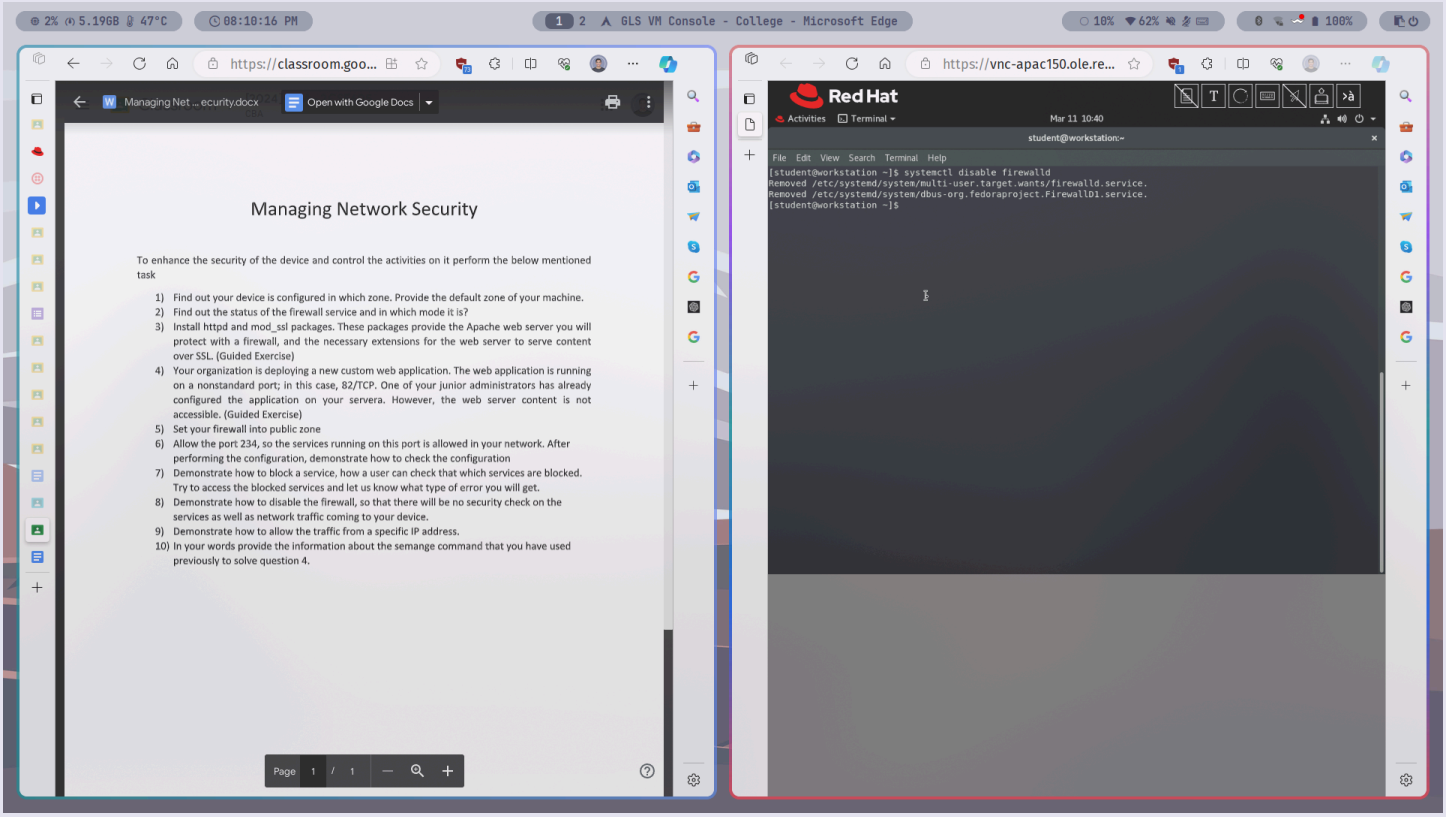


Commands :

- **sudo firewall-cmd --list-services** (to list firewall services)
- **sudo firewall-cmd --remove-service=ssh --permanent** (to remove ssh service permanently)
- **sudo firewall-cmd --reload** (to reload firewall daemon)

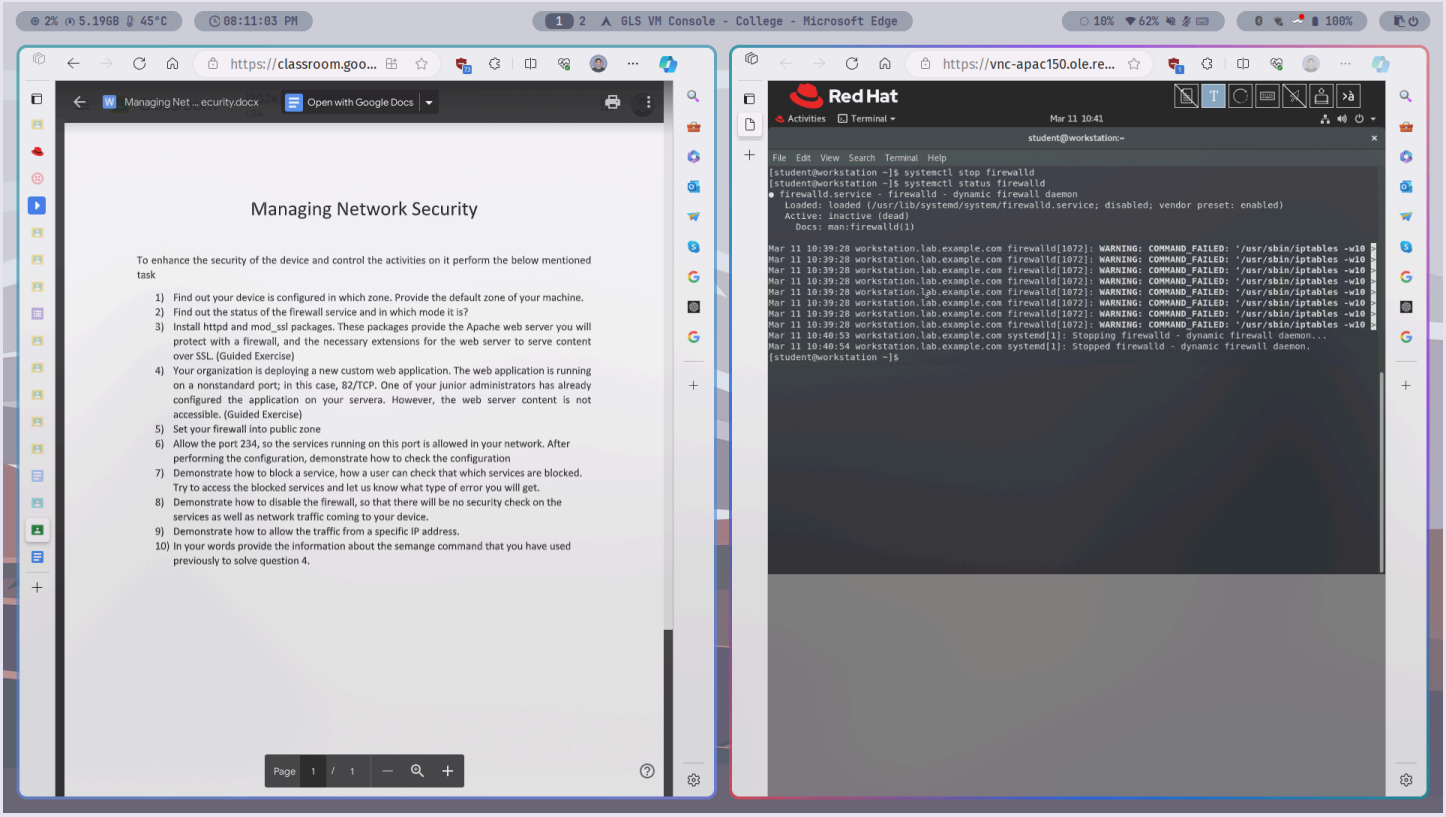
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

8) Demonstrate how to disable the firewall, so that there will be no security check on the services as well as network traffic coming to your device.



Command : **systemctl disable firewalld**

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

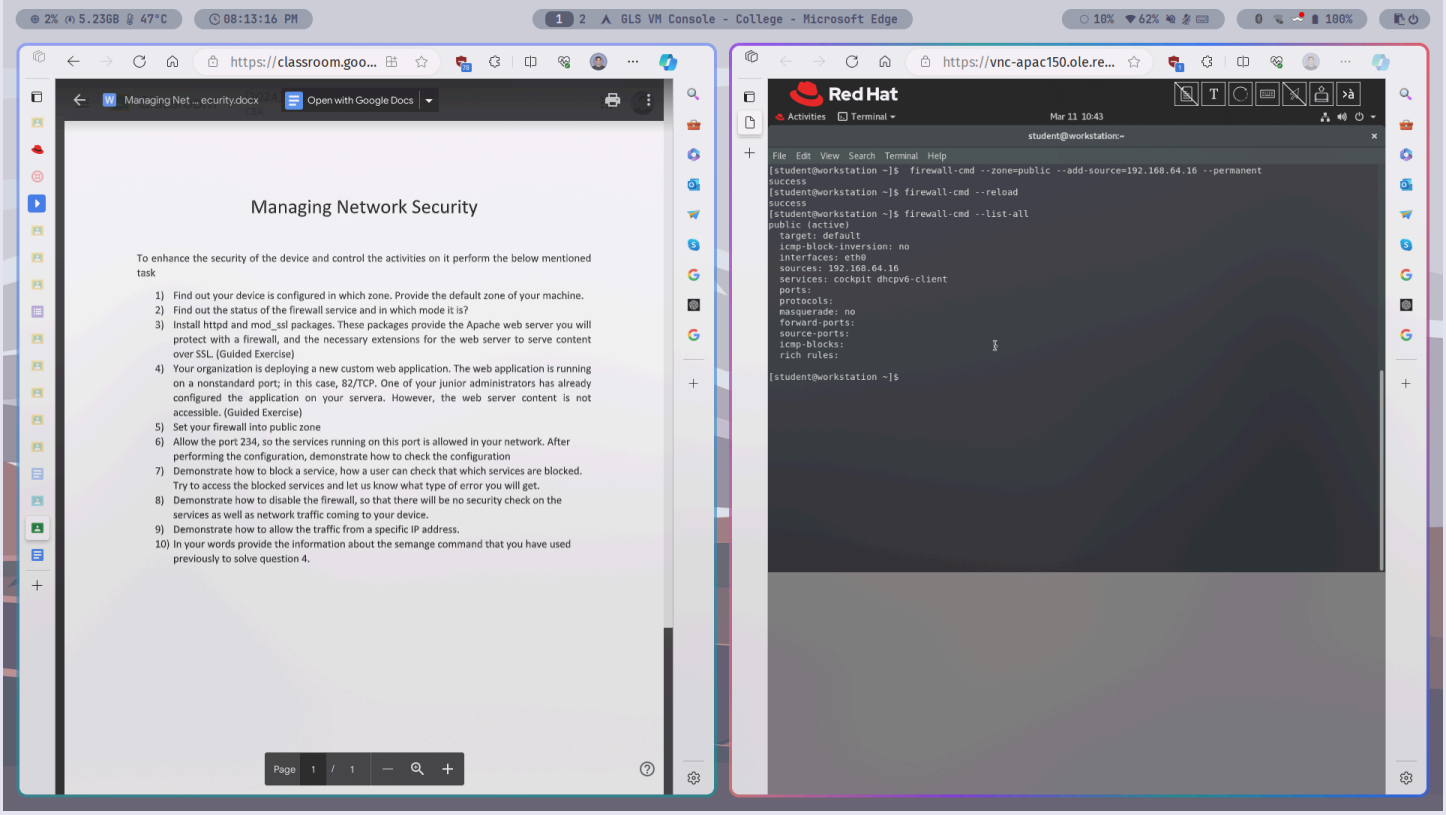


Commands :

- **systemctl stop firewalld**
- **systemctl status firewalld**

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

9) Demonstrate how to allow the traffic from a specific IP address.



Commands :

- **firewall-cmd --zone=public --add-source=192.168.64.16 --permanent** (to add source of IP sepcified and allow it permanently in public zone)
- **firewall-cmd --reload** (to reload the firewall dameon)
- **firewall-cmd --list-all** (to list all details of firewall)

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 9

10) In your words provide the information about the semange command that you have used previously to solve question 4.

→ `semanage` is a handy tool for managing security policies in SELinux environments. It lets you tweak settings like file permissions and port labeling easily. With it, you can add, delete, or change rules to keep your system secure. `semanage` simplifies SELinux configuration, making it accessible without diving into complex policy files. It's a key tool for maintaining system integrity in SELinux setups.

→ Here, specifically, it is used for port policies