



## LAB 5

### DOCKER, SAMBA, DNS và Firewall

Họ tên và MSSV: Trương Đặng Trúc Lâm B2111933

Nhóm học phần: M03

*- Các sinh viên bị phát hiện sao chép bài của nhau sẽ nhận 0đ cho tất cả bài thực hành của môn này.*

*- Bài nộp phải ở dạng PDF, hình minh họa phải rõ ràng chi tiết.*

#### 1. Triển khai dịch vụ WEB sử dụng Docker

1.1. Thực hiện cài đặt CentOS 9 vào máy tính cá nhân (hoặc máy ảo).

1.2. Cấu hình mạng cho máy ảo giao tiếp được với máy vật lý và kết nối được vào Internet. (Câu 2 - Lab04)

```
B2111933@localhost:~  
[B2111933@myserver ~]$ ifconfig  
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.250 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::a00:27ff:fede:3b4 prefixlen 64 scopeid 0x20<link>  
    inet6 2402:800:6390:f1d2:a00:27ff:fede:3b4 prefixlen 64 scopeid 0x0<global>  
    ether 08:00:27:de:03:b4 txqueuelen 1000 (Ethernet)  
    RX packets 869721 bytes 1288281754 (1.1 GiB)  
    RX errors 0 dropped 29 overruns 0 frame 0  
    TX packets 289185 bytes 27572652 (26.2 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Cấu hình mạng của máy ảo CentOS

```
C:\Windows\system32\cmd.exe  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Users\Admin>ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Local Area Connection:  
  
    Connection-specific DNS Suffix . :  
    IPv4 Address. . . . . : 192.168.1.10  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . : 192.168.1.1
```

Cấu hình mạng của máy vật lý

```
B2111933@localhost:~  
[B2111933@myserver ~]$ ping -c 3 192.168.1.10  
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.  
64 bytes from 192.168.1.10: icmp_seq=1 ttl=128 time=0.727 ms  
64 bytes from 192.168.1.10: icmp_seq=2 ttl=128 time=0.515 ms  
64 bytes from 192.168.1.10: icmp_seq=3 ttl=128 time=0.464 ms  
  
--- 192.168.1.10 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2005ms  
rtt min/avg/max/mdev = 0.464/0.568/0.727/0.113 ms  
[B2111933@myserver ~]$  
  
C:\Users\Admin>ping 192.168.1.250  
  
Pinging 192.168.1.250 with 32 bytes of data:  
Reply from 192.168.1.250: bytes=32 time<1ms TTL=64  
Reply from 192.168.1.250: bytes=32 time<1ms TTL=64  
Reply from 192.168.1.250: bytes=32 time<1ms TTL=64  
Reply from 192.168.1.250: bytes=32 time<1ms TTL=64  
  
Ping statistics for 192.168.1.250:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 0ms, Average = 0ms  
  
C:\Users\Admin>
```

Kết nối giữa hai máy là thông thoáng.

```
B2111933@localhost:~  
[B2111933@myserver ~]$ ping -c 3 google.com  
PING google.com(hkg07s46-in-x0e.1e100.net (2404:6800:4005:804::200e)) 56 data bytes  
64 bytes from hkg12s09-in-x0e.1e100.net (2404:6800:4005:804::200e): icmp_seq=1 ttl=57 time=64.1 ms  
64 bytes from hkg12s09-in-x0e.1e100.net (2404:6800:4005:804::200e): icmp_seq=2 ttl=57 time=62.8 ms  
64 bytes from hkg07s46-in-x0e.1e100.net (2404:6800:4005:804::200e): icmp_seq=3 ttl=57 time=62.7 ms  
  
--- google.com ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2004ms  
rtt min/avg/max/mdev = 62.680/63.177/64.103/0.654 ms  
[B2111933@myserver ~]$
```

Máy CentOS có thể kết nối Internet.

- 1.3. Tạo thư mục ~/myweb, sau đó tạo một trang web đơn giản index.html lưu vào thư mục ~/myweb.(Câu 6 - Lab04)

Tắt tường lửa:

```
$sudo systemctl stop firewalld
```

```
B2111933@localhost:~  
[B2111933@myserver ~]$ pwd  
/home/B2111933  
[B2111933@myserver ~]$ mkdir myweb  
[B2111933@myserver ~]$ ls  
104247203_255166992412777_352350681687680961_n.jpg  Desktop  index.html  myweb  qwerty  
ABC  Documents  info.sh  Pictures  Templates  
backup.sh  Downloads  Music  Public  Videos  
[B2111933@myserver ~]$
```

Tạo thư mục **myweb**

```
B2111933@localhost:~  
[B2111933@myserver ~]$ mv index.html myweb  
[B2111933@myserver ~]$ ls myweb  
index.html  
[B2111933@myserver ~]$
```

Di chuyển tập tin **index.html** ở **Lab 4** vào thư mục **myweb**

```
B2111933@localhost:~  
[B2111933@myserver ~]$ sudo systemctl stop firewalld  
[sudo] password for B2111933:  
[B2111933@myserver ~]$ sudo systemctl status firewalld  
● firewalld.service - firewalld - dynamic firewall daemon  
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)  
   Active: inactive (dead) since Tue 2023-04-04 00:41:46 +07; 49min ago  
     Duration: 1month 5d 2h 53min 49.219s  
    Docs: man:firewalld(1)  
   Main PID: 790 (code=exited, status=0/SUCCESS)  
    CPU: 905ms
```

Tắt **tường lửa** và kiểm tra trạng thái của **tường lửa**

**Tìm hiểu và thực hiện các yêu cầu sau (kèm hình minh họa cho từng bước):**

**1.4. Cài đặt Docker lên máy ảo CentOS 9**

- Gỡ bỏ PodMan (do sẽ đụng độ với Docker)

```
$sudo dnf -y remove podman runc
```

```
B2111933@localhost:~  
[B2111933@myserver ~]$ sudo dnf -y remove podman runc  
[sudo] password for B2111933:  
Dependencies resolved.  
=====
```

Package	Architecture	Version	Repository
Removing:			
podman	x86_64	2:4.4.0-1.el9	@appstream
runc	x86_64	4:1.1.4-1.el9	@appstream

```
=====
```

```
Verifying      : podman-2:4.4.0-1.el9.x86_64
Verifying      : runc-4:1.1.4-1.el9.x86_64
Verifying      : shadow-utils-subid-2:4.9-6.el9.x86_64

Removed:
cockpit-podman-61-1.el9.noarch common-2:2.1.5-1.el9.x86_64
runc-4:1.1.4-1.el9.x86_64      shadow-utils-subid-2:4.9-6.el9.x86_64

Complete!
[B2111933@myserver ~]$
```

**PodMan** là một nền tảng ảo hóa cho phép ta tạo các container tương tự như **Docker**  
Ta cần phải xóa **PodMan** để tránh đụng độ với **Docker**

- Cài đặt công cụ yum-utils

```
$sudo dnf install -y yum-utils
```

```
B2111933@localhost:~
[B2111933@myserver ~]$ sudo dnf install -y yum-utils
Last metadata expiration check: 0:29:07 ago on Tue 04 Apr 2023 01:32:05 AM +07.
Dependencies resolved.
=====
Package                        Architecture      Version           Repository
=====
Installing:
yum-utils                      noarch            4.3.0-4.el9      baseos

Running transaction
Preparing      :
Installing     : yum-utils-4.3.0-4.el9.noarch
Running scriptlet: yum-utils-4.3.0-4.el9.noarch
Verifying      : yum-utils-4.3.0-4.el9.noarch

Installed:
yum-utils-4.3.0-4.el9.noarch

Complete!
[B2111933@myserver ~]$
```

Cài đặt thành công công cụ **yum-utils**

- Thêm địa repo của Docker vào công cụ yum

```
$sudo yum-config-manager \
--add-repo \
https://download.docker.com/linux/centos/docker-ce.repo
#Viết liên tục lệnh trên hoặc xuống hàng bằng enter.
```

```
B2111933@localhost:~  
[B2111933@myserver ~]$ sudo yum-config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo  
Adding repo from: https://download.docker.com/linux/centos/docker-ce.repo  
[B2111933@myserver ~]$
```

Thêm thành công địa chỉ repository của Docker vào công cụ yum

- Cài đặt Docker

`$sudo dnf install docker-ce -y`

```
B2111933@localhost:~ — sudo dnf install docker-ce -y  
[B2111933@myserver ~]$ sudo dnf install docker-ce -y  
Docker CE Stable - x86_64 68 kB/s | 21 kB 00:00  
Dependencies resolved.  
=====
```

Package	Arch	Version	Repository	Size
docker-ce-3:23.0.2-1.el9.x86_64				
docker-ce-cli-1:23.0.2-1.el9.x86_64				
docker-ce-rootless-extras-23.0.2-1.el9.x86_64				
docker-compose-plugin-2.17.2-1.el9.x86_64				
docker-scan-plugin-0.23.0-3.el9.x86_64				

```
Complete!  
[B2111933@myserver ~]$
```

Cài đặt Docker thành công.

- Thêm người dùng hiện tại vào nhóm docker để sử dụng các lệnh của Docker mà không cần quyền sudo

`$sudo usermod -aG docker $USER`

```
B2111933@localhost:~  
[B2111933@myserver ~]$ sudo usermod -aG docker B2111933  
[B2111933@myserver ~]$ groups B2111933  
B2111933 : B2111933 wheel docker  
[B2111933@myserver ~]$
```

Sau khi cài đặt Docker vào CentOS 9 thì nhóm docker sẽ được tạo ra. Để sử dụng các lệnh của Docker mà không cần quyền sudo thì ta thêm người dùng vào nhóm docker

- Login lại vào shell để việc thêm người dùng vào nhóm có tác dụng

`$su - $USER`

```
B2111933@localhost:~  
[B2111933@myserver ~]$ su B2111933  
Password:  
[B2111933@myserver ~]$
```

Thông thường ta phải **logout** và **login** lại thì việc thêm người dùng vào nhóm mới có tác dụng. Tuy nhiên ta có thể **login** lại vào **shell** để nhanh gọn hơn.

- Chạy dịch vụ Docker

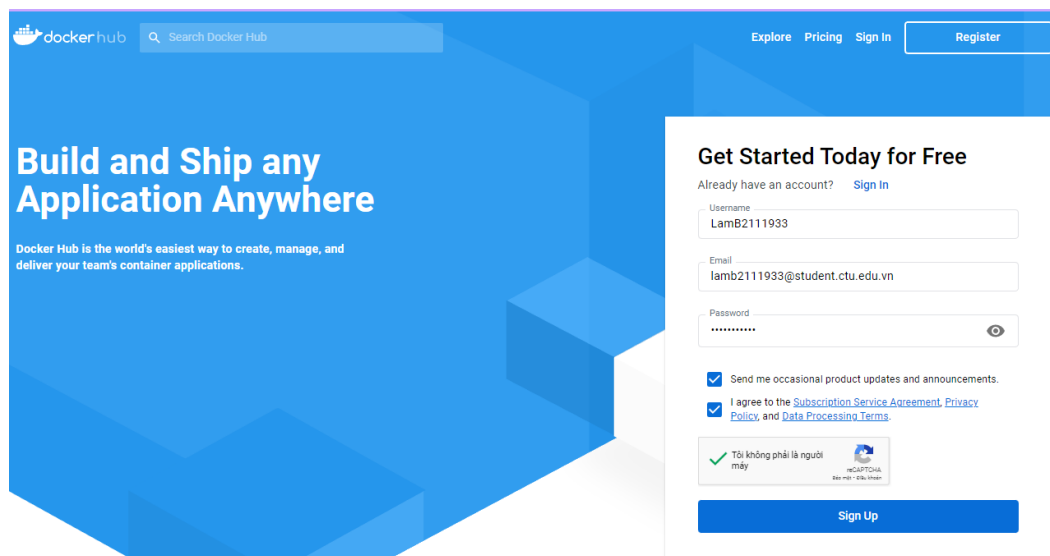
```
$sudo systemctl start docker  
$sudo systemctl enable docker
```

```
B2111933@localhost:~ — sudo systemctl status docker  
[B2111933@myserver ~]$ sudo systemctl start docker  
[B2111933@myserver ~]$ sudo systemctl enable docker  
Created symlink /etc/systemd/system/multi-user.target.wants/docker.service → /usr/lib/s  
ystemd/system/docker.service.  
[B2111933@myserver ~]$ sudo systemctl status docker  
● docker.service - Docker Application Container Engine  
   Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; preset: disabled)  
   Active: active (running) since Tue 2023-04-04 02:22:55 +07; 16s ago  
TriggeredBy: ● docker.socket  
   Docs: https://docs.docker.com  
   Main PID: 100831 (dockerd)
```

Chạy dịch vụ **Docker** và kiểm tra trạng thái.

- Tạo 1 tài khoản trên DockerHub (<https://hub.docker.com/>), sau đó đăng nhập sử dụng lệnh sau:

```
$docker login -u <docker-username>
```



Tạo một tài khoản trên **DockerHub**

```
B2111933@localhost:~
[B2111933@myserver ~]$ docker login -u lamb2111933
Password:
WARNING! Your password will be stored unencrypted in /home/B2111933/.docker/config.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credentials-store

Login Succeeded
[B2111933@myserver ~]$
```

Đăng nhập thành công

- Kiểm tra docker bằng cách tải image hello-world và tạo container tương ứng. Nếu xuất hiện thông điệp chào mừng từ Docker là cài đặt thành công.

```
$docker run hello-world
```

```
B2111933@localhost:~
[B2111933@myserver ~]$ docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
2db29710123e: Pull complete
Digest: sha256:4e83453afed1b4fala3500525091dbfca6ce1e66903fd4c01ff015dbcb1ba33e
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
1. The Docker client contacted the Docker daemon.
2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
   (amd64)
3. The Docker daemon created a new container from that image which runs the
   executable that produces the output you are currently reading.
4. The Docker daemon streamed that output to the Docker client, which sent it
   to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
$ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
https://hub.docker.com/

For more examples and ideas, visit:
https://docs.docker.com/get-started/

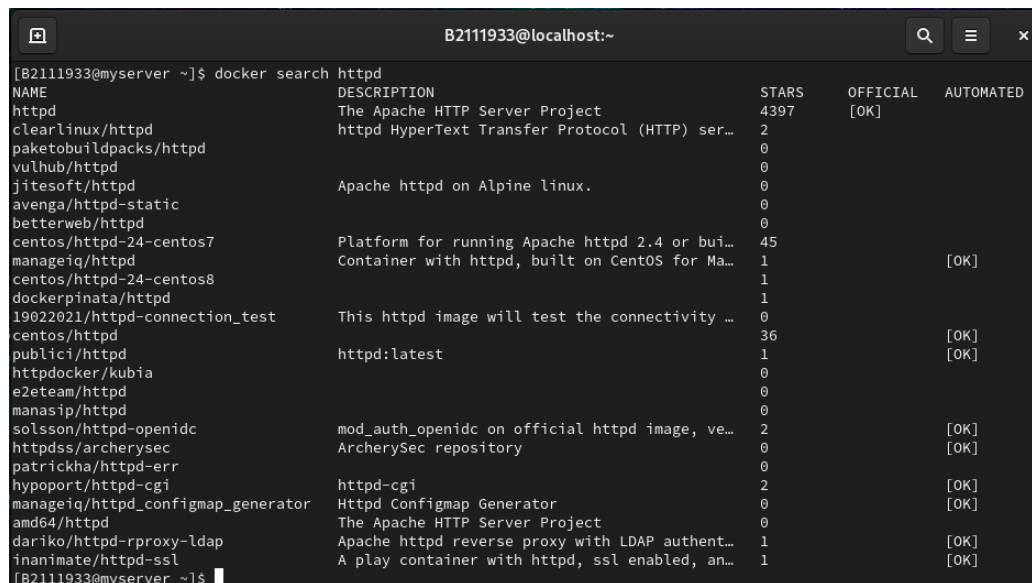
[B2111933@myserver ~]$
```

Kiểm tra **docker** bằng cách tải **image hello-world** và tạo **container** tương ứng. Lúc này trên màn hình xuất hiện **thông điệp chào mừng từ Docker** tức là ta cài đặt thành công.

- 1.5. Triển khai dịch vụ web server lên máy ảo CentOS 9 sử dụng một Docker container

- Tìm kiếm image với từ khóa httpd, kết quả sẽ thấy 1 image tên httpd ở dòng đầu tiên.

```
$docker search httpd
```



NAME	DESCRIPTION	STARS	OFFICIAL	AUTOMATED
httpd	The Apache HTTP Server Project	4397	[OK]	
clearlinux/httpd	httpd HyperText Transfer Protocol (HTTP) ser...	2		
paketobuildpacks/httpd		0		
vulhub/httpd		0		
jitesoft/httpd	Apache httpd on Alpine linux.	0		
avenga/httpd-static		0		
betterweb/httpd		0		
centos/httpd-24-centos7	Platform for running Apache httpd 2.4 or bui...	45		
manageiq/httpd	Container with httpd, built on CentOS for Ma...	1		[OK]
centos/httpd-24-centos8		1		
dockerpinata/httpd		1		
19022021/httpd-connection_test	This httpd image will test the connectivity ...	0		
centos/httpd		36		[OK]
publici/httpd	httpd:latest	1		[OK]
httpdocker/kubia		0		
e2eteam/httpd		0		
manasip/httpd		0		
solsson/httpd-openidc	mod_auth_openidc on official httpd image, ve...	2		[OK]
httpdss/archerysec	ArcherySec repository	0		[OK]
patrickha/httpd-err		0		
hypoport/httpd-cgi	httpd-cgi	2		[OK]
manageiq/httpd_configmap_generator	Httpd Configmap Generator	0		[OK]
amd64/httpd	The Apache HTTP Server Project	0		
dariiko/httpd-rproxy-ldap	Apache httpd reverse proxy with LDAP authent...	1		[OK]
inanimate/httpd-ssl	A play container with httpd, ssl enabled, an...	1		[OK]

Tìm kiếm **image** với từ khóa **httpd** sẽ cho ra nhiều kết quả, ta thấy được một **image** tên **httpd** ở dòng đầu tiên.

- Tạo container từ image httpd

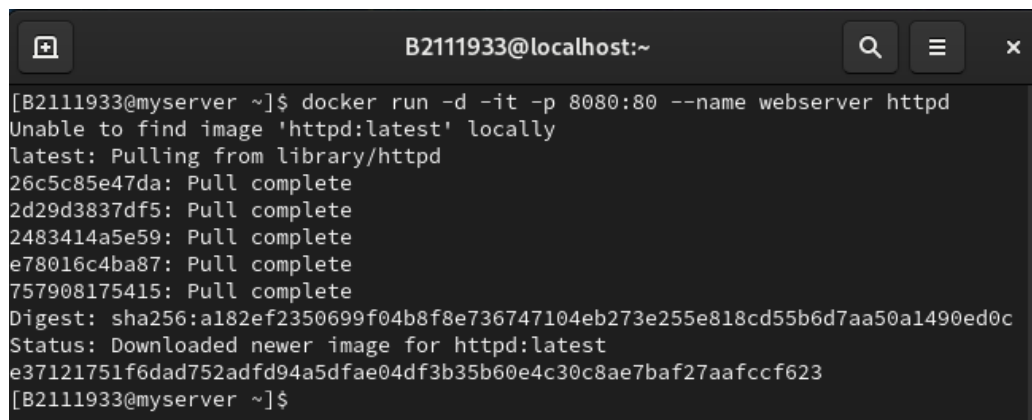
```
$docker run -d -it -p 8080:80 --name webserver httpd
```

-d: chạy container ở chế độ background

-it: tạo shell để tương tác với container

--name webserver: đặt tên container là webserver

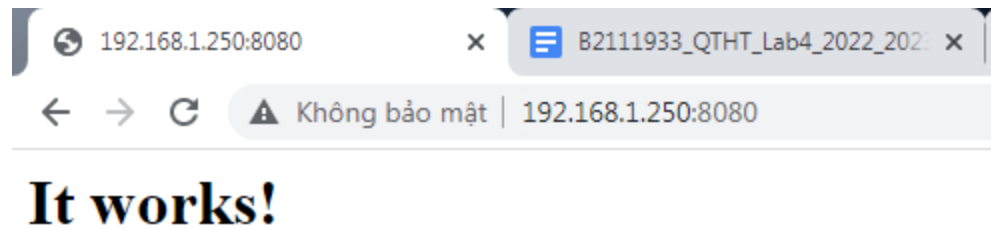
-p 8080:80 gắn cổng 8080 của máy CentOS vào cổng 80 của container.



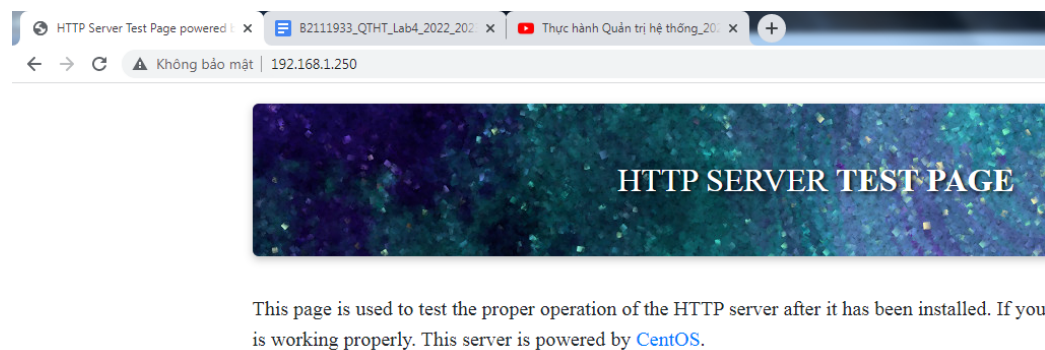
```
[B2111933@myserver ~]$ docker run -d -it -p 8080:80 --name webserver httpd
Unable to find image 'httpd:latest' locally
latest: Pulling from library/httpd
26c5c85e47da: Pull complete
2d29d3837df5: Pull complete
2483414a5e59: Pull complete
e78016c4ba87: Pull complete
757908175415: Pull complete
Digest: sha256:a182ef2350699f04b8f8e736747104eb273e255e818cd55b6d7aa50a1490ed0c
Status: Downloaded newer image for httpd:latest
e37121751f6dad752adfd94a5dfae04df3b35b60e4c30c8ae7baf27aafccf623
[B2111933@myserver ~]$
```

Ta thực hiện lệnh trên cùng với các tham số theo yêu cầu.





Truy cập đến cổng **8080** của **máy CentOS** từ **máy vật lý** sẽ nhận thông báo thành công



Nếu ta truy cập cổng **80** của **máy CentOS** thì sẽ được đưa đến **webserver** của **Lab4**

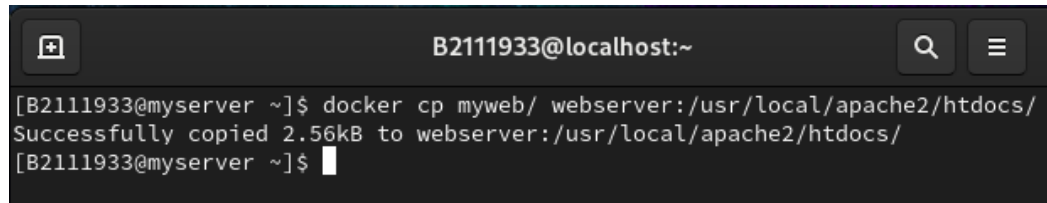
- Sao chép thư mục `~/myweb` vào thư mục gốc của dịch vụ của web trên Docker container.

A screenshot of a terminal window. The title bar shows 'B2111933@localhost:~ — nano myweb/index.html'. The terminal content shows the following HTML code:

```
<!doctype html>
<html>
<head>
<meta charset="utf-8">
<title>Swim Swim</title>
</head>
<body>
<H1>Moo Moo<H1>
<marquee>Designed by B2111933</marquee>
</body>
</html>
```

Thay đổi một chút nội dung tập tin `~/myweb/index.html` để phân biệt với tập tin `index.html` ở Lab4

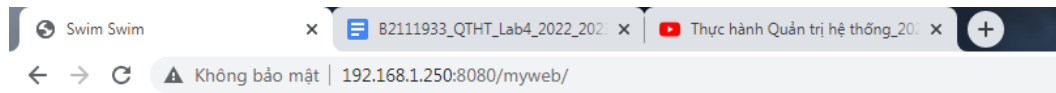
```
$docker cp myweb/ webserver:/usr/local/apache2/htdocs/
```



```
B2111933@localhost:~  
[B2111933@myserver ~]$ docker cp myweb/ webserver:/usr/local/apache2/htdocs/  
Successfully copied 2.56kB to webserver:/usr/local/apache2/htdocs/  
[B2111933@myserver ~]$
```

Sao chép thành công tập tin đến **container** ta đã tạo ra

- Trên máy vật lý, mở trình duyệt web và truy cập vào địa chỉ `http://<Địa chỉ IP máy ảo CentOS>:8080/myweb` để kiểm chứng trang web vừa tạo.



**Moo Moo**

**Designed by B2111933**

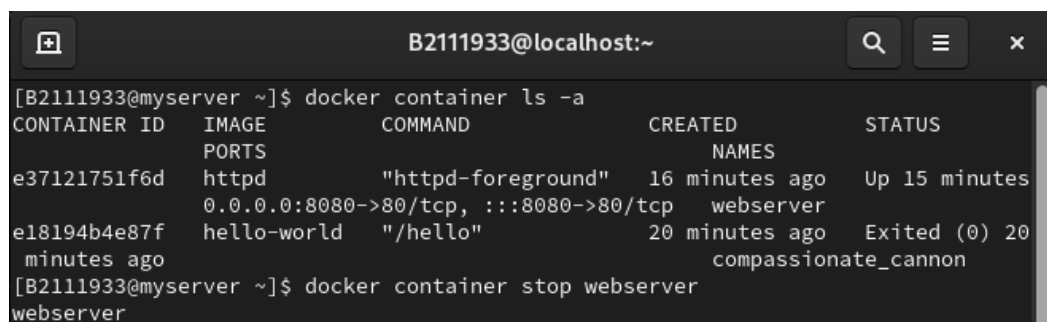
Truy cập đến **trang web vừa tạo ở cổng 8080** của máy ảo CentOS



**Welcome!**

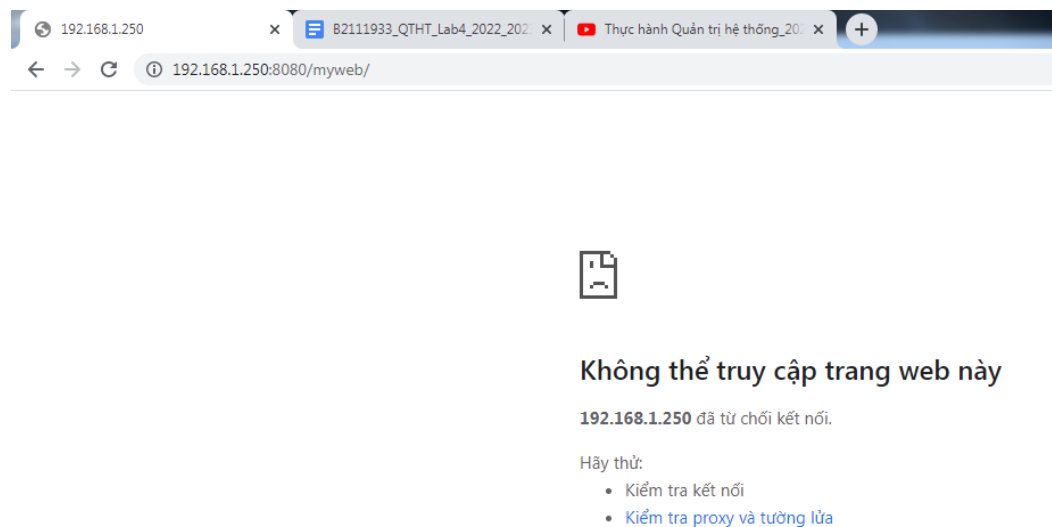
**Designed by B12345678**

Phân biệt với **trang web được tạo ở Lab4 ở cổng 80** của máy ảo CentOS

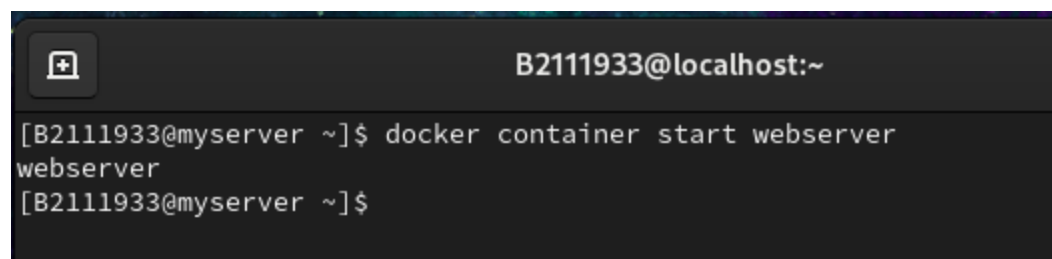


```
B2111933@localhost:~  
[B2111933@myserver ~]$ docker container ls -a  
CONTAINER ID   IMAGE      COMMAND                  CREATED          STATUS  
e37121751f6d   httpd      "httpd-foreground"      16 minutes ago  Up 15 minutes  
e18194b4e87f   hello-world "/hello"                 20 minutes ago  Exited (0) 20  
minutes ago    compassionate_cannon  
[B2111933@myserver ~]$ docker container stop webserver  
webserver
```

Ta có thể **dừng container** với lệnh **docker container stop <tên container>**



Khi ấy **trang web** ở **cổng 8080** của **máy ảo CentOS** không thể truy cập được



Để khởi động **container webserver** cùng với việc có thể truy cập lại **trang web trên** Ta chỉ việc gõ lệnh **docker container start <tên container>**

## 2. Cài đặt và cấu hình dịch vụ SAMBA

Samba là dịch vụ chia sẻ file giữa các hệ điều hành khác nhau như Windows và Linux bằng cách sử dụng giao thức SMB/CIFS. Trong bài thực hành sinh viên sẽ cài đặt và cấu hình dịch vụ Samba trên máy chủ CentOS và sử dụng máy Windows để truy cập tới dịch vụ.

**Tim hiểu và thực hiện các yêu cầu sau (kèm hình minh họa cho từng bước):**

- Cài đặt dịch vụ Samba:

```
$sudo dnf install -y samba
```

```
B2111933@localhost:~ — sudo dnf install -y samba
[B2111933@myserver ~]$ sudo dnf install -y samba
[sudo] password for B2111933:
Sorry, try again.
[sudo] password for B2111933:
Last metadata expiration check: 0:20:48 ago on Fri 14 Apr 2023 05:48:41 PM +07.
Dependencies resolved.
=====
Package                        Arch      Version      Repository    Size
=====
Installing:
samba                          x86_64    4.17.5-102.el9    baseos        981 k

Installed:
libnetapi-4.17.5-102.el9.x86_64
samba-4.17.5-102.el9.x86_64
samba-common-tools-4.17.5-102.el9.x86_64
samba-dcerpc-4.17.5-102.el9.x86_64
samba-ldb-ldap-modules-4.17.5-102.el9.x86_64
samba-libs-4.17.5-102.el9.x86_64

Complete!
[B2111933@myserver ~]$
```

Cài đặt thành công dịch vụ **Samba**

- Tạo người dùng và nhóm người dùng chia sẻ dữ liệu:

```
$sudo adduser tuanthai
```

```
B2111933@localhost:~
[B2111933@myserver ~]$ sudo adduser tuanthai
[B2111933@myserver ~]$
```

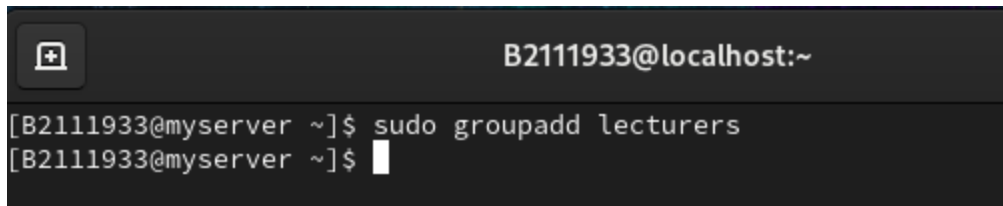
Tạo người dùng **tuanthai**

```
$sudo passwd tuanthai
```

```
B2111933@localhost:~
[B2111933@myserver ~]$ sudo passwd tuanthai
Changing password for user tuanthai.
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a (reversed) dictionary word
Retype new password:
passwd: all authentication tokens updated successfully.
[B2111933@myserver ~]$
```

Tạo mật khẩu cho người dùng **tuanthai**

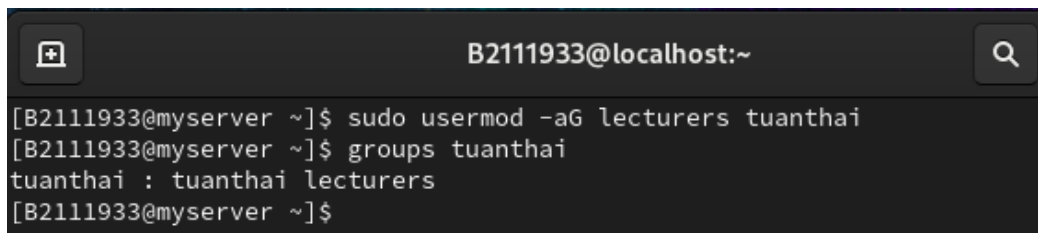
```
$sudo groupadd lecturers
```



```
B2111933@localhost:~  
[B2111933@myserver ~]$ sudo groupadd lecturers  
[B2111933@myserver ~]$
```

Tạo nhóm người dùng **lecturers**

```
$sudo usermod -a -G lecturers tuanthai
```

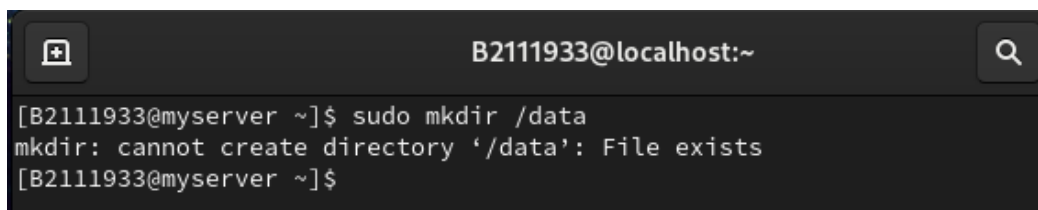


```
B2111933@localhost:~  
[B2111933@myserver ~]$ sudo usermod -aG lecturers tuanthai  
[B2111933@myserver ~]$ groups tuanthai  
tuanthai : tuanthai lecturers  
[B2111933@myserver ~]$
```

Thêm người dùng **tuanthai** vào nhóm **lecturers** và kiểm tra kết quả.

- Tạo thư mục cần chia sẻ và phân quyền:

```
$sudo mkdir /data
```

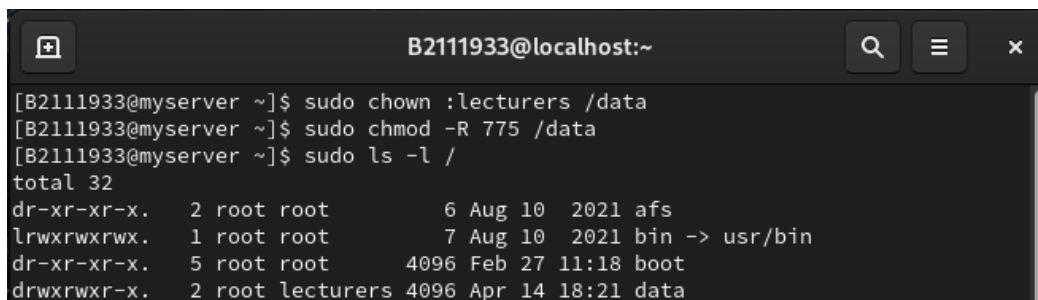


```
B2111933@localhost:~  
[B2111933@myserver ~]$ sudo mkdir /data  
mkdir: cannot create directory '/data': File exists  
[B2111933@myserver ~]$
```

Thư mục **/data** đã được tạo sẵn ở các lab trước đây

```
$sudo chown :lecturers /data
```

```
$sudo chmod -R 775 /data
```

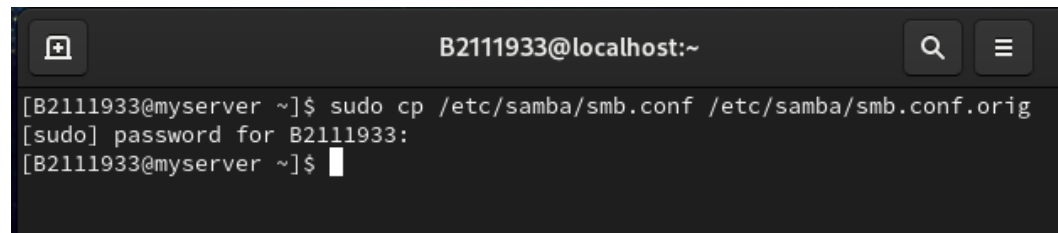


```
B2111933@localhost:~  
[B2111933@myserver ~]$ sudo chown :lecturers /data  
[B2111933@myserver ~]$ sudo chmod -R 775 /data  
[B2111933@myserver ~]$ sudo ls -l /  
total 32  
dr-xr-xr-x.  2 root root      6 Aug 10  2021 afs  
lrwxrwxrwx.  1 root root      7 Aug 10  2021 bin -> usr/bin  
dr-xr-xr-x.  5 root root    4096 Feb 27 11:18 boot  
drwxrwxr-x.  2 root lecturers 4096 Apr 14 18:21 data
```

Ta tiến hành chuyển quyền sở hữu thư mục **/data** cho nhóm người dùng **lecturers**, sau đó ta phân quyền lại cho thư mục **/data** theo yêu cầu và kiểm tra kết quả

- Cấu hình dịch vụ Samba:

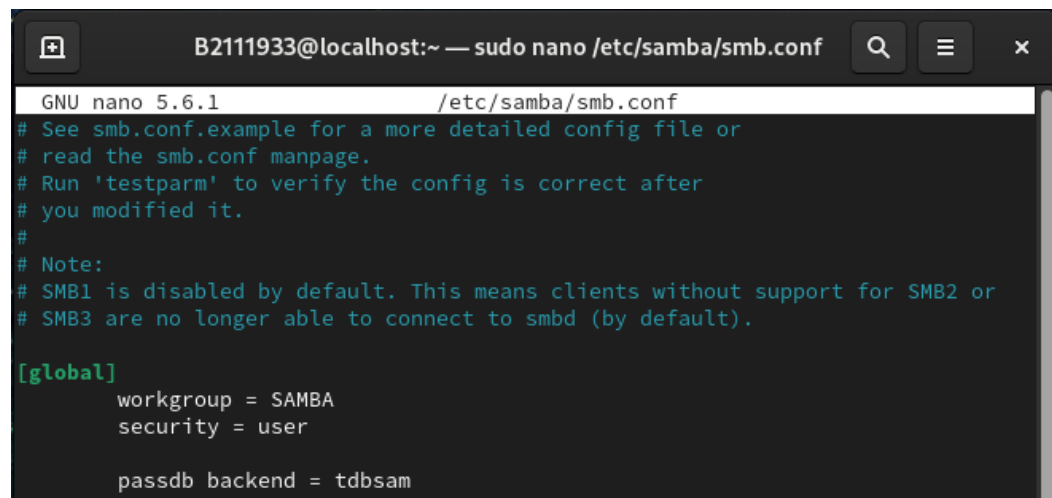
```
$sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.orig
```



```
B2111933@localhost:~  
[B2111933@myserver ~]$ sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.orig  
[sudo] password for B2111933:  
[B2111933@myserver ~]$
```

Ta tiến hành tạo bản sao của file cấu hình dịch vụ Samba **/etc/samba/smb.conf**  
Để sau này nếu cần ta có thể khôi phục lại cấu hình cũ

```
$sudo nano /etc/samba/smb.conf
```



```
B2111933@localhost:~ — sudo nano /etc/samba/smb.conf  
GNU nano 5.6.1 /etc/samba/smb.conf  
# See smb.conf.example for a more detailed config file or  
# read the smb.conf manpage.  
# Run 'testparm' to verify the config is correct after  
# you modified it.  
#  
# Note:  
# SMB1 is disabled by default. This means clients without support for SMB2 or  
# SMB3 are no longer able to connect to smbd (by default).  
  
[global]  
    workgroup = SAMBA  
    security = user  
  
    passdb backend = tdbsam
```

Cấu hình **dịch vụ Samba** với công cụ **nano**

#Thêm đoạn cấu hình bên dưới vào cuối tập tin

```
[data]  
    comment = Shared folder for lecturers  
    path = /data  
    browsable = yes  
    writable = yes  
    read only = no  
    valid users = @lecturers
```

```
B2111933@localhost:~ — sudo nano /etc/samba/smb.conf
GNU nano 5.6.1 /etc/samba/smb.conf
[print$]
comment = Printer Drivers
path = /var/lib/samba/drivers
write list = @printadmin root
force group = @printadmin
create mask = 0664
directory mask = 0775
[data]
comment = Shared folder for lecturers
path = /data
browsable = yes
writable = yes
read only = no
valid users = @lecturers
```

**[data]:** Thư mục chia sẻ có tên là **data** cho phép các máy tính khác kết nối tới.

**comment:** ghi chú cho thư mục này

**path:** đường dẫn đến thư mục **data** ta vừa tạo

**browsable:** cho phép các người dùng liệt kê nội dung tập tin

**writable:** cho phép các người dùng tạo thư mục hay tập tin mới trong thư mục **data**

**read only = no:** ở đây không giới hạn **read only**

**valid users:** cho phép những người dùng kết nối đến thư mục **data**

- Thêm người dùng cho dịch vụ Samba:

```
$sudo smbpasswd -a tuanthai
```

#Đặt mật khẩu Samba cho người dùng

```
B2111933@localhost:~
[B2111933@myserver ~]$ sudo smbpasswd -a tuanthai
[sudo] password for B2111933:
New SMB password:
Retype new SMB password:
Added user tuanthai.
[B2111933@myserver ~]$
```

**Đặt mật khẩu** cho người dùng **tuanthai** trên dịch vụ **Samba** (thêm người dùng **tuanthai** vào dịch vụ **Samba**)

- Cấu hình SELINUX cho phép Samba

```
$sudo setsebool -P samba_export_all_rw on
```

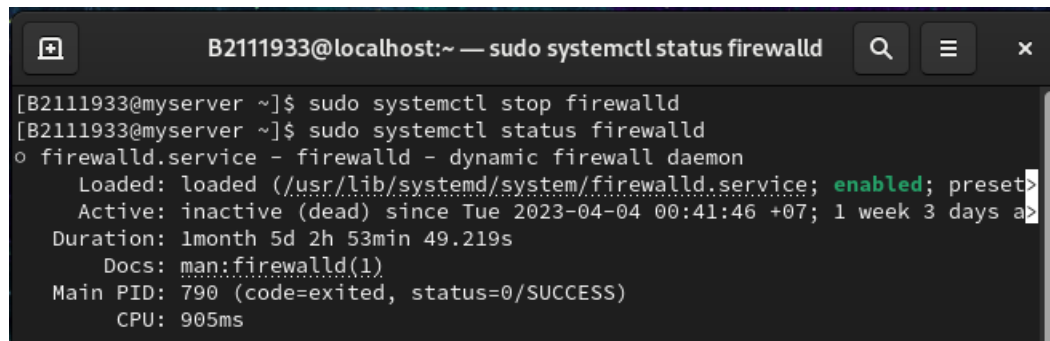
```
$sudo setsebool -P samba_enable_home_dirs on
```

```
B2111933@localhost:~
[B2111933@myserver ~]$ sudo setsebool -P samba_export_all_rw on
[B2111933@myserver ~]$ sudo setsebool -P samba_enable_home_dirs on
[B2111933@myserver ~]$
```

Cho phép **Samba** chia sẻ tập tin và cho phép người dùng chia sẻ thư mục home

- Tắt tường lửa:

```
$sudo systemctl stop firewalld
```



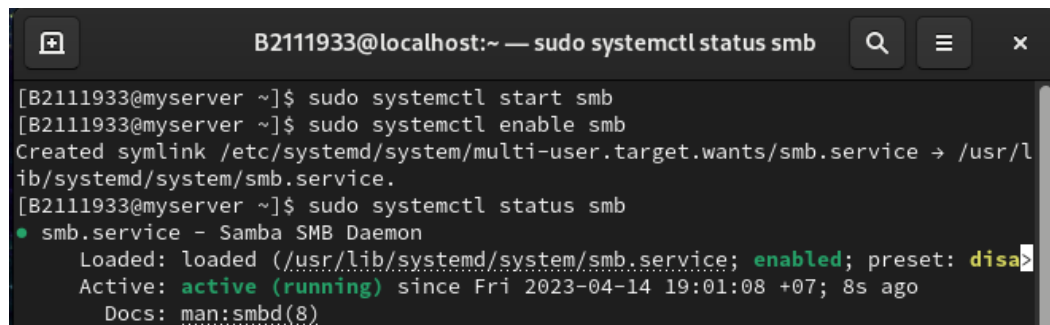
```
B2111933@localhost:~ — sudo systemctl status firewalld
[B2111933@myserver ~]$ sudo systemctl stop firewalld
[B2111933@myserver ~]$ sudo systemctl status firewalld
o firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset>
   Active: inactive (dead) since Tue 2023-04-04 00:41:46 +07; 1 week 3 days a>
   Duration: 1month 5d 2h 53min 49.219s
   Docs: man:firewalld(1)
   Main PID: 790 (code=exited, status=0/SUCCESS)
   CPU: 905ms
```

Tắt tường lửa và kiểm tra kết quả.

- Khởi động cho phép Samba tự động thực thi khi khởi động hệ điều hành:

```
$sudo systemctl start smb
```

```
$sudo systemctl enable smb
```



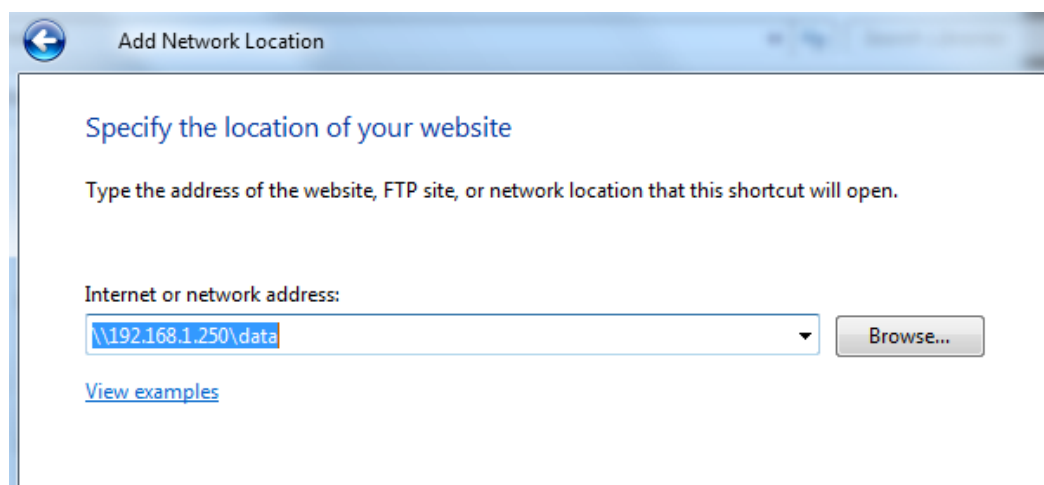
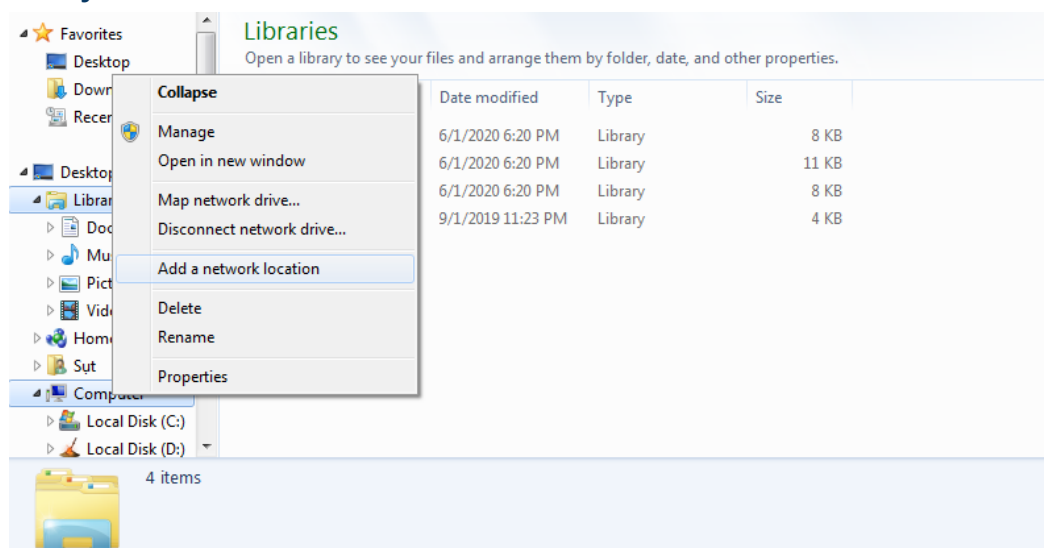
```
B2111933@localhost:~ — sudo systemctl status smb
[B2111933@myserver ~]$ sudo systemctl start smb
[B2111933@myserver ~]$ sudo systemctl enable smb
Created symlink /etc/systemd/system/multi-user.target.wants/smb.service → /usr/l
ib/systemd/system/smb.service.
[B2111933@myserver ~]$ sudo systemctl status smb
● smb.service - Samba SMB Daemon
   Loaded: loaded (/usr/lib/systemd/system/smb.service; enabled; preset: disa>
   Active: active (running) since Fri 2023-04-14 19:01:08 +07; 8s ago
   Docs: man:smbd(8)
```

Khởi động **Samba** và cho phép **Samba** tự động thực thi khi khởi động hệ điều hành.  
Kiểm tra trạng thái của dịch vụ **Samba**.

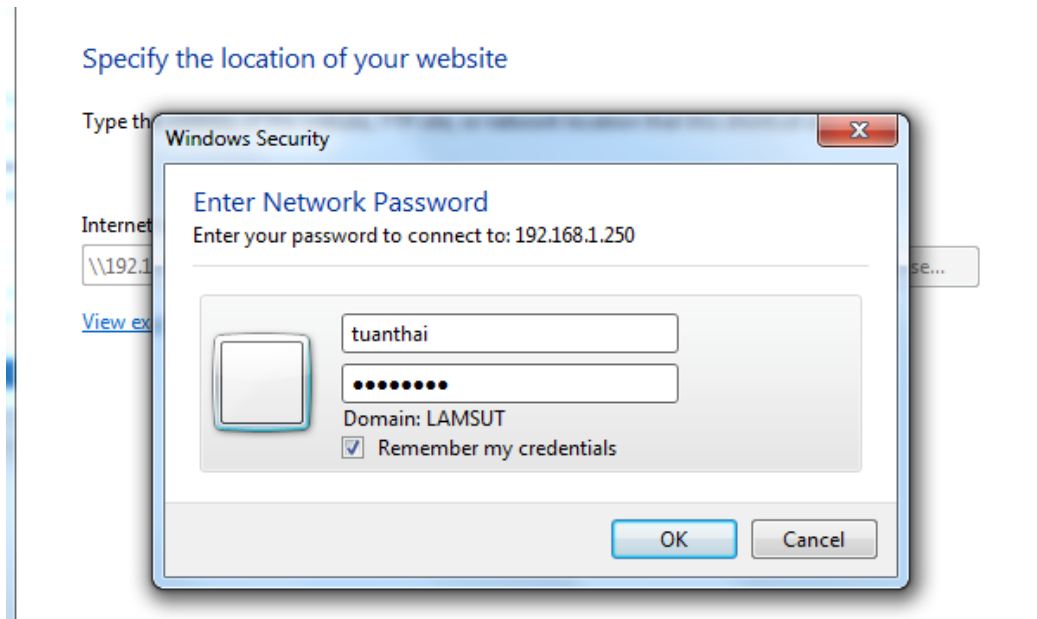
- Trên File Explorer của máy Windows, chọn tính năng “Add a network location” để nối kết tới Samba server sử dụng địa chỉ \\<IP máy CentOS>\data



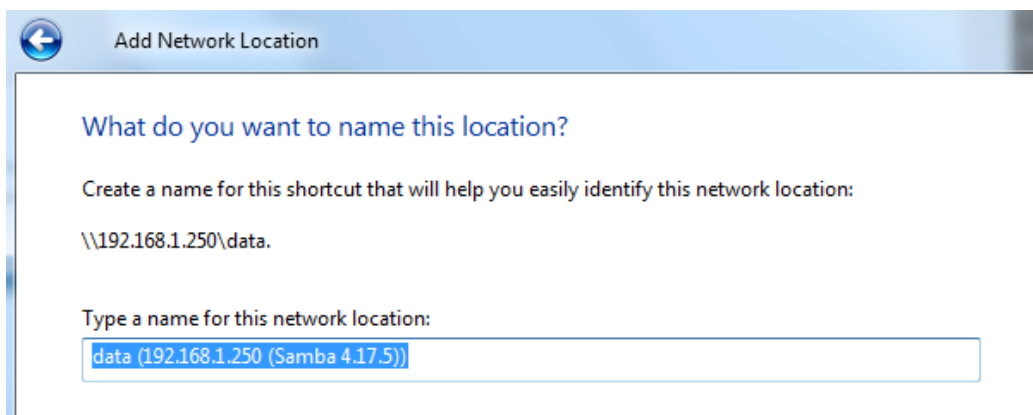
### Ở máy Windows:



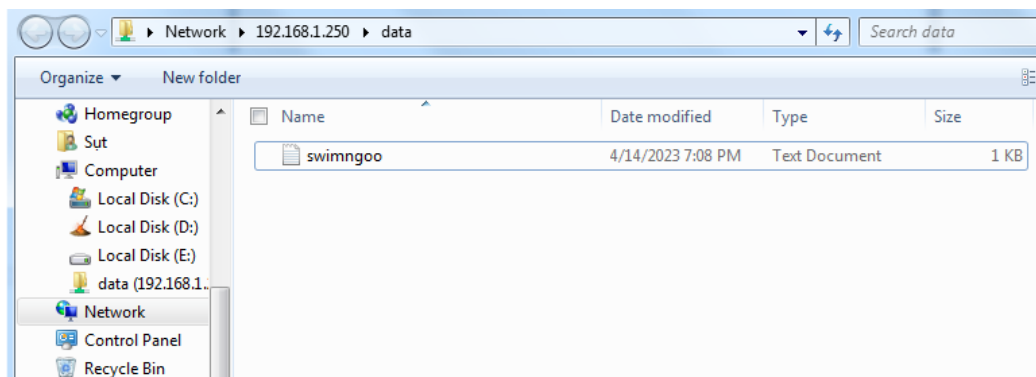
Kết nối tới **Samba server**



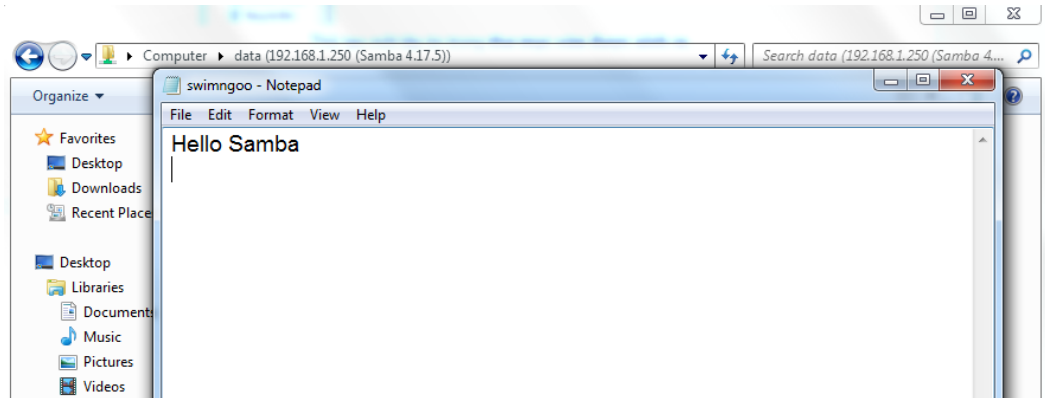
Xác thực tài khoản **tuanthai**



Lúc này một thư mục **Samba** đã được tạo ra.



Thử tạo một tập tin trong thư mục vừa được sinh ra.



Thay đổi nội dung tập tin

**Trở về máy CentOS và kiểm tra kết quả:**

```
B2111933@localhost:~  
[B2111933@myserver ~]$ ls /data  
swimngoo.txt  
[B2111933@myserver ~]$ cat /data/swimngoo.txt  
Hello Samba  
[B2111933@myserver ~]$
```

Kiểm tra thư mục **Samba** và đọc **tập tin** ta vừa tạo ra từ máy vật lý.

### 3. Cài đặt và cấu hình dịch vụ DNS

DNS (Domain Name System) là giải pháp dùng tên miền thay cho địa chỉ IP khó nhớ khi sử dụng các dịch vụ trên mạng. Truy cập đến website của Trường CNTT-TT- Trường ĐH Cần Thơ bằng địa chỉ nào dễ nhớ hơn ?

<http://123.30.143.202> hay <http://www.cit.ctu.edu.vn>

Trong bài thực hành này sinh viên cần cài đặt phần mềm BIND trên CentOS để phân giải tên miền "qtht.com.vn"

**Tìm hiểu và thực hiện các yêu cầu sau (kèm hình minh họa cho từng bước):**

#### 3.1. Cài đặt BIND và các công cụ cần thiết:

```
$sudo dnf install bind bind-utils -y
```

```
B2111933@localhost:~ — sudo dnf install bind bind-utils -y  
[B2111933@myserver ~]$ sudo dnf install bind bind-utils -y  
[sudo] password for B2111933:  
Last metadata expiration check: 1:29:01 ago on Fri 14 Apr 2023 05:48:41 PM +07.  
Package bind-utils-32:9.16.23-7.el9.x86_64 is already installed.  
Dependencies resolved.  
=====
```

Package	Arch	Version	Repository	Size
Installing:				
bind	x86_64	32:9.16.23-11.el9	appstream	503 k

```
=====
```

```
Upgraded:
  bind-libs-32:9.16.23-11.el9.x86_64    bind-license-32:9.16.23-11.el9.noarch
  bind-utils-32:9.16.23-11.el9.x86_64
Installed:
  bind-32:9.16.23-11.el9.x86_64
  bind-dnssec-doc-32:9.16.23-11.el9.noarch
  bind-dnssec-utils-32:9.16.23-11.el9.x86_64
  python3-bind-32:9.16.23-11.el9.noarch
  python3-ply-3.11-14.el9.noarch

Complete!
[B2111933@myserver ~]$
```

Quá trình cài đặt hoàn tất

### 3.2. Cấu hình DNS server:

```
$sudo nano /etc/named.conf
#(tham khảo file mẫu)
...
options {
    listen-on port 53 { 127.0.0.1; any; };
    ...
    allow-query      { localhost; any; };
    recursion yes;
    forwarders {192.168.55.1; };
    ..
};

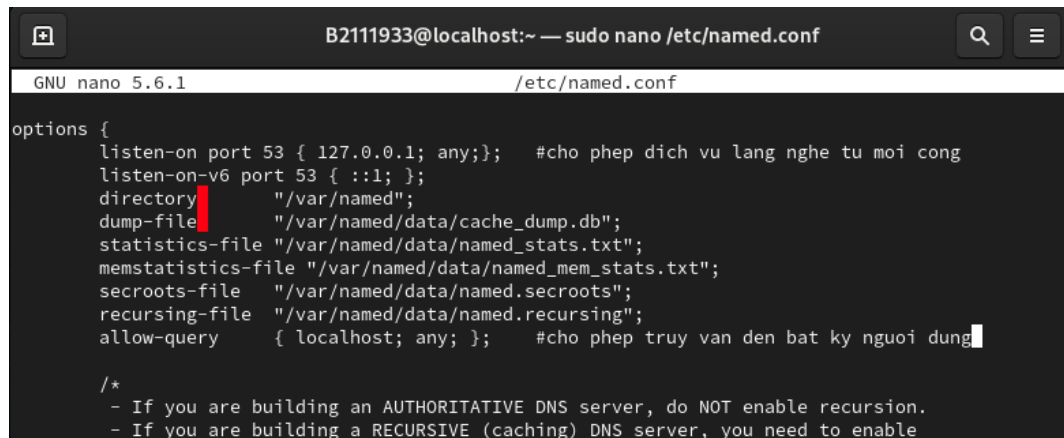
logging {
    ..
};

zone "." IN {
    ...
};

zone "qtht.com.vn" IN {
    type master;
    file "forward.qtht";
    allow-update { none; };
};

zone "55.168.192.in-addr.arpa" IN {
    type master;
    file "reverse.qtht";
```

```
allow-update { none; };  
};  
...
```



The screenshot shows a terminal window with the title "B2111933@localhost:~ — sudo nano /etc/named.conf". The editor is GNU nano 5.6.1. The content of the file is as follows:

```
options {  
    listen-on port 53 { 127.0.0.1; any; }; #cho phép dịch vụ lắng nghe từ mọi cổng  
    listen-on-v6 port 53 { ::1; };  
    directory "/var/named";  
    dump-file "/var/named/data/cache_dump.db";  
    statistics-file "/var/named/data/named_stats.txt";  
    memstatistics-file "/var/named/data/named_mem_stats.txt";  
    secroots-file "/var/named/data/named.secroots";  
    recursing-file "/var/named/data/named.recursing";  
    allow-query { localhost; any; }; #cho phép truy vấn đến bất kỳ người dùng  
  
    /*  
    - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.  
    - If you are building a RECURSIVE (caching) DNS server, you need to enable
```



The screenshot shows a terminal window with the title "B2111933@localhost:~ — sudo nano /etc/named.conf". The editor is GNU nano 5.6.1. The content of the file is as follows:

```
    - If you are building a RECURSIVE (caching) DNS server, you need to enable  
    recursion.  
    - If your recursive DNS server has a public IP address, you MUST enable access  
    control to limit queries to your legitimate users. Failing to do so will  
    cause your server to become part of large scale DNS amplification  
    attacks. Implementing BCP38 within your network would greatly  
    reduce such attack surface  
    */  
    recursion yes;  
    forwarders {8.8.8.8; 8.8.4.4; }; #nếu có truy vấn nào đó không truy vấn được thì sẽ chuyển đến  
  
    dnssec-validation no; #nhỏ chuyển thành no  
  
    managed-keys-directory "/var/named/dynamic";  
    geoip-directory "/usr/share/GeoIP";
```



The screenshot shows a terminal window with the title "B2111933@localhost:~ — sudo nano /etc/named.conf". The editor is GNU nano 5.6.1. The content of the file is as follows:

```
    type hint;  
    file "named.ca";  
};  
  
zone "qtht.com.vn" IN {  
    type master;  
    file "forward.qtht";  
    allow-update { none; };  
}; #phân giải xuôi (chuyển tên miền sang địa chỉ IP)  
  
zone "1.168.192.in-addr.arpa" IN { #nhánh mạng máy CentOS đang kết nối là 192.168.1.0  
    type master;  
    file "reverse.qtht";  
    allow-update { none; };  
}; #phân giải ngược (chuyển địa chỉ IP sang tên miền)
```

Cấu hình **DNS Server** theo gợi ý.

### 3.3. Tạo tập tin cấu hình phân giải xuôi:

```

B2111933@localhost:~
[B2111933@myserver ~]$ sudo ls -l /var/named/
[sudo] password for B2111933:
total 16
drwxrwx---. 2 named named    6 Feb 27 21:25 data
drwxrwx---. 2 named named    6 Feb 27 21:25 dynamic
-rw-r-----. 1 root  named 2253 Feb 27 21:25 named.ca
-rw-r-----. 1 root  named 152 Feb 27 21:25 named.empty
-rw-r-----. 1 root  named 152 Feb 27 21:25 named.localhost
-rw-r-----. 1 root  named 168 Feb 27 21:25 named.loopback
drwxrwx---. 2 named named    6 Feb 27 21:25 slaves
[B2111933@myserver ~]$

```

Tập tin cho phép phân giải miền **localhost**

```
$sudo cp /var/named/named.localhost /var/named/forward.qtht
```

```

B2111933@localhost:~
[B2111933@myserver ~]$ sudo cp /var/named/named.localhost /var/named/forward.qtht
[B2111933@myserver ~]$ sudo ls -l /var/named/
total 20
drwxrwx---. 2 named named    6 Feb 27 21:25 data
drwxrwx---. 2 named named    6 Feb 27 21:25 dynamic
-rw-r-----. 1 root  root   152 Apr 14 19:55 forward.qtht
-rw-r-----. 1 root  named 2253 Feb 27 21:25 named.ca
-rw-r-----. 1 root  named 152 Feb 27 21:25 named.empty
-rw-r-----. 1 root  named 152 Feb 27 21:25 named.localhost
-rw-r-----. 1 root  named 168 Feb 27 21:25 named.loopback
drwxrwx---. 2 named named    6 Feb 27 21:25 slaves
[B2111933@myserver ~]$

```

Sao chép sang tập tin **forward.qtht**

```
$sudo chgrp named /var/named/forward.qtht
```

```

B2111933@localhost:~
[B2111933@myserver ~]$ sudo chgrp named /var/named/forward.qtht
[B2111933@myserver ~]$ sudo ls -l /var/named/
total 20
drwxrwx---. 2 named named    6 Feb 27 21:25 data
drwxrwx---. 2 named named    6 Feb 27 21:25 dynamic
-rw-r-----. 1 root  named 152 Apr 14 19:55 forward.qtht
-rw-r-----. 1 root  named 2253 Feb 27 21:25 named.ca
-rw-r-----. 1 root  named 152 Feb 27 21:25 named.empty
-rw-r-----. 1 root  named 152 Feb 27 21:25 named.localhost
-rw-r-----. 1 root  named 168 Feb 27 21:25 named.loopback
drwxrwx---. 2 named named    6 Feb 27 21:25 slaves
[B2111933@myserver ~]$

```

Đổi nhóm chủ sở hữu sang nhóm **named** vì dịch vụ **DNS** sẽ không thể đọc được nội dung tập tin nếu chủ sở hữu là nhóm **root**

```
$sudo nano /var/named/forward.qtht
#(tham khảo file mẫu)
$TTL 1D
@      IN      SOA  @  qtht.com.vn. (
                                0      ;Serial
                                1D     ;Refresh
                                1H     ;Retry
                                1W     ;Expire
                                3H     ;Minimum TTL
)
@      IN      NS   dns.qtht.com.vn.
dns    IN      A    192.168.55.250
www    IN      A    192.168.55.250
htq1   IN      A    8.8.8.8
```

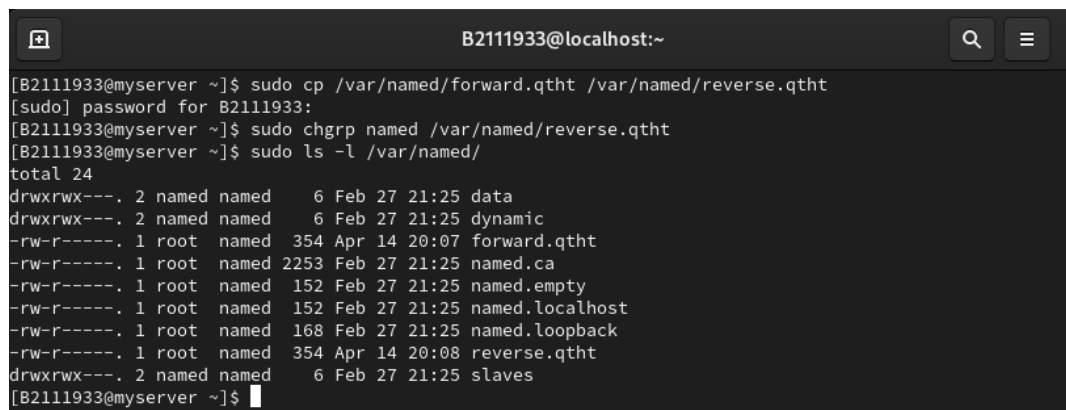


```
B2111933@localhost:~ — sudo nano /var/named/forward.qtht
GNU nano 5.6.1 /var/named/forward.qtht
$TTL 1D
@      IN      SOA  @  qtht.com.vn. (
                                0      ;Serial
                                1D     ;Refresh
                                1H     ;Retry
                                1W     ;Expire
                                3H     ;Minimum TTL
)
@      IN      NS   dns.qtht.com.vn.
dns    IN      A    192.168.1.250
www    IN      A    192.168.1.250
htq1   IN      A    8.8.8.8
```

Cấu hình tập tin **phân giải xuôi** theo gợi ý.

### 3.4. Tạo tập tin cấu hình phân giải ngược:

```
$sudo cp /var/named/forward.qtht /var/named/reverse.qtht
$sudo chgrp named /var/named/reverse.qtht
```



```
B2111933@localhost:~
[B2111933@myserver ~]$ sudo cp /var/named/forward.qtht /var/named/reverse.qtht
[sudo] password for B2111933:
[B2111933@myserver ~]$ sudo chgrp named /var/named/reverse.qtht
[B2111933@myserver ~]$ sudo ls -l /var/named/
total 24
drwxrwx---. 2 named named   6 Feb 27 21:25 data
drwxrwx---. 2 named named   6 Feb 27 21:25 dynamic
-rw-r-----. 1 root  named  354 Apr 14 20:07 forward.qtht
-rw-r-----. 1 root  named 2253 Feb 27 21:25 named.ca
-rw-r-----. 1 root  named  152 Feb 27 21:25 named.empty
-rw-r-----. 1 root  named  152 Feb 27 21:25 named.localhost
-rw-r-----. 1 root  named  168 Feb 27 21:25 named.loopback
-rw-r-----. 1 root  named  354 Apr 14 20:08 reverse.qtht
drwxrwx---. 2 named named   6 Feb 27 21:25 slaves
[B2111933@myserver ~]$
```

Sao chép nội dung tập tin **forward.qtht** sang tập tin **reverse.qtht** và chuyển quyền sở hữu tập tin **reverse.qtht** sang nhóm **named**.

```
$sudo nano /var/named/reverse.qtht
```

```
$TTL 1D
@      IN      SOA  @  qtht.com.vn. (
                        0      ;Serial
                        1D     ;Refresh
                        1H     ;Retry
                        1W     ;Expire
                        3H     ;Minimum TTL
)
@      IN      NS   dns.qtht.com.vn.
dns    IN      A    192.168.55.250
250    IN      PTR  www.qtht.com.vn.
```

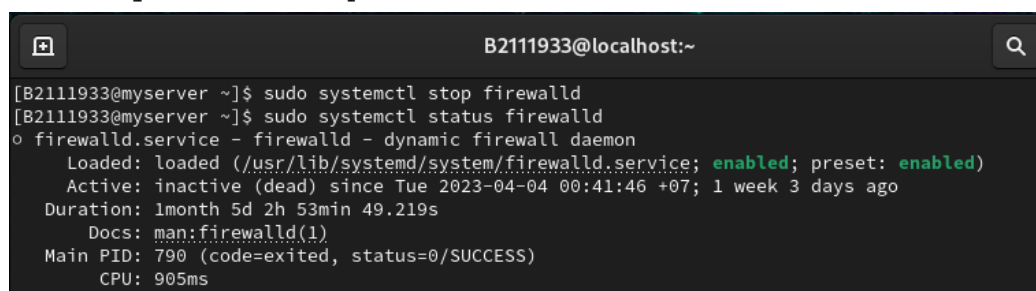


Cấu hình tập tin **phân giải ngược** theo gợi ý.

### 3.5. Kiểm tra và sử dụng dịch vụ DNS

- Tắt tường lửa:

```
$sudo systemctl stop firewalld
```

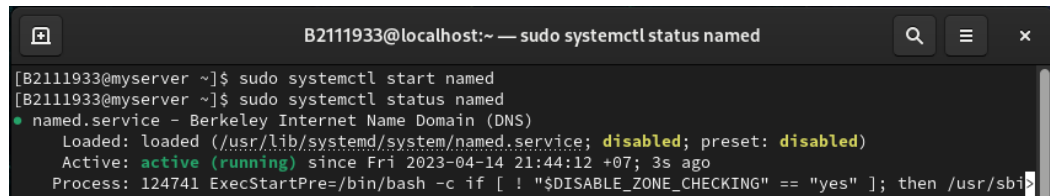


Tắt tường lửa và kiểm tra trạng thái



- Khởi động dịch vụ DNS:

```
$sudo systemctl start named
```

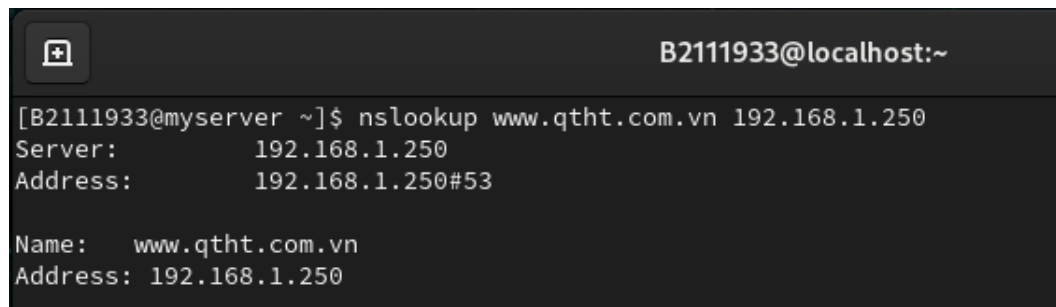


```
B2111933@localhost:~ — sudo systemctl status named
[B2111933@myserver ~]$ sudo systemctl start named
[B2111933@myserver ~]$ sudo systemctl status named
• named.service - Berkeley Internet Name Domain (DNS)
  Loaded: loaded (/usr/lib/systemd/system/named.service; disabled; preset: disabled)
  Active: active (running) since Fri 2023-04-14 21:44:12 +07; 3s ago
  Process: 124741 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" == "yes" ]; then /usr/sbi>
```

Khởi động dịch vụ **DNS** và kiểm tra trạng thái

- Kiểm tra kết quả:

```
nslookup www.qtht.com.vn <địa chỉ IP máy ảo>
```

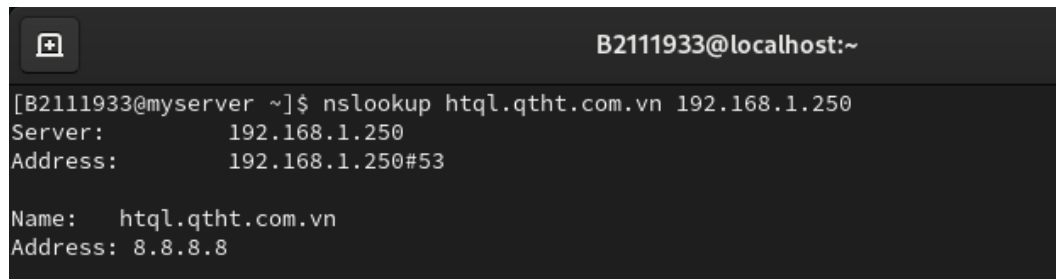


```
B2111933@localhost:~
[B2111933@myserver ~]$ nslookup www.qtht.com.vn 192.168.1.250
Server:          192.168.1.250
Address:         192.168.1.250#53

Name:   www.qtht.com.vn
Address: 192.168.1.250
```

Chuyển đổi tên miền [www.qtht.com.vn](http://www.qtht.com.vn)

```
nslookup htql.qtht.com.vn <địa chỉ IP máy ảo>
```

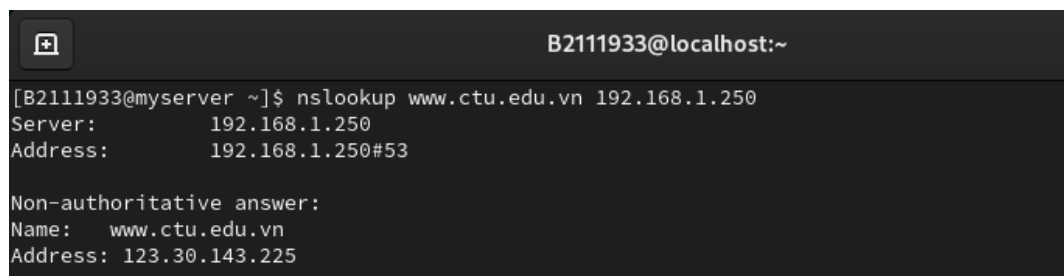


```
B2111933@localhost:~
[B2111933@myserver ~]$ nslookup htql.qtht.com.vn 192.168.1.250
Server:          192.168.1.250
Address:         192.168.1.250#53

Name:   htql.qtht.com.vn
Address: 8.8.8.8
```

Phân giải tên miền [htql.qtht.com.vn](http://htql.qtht.com.vn)

```
nslookup www.ctu.edu.vn <địa chỉ IP máy ảo>
```



```
B2111933@localhost:~
[B2111933@myserver ~]$ nslookup www.ctu.edu.vn 192.168.1.250
Server:          192.168.1.250
Address:         192.168.1.250#53

Non-authoritative answer:
Name:   www.ctu.edu.vn
Address: 123.30.143.225
```

Dịch vụ **DNS** không thể phân giải tên miền [www.ctu.edu.vn](http://www.ctu.edu.vn) nên sẽ chuyển tiếp tới **DNS server** mà ta đã cấu hình ở **câu 3.2**

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Admin>nslookup www.qtht.com.vn 192.168.1.250
Server: www.qtht.com.vn
Address: 192.168.1.250

Name: www.qtht.com.vn
Address: 192.168.1.250

C:\Users\Admin>nslookup htql.qtht.com.vn 192.168.1.250
Server: www.qtht.com.vn
Address: 192.168.1.250

Name: htql.qtht.com.vn
Address: 8.8.8.8

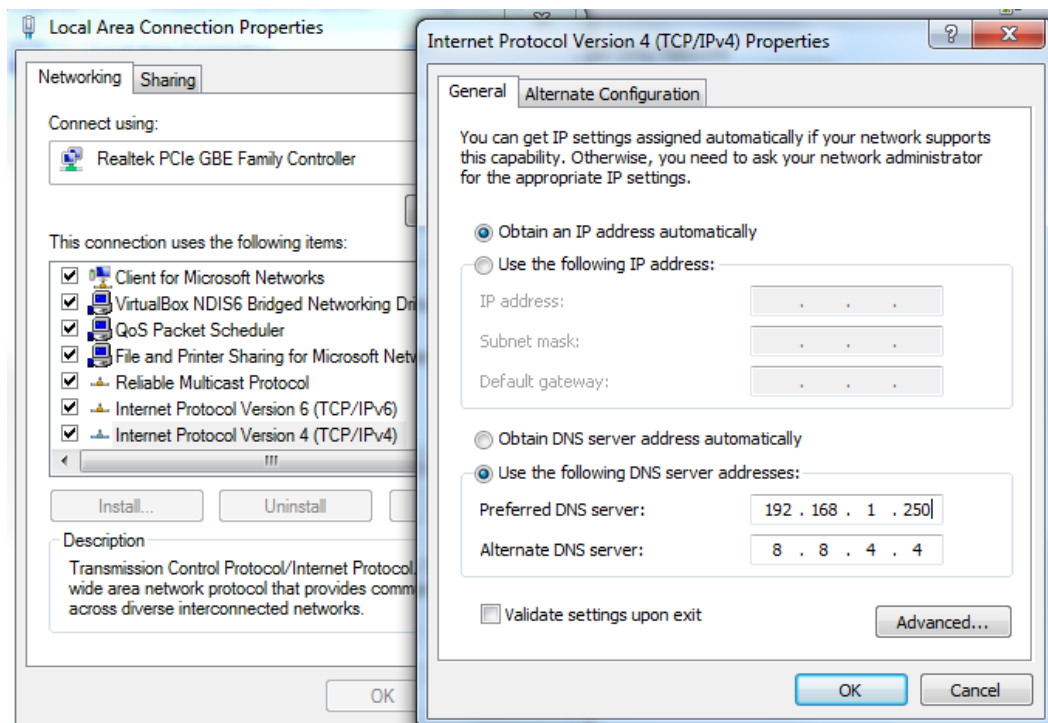
C:\Users\Admin>nslookup www.ctu.edu.vn 192.168.1.250
Server: www.qtht.com.vn
Address: 192.168.1.250

Non-authoritative answer:
Name: www.ctu.edu.vn
Address: 123.30.143.225

C:\Users\Admin>
```

Ta cũng có thể kiểm tra trên **máy vật lý**

- Trên máy vật lý, cấu hình DNS server là IP của máy ảo CentOS. Sau đó, mở trình duyệt web và truy cập vào địa chỉ <http://www.qtht.com.vn/myweb>



Cấu hình **DNS server** là IP của **máy ảo CentOS** trên **máy vật lý**

```
B2111933@localhost:~  
[B2111933@myserver ~]$ sudo systemctl status httpd  
[sudo] password for B2111933:  
● httpd.service - The Apache HTTP Server  
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)  
   Active: active (running) since Tue 2023-04-04 00:56:49 +07; 1 week 3 days ago  
     Docs: man:httpd.service(8)  
  Main PID: 92203 (httpd)  
    Status: "Total requests: 14; Idle/Busy workers 100/0;Requests/sec: 1.49e-05; Bytes served/sec:  
    Tasks: 278 (limit: 23052)  
   Memory: 44.1M  
      CPU: 20.061s  
   CGroup: /system.slice/httpd.service
```

Kiểm tra dịch vụ **webserver** trên máy ảo CentOS



#### 4. Cấu hình tường lửa Firewallld

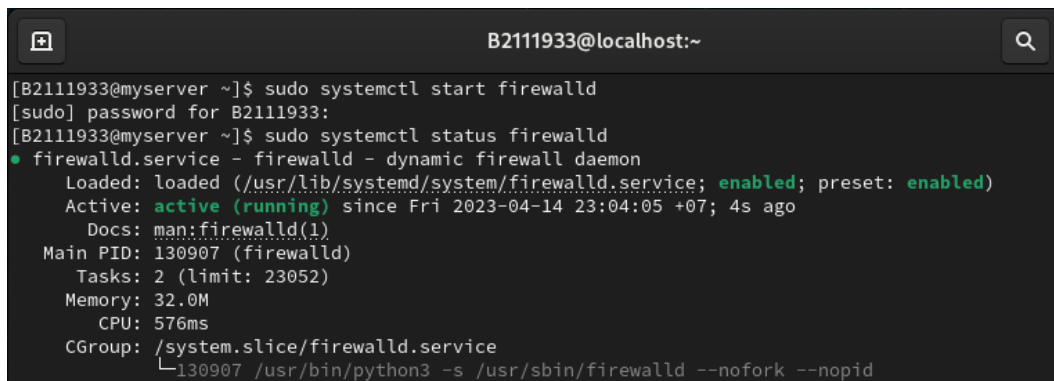
Công cụ Firewallld (dynamic firewall daemon) cung cấp dịch vụ tường lửa mạnh mẽ, toàn diện; được cài đặt mặc định cho nhiều bản phân phối Linux. Từ CentOS 7 trở về sau, tường lửa Firewallld được thay thế cho tường lửa iptables với những khác biệt cơ bản:

- Firewallld sử dụng “zone” như là một nhóm các quy tắc (rule) áp đặt lên những luồng dữ liệu. Một số zone có sẵn thường dùng:
  - *drop*: ít tin cậy nhất – toàn bộ các kết nối đến sẽ bị từ chối.
  - *public*: đại diện cho mạng công cộng, không đáng tin cậy. Các máy tính/services khác không được tin tưởng trong hệ thống nhưng vẫn cho phép các kết nối đến tùy từng trường hợp cụ thể.
  - *trusted*: đáng tin cậy nhất – tin tưởng toàn bộ thiết bị trong hệ thống.
- Firewallld quản lý các quy tắc được thiết lập tự động, có tác dụng ngay lập tức mà không làm mất đi các kết nối và session hiện có.
  - *Runtime* (mặc định): có tác dụng ngay lập tức nhưng mất hiệu lực khi reboot hệ thống.
  - *Permanent*: không áp dụng cho hệ thống đang chạy, cần reload mới có hiệu lực, tác dụng vĩnh viễn cả khi reboot hệ thống.

Tìm hiểu và thực hiện các yêu cầu sau (kèm hình minh họa cho từng bước):

- Khởi động tường lửa firewallld

```
$sudo systemctl start firewallld
```

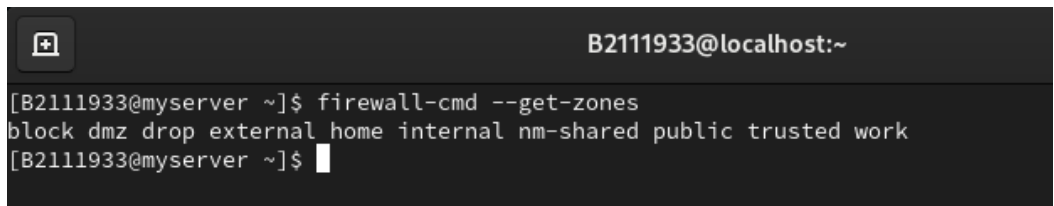


```
B2111933@localhost:~
[B2111933@myserver ~]$ sudo systemctl start firewallld
[sudo] password for B2111933:
[B2111933@myserver ~]$ sudo systemctl status firewallld
● firewallld.service - firewallld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
   Active: active (running) since Fri 2023-04-14 23:04:05 +07; 4s ago
     Docs: man:firewalld(1)
    Main PID: 130907 (firewalld)
      Tasks: 2 (limit: 23052)
     Memory: 32.0M
        CPU: 576ms
    CGroup: /system.slice/firewalld.service
            └─130907 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid
```

Khởi động tường lửa firewallld và kiểm tra trạng thái

- Liệt kê tất cả các zone đang có trong hệ thống

```
$firewall-cmd --get-zones
```

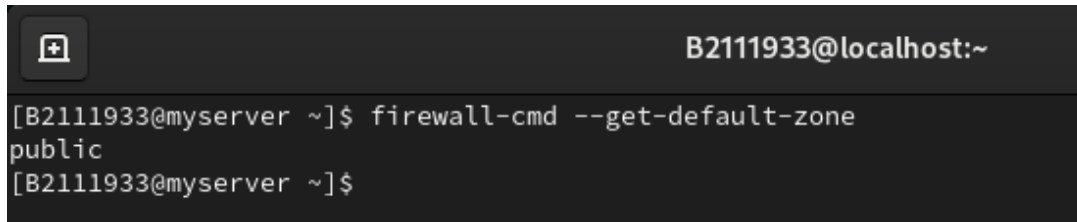


```
B2111933@localhost:~
[B2111933@myserver ~]$ firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
[B2111933@myserver ~]$
```

Liệt kê tất cả các **zone** đang có trong hệ thống, tiêu biểu là **drop**, **public**, **trusted**

- Kiểm tra zone mặc định

```
$firewall-cmd --get-default-zone
```



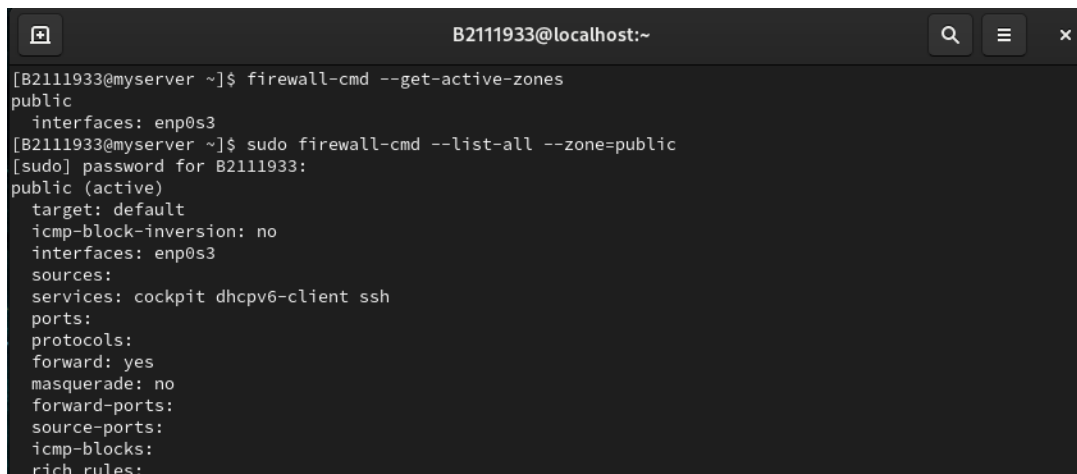
```
B2111933@localhost:~  
[B2111933@myserver ~]$ firewall-cmd --get-default-zone  
public  
[B2111933@myserver ~]$
```

Khi chúng ta thêm các cấu hình vào tường lửa mà không ghi rõ **zone** nào thì mặc nhiên các thay đổi ấy sẽ áp dụng lên zone **public**.

- Kiểm tra zone đang được sử dụng bởi giao diện mạng (thường là *public*); và xem các rules của zone

```
$firewall-cmd --get-active-zones
```

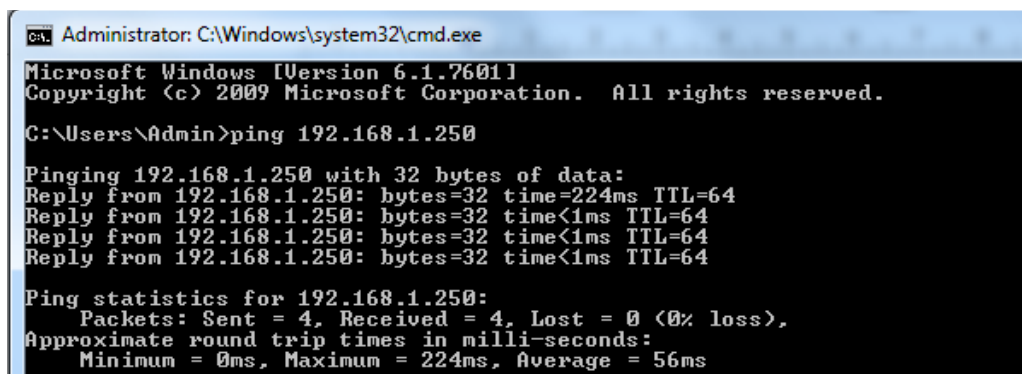
```
$sudo firewall-cmd --list-all --zone=public
```



```
B2111933@localhost:~  
[B2111933@myserver ~]$ firewall-cmd --get-active-zones  
public  
  interfaces: enp0s3  
[B2111933@myserver ~]$ sudo firewall-cmd --list-all --zone=public  
[sudo] password for B2111933:  
public (active)  
  target: default  
  icmp-block-inversion: no  
  interfaces: enp0s3  
  sources:  
  services: cockpit dhcpv6-client ssh  
  ports:  
  protocols:  
  forward: yes  
  masquerade: no  
  forward-ports:  
  source-ports:  
  icmp-blocks:  
  rich rules:
```

Ta thấy rằng giao diện card mạng **enp0s3** sử dụng zone **public** và các **rules** của zone. Do **target: default** nên zone này chỉ cho phép một số dịch vụ mạng chỉ định.

- Từ máy vật lý, ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS. Cho biết kết quả.



```
Administrator: C:\Windows\system32\cmd.exe  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Users\Admin>ping 192.168.1.250  
  
Pinging 192.168.1.250 with 32 bytes of data:  
Reply from 192.168.1.250: bytes=32 time=224ms TTL=64  
Reply from 192.168.1.250: bytes=32 time<1ms TTL=64  
Reply from 192.168.1.250: bytes=32 time<1ms TTL=64  
Reply from 192.168.1.250: bytes=32 time<1ms TTL=64  
  
Ping statistics for 192.168.1.250:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 224ms, Average = 56ms
```

Do rule không chặn **icmp** nên ta có thể ping được tới máy CentOS từ máy vật lý.

Basic SSH settings

Remote host \*192.168.1.250Specify usernamePort 22

Advanced SSH settings

Terminal settingsNetwork settingsBookmark settings

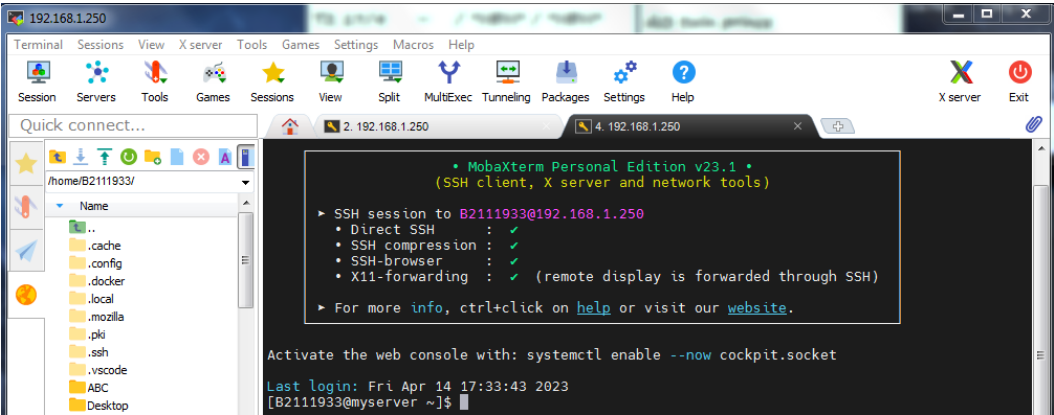
☒X11-Forwarding☒CompressionRemote environment: Interactive shell

Execute command:Do not exit after command ends

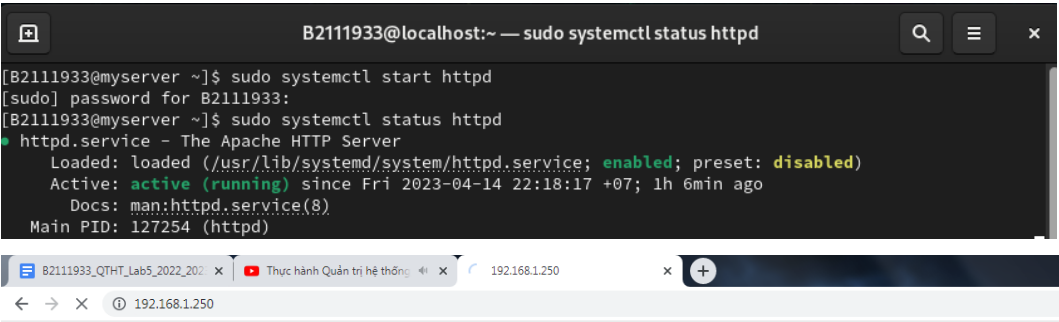
SSH-browser type: SFTP protocolFollow SSH path (experimental)

☒Use private keyC:\Users\Admin\Desktop\id\_rsaExpert SSH settings

Execute macro at session start: <none>



Dịch vụ **SSH** cũng được cho phép nên ta có thể kết nối **SSH**



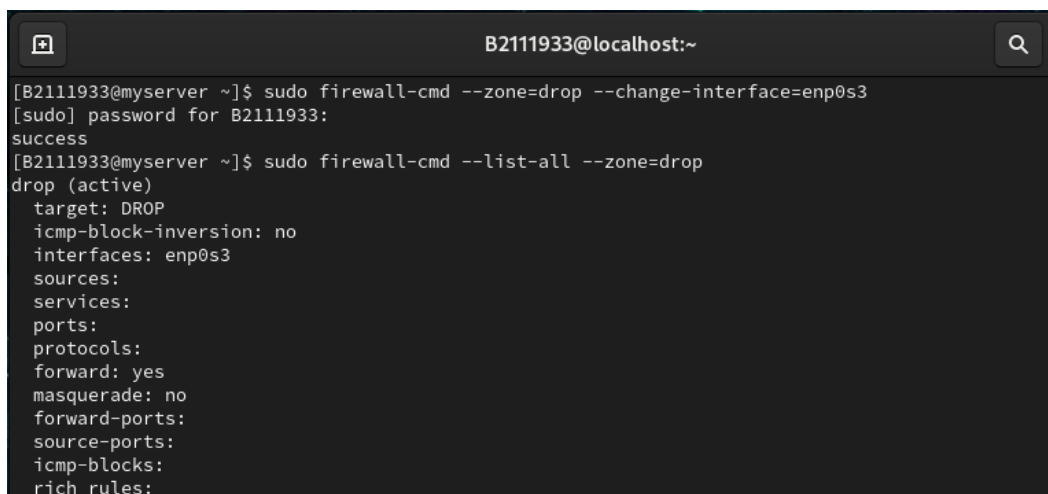
Không thể truy cập trang web này

192.168.1.250 mất quá nhiều thời gian để phản hồi.

Do zone **public** chưa cho phép dịch vụ **http** nên ta không thể truy cập dịch vụ **web**,

- Chuyển giao diện mạng sang zone *drop*; và xem các rules của zone

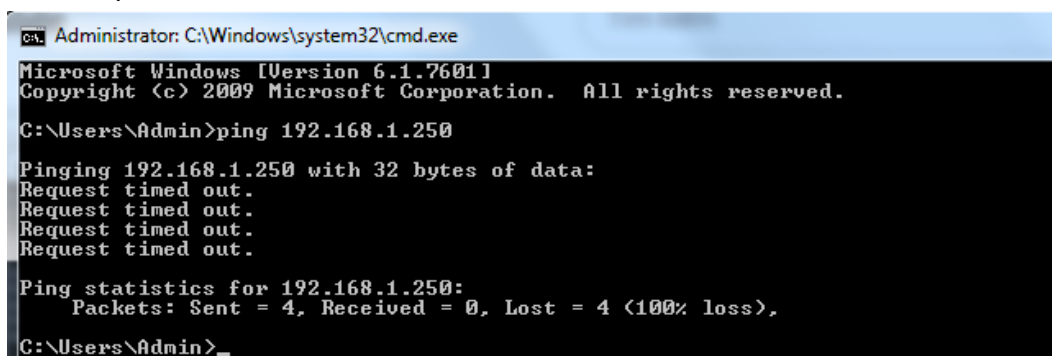
```
$sudo firewall-cmd --zone=drop --change-interface=enp0s3  
$sudo firewall-cmd --list-all --zone=drop
```



```
B2111933@localhost:~  
[B2111933@myserver ~]$ sudo firewall-cmd --zone=drop --change-interface=enp0s3  
[sudo] password for B2111933:  
success  
[B2111933@myserver ~]$ sudo firewall-cmd --list-all --zone=drop  
drop (active)  
  target: DROP  
  icmp-block-inversion: no  
  interfaces: enp0s3  
  sources:  
  services:  
  ports:  
  protocols:  
  forward: yes  
  masquerade: no  
  forward-ports:  
  source-ports:  
  icmp-blocks:  
  rich rules:
```

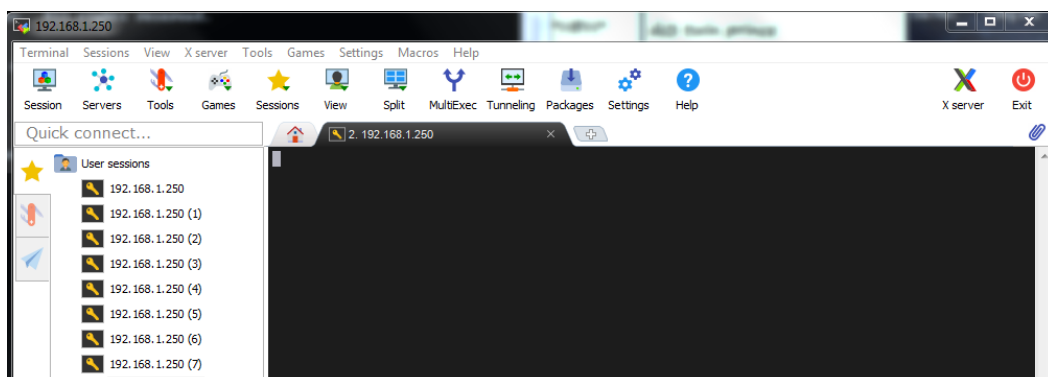
Chuyển giao diện mạng sang zone **drop**; và xem các **rules** của **zone**. Ta thấy rằng **zone** này chặn tất cả dịch vụ mạng

- Từ máy vật lý, ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS. Cho biết kết quả.

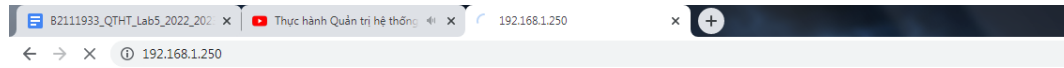


```
Administrator: C:\Windows\system32\cmd.exe  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Users\Admin>ping 192.168.1.250  
  
Pinging 192.168.1.250 with 32 bytes of data:  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
  
Ping statistics for 192.168.1.250:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
  
C:\Users\Admin>
```

Ta không thể ping được đến máy **CentOS**



Ta cũng không thể kết nối **SSH** đến máy **CentOS**



Không thể truy cập trang web này

192.168.1.250 mất quá nhiều thời gian để phản hồi.

Và ta cũng không thể nối kết với **dịch vụ web**

- Chuyển giao diện mạng sang zone *trusted*; và xem các rules của zone  
\$sudo firewall-cmd --zone=trusted --change-interface=enp0s3  
\$sudo firewall-cmd --list-all --zone=trusted

```
B2111933@localhost:~  
[B2111933@myserver ~]$ sudo firewall-cmd --zone=trusted --change-interface=enp0s3  
[sudo] password for B2111933:  
success  
[B2111933@myserver ~]$ sudo firewall-cmd --list-all --zone=trusted  
trusted (active)  
target: ACCEPT  
icmp-block-inversion: no  
interfaces: enp0s3  
sources:  
services:  
ports:  
protocols:  
forward: yes  
masquerade: no  
forward-ports:  
source-ports:  
icmp-blocks:  
rich rules:  
[B2111933@myserver ~]$
```

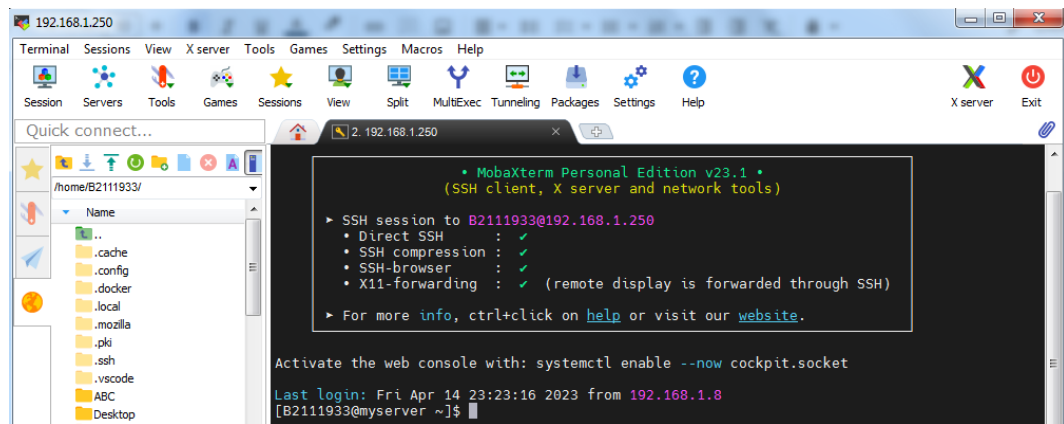
Chuyển giao diện mạng sang zone **trusted**; và xem các **rules** của **zone**. Ta thấy rằng zone **trusted** cho phép tất cả dịch vụ mạng (**target: ACCEPT**)

- Từ máy vật lý, ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS. Cho biết kết quả.

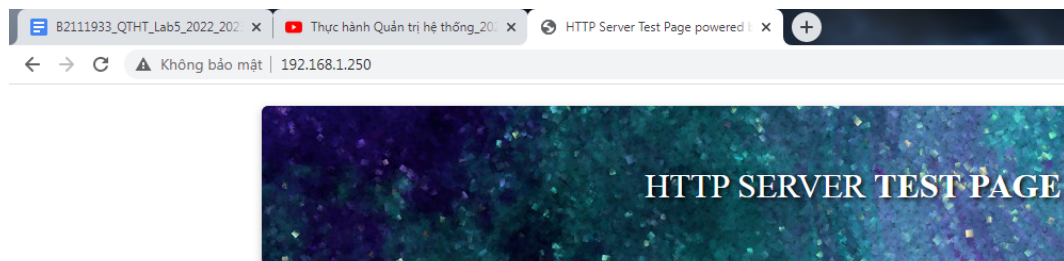
```
Administrator: C:\Windows\system32\cmd.exe  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Users\Admin>ping 192.168.1.250  
  
Pinging 192.168.1.250 with 32 bytes of data:  
Reply from 192.168.1.250: bytes=32 time<1ms TTL=64  
Reply from 192.168.1.250: bytes=32 time<1ms TTL=64  
Reply from 192.168.1.250: bytes=32 time<1ms TTL=64  
Reply from 192.168.1.250: bytes=32 time<1ms TTL=64  
  
Ping statistics for 192.168.1.250:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 0ms, Average = 0ms  
  
C:\Users\Admin>
```

Ta có thể ping được tới máy **CentOS**





Ta cũng có thể kết nối SSH



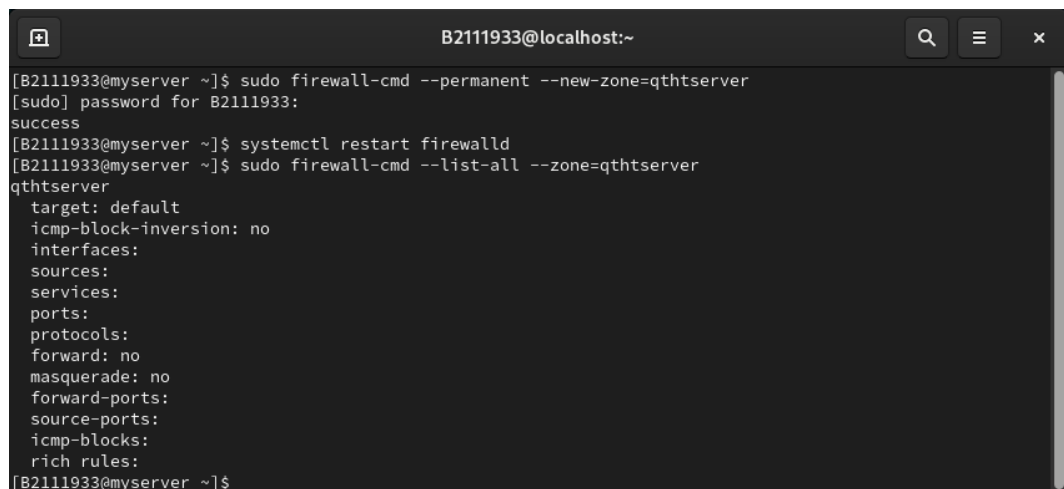
Tương tự ta có thể kết nối dịch vụ web

- Tạo zone mới có tên là *qthtserver*

```
$sudo firewall-cmd --permanent --new-zone=qthtserver
```

```
$sudo systemctl restart firewalld
```


```
$sudo firewall-cmd --list-all --zone=qthtserver
```



Tạo zone mới có tên là **qthtserver** luôn khả dụng sau khi restart máy và liệt kê các **rules** của zone **qthtserver**

- Cho phép các dịch vụ HTTP, DNS, SAMBA, FTP và cổng 9999/tcp hoạt động trên zone **qthtserver**

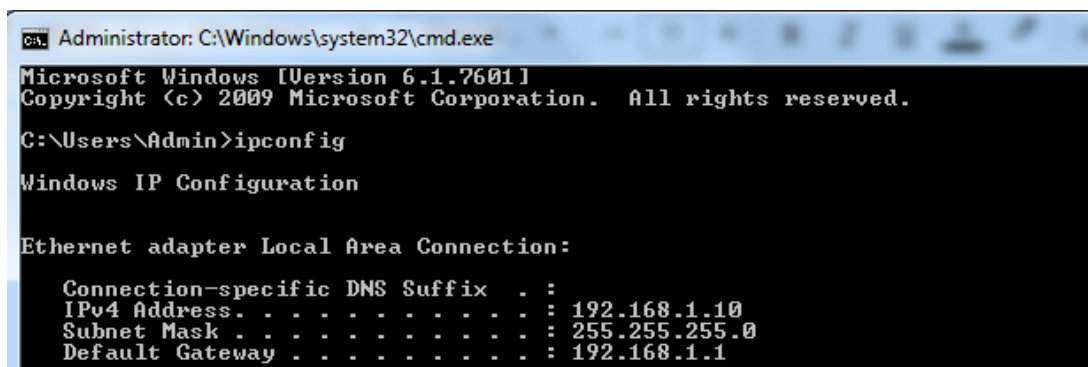
```
$sudo firewall-cmd --permanent --zone=qthtserver --add-service=http
$sudo firewall-cmd --permanent --zone=qthtserver --add-service=dns
$sudo firewall-cmd --permanent --zone=qthtserver --add-service=samba
$sudo firewall-cmd --permanent --zone=qthtserver --add-service=ftp
$sudo firewall-cmd --permanent --zone=qthtserver --add-port=9999/tcp
```



A terminal window titled 'B2111933@localhost:~' showing the execution of firewall commands. The user runs 'sudo firewall-cmd --permanent --zone=qthtserver --add-service=http', followed by 'sudo firewall-cmd --permanent --zone=qthtserver --add-service=dns', 'sudo firewall-cmd --permanent --zone=qthtserver --add-service=samba', 'sudo firewall-cmd --permanent --zone=qthtserver --add-service=ftp', and finally 'sudo firewall-cmd --permanent --zone=qthtserver --add-port=9999/tcp'. Each command is followed by a 'success' message.

Cho phép các dịch vụ theo yêu cầu và cổng 9999/tcp hoạt động trên zone **qthtserver**

- Thêm rule để chỉ cho phép máy vật lý có thể SSH tới máy CentOS
- ```
$sudo firewall-cmd --permanent --zone=qthtserver --add-rich-rule='rule family=ipv4 source address=<IP máy vật lý>/32 port port=22 protocol=tcp accept'
```



A Windows command prompt window titled 'Administrator: C:\Windows\system32\cmd.exe' showing the output of the 'ipconfig' command. The output displays the IP configuration for the 'Ethernet adapter Local Area Connection:', including the IPv4 Address (192.168.1.10), Subnet Mask (255.255.255.0), and Default Gateway (192.168.1.1).

Kiểm tra địa chỉ IP máy vật lý

```
B2111933@localhost:~  
[B2111933@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-rich-rule='rule family=ipv4  
source address=192.168.1.10/32 port port=22 protocol=tcp accept'  
success  
[B2111933@myserver ~]$
```

Những gói mạng nào là giao thức **IP4** có địa chỉ gửi đúng **192.168.1.10** truy cập đến **cổng 22** thì mới được chấp nhận (ở đây là **máy vật lý**)

- Khởi động lại tường lửa firewalld

```
$sudo systemctl restart firewalld
```

```
B2111933@localhost:~  
[B2111933@myserver ~]$ sudo systemctl restart firewalld  
[B2111933@myserver ~]$ sudo systemctl status firewalld  
● firewalld.service - firewalld - dynamic firewall daemon  
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)  
   Active: active (running) since Sat 2023-04-15 00:57:02 +07; 8s ago  
     Docs: man:firewalld(1)  
  Main PID: 139003 (firewalld)  
    Tasks: 2 (limit: 23052)  
   Memory: 23.8M  
      CPU: 320ms  
   CGroup: /system.slice/firewalld.service  
           └─139003 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid
```

Khởi động lại **tường lửa firewalld** và kiểm tra trạng thái

- Chuyển giao diện mạng sang zone qthtserver; và xem các rules của zone

```
$sudo firewall-cmd --permanent --zone=qthtserver
```

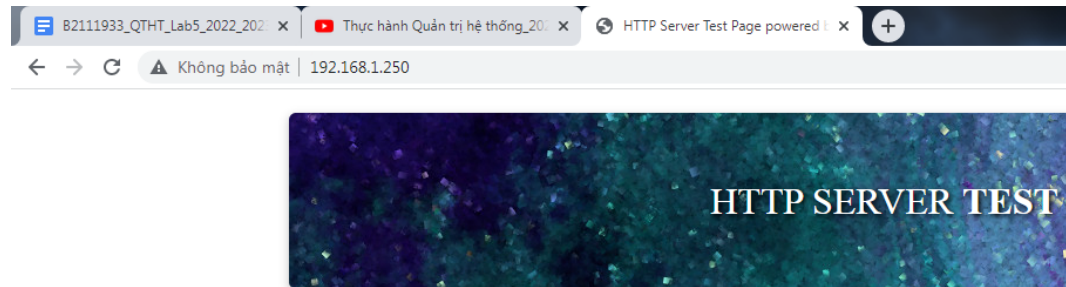
```
--change-interface=enp0s3
```

```
$sudo firewall-cmd --list-all --zone=qthtserver
```

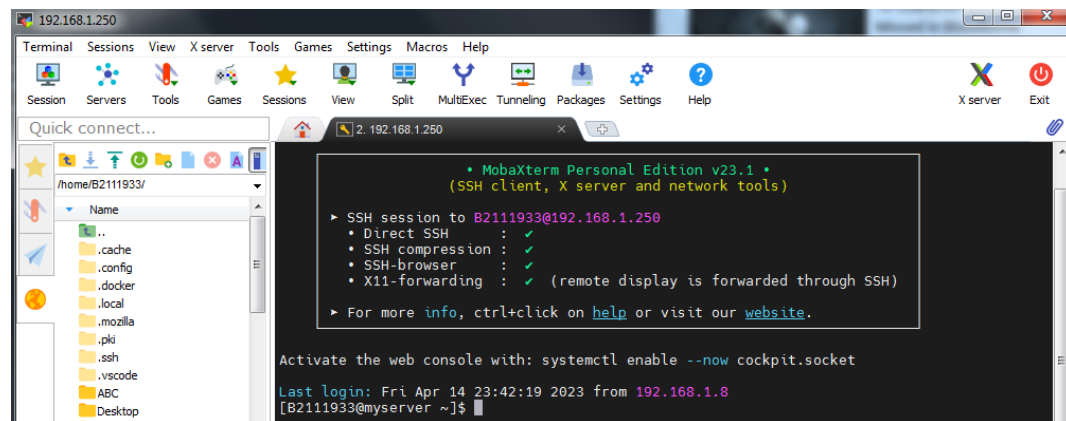
```
B2111933@localhost:~  
[B2111933@myserver ~]$ sudo firewall-cmd --zone=qthtserver --change-interface=enp0s3  
success  
[B2111933@myserver ~]$ sudo firewall-cmd --list-all --zone=qthtserver  
qthtserver (active)  
target: default  
icmp-block-inversion: no  
interfaces: enp0s3  
sources:  
services: dns ftp http samba  
ports: 9999/tcp  
protocols:  
forward: no  
masquerade: no  
forward-ports:  
source-ports:  
icmp-blocks:  
rich rules:  
    rule family="ipv4" source address="192.168.1.10/32" port port="22" protocol="tcp" accept  
[B2111933@myserver ~]$
```

Chuyển **giao diện mạng** sang zone **qthtserver**; các rules của **zone** đã được áp dụng

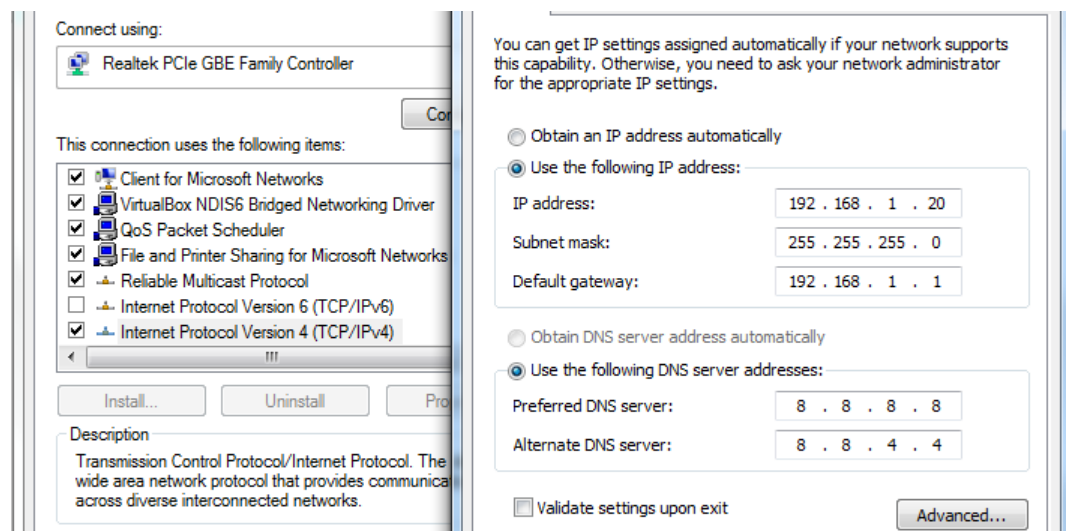
- Kiểm tra máy vật lý có thể truy cập được tới các dịch vụ trên máy CentOS hay không.



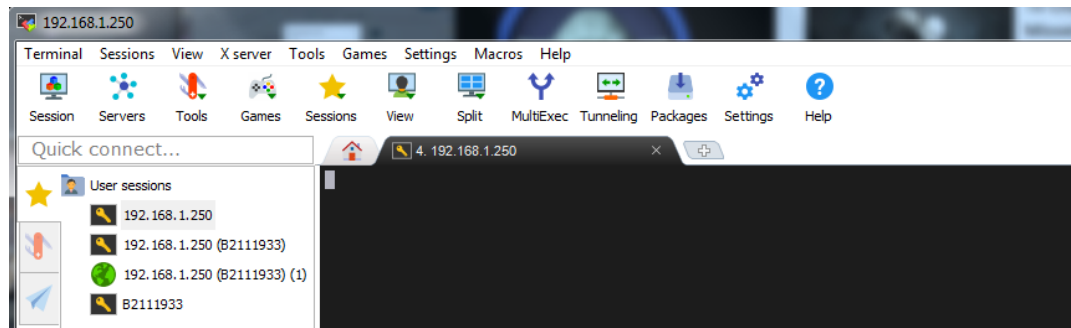
Ta có thể truy cập dịch vụ **http** bình thường



Ta cũng có thể truy cập đến dịch vụ **SSH**



Thử đổi **địa chỉ IP** của máy vật lý



Lúc bấy giờ ta không thể kết nối **SSH** đến máy **CentOS** được nữa

--- Hết ---