



## LAB 5

### DOCKER, SAMBA, DNS và Firewall

Họ tên và MSSV: Lê Hải Đăng - B2203716

Nhóm học phần: 03

- 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)
- 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`

```

Last login: Fri Nov 8 20:06:04 2024
[b2203716@haidang ~]$ ls
backup  Documents  haidangle243.html  Music  Templates
backup.sh  Downloads  index.html  Pictures  tmp
Desktop  haidang.html  info.sh  Public  Videos
[b2203716@haidang ~]$ ls -l
total 12
drwxr-xr-x. 2 b2203716 b2203716 22 Oct 7 14:23 backup
-rwxrwxrwx. 1 b2203716 b2203716 281 Oct 7 14:29 backup.sh
drwxr-xr-x. 2 b2203716 b2203716 23 Aug 20 16:02 Desktop
drwxr-xr-x. 2 b2203716 b2203716 44 Aug 20 16:02 Documents
drwxr-xr-x. 2 b2203716 b2203716 6 Aug 20 13:59 Downloads
-rw-r--r--. 1 b2203716 b2203716 0 Oct 19 22:29 haidang.html
-rw-r--r--. 1 b2203716 b2203716 0 Oct 20 12:53 haidangle243.html
-rw-r--r--. 1 b2203716 b2203716 216 Oct 20 13:35 index.html
-rwxrwxrwx. 1 root root 432 Oct 5 15:50 info.sh
drwxr-xr-x. 2 b2203716 b2203716 6 Aug 20 13:59 Music
drwxr-xr-x. 2 b2203716 b2203716 147 Oct 5 15:31 Pictures
drwxr-xr-x. 2 b2203716 b2203716 6 Aug 20 13:59 Public
drwxr-xr-x. 2 b2203716 b2203716 6 Aug 20 13:59 Templates
drwxr-xr-x. 2 b2203716 b2203716 22 Oct 5 16:11 tmp
drwxr-xr-x. 2 b2203716 b2203716 6 Aug 20 13:59 Videos
[b2203716@haidang ~]$ sudo cat index.html
[sudo] password for b2203716:
<!doctype html>
<html>
<head>
<meta charset="utf-8">
<title>Ting công ty bánh kẹo Lương Sơn Bạc</title>
</head>
<body>
<H1>Welcome!<H1>
<marquee>Designed by B12345678</marquee>
</body>
</html>
[b2203716@haidang ~]$ sudo systemctl stop s?ewalld
[b2203716@haidang ~]$ sudo systemctl stop firewalld
[b2203716@haidang ~]$ sudo systemctl status firewalld
o firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
   Active: inactive (dead) since Fri 2024-11-08 20:16:30 +07; 29s ago
     Duration: 11min 4.474s
    Docs: man:firewalld(1)
   Process: 861 ExecStart=/usr/sbin/firewalld --nofork --nopid $FIREWALLD_ARGS (code=exited, status=0/SUCCESS)
    Main PID: 861 (code=exited, status=0/SUCCESS)
      CPU: 2.322s

Nov 08 20:05:24 haidang systemd[1]: Starting firewalld - dynamic firewall daemon...
Nov 08 20:05:26 haidang systemd[1]: Started firewalld - dynamic firewall daemon.
Nov 08 20:16:30 haidang systemd[1]: Stopping firewalld - dynamic firewall daemon...
Nov 08 20:16:30 haidang systemd[1]: firewalld.service: Deactivated successfully.
Nov 08 20:16:30 haidang systemd[1]: Stopped firewalld - dynamic firewall daemon.
Nov 08 20:16:30 haidang systemd[1]: firewalld.service: Consumed 2.322s CPU time.
[b2203716@haidang ~]$
    
```

**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
```

```
[b2203716@haidang ~]$ sudo dnf -y remove podman runc
```

```
Removed:
cockpit-podman-93-1.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-2:5.2.2-1.el9.x86_64

Complete!
```

- Cài đặt công cụ yum-utils

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

```
[b2203716@haidang ~]$ sudo dnf install -y yum-utils
```

```
Upgraded:
dnf-plugins-core-4.3.0-17.el9.noarch
python3-dnf-plugins-core-4.3.0-17.el9.noarch
Installed:
yum-utils-4.3.0-17.el9.noarch

Complete!
```

- Thêm địa chỉ repo của Docker vào công cụ yum

```
$sudo yum-config-manager \
--add-repo \
https://download.docker.com/linux/centos/docker-ce.repo
```

```
[b2203716@haidang ~]$ 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
[b2203716@haidang ~]$
```

**#Viết liên tục lệnh trên hoặc xuống hàng bằng enter.**

- Cài đặt Docker

```
$sudo dnf install docker-ce -y
```

```
[b2203716@haidang ~]$ sudo dnf install docker-ce -y
```

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

```
$sudo usermod -aG docker $USER
```

```
[b2203716@haidang ~]$ sudo usermod -aG docker $USER
[sudo] password for b2203716:
[b2203716@haidang ~]$
```

- Login lại vào shell để việc thêm người dùng vào nhóm có tác dụng  
\$su - \$USER

```
[b2203716@haidang ~]$ su - $USER
Password:
```

- Chạy dịch vụ Docker  
\$sudo systemctl start docker  
\$sudo systemctl enable docker

```
[b2203716@haidang ~]$ sudo systemctl start docker
[b2203716@haidang ~]$ sudo systemctl enable docker
Created symlink /etc/systemd/system/multi-user.target.wants/docker.service → /usr/lib/systemd/system/docker.service.
[b2203716@haidang ~]$
```

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

```
[b2203716@haidang ~]$ docker login -u b2203716
Password:
WARNING! Your password will be stored unencrypted in /home/b2203716/.docker/config.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credential-stores

Login Succeeded
[b2203716@haidang ~]$
```

- 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

```
[b2203716@haidang ~]$ docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
c1ec31eb5944: Pull complete
Digest: sha256:d211f485f2dd1dee407a80973c8f129f00d54604d2c90732e8e320e5038a0348
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/

[b2203716@haidang ~]$
```

#### 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
```

```
[b2203716@haidang ~]$ docker search httpd
```

NAME	DESCRIPTION	STARS	OFFICIAL
httpd	The Apache HTTP Server Project	4807	[OK]
manageiq/httpd	Container with httpd, built on CentOS for Ma...	1	
paketobuildpacks/httpd		0	
vulhub/httpd		0	
jitesoft/httpd	Apache httpd on Alpine linux.	0	
openquantumsafe/httpd	Demo of post-quantum cryptography in Apache ...	14	
openeuler/httpd		0	
betterweb/httpd		0	
dockerpinata/httpd		1	
centos/httpd		36	
e2eteam/httpd		0	
manasip/httpd		0	
amd64/httpd	The Apache HTTP Server Project	1	
futdryt/httpd		0	
ppc64le/httpd	The Apache HTTP Server Project	0	
arm64v8/httpd	The Apache HTTP Server Project	11	
9af925e7043/httpd		0	
arm32v7/httpd	The Apache HTTP Server Project	11	
s390x/httpd	The Apache HTTP Server Project	1	
tugboatqa/httpd	The Apache HTTP Server Project	0	
i386/httpd	The Apache HTTP Server Project	1	
signiant/httpd	httpd (apache2) base container with a custom...	0	
armhf/httpd	The Apache HTTP Server Project	8	
inventis/httpd	apache container with support for https only	0	
publici/httpd	httpd:latest	1	

- 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.

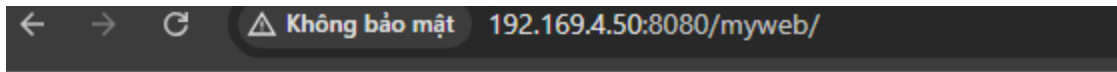
```
[b2203716@haidang ~]$ docker run -d -it -p 8080:80 --name webserver httpd
Unable to find image 'httpd:latest' locally
latest: Pulling from library/httpd
a480a496ba95: Pull complete
3a2663e66670: Pull complete
4f4fb700ef54: Pull complete
dbde712f81fb: Pull complete
867b2ea3628d: Pull complete
6bd9d3710aae: Pull complete
Digest: sha256:bbea29057f25d9543e6a96a8e3cc7c7c937206d20eab2323f478fdb2469d536d
Status: Downloaded newer image for httpd:latest
f3ebcf06029f7661dc4ed25d5d764dd7d35c0cdd6c8b82d2b53e12ff696963f0
[b2203716@haidang ~]$
```

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

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

```
[b2203716@haidang local]$ docker cp /var/www/html/myweb/ webserver:/usr/local/apache2/htdocs/
Successfully copied 2.56kB to webserver:/usr/local/apache2/htdocs/
[b2203716@haidang local]$
```

- 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.



# Welcome!

## Designed by le hai dang b2203716

### 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:

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

```
[b2203716@haidang ~]$ sudo dnf install -y samba  
[sudo] password for b2203716:
```

```
Installed:  
libnetapi-4.20.2-2.el9.x86_64          samba-4.20.2-2.el9.x86_64  
samba-common-tools-4.20.2-2.el9.x86_64  samba-dcerpc-4.20.2-2.el9.x86_64  
samba-ldb-ldap-modules-4.20.2-2.el9.x86_64  samba-libs-4.20.2-2.el9.x86_64  
Complete!
```

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

```
$sudo adduser baole
```

```
[b2203716@haidang ~]$ sudo adduser haidang  
[b2203716@haidang ~]$ █
```

```
$sudo passwd baole
```

```
[b2203716@haidang ~]$ sudo passwd haidang  
Changing password for user haidang.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[b2203716@haidang ~]$ █
```

```
$sudo groupadd lecturers
```

```
[b2203716@haidang ~]$ sudo groupadd lecturers  
[b2203716@haidang ~]$ █
```

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

```
[b2203716@haidang ~]$ sudo usermod -a -G lecturers haidang
[b2203716@haidang ~]$
```

- Tạo thư mục cần chia sẻ và phân quyền:

```
$sudo mkdir /data
```

```
[b2203716@haidang ~]$ sudo mkdir data
```

```
[b2203716@haidang ~]$ ls -l /
total 32
dr-xr-xr-x.  2 root root    6 Jun 25 21:23 afs
drwxr-xr-x.  2 root root   28 Oct  7 14:31 backup
lrwxrwxrwx.  1 root root    7 Jun 25 21:23 bin -> usr/bin
dr-xr-xr-x.  5 root root 4096 Sep 15 21:24 boot
drwxr-xr-x.  3 root root 4096 Sep 16 00:13 data
drwxr-xr-x. 20 root root 3380 Nov  8 20:05 dev
drwxr-xr-x. 136 root root 8192 Nov  8 22:09 etc
```

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

```
[b2203716@haidang ~]$ sudo chown :lecturers /data
[b2203716@haidang ~]$
```

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

```
[b2203716@haidang ~]$ sudo chown :lecturers /data
[b2203716@haidang ~]$ sudo chmod -R 775 /data
[b2203716@haidang ~]$ ls -l /
total 32
dr-xr-xr-x.  2 root root    6 Jun 25 21:23 afs
drwxr-xr-x.  2 root root   28 Oct  7 14:31 backup
lrwxrwxrwx.  1 root root    7 Jun 25 21:23 bin -> usr/bin
dr-xr-xr-x.  5 root root 4096 Sep 15 21:24 boot
drwxrwxr-x.  3 root lecturers 4096 Sep 16 00:13 data
drwxr-xr-x. 20 root root 3380 Nov  8 20:05 dev
```

- Cấu hình dịch vụ Samba:

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

```
[b2203716@haidang ~]$ sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.orig
[b2203716@haidang ~]$
```

```
$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

GNU nano 5.6.1 /etc/samba/smb.conf Modified
# 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

    printing = cups
    printcap name = cups
    load printers = yes
    cups options = raw

[homes]
    comment = Home Directories
    valid users = %S, %D%w%S
    browseable = No
    read only = No
    inherit acls = Yes

[printers]
    comment = All Printers
    path = /var/tmp
    printable = Yes
    create mask = 0600
    browseable = No

[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
```

- Thêm người dùng cho dịch vụ Samba:

```
$sudo smbpasswd -a baole
```

```
#Đặt mật khẩu Samba cho người dùng
```

```
[b2203716@haidang ~]$ sudo smbpasswd -a haidang
New SMB password:
Retype new SMB password:
Added user haidang.
[b2203716@haidang ~]$
```

- Cấu hình SELINUX cho phép Samba

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

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

```
[b2203716@haidang ~]$ sudo setsebool -P samba_export_all_rw on
[b2203716@haidang ~]$ sudo setsebool -P samba_enable_home_dirs on
[b2203716@haidang ~]$ sudo systemctl stop firewalld
[b2203716@haidang ~]$
```

- Tắt tường lửa:

```
$sudo systemctl stop firewalld
```

```
[b2203716@haidang ~]$ sudo setsebool -P samba_export_all_rw on
[b2203716@haidang ~]$ sudo setsebool -P samba_enable_home_dirs on
[b2203716@haidang ~]$ sudo systemctl stop firewalld
[b2203716@haidang ~]$
```

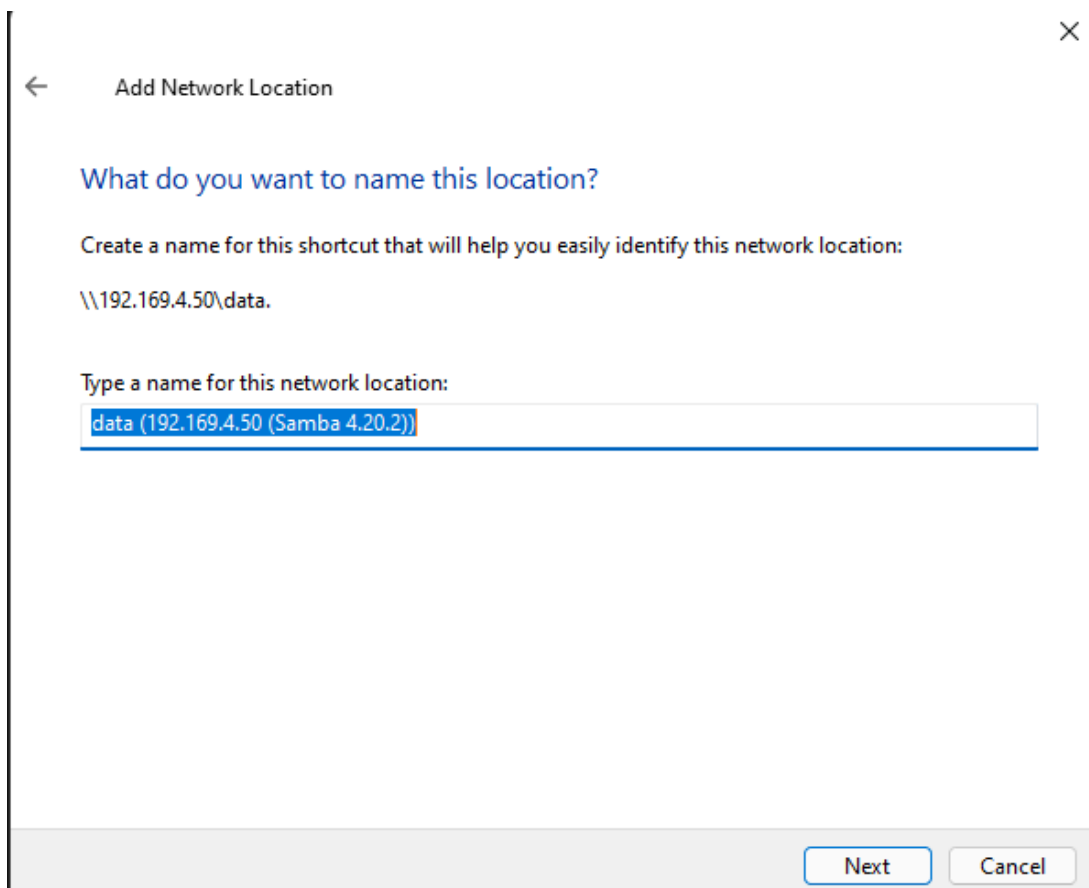
- Khởi động cho phép Samba tự động thực thi khi khởi động hệ điều hành:

```
$sudo systemctl start smb
```

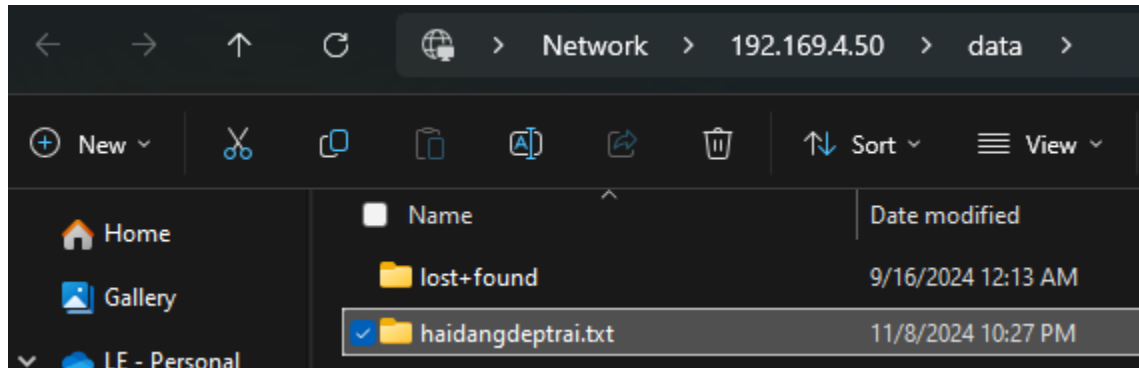
```
$sudo systemctl enable smb
```

```
[b2203716@haidang ~]$ sudo systemctl start smb
[b2203716@haidang ~]$ sudo systemctl enable smb
Created symlink /etc/systemd/system/multi-user.target.wants/smb.service → /usr/lib/systemd/system/smb.service.
[b2203716@haidang ~]$
```

- 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







```
[b2203716@haidang ~]$ ls /data
haidangdeptrai.txt  lost+found
[b2203716@haidang ~]$
```

### 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 để 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
```

```
[b2203716@haidang ~]$ sudo dnf install bind bind-utils -y
[sudo] password for b2203716:
```

```
Upgraded:
  bind-libs-32:9.16.23-24.el9.x86_64      bind-license-32:9.16.23-24.el9.noarch
  bind-utils-32:9.16.23-24.el9.x86_64
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:

```
$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 {8.8.8.8; };
```

```
    ..
```

```
};
```

```
logging {  
    ..  
};  
  
zone "." IN {  
    ...  
};  
  
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; };  
};  
...
```

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

```
zone "qtht.com.vn" IN {  
    type master;  
    file "forward.qtht";  
    allow-update { none; };  
};  
zone "4.169.192.in-addr.arpa" IN {  
    type master;  
    file "reverse.qtht";  
    allow-update { none; };  
};
```

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

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

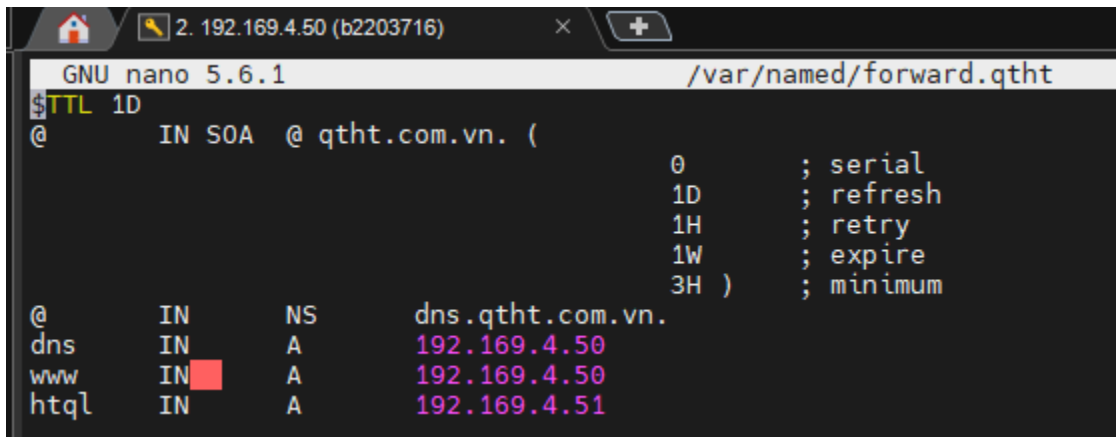
```
$sudo nano /var/named/forward.qtht
```

```
[b2203716@haidang ~]$ sudo cp /var/named/named.localhost /var/named/forward.qtht
[sudo] password for b2203716:
[b2203716@haidang ~]$ sudo chgrp named /var/named/forward.qtht
[b2203716@haidang ~]$ sudo nano /var/named/forward.qtht
[b2203716@haidang ~]$ clear
```

\$(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    192.168.1.20
www    IN      A    192.168.1.20
htql   IN      A    192.168.1.21
```



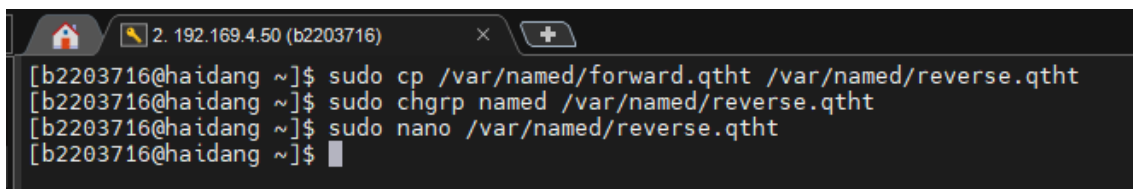
```
GNU nano 5.6.1 /var/named/forward.qtht
$TTL 1D
@      IN      SOA  @  qtht.com.vn. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )   ; minimum
@      IN      NS   dns.qtht.com.vn.
dns    IN      A    192.169.4.50
www    IN      A    192.169.4.50
htql   IN      A    192.169.4.51
```

### 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
```

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



```
[b2203716@haidang ~]$ sudo cp /var/named/forward.qtht /var/named/reverse.qtht
[b2203716@haidang ~]$ sudo chgrp named /var/named/reverse.qtht
[b2203716@haidang ~]$ sudo nano /var/named/reverse.qtht
[b2203716@haidang ~]$
```

```
$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       192.168.1.20
20      IN      PTR     www.qtht.com.vn.

```

```

GNU nano 5.6.1 /var/named/reverse.qtht
$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       192.169.4.50
50      IN      PTR     www.qtht.com.vn.

```

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

- Tắt tường lửa:  
\$sudo systemctl stop firewalld
- Khởi động dịch vụ DNS:  
\$sudo systemctl start named

```

[b2203716@haidang ~]$ sudo systemctl stop firewalld
[b2203716@haidang ~]$ sudo systemctl start named
[b2203716@haidang ~]$

```

- Kiểm tra kết quả:  
nslookup www.qtht.com.vn <địa chỉ IP máy ảo>

```

[b2203716@haidang ~]$ nslookup www.qtht.com.vn 192.169.4.50
Server:          192.169.4.50
Address:         192.169.4.50#53

Name:   www.qtht.com.vn
Address: 192.169.4.50
[b2203716@haidang ~]$

```

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

```
[b2203716@haidang ~]$ nslookup htql.qtht.com.vn 192.169.4.50
Server:      192.169.4.50
Address:     192.169.4.50#53

Name:   htql.qtht.com.vn
Address: 192.169.4.51

[b2203716@haidang ~]$
```

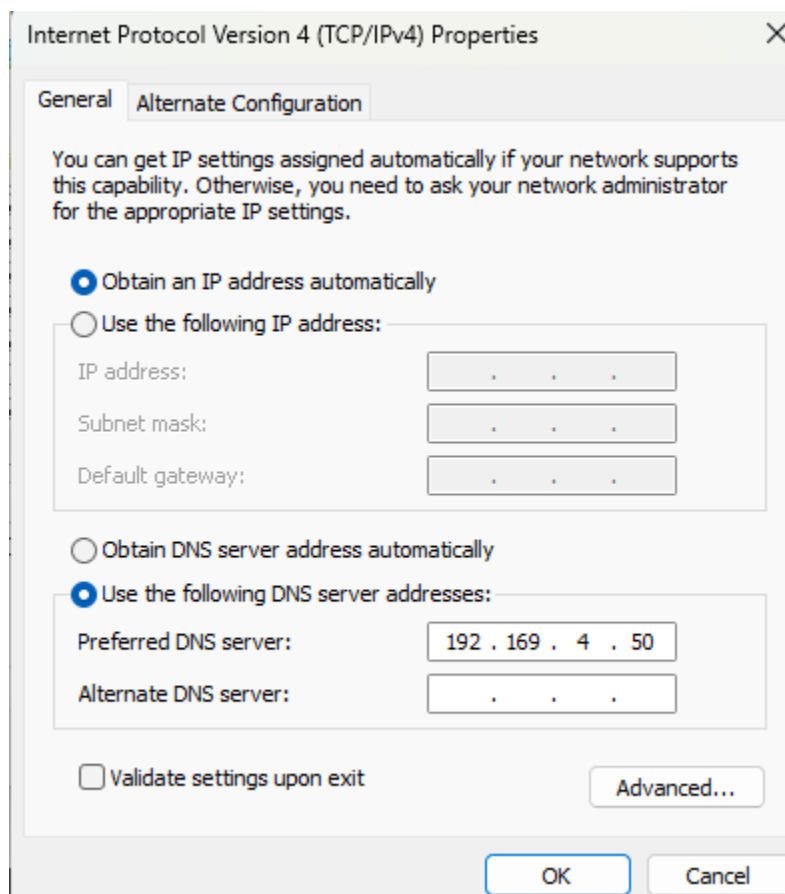
nslookup www.ctu.edu.vn <địa chỉ IP máy ảo>

```
[b2203716@haidang ~]$ nslookup www.ctu.edu.vn 192.169.4.50
Server:      192.169.4.50
Address:     192.169.4.50#53

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

[b2203716@haidang ~]$
```

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





#### 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
```

```
[b2203716@haidang ~]$ sudo systemctl start firewallld
[sudo] password for b2203716:
[b2203716@haidang ~]$ sudo systemctl status firewallld
● firewallld.service - firewallld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewallld.service; enabled; preset: enabled)
   Active: active (running) since Fri 2024-11-08 23:17:04 +07; 9s ago
     Docs: man:firewalld(1)
    Main PID: 38786 (firewalld)
      Tasks: 2 (limit: 48783)
     Memory: 25.1M
        CPU: 511ms
    CGroup: /system.slice/firewallld.service
            └─38786 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid

Nov 08 23:17:04 haidang systemd[1]: Starting firewallld - dynamic firewall daemon...
Nov 08 23:17:04 haidang systemd[1]: Started firewallld - dynamic firewall daemon.
[b2203716@haidang ~]$
```

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

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

```
[b2203716@haidang ~]$ firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
[b2203716@haidang ~]$
```

- Kiểm tra zone mặc định

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

```
[b2203716@haidang ~]$ firewall-cmd --get-default-zone
public
[b2203716@haidang ~]$
```

- 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
```

```
[b2203716@haidang ~]$ firewall-cmd --get-active-zones
public
    interfaces: enp0s3
[b2203716@haidang ~]$
```

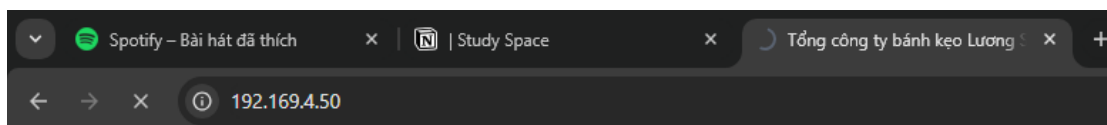
```
$sudo firewall-cmd --list-all --zone=public
```

```
[b2203716@haidang ~]$ sudo firewall-cmd --list-all --zone=public
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:
[b2203716@haidang ~]$
```

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

```
PS C:\Users\HAIDA> ping 192.169.4.50
```

```
Pinging 192.169.4.50 with 32 bytes of data:
Reply from 192.169.4.50: bytes=32 time<1ms TTL=64
Reply from 192.169.4.50: bytes=32 time<1ms TTL=64
Reply from 192.169.4.50: bytes=32 time<1ms TTL=64
Reply from 192.169.4.50: bytes=32 time<1ms TTL=64
```



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

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

```
[b2203716@haidang ~]$ sudo firewall-cmd --zone=drop --change-interface=enp0s3
success
[b2203716@haidang ~]$
```

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

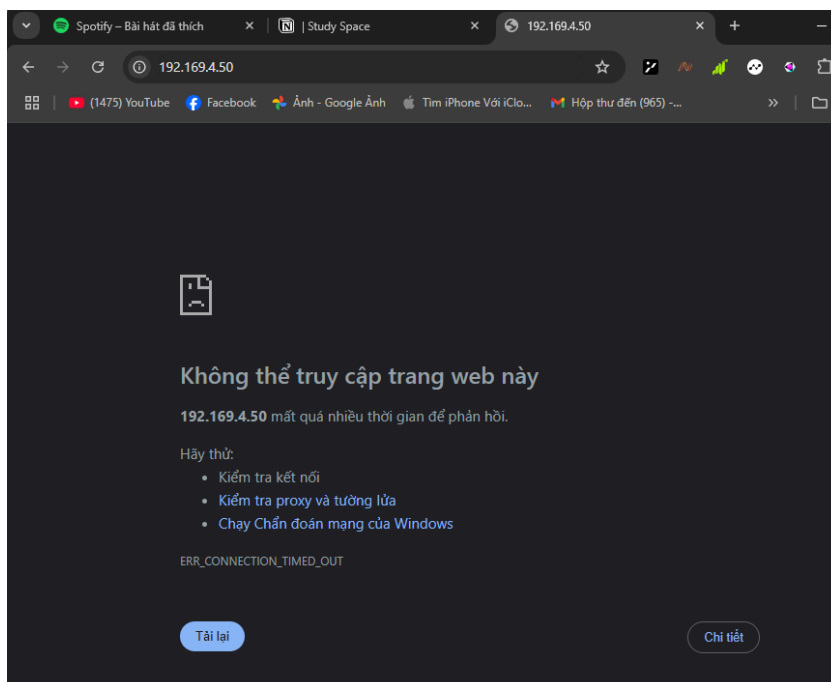
```
[b2203716@haidang ~]$ sudo firewall-cmd --list-all --zone=drop
drop (active)
  target: DROP
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services:
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[b2203716@haidang ~]$
```

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

```
PS C:\Users\HAIDA> ping 192.169.4.50

Pinging 192.169.4.50 with 32 bytes of data:
Request timed out.
```





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

```
$sudo firewall-cmd --zone=trusted --change-interface=enp0s3
```

```
[b2203716@haidang ~]$ sudo firewall-cmd --zone=trusted --change-interface=enp0s3
success
[b2203716@haidang ~]$
```

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

```
[b2203716@haidang ~]$ 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:
[b2203716@haidang ~]$
```

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

```
PS C:\Users\HAIDA> ping 192.169.4.50

Pinging 192.169.4.50 with 32 bytes of data:
Reply from 192.169.4.50: bytes=32 time<1ms TTL=64
Reply from 192.169.4.50: bytes=32 time<1ms TTL=64
Reply from 192.169.4.50: bytes=32 time<1ms TTL=64
Reply from 192.169.4.50: bytes=32 time<1ms TTL=64

Ping statistics for 192.169.4.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\HAIDA>
```

**CentOS**

## HTTP Server Test Page

This page is used to test the proper operation of the HTTP server after it has been installed. If you can read this page it means that this site is working properly. This server is powered by CentOS.

**If you are a member of the general public:**

The website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

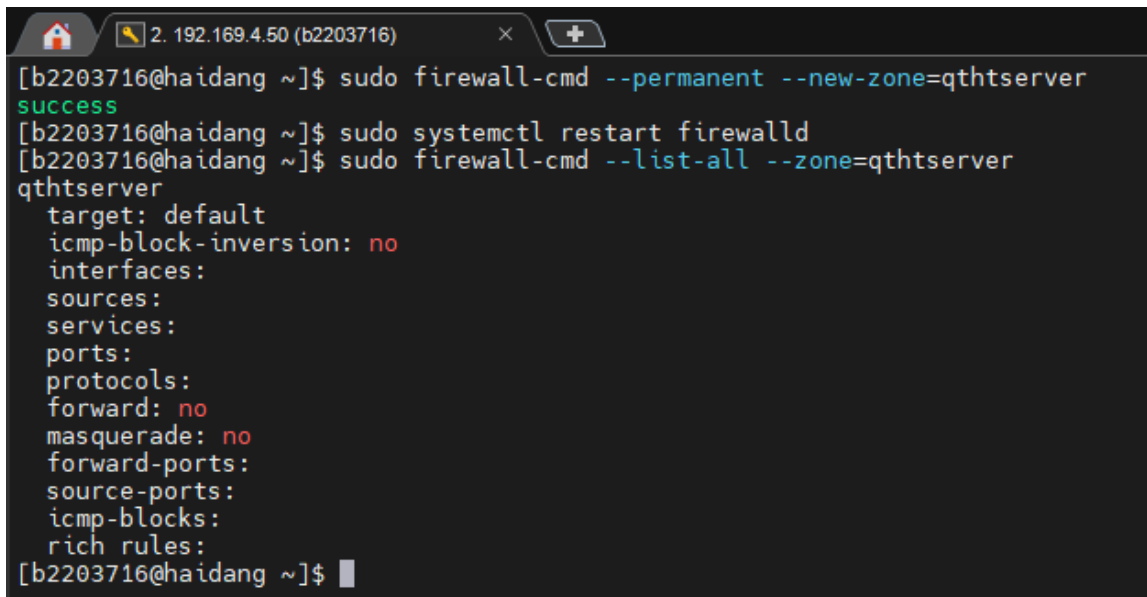
For example, if you experienced problems while visiting [www.example.com](http://www.example.com), you should send e-mail to "webmaster@example.com".

**Important Note!**

The CentOS Project has nothing to do with this website or its content, it just provides the software that makes the website run.

- 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
```



```
[b2203716@haidang ~]$ sudo firewall-cmd --permanent --new-zone=qthtserver
success
[b2203716@haidang ~]$ sudo systemctl restart firewalld
[b2203716@haidang ~]$ sudo firewall-cmd --list-all --zone=qthtserver
qthtserver
target: default
icmp-block-inversion: no
interfaces:
sources:
services:
ports:
protocols:
forward: no
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
[b2203716@haidang ~]$
```

- 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-service=ssh
$sudo firewall-cmd --permanent --zone=qthtserver --add-port=9999/tcp
```



```
[b2203716@haidang ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=http
success
[b2203716@haidang ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=dns
success
[b2203716@haidang ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=samba
success
[b2203716@haidang ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=ftp
success
[b2203716@haidang ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=ssh
success
[b2203716@haidang ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-port=9999/tcp
success
[b2203716@haidang ~]$
```

- Khởi động lại tường lửa firewalld
- ```
$sudo systemctl restart firewalld
```

```
[b2203716@haidang ~]$ sudo systemctl restart firewalld
[b2203716@haidang ~]$
```

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

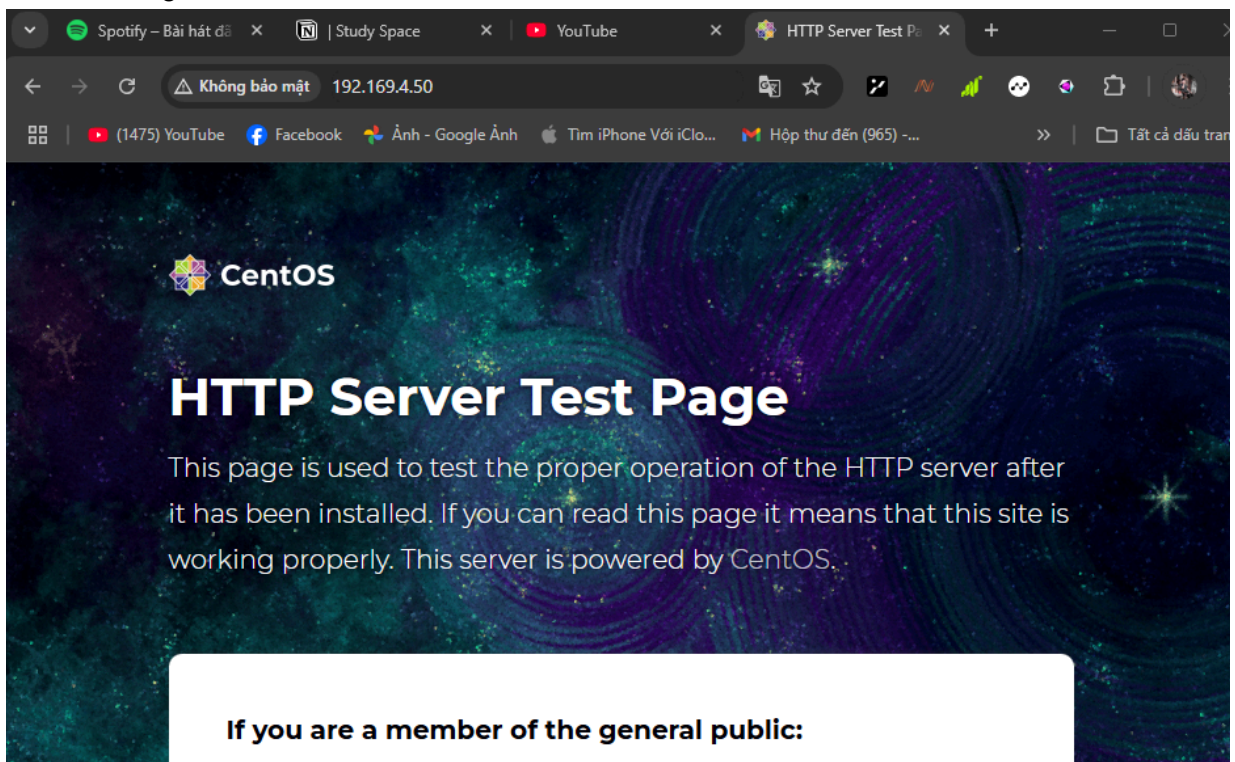
```
$sudo firewall-cmd --permanent --zone=qthtserver
```

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

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

```
[b2203716@haidang ~]$ sudo firewall-cmd --permanent --zone=qthtserver --change-interface=enp0s3
The interface is under control of NetworkManager, setting zone to 'qthtserver'.
success
[b2203716@haidang ~]$ sudo firewall-cmd --list-all --zone=qthtserver
qthtserver (active)
target: default
icmp-block-inversion: no
interfaces: enp0s3
sources:
services: dns ftp http samba ssh
ports: 9999/tcp
protocols:
forward: no
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
[b2203716@haidang ~]$
```

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



--- Hết ---