



LAB 5

DOCKER, SAMBA, DNS và Firewall

Họ tên và MSSV: Lê Bích Trâm B2204973

Nhóm học phần: 4

- 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. Hình minh họa chỉ cần chụp ở nội dung thực hiện, không chụp toàn màn hình.
- Video hướng dẫn ở cuối bài.

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)
- 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:

Lệnh thực hiện: `sudo systemctl stop firewalld`

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)
- Lệnh thực hiện: **`sudo dnf -y remove podman runc`**

```
[B2204973@localhost ~]$ sudo dnf -y remove podman runc
[sudo] password for B2204973:
```

```
Removed:
cockpit-podman-92-1.el9.noarch
common-3:2.1.12-1.el9.x86_64
passt-0^20240806.gee36266-2.el9.x86_64
passt-selinux-0^20240806.gee36266-2.el9.noarch
podman-2:5.2.1-1.el9.x86_64
```

Complete!

- Cài đặt công cụ yum-utils

Lệnh thực hiện: **`sudo dnf install -y yum-utils`**

```
[B2204973@localhost ~]$ sudo dnf install -y yum-utils
Updating Subscription Management repositories.
Unable to read consumer identity
```

```
Installed:
  yum-utils-4.3.0-17.el9.noarch

Complete!
```

- Thêm địa repo của Docker vào công cụ yum

Lệnh thực hiện: **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.

```
[B2204973@localhost ~]$ sudo yum-config-manager --add-repo \https://download.do
cker.com/linux/centos/docker-ce.repo
Updating Subscription Management repositories.
```

```
Adding repo from: https://download.docker.com/linux/centos/docker-ce.repo
[B2204973@localhost ~]$
```

- Cài đặt Docker

Lệnh thực hiện: **sudo dnf install docker-ce -y**

```
[B2204973@localhost ~]$ sudo dnf install -y docker-ce
Updating Subscription Management repositories.
```

```
Installed:
  containerd.io-1.7.22-3.1.el9.x86_64
  docker-buildx-plugin-0.17.1-1.el9.x86_64
  docker-ce-3:27.3.1-1.el9.x86_64
  docker-ce-cli-1:27.3.1-1.el9.x86_64
  docker-ce-rootless-extras-27.3.1-1.el9.x86_64
  docker-compose-plugin-2.29.7-1.el9.x86_64

Complete!
```

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

Lệnh thực hiện: **sudo usermod -aG docker \$USER**

```
[B2204973@localhost ~]$ sudo usermod -aG docker $USER
[B2204973@localhost ~]$
```

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

Lệnh thực hiện: **su - \$USER**

```
[B2204973@localhost ~]$ su - $USER
Password:
```

- Chạy dịch vụ Docker

Lệnh thực hiện: **sudo systemctl start docker**

```
[B2204973@localhost ~]$ sudo systemctl start docker
[B2204973@localhost ~]$
```

Lệnh thực hiện: **sudo systemctl enable docker**

```
[B2204973@localhost ~]$ sudo systemctl enable docker
Created symlink /etc/systemd/system/multi-user.target.wants/docker.service → /usr/lib/systemd/system/docker.service.
```

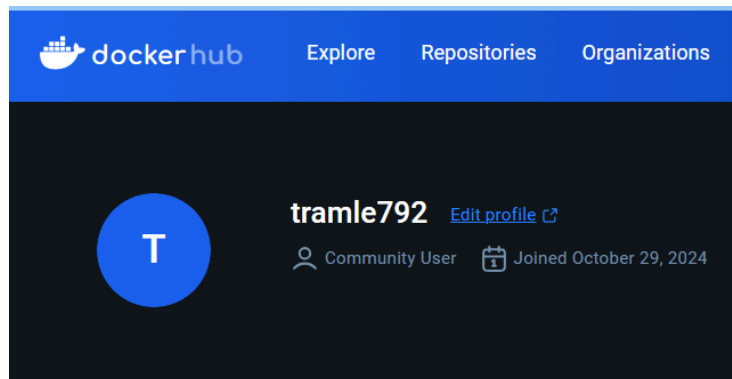
- Kiểm tra lại thấy docker đã chạy trên máy

Lệnh thực hiện: **sudo systemctl status docker**

```
[B2204973@localhost ~]$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
   Loaded: loaded (/usr/lib/systemd/system/docker.service; vendor preset: enabled)
   Active: active (running) since Tue 2024-10-29 10:44:10 UTC; 1min 45s ago
     Triggers: ● docker.socket
```

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

Tạo 1 tài khoản trên dorkerhub



Đăng nhập:

- Lệnh thực hiện: **docker login -u tramle792**

```
[B2204973@localhost ~]$ docker login -u tramle792
Password:
WARNING! Your password will be stored unencrypted in /root/.docker/config.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credential-helper-configuration

Login Succeeded
[B2204973@localhost ~]$
```

- 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.

Lệnh thực hiện: **docker run hello-world**

```
[B2204973@localhost ~]$ docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
0ad24096d23b: Pull complete
Digest: sha256:3b6913a267eef7bfc495946867f32794f1e5b26c32b157e7e5a701838e1e58eb
Status: Downloaded newer image for hello-world:latest
Hello from Docker!
This message shows that your installation appears to be working correctly.
```

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.

Lệnh thực hiện: **docker search httpd**

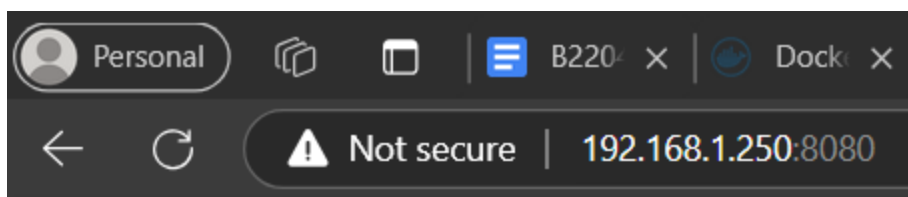
```
[B2204973@localhost ~]$ docker search httpd
NAME                DESCRIPTION
httpd               The Apache HTTP Server Project
manageiq/httpd      Container with httpd, built on CentOS for Ma...
```

- Tạo container từ image httpd

Lệnh thực hiện: **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.

```
[B2204973@localhost ~]$ docker run -d -it -p 8080:80 --name webserver httpd
Unable to find image 'httpd:latest' locally
```



It works!

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

Để phân biệt với bài thực hành 4 (đổi ngược lại mã số sinh viên: B2204973-> B3794022). Chỉnh lại nội dung file index.html:

Lệnh thực hiện: **nano ./myweb/index.html**

```
[B2204973@localhost ~]$ nano ./myweb/index.html
[B2204973@localhost ~]$
```

```
GNU nano 5.6.1                               ./myweb/index.html
<!doctype html>
<html>
<head>
<meta charset="utf-8">
<title>Tổng công ty bánh kẹo Lương Sơn Bạc</title>
</head>
<body>
<H1>Welcome!<H1>
<marquee>Designed by B3794022</marquee>
</body>
</html>
```

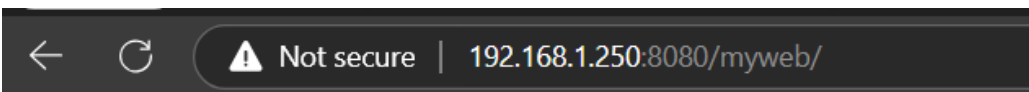
- Sao chép thư mục ~/myweb vào thư mục gốc của dịch vụ của web trên Docker container.

Lệnh thực hiện: **docker cp myweb/ webserver:/usr/local/apache2/htdocs/**

```
[B2204973@localhost ~]$ docker cp myweb/ webserver:/usr/local/apache2/htdocs/
Successfully copied 2.56kB to webserver:/usr/local/apache2/htdocs/
[B2204973@localhost ~]$
```

- 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.

Truy cập: **192.168.1.250:8080/myweb/**



Welcome!

Designed by B3794022

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.

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

- Cài đặt dịch vụ Samba:

Lệnh thực hiện: **sudo dnf install -y samba**

```
[B2204973@localhost ~]$ sudo dnf install -y samba
[sudo] password for B2204973:
Updating Subscription Management repositories.

Installed:
  libnetapi-4.20.2-2.el9.x86_64
  samba-common-tools-4.20.2-2.el9.x86_64
  samba-ldb-ldap-modules-4.20.2-2.el9.x86_64

Complete!
```

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

Lệnh thực hiện: **sudo adduser tramle**

```
[B2204973@localhost ~]$ sudo adduser tramle
[B2204973@localhost ~]$
```

Lệnh thực hiện: **sudo passwd tramle**

```
[B2204973@localhost ~]$ sudo passwd tramle
Changing password for user tramle.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[B2204973@localhost ~]$
```

Lệnh thực hiện: **sudo groupadd lecturers**

```
[B2204973@localhost ~]$ sudo groupadd lecturers
[B2204973@localhost ~]$
```

Lệnh thực hiện: **sudo usermod -a -G lecturers tramle**

```
[B2204973@localhost ~]$ sudo usermod -a -G lecturers tramle
[B2204973@localhost ~]$
```

- Tạo thư mục cần chia sẻ và phân quyền:

Lệnh thực hiện: **sudo mkdir /data**

```
[B2204973@localhost ~]$ sudo mkdir /data
[B2204973@localhost ~]$
```

Lệnh thực hiện: **sudo chown :lecturers /data**

```
[B2204973@localhost ~]$ sudo chown :lecturers /data
[B2204973@localhost ~]$
```

Lệnh thực hiện: **sudo chmod -R 775 /data**

```
[B2204973@localhost ~]$ sudo chmod -R 775 /data
[B2204973@localhost ~]$
```

- Kiểm tra lại ta thấy trên thư mục gốc đã có thư mục data với chủ sở hữu là lecturers, nhóm chủ sở hữu có toàn quyền

Lệnh thực hiện: **ls -l /**

```
[B2204973@localhost ~]$ ls -l /
total 24
dr-xr-xr-x.  2 root root      6 Jun 25 21:23 afs
lrwxrwxrwx.  1 root root      7 Jun 25 21:23 bin -> usr/bin
dr-xr-xr-x.  5 root root 4096 Oct 29 09:35 boot
drwxrwxr-x.  2 root lecturers 35 Nov  1 09:54 data
drwxr-xr-x.  20 root root 32768 Nov  1 09:36 dev
```

- Cấu hình dịch vụ Samba:

Lệnh thực hiện: **sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.orig**

```
[B2204973@localhost ~]$ sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.orig
[B2204973@localhost ~]$
```

Lệnh thực hiện: **sudo nano /etc/samba/smb.conf**

#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
```

```
[B2204973@localhost ~]$ sudo nano /etc/samba/smb.conf
[B2204973@localhost ~]$
```

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

- Thêm người dùng cho dịch vụ Samba:
Lệnh thực hiện: **sudo smbpasswd -a tramle**
#Đặt mật khẩu Samba cho người dùng

```
[B2204973@localhost ~]$ sudo smbpasswd -a tramle
New SMB password:
Retype new SMB password:
Added user tramle.
[B2204973@localhost ~]$
```

- Cấu hình SELINUX cho phép Samba vào thư mục home
Lệnh thực hiện: **sudo setsebool -P samba_export_all_rw on**

```
[B2204973@localhost ~]$ sudo setsebool -P samba_export_all_rw on
[B2204973@localhost ~]$
```

- Lệnh thực hiện: **sudo setsebool -P samba_enable_home_dirs on**

```
[B2204973@localhost ~]$ sudo setsebool -P samba_enable_home_dirs on
[B2204973@localhost ~]$
```

- Tắt tường lửa:
Lệnh thực hiện: **sudo systemctl stop firewalld**

```
[B2204973@localhost ~]$ sudo systemctl stop firewalld
[B2204973@localhost ~]$
```

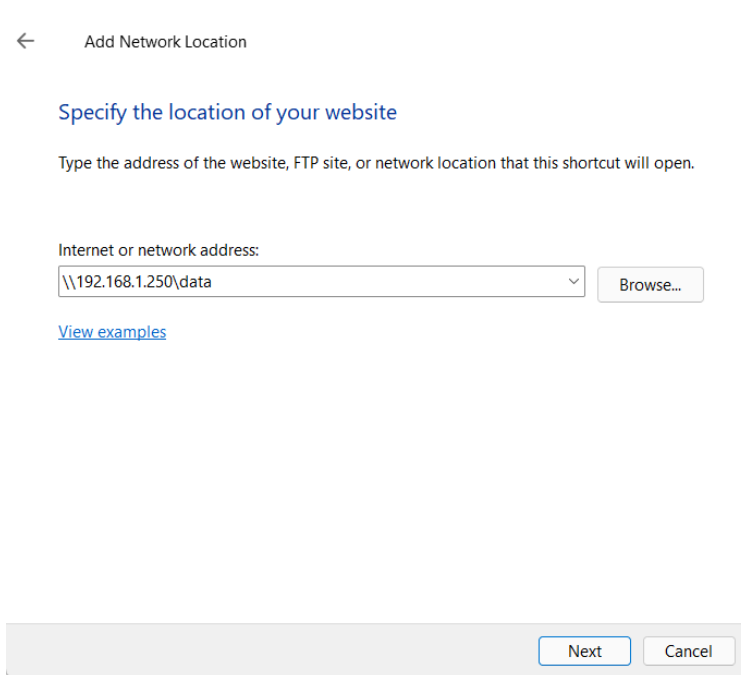
- Khởi động cho phép Samba tự động thực thi khi khởi động hệ điều hành:
Lệnh thực hiện: **sudo systemctl start smb**

```
[B2204973@localhost ~]$ sudo systemctl start smb
[B2204973@localhost ~]$
```


Lệnh thực hiện:

```
[B2204973@localhost ~]$ sudo systemctl enable smb
Created symlink /etc/systemd/system/multi-user.target.wants/smb.service → /usr/lib/systemd/system/smb.service.
[B2204973@localhost ~]$
```

- 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



← Add Network Location

Specify the location of your website

Type the address of the website, FTP site, or network location that this shortcut will open.

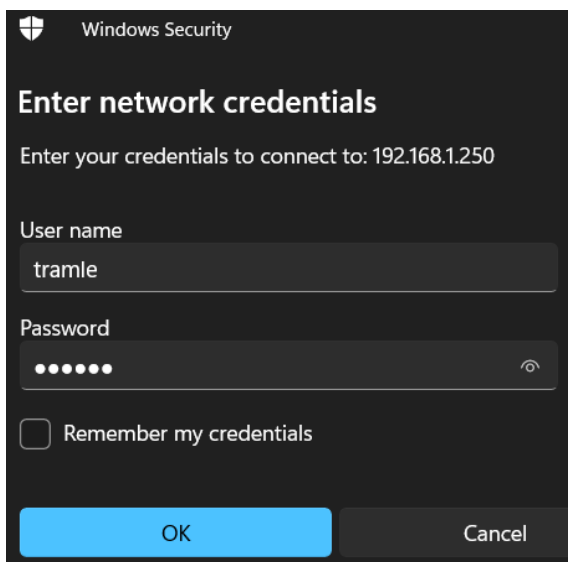
Internet or network address:

\\192.168.1.250\data

[View examples](#)

[Browse...](#)

Next Cancel



Windows Security

Enter network credentials

Enter your credentials to connect to: 192.168.1.250

User name

tramle

Password

•••••

☐ Remember my credentials

OK Cancel

What do you want to name this location?

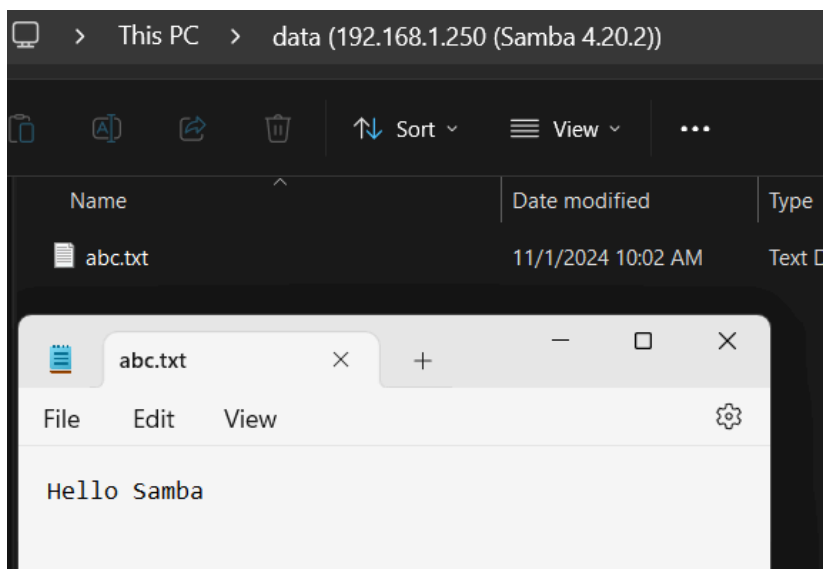
Create a name for this shortcut that will help you easily identify this network location:

\\192.168.1.250\data.

Type a name for this network location:

data (192.168.1.250 (Samba 4.20.2))

- Trên máy windows tạo tập tin abc.txt với nội dung Hello Samba



- Kiểm tra lại trên máy CentOS

Lệnh thực hiện: **ls /data**

```
[B2204973@localhost ~]$ ls /data
abc.txt
[B2204973@localhost ~]$
```

Lệnh thực hiện: **cat /data/abc.txt**

```
[B2204973@localhost ~]$ cat /data/abc.txt
Hello Samba
[B2204973@localhost ~]$
```

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:

Lệnh thực hiện: **sudo dnf install bind bind-utils -y**

```
[B2204973@localhost ~]$ sudo dnf install bind bind-utils -y
Updating Subscription Management repositories.
```

```
Installed:
bind-32:9.16.23-24.el9.x86_64
bind-dnssec-doc-32:9.16.23-24.el9.noarch
bind-dnssec-utils-32:9.16.23-24.el9.x86_64
python3-bind-32:9.16.23-24.el9.noarch
python3-ply-3.11-14.el9.noarch

Complete!
```

3.2. Cấu hình DNS server:

Lệnh thực hiện: **sudo nano /etc/named.conf**

```
[B2204973@localhost ~]$ sudo nano /etc/named.conf
[B2204973@localhost ~]$
```

```
#(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; };  
};  
...
```

```
options {  
    listen-on port 53 { 127.0.0.1; any; };
```

```
allow-query { localhost; any; };
```

```
recursion yes;  
forwarders {192.168.1.1; } ;
```

```
zone "qtht.com.vn" IN{  
    type master;  
    file "forward.qtht";  
    allow-update {none; };  
};  
  
zone "1.168.192.in-addr.arpa" IN{  
    type master;  
    file "reverse.qtht";  
    allow-update {none; };  
};
```

3.3. Tạo tập tin cấu hình phân giải xuôi:

Lệnh thực hiện: **sudo cp /var/named/named.localhost
/var/named/forward.qtht**

```
[B2204973@localhost ~]$ sudo cp /var/named/named.localhost /var/named/  
forward.qtht  
[B2204973@localhost ~]$
```

Lệnh thực hiện: **sudo chgrp named /var/named/forward.qtht**

```
[B2204973@localhost ~]$ sudo chgrp named /var/named/forward.qtht  
[B2204973@localhost ~]$
```

- Kiểm tra thấy chủ sở hữu của tập tin đã được đổi

Lệnh thực hiện: **sudo ls -l /var/named/**

```
[B2204973@localhost ~]$ sudo ls -l /var/named/  
total 20  
drwxrwx---. 2 named named    6 Sep  5 21:12 data  
drwxrwx---. 2 named named    6 Sep  5 21:12 dynamic  
-rw-r-----. 1 root  named 152 Nov  1 12:22 forward.qtht
```

Lệnh thực hiện: **sudo nano /var/named/forward.qtht**

```
[B2204973@localhost ~]$ sudo nano /var/named/forward.qtht  
[B2204973@localhost ~]$
```

#(tham khảo file mẫu)

Lệnh thực hiện: TTL 1D

```
@    IN    SOA    @  qtht.com.vn. (
                                0      ;Serial
                                1D     ;Refresh
                                1H     ;Retry
                                1W     ;Expire
                                3H     ;Minimum TTL
)
dns   IN    NS    dns.qtht.com.vn.
dns   IN    A     192.168.1.250
www   IN    A     192.168.1.250
htql  IN    A     8.8.8.8
```

```
$TTL 1D
@      IN SOA  @ qtht.com.vn. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )   ; minimum
@      IN     NS      dns.qtht.com.vn.
dns    IN     A       192.168.1.250
www    IN     A       192.168.1.250
htql   IN     A       8.8.8.8
```

3.4. Tạo tập tin cấu hình phân giải ngược:

Lệnh thực hiện: **sudo cp /var/named/forward.qtht /var/named/reverse.qtht**

```
[B2204973@localhost ~]$ sudo cp /var/named/forward.qtht /var/named/
reverse.qtht
[sudo] password for B2204973:
[B2204973@localhost ~]$
```

Lệnh thực hiện: **sudo chgrp named /var/named/reverse.qtht**

```
[B2204973@localhost ~]$ sudo chgrp named /var/named/reverse.qtht
[B2204973@localhost ~]$
```

Lệnh thực hiện: **sudo nano /var/named/reverse.qtht**

```
[B2204973@localhost ~]$ sudo nano /var/named/reverse.qtht
[B2204973@localhost ~]$
```

Lệnh thực hiện: 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
250    IN      PTR  www.qtht.com.vn.
```

```
$TTL 1D
@      IN SOA  @ qtht.com.vn. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )   ; minimum
@      IN     NS      dns.qtht.com.vn.
dns    IN     A       192.168.1.250
250    IN     PTR     www.qtht.com.vn.
```

3.5. Kiểm tra và sử dụng dịch vụ DNS

- Tắt tường lửa:

Lệnh thực hiện: **sudo systemctl stop firewalld**

```
[B2204973@localhost ~]$ sudo systemctl stop firewalld
[B2204973@localhost ~]$
```

- Khởi động dịch vụ DNS:

Lệnh thực hiện: **sudo systemctl start named**

```
[B2204973@localhost ~]$ sudo systemctl start named
[B2204973@localhost ~]$
```

- Kiểm tra trạng thái dịch vụ

Lệnh thực hiện: **sudo systemctl status named**

```
[B2204973@localhost ~]$ sudo systemctl status named
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.s
   Active: active (running) since Fri 2024-11-01 1
```

- Kiểm tra kết quả:

Lệnh thực hiện: **nslookup www.qtht.com.vn 192.168.1.250**

```
[B2204973@localhost ~]$ 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
```

Lệnh thực hiện: **nslookup htql.qtht.com.vn 192.168.1.250**

```
[B2204973@localhost ~]$ nslookup htql.qtht.com.vn 192.168.1.250
Server:          192.168.1.250
Address:         192.168.1.250#53

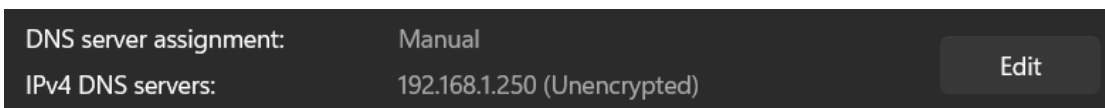
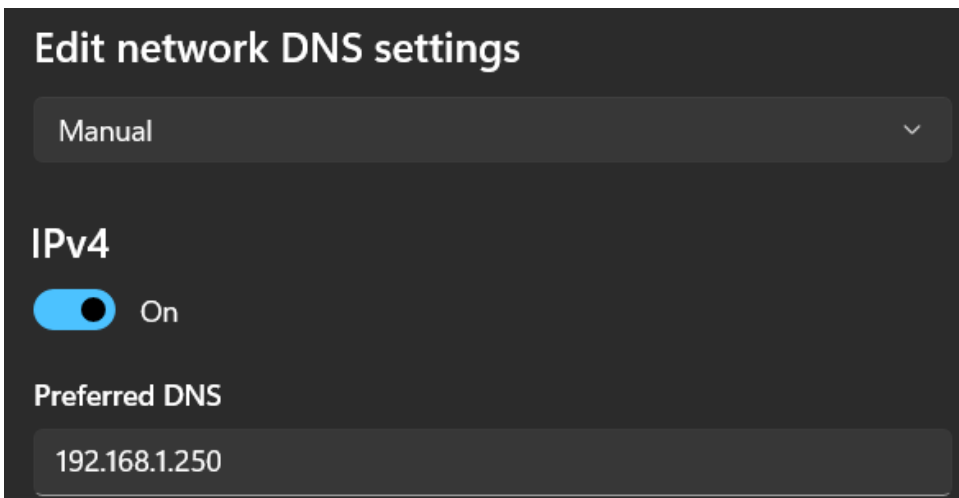
Name:   htql.qtht.com.vn
Address: 8.8.8.8
```

Lệnh thực hiện: **nslookup www.ctu.edu.vn 192.168.1.250**

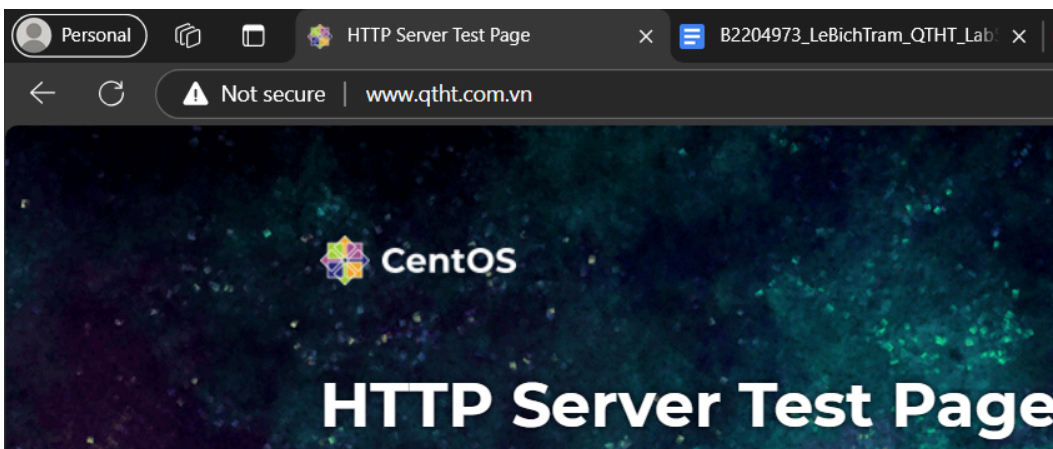
```
[B2204973@localhost ~]$ nslookup www.ctu.edu.vn 192.168.1.250
Server:          192.168.1.250
Address:         192.168.1.250#53

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

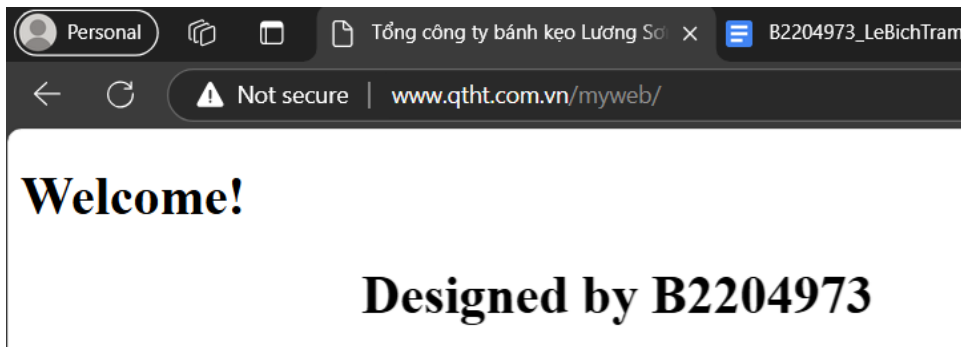
- Trên máy vật lý, cấu hình DNS server là IP của máy ảo CentOS. Sau đó, mở trình duyệt web và truy cập vào địa chỉ <http://www.qtht.com.vn/myweb>
- Cấu hình DNS server thành IP của máy ảo CentOS: **192.168.1.250**



- Truy cập vào địa chỉ <http://www.qtht.com.vn>



- Truy cập vào địa chỉ <http://www.qtht.com.vn/myweb>



4. Cấu hình tường lửa FirewallD

Công cụ FirewallD (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 FirewallD được thay thế cho tường lửa iptables với những khác biệt cơ bản:

- FirewallD 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.
- FirewallD 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 firewalld

Lệnh thực hiện: **sudo systemctl start firewalld**

```
[B2204973@localhost ~]$ sudo systemctl start firewalld
[sudo] password for B2204973:
[B2204973@localhost ~]$
```

- Kiểm tra trạng thái tường lửa

Lệnh thực hiện: **sudo systemctl status firewalld**

```
[B2204973@localhost ~]$ sudo systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.se
   Active: active (running) since Fri 2024-11-01 14:53:
```

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

Lệnh thực hiện: **firewall-cmd --get-zones**

```
[B2204973@localhost ~]$ firewall-cmd --get-zones
block dmz docker drop external home internal nm-shared public trusted work
[B2204973@localhost ~]$
```

- Kiểm tra zone mặc định

Lệnh thực hiện: **firewall-cmd --get-default-zone**

```
[B2204973@localhost ~]$ firewall-cmd --get-default-zone
public
[B2204973@localhost ~]$
```

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

Lệnh thực hiện: **firewall-cmd --get-active-zones**

```
[B2204973@localhost ~]$ firewall-cmd --get-active-zones
docker
  interfaces: docker0
public
  interfaces: enp0s3
[B2204973@localhost ~]$
```

Lệnh thực hiện: **sudo firewall-cmd --list-all --zone=public**

```
[B2204973@localhost ~]$ sudo firewall-cmd --list-all --zone=public
[sudo] password for B2204973:
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:
[B2204973@localhost ~]$
```

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

- Ping từ máy vật lý đến máy ảo: **ping 192.168.1.250**

```
C:\Users\HP>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\HP>
```

Kết quả: thành công

- Kết nối với dịch vụ ssh trên CentOS

```
• MobaXterm Personal Edition v24.1 •
  (SSH client, X server and network tools)

➤ SSH session to B2204973@192.168.1.250
  • Direct SSH : ✓
  • SSH compression : ✓
  • SSH-browser : ✓
  • X11-forwarding : ✓ (remote display is forwarded through SSH)

➤ For more info, ctrl+click on help or visit our website.

Activate the web console with: systemctl enable --now cockpit.socket

Last login: Fri Nov  1 14:05:25 2024
/usr/bin/xauth: file /home/B2204973/.Xauthority does not exist
[B2204973@localhost ~]$
```

Kết quả: thành công

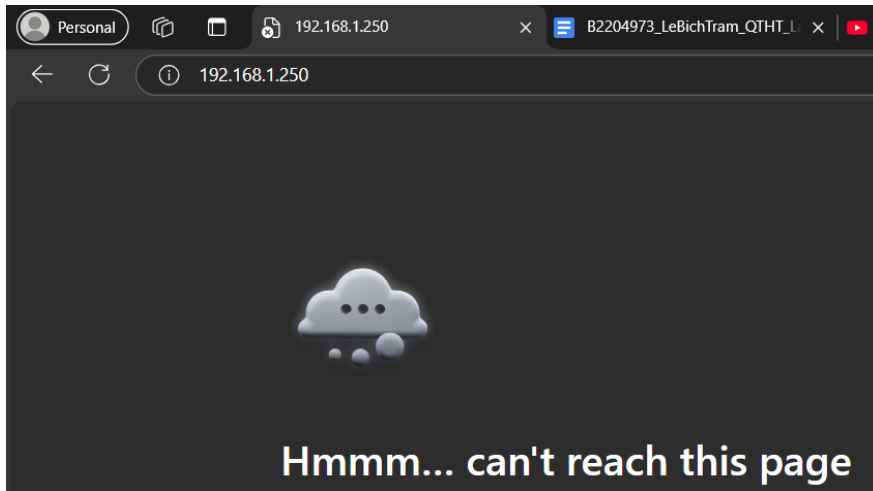
- Trên CentOS khởi động dịch vụ web

```
[B2204973@localhost ~]$ sudo systemctl start httpd
[B2204973@localhost ~]$
```

Kiểm tra trạng thái dịch vụ web ta thấy dịch vụ web đang chạy

```
[B2204973@localhost ~]$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.se
   Active: active (running) since Fri 2024-11-01 14
```

- Thử truy cập webserver trên máy Centos



Kết quả: thất bại

-> ta không kết nối với dịch vụ web được, bởi vì zone public không cho phép

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

Lệnh thực hiện: **sudo firewall-cmd --zone=drop --change-interface=enp0s3**

```
[B2204973@localhost ~]$ sudo firewall-cmd --zone=drop --change-interface=enp0s3
success
[B2204973@localhost ~]$
```

Lệnh thực hiện: **sudo firewall-cmd --list-all --zone=drop**

```
[B2204973@localhost ~]$ sudo firewall-cmd --list-all --zone=drop
drop (active)
target: DROP
```

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

➤ ping từ máy vật lý sang máy ảo : **ping 192.168.1.250**

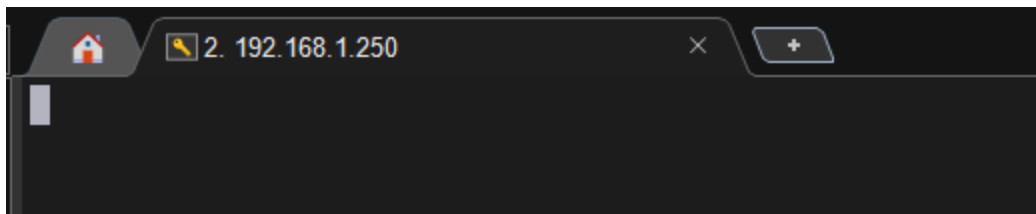
```
C:\Users\HP>ping 192.168.1.250

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),
```

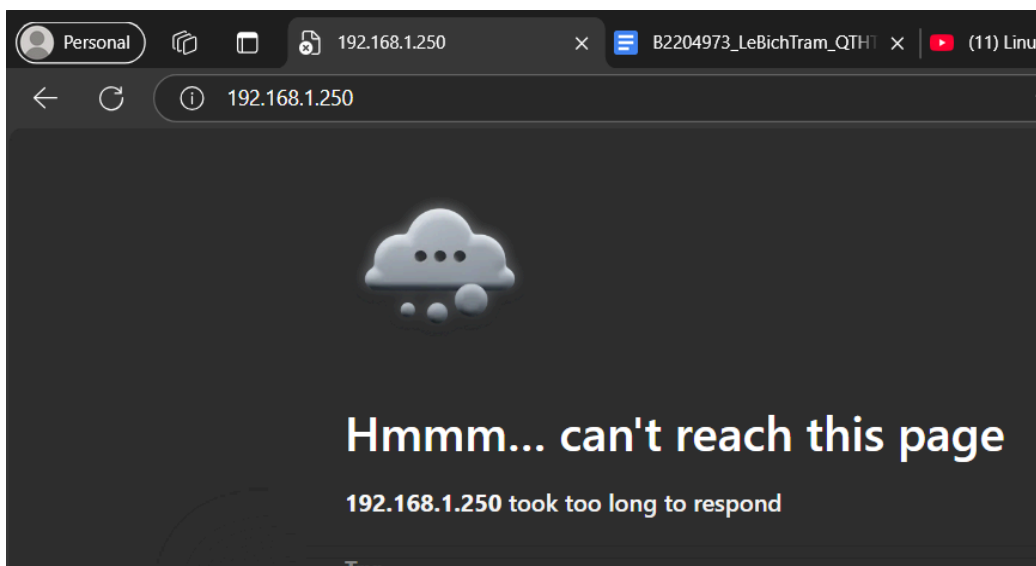
Kết quả: không được

➤ Nối kết ssh với máy centos



Kết quả: không được

➤ Nối kết với web



Kết quả: không được

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

Lệnh thực hiện: **sudo firewall-cmd --zone=trusted --change-interface=enp0s3**

```
[B2204973@localhost ~]$ sudo firewall-cmd --zone=trusted --change-interface=enp0s3
success
[B2204973@localhost ~]$
```

Lệnh thực hiện: **sudo firewall-cmd --list-all --zone=trusted**

```
[B2204973@localhost ~]$ sudo firewall-cmd --list-all --zone=trusted
trusted (active)
target: ACCEPT
```

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

- ping từ máy vật lý sang máy ảo : ping 192.168.1.250

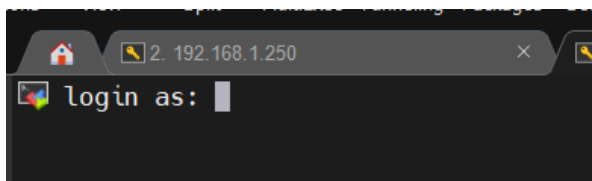
```
C:\Users\HP>ping 192.168.1.250

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 = 1ms, Average = 0ms
```

Kết quả: thành công

- Kết nối ssh với máy CentOS



```
• MobaXterm Personal Edition v24.1 •
(SSH client, X server and network tools)

➤ SSH session to B2204973@192.168.1.250
  • Direct SSH      : ✓
  • SSH compression : ✓
  • SSH-browser     : ✓
  • X11-forwarding  : ✓ (remote display is forwarded through SSH)

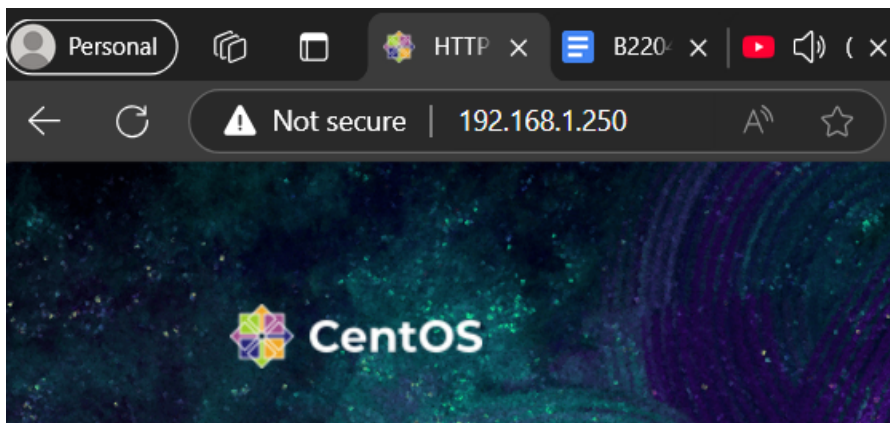
➤ For more info, ctrl+click on help or visit our website.

Activate the web console with: systemctl enable --now cockpit.socket

Last login: Fri Nov  1 16:10:16 2024
[B2204973@localhost ~]$
```

Kết quả: thành công

- Nối kết với dịch vụ web có thể thực hiện được



Kết quả thành công

- Tạo zone mới có tên là *qthtserver*

Lệnh thực hiện: **sudo firewall-cmd --permanent --new-zone=qthtserver**

```
[B2204973@localhost ~]$ sudo firewall-cmd --permanent --new-zone=qthtserver
[sudo] password for B2204973:
success
[B2204973@localhost ~]$ █
```

Lệnh thực hiện: **sudo systemctl restart firewallld**

```
[B2204973@localhost ~]$ sudo systemctl restart firewallld
[B2204973@localhost ~]$
```

Lệnh thực hiện: **sudo firewall-cmd --list-all --zone=qthtserver**

```
[B2204973@localhost ~]$ sudo firewall-cmd --list-all --zone=qthtserver
qthtserver
target: default
```

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

Lệnh thực hiện: **sudo firewall-cmd --permanent --zone=qthtserver --add-service=http**

```
[B2204973@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=http
success
```

Lệnh thực hiện: **sudo firewall-cmd --permanent --zone=qthtserver --add-service=dns**

```
[B2204973@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=dns
success
[B2204973@localhost ~]$
```

Lệnh thực hiện: **sudo firewall-cmd --permanent --zone=qthtserver --add-service=samba**

```
[B2204973@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=samba
success
[B2204973@localhost ~]$ █
```

Lệnh thực hiện: **sudo firewall-cmd --permanent --zone=qthtserver --add-service=ftp**

```
[B2204973@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=ftp
success
[B2204973@localhost ~]$ █
```

Lệnh thực hiện: **sudo firewall-cmd --permanent --zone=qthtserver --add-port=9999/tcp**


```
[B2204973@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-port=9999/tcp
success
[B2204973@localhost ~]$
```

- Thêm rule để chỉ cho phép máy vật lý có thể SSH tới máy CentOS
Lệnh thực hiện: **sudo firewall-cmd --permanent --zone=qthtserver --add-rich-rule='rule family=ipv4 source address=192.168.1.14/32 port port=22 protocol=tcp accept'**

```
[B2204973@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-rich-rule='rule family=ipv4 source address=192.168.1.14/32 port port=22 protocol=tcp accept'
[sudo] password for B2204973:
success
```

- Khởi động lại tường lửa firewalld
Lệnh thực hiện: **sudo systemctl restart firewalld**

```
[B2204973@localhost ~]$ sudo systemctl restart firewalld
[B2204973@localhost ~]$
```

- Chuyển giao diện mạng sang zone `qthtserver`; và xem các rules của zone
Lệnh thực hiện: **sudo firewall-cmd --permanent --zone=qthtserver --change-interface=enp0s3**

```
[B2204973@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --change-interface=enp0s3
The interface is under control of NetworkManager, setting zone to 'qthtserver'.
success
[B2204973@localhost ~]$
```

- Lệnh thực hiện: **sudo firewall-cmd --list-all --zone=qthtserver**

```
[B2204973@localhost ~]$ 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="192.168.1.14/32" port port="22"
    protocol="tcp" accept
[B2204973@localhost ~]$
```

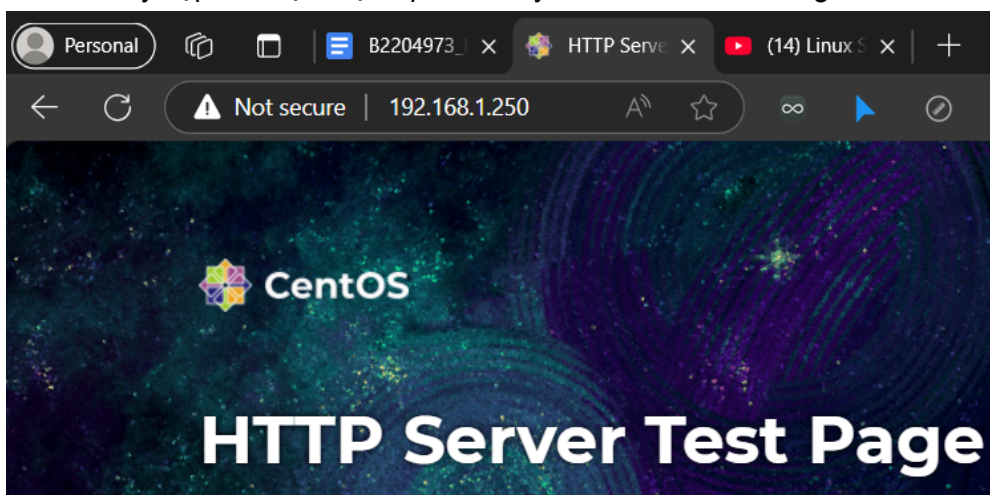

- Kiểm tra máy vật lý có thể truy cập được tới các dịch vụ trên máy CentOS hay không.
- ❖ Ping từ máy vật lý sang máy centos bình thường: ping 192.168.1.250

```
C:\Users\HP>ping 192.168.1.250

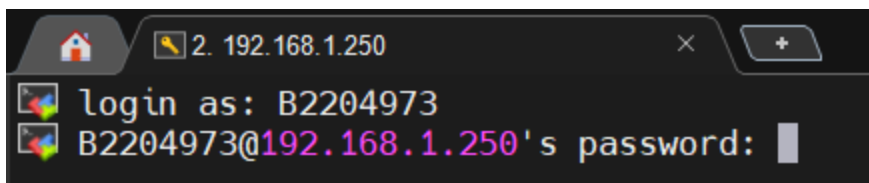
Pinging 192.168.1.250 with 32 bytes of data:
Reply from 192.168.1.250: bytes=32 time<1ms TTL=64
Reply from 192.168.1.250: bytes=32 time<1ms TTL=64
Reply from 192.168.1.250: bytes=32 time<1ms TTL=64
Reply from 192.168.1.250: bytes=32 time<1ms TTL=64

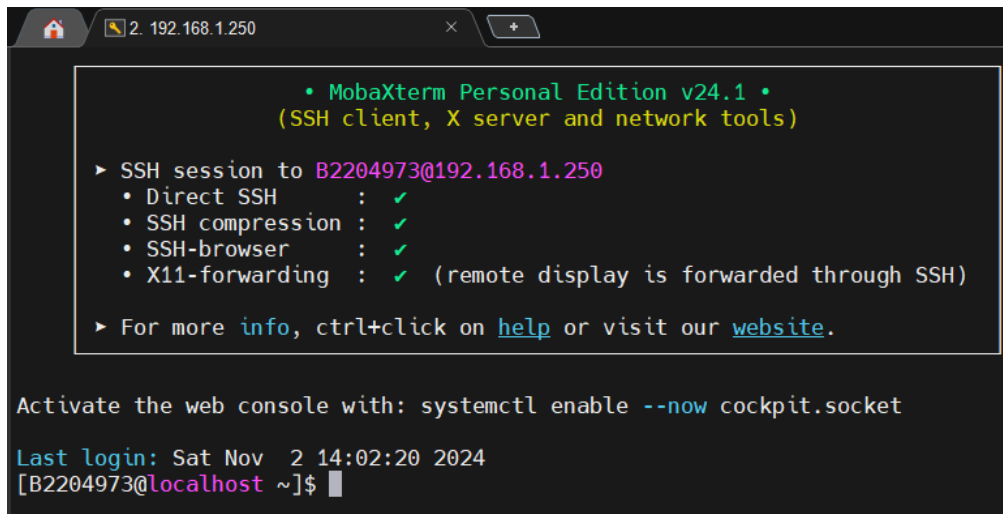
Ping statistics for 192.168.1.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- ❖ Truy cập đến dịch vụ http trên máy CentOS bình thường



- ❖ Truy cập đến dịch vụ ssh trên máy CentOS bình thường





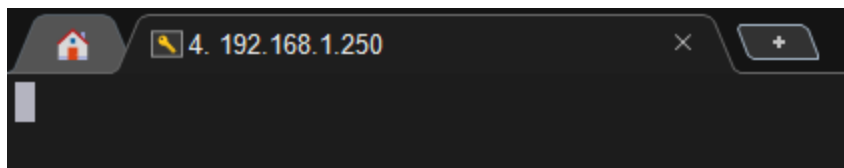
```
• MobaXterm Personal Edition v24.1 •  
(SSH client, X server and network tools)  
  
➤ SSH session to B2204973@192.168.1.250  
• Direct SSH : ✓  
• SSH compression : ✓  
• SSH-browser : ✓  
• X11-forwarding : ✓ (remote display is forwarded through SSH)  
  
➤ For more info, ctrl+click on help or visit our website.  
  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Sat Nov  2 14:02:20 2024  
[B2204973@localhost ~]$
```

- Thử đổi ip máy vật lý từ 192.168.1.14 sang 192.168.1.222 và truy cập dịch vụ ssh

IP assignment:	Manual
IPv4 address:	192.168.1.222
IPv4 mask:	255.255.255.0
IPv4 gateway:	192.168.1.1

Edit

Ta thấy dịch vụ ssh đứng treo và **không nối kết được**.



--- Hết ---

Video hướng dẫn làm bài:

- + Hướng dẫn làm bài: <https://youtu.be/MgrW8zeh02E>
- + Hướng dẫn câu 1: <https://youtu.be/0oW0TF1iVQs>
- + Hướng dẫn câu 2: <https://youtu.be/ZuRg100dtJQ>
- + Hướng dẫn câu 3: https://youtu.be/89mAL_T_uuY
- + Hướng dẫn câu 4: <https://youtu.be/cS3Qv90bBQ8>