



LAB 5

DOCKER, SAMBA, DNS và Firewall

Họ tên và MSSV: Huỳnh Trung Tín B2012045

Nhóm học phần: Nhóm 07

- 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)

```
[B2012045@b2012045 ~]$ ping -c 3 172.20.10.1
PING 172.20.10.1 (172.20.10.1) 56(84) bytes of data.
64 bytes from 172.20.10.1: icmp_seq=1 ttl=64 time=4.52 ms
64 bytes from 172.20.10.1: icmp_seq=2 ttl=64 time=5.48 ms
64 bytes from 172.20.10.1: icmp_seq=3 ttl=64 time=8.22 ms

--- 172.20.10.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 4.519/6.071/8.217/1.566 ms
```

```
[B2012045@b2012045 ~]$ ping -c 3 172.20.10.2
PING 172.20.10.2 (172.20.10.2) 56(84) bytes of data.
64 bytes from 172.20.10.2: icmp_seq=1 ttl=128 time=3.70 ms
64 bytes from 172.20.10.2: icmp_seq=2 ttl=128 time=3.14 ms
64 bytes from 172.20.10.2: icmp_seq=3 ttl=128 time=2.44 ms

--- 172.20.10.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 2.435/3.091/3.701/0.517 ms
```

```
[B2012045@b2012045 ~]$ ping -c 3 google.com
PING google.com (142.250.204.110) 56(84) bytes of data.
64 bytes from hkg07s40-in-f14.1e100.net (142.250.204.110): icmp_seq=1 ttl=114 time=82.3 ms
64 bytes from hkg07s40-in-f14.1e100.net (142.250.204.110): icmp_seq=2 ttl=114 time=129 ms
64 bytes from hkg07s40-in-f14.1e100.net (142.250.204.110): icmp_seq=3 ttl=114 time=136 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2006ms
rtt min/avg/max/mdev = 82.288/115.634/135.690/23.740 ms
```

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

```
[B2012045@localhost ~]$ cat /var/www/html/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 B12345678</marquee>
</body>
</html>
[B2012045@localhost ~]$
```

Tắt tường lửa:

```
$sudo systemctl stop firewalld
```

```
[B2012045@localhost ~]$ sudo systemctl stop firewalld
[sudo] password for B2012045:
[B2012045@localhost ~]$
```

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
```

```
[B2012045@b2012045 ~]$ sudo dnf -y remove podman runc
[sudo] password for B2012045:
Dependencies resolved.
```

Package	Arch	Version	Repository	Size
Removing:				
podman	x86_64	2:4.2.0-3.el9	@AppStream	41 M
runc	x86_64	4:1.1.4-1.el9	@AppStream	9.5 M
Removing dependent packages:				
buildah	x86_64	1:1.27.0-2.el9	@AppStream	26 M
cockpit-podman	noarch	53-1.el9	@AppStream	548 k
Removing unused dependencies:				
aardvark-dns	x86_64	2:1.1.0-4.el9	@AppStream	3.1 M
common	x86_64	2:2.1.4-1.el9	@AppStream	170 k
container-selinux	noarch	3:2.189.0-1.el9	@AppStream	57 k
containers-common	x86_64	2:1-44.el9	@AppStream	408 k
criu	x86_64	3.17-4.el9	@AppStream	1.5 M
criu-libs	x86_64	3.17-4.el9	@AppStream	85 k
crun	x86_64	1.5-1.el9	@AppStream	429 k
fuse-overlayfs	x86_64	1.9-1.el9	@AppStream	148 k
libnet	x86_64	1.2-6.el9	@AppStream	128 k
libslirp	x86_64	4.4.0-4.el9	@AppStream	129 k

```

verifying      : fuse-overlayfs-1.9-1.el9.x86_64      10/19
Verifying      : libnet-1.2-6.el9.x86_64             11/19
Verifying      : libslirp-4.4.0-4.el9.x86_64         12/19
Verifying      : netavark-2:1.1.0-6.el9.x86_64        13/19
Verifying      : podman-2:4.2.0-3.el9.x86_64          14/19
Verifying      : podman-catatonit-2:4.2.0-3.el9.x86_64 15/19
Verifying      : runc-4:1.1.4-1.el9.x86_64           16/19
Verifying      : shadow-utils-subid-2:4.9-6.el9.x86_64 17/19
Verifying      : slirp4netns-1.2.0-2.el9.x86_64       18/19
Verifying      : yajl-2.1.0-21.el9.x86_64            19/19

Removed:
aardvark-dns-2:1.1.0-4.el9.x86_64      buildah-1:1.27.0-2.el9.x86_64
cockpit-podman-53-1.el9.noarch          common-2:2.1.4-1.el9.x86_64
container-selinux-3:2.189.0-1.el9.noarch containers-common-2:1-44.el9.x86_64
criu-3.17-4.el9.x86_64                  criu-libs-3.17-4.el9.x86_64
crun-1.5-1.el9.x86_64                   fuse-overlayfs-1.9-1.el9.x86_64
libnet-1.2-6.el9.x86_64                 libslirp-4.4.0-4.el9.x86_64
netavark-2:1.1.0-6.el9.x86_64           podman-2:4.2.0-3.el9.x86_64
podman-catatonit-2:4.2.0-3.el9.x86_64   runc-4:1.1.4-1.el9.x86_64
shadow-utils-subid-2:4.9-6.el9.x86_64   slirp4netns-1.2.0-2.el9.x86_64
yajl-2.1.0-21.el9.x86_64

Complete!

```

- Cài đặt công cụ yum-utils

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

```

[B2012045@b2012045 ~]$ sudo dnf install -y yum-utils
CentOS Stream 9 - BaseOS      892 B/s | 4.3 kB    00:04
CentOS Stream 9 - AppStream    3.5 kB/s | 4.4 kB    00:01
CentOS Stream 9 - Extras packages 3.9 kB/s | 5.4 kB    00:01
Dependencies resolved.
=====
Package                        Arch      Version      Repository    Size
=====
Installing:
yum-utils                      noarch    4.3.0-1.el9  baseos       41 k
Upgrading:
dnf-plugins-core               noarch    4.3.0-1.el9  baseos       35 k
python3-dnf-plugins-core       noarch    4.3.0-1.el9  baseos      245 k
Transaction Summary
=====
Install 1 Package
Upgrade 2 Packages

Total download size: 321 k
Downloading Packages:
(1/3): dnf-plugins-core-4.3.0-1.el9.noarch.rpm 13 kB/s | 35 kB    00:02

```

```
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      : 
  Upgrading      : python3-dnf-plugins-core-4.3.0-1.el9.noarch
  Upgrading      : dnf-plugins-core-4.3.0-1.el9.noarch
  Installing     : yum-utils-4.3.0-1.el9.noarch
  Cleanup        : dnf-plugins-core-4.1.0-3.el9.noarch
  Cleanup        : python3-dnf-plugins-core-4.1.0-3.el9.noarch
  Running scriptlet: python3-dnf-plugins-core-4.1.0-3.el9.noarch
  Verifying      : yum-utils-4.3.0-1.el9.noarch
  Verifying      : dnf-plugins-core-4.3.0-1.el9.noarch
  Verifying      : dnf-plugins-core-4.1.0-3.el9.noarch
  Verifying      : python3-dnf-plugins-core-4.3.0-1.el9.noarch
  Verifying      : python3-dnf-plugins-core-4.1.0-3.el9.noarch

Upgraded:
  dnf-plugins-core-4.3.0-1.el9.noarch
  python3-dnf-plugins-core-4.3.0-1.el9.noarch
Installed:
  yum-utils-4.3.0-1.el9.noarch

Complete!
```

- Thêm địa repo của Docker vào công cụ yum

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

```
[B2012045@b2012045 ~]$ sudo yum-config-manager --add-repo \https://download.doc
ker.com/linux/centos/docker-ce.repo
Adding repo from: https://download.docker.com/linux/centos/docker-ce.repo
```

- Cài đặt Docker

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

```
[B2012045@b2012045 ~]$ sudo dnf install -y docker-ce
Docker CE Stable - x86_64                        8.8 kB/s | 12 kB      00:01
Dependencies resolved.
=====
Package                                Arch      Version                               Repository      Size
=====
Installing:
docker-ce                             x86_64    3:20.10.21-3.el9                     docker-ce-stable 21 M
Installing dependencies:
container-selinux                     noarch    3:2.191.0-1.el9                       appstream        49 k
containerd.io                         x86_64    1.6.9-3.1.el9                         docker-ce-stable 32 M
docker-ce-cli                         x86_64    1:20.10.21-3.el9                     docker-ce-stable 29 M
docker-ce-rootless-extras            x86_64    20.10.21-3.el9                       docker-ce-stable 3.7 M
fuse-overlayfs                        x86_64    1.9-1.el9                             appstream        72 k
libslirp                             x86_64    4.4.0-4.el9                           appstream        69 k
slirp4netns                          x86_64    1.2.0-2.el9                           appstream        47 k
Installing weak dependencies:
docker-scan-plugin                    x86_64    0.21.0-3.el9                         docker-ce-stable 3.8 M

Transaction Summary
=====
Install 9 Packages
```

```
Running scriptlet: container-selinux-3:2.191.0-1.el9.noarch      9/9
Running scriptlet: docker-ce-3:20.10.21-3.el9.x86_64           9/9
Verifying          : container-selinux-3:2.191.0-1.el9.noarch    1/9
Verifying          : fuse-overlayfs-1.9-1.el9.x86_64            2/9
Verifying          : libslirp-4.4.0-4.el9.x86_64                3/9
Verifying          : slirp4netns-1.2.0-2.el9.x86_64             4/9
Verifying          : containerd.io-1.6.9-3.1.el9.x86_64         5/9
Verifying          : docker-ce-3:20.10.21-3.el9.x86_64         6/9
Verifying          : docker-ce-cli-1:20.10.21-3.el9.x86_64     7/9
Verifying          : docker-ce-rootless-extras-20.10.21-3.el9.x86_64 8/9
Verifying          : docker-scan-plugin-0.21.0-3.el9.x86_64    9/9

Installed:
container-selinux-3:2.191.0-1.el9.noarch
containerd.io-1.6.9-3.1.el9.x86_64
docker-ce-3:20.10.21-3.el9.x86_64
docker-ce-cli-1:20.10.21-3.el9.x86_64
docker-ce-rootless-extras-20.10.21-3.el9.x86_64
docker-scan-plugin-0.21.0-3.el9.x86_64
fuse-overlayfs-1.9-1.el9.x86_64
libslirp-4.4.0-4.el9.x86_64
slirp4netns-1.2.0-2.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
```

```
[B2012045@b2012045 ~]$ sudo usermod -aG docker $USER
[sudo] password for B2012045:
```

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

```
[B2012045@b2012045 ~]$ su - $USER
Password:
```

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

```
[B2012045@b2012045 ~]$ sudo systemctl start docker
[B2012045@b2012045 ~]$ sudo systemctl enable docker
Created symlink /etc/systemd/system/multi-user.target.wants/docker.service → /usr/lib/systemd/system/docker.service.
```

```
[B2012045@b2012045 ~]$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
   Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; vendor pre>
   Active: active (running) since Sun 2022-11-13 19:56:59 +07; 27s ago
 TriggeredBy: ● docker.socket
     Docs: https://docs.docker.com
    Main PID: 6279 (dockerd)
       Tasks: 7
      Memory: 90.9M
         CPU: 594ms
    CGroup: /system.slice/docker.service
            └─6279 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/cont>

Nov 13 19:56:57 b2012045 dockerd[6279]: time="2022-11-13T19:56:57.293752613+07:>
Nov 13 19:56:57 b2012045 dockerd[6279]: time="2022-11-13T19:56:57.303356285+07:>
Nov 13 19:56:57 b2012045 dockerd[6279]: time="2022-11-13T19:56:57.508666293+07:>
Nov 13 19:56:58 b2012045 dockerd[6279]: time="2022-11-13T19:56:58.945714265+07:>
Nov 13 19:56:59 b2012045 dockerd[6279]: time="2022-11-13T19:56:59.209568228+07:>
Nov 13 19:56:59 b2012045 dockerd[6279]: time="2022-11-13T19:56:59.584781952+07:>
Nov 13 19:56:59 b2012045 dockerd[6279]: time="2022-11-13T19:56:59.813574512+07:>
Nov 13 19:56:59 b2012045 dockerd[6279]: time="2022-11-13T19:56:59.813959892+07:>
Nov 13 19:56:59 b2012045 systemd[1]: Started Docker Application Container Engin>
Nov 13 19:56:59 b2012045 dockerd[6279]: time="2022-11-13T19:56:59.941571917+07:>
[B2012045@b2012045 ~]$
```

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

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

```
[B2012045@b2012045 ~]$ docker login -u b2012045
Password:
WARNING! Your password will be stored unencrypted in /home/B2012045/.docker/conf
ig.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credentials-store

Login Succeeded
```

- 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
```

```
[B2012045@b2012045 ~]$ docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
2db29710123e: Pull complete
Digest: sha256:faa03e786c97f07ef34423fccceec2398ec8a5759259f94d99078f264e9d7af
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/
```

- 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
```



```
[B2012045@localhost ~]$ docker search httpd
NAME                                DESCRIPTION
STARS    OFFICIAL    AUTOMATED
httpd
  4240    [OK]
centos/httpd-24-centos7
  44
centos/httpd
  35
solsson/httpd-openidc
  2
clearlinux/httpd
  2
hypoport/httpd-cgi
  2
dockerpinata/httpd
  1
centos/httpd-24-centos8
  1
inanimate/httpd-ssl
  1
publici/httpd
  1
```

- Tạo container từ image httpd

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

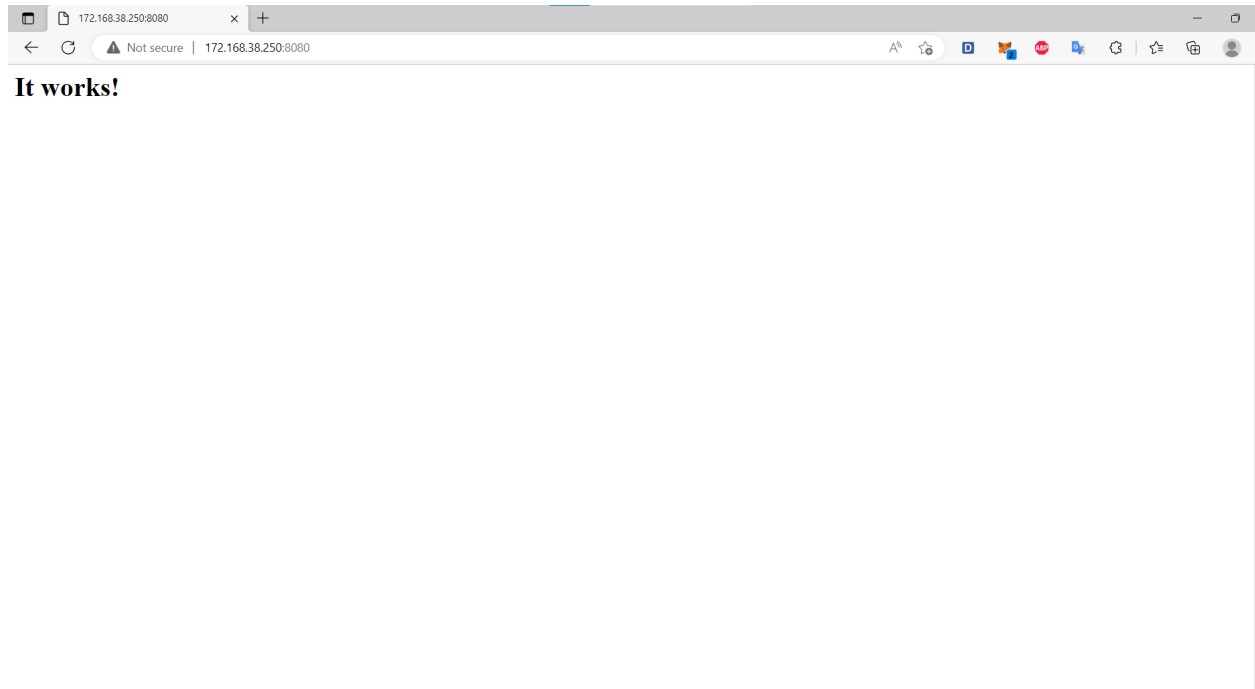
-d: chạy container ở chế độ background

-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.

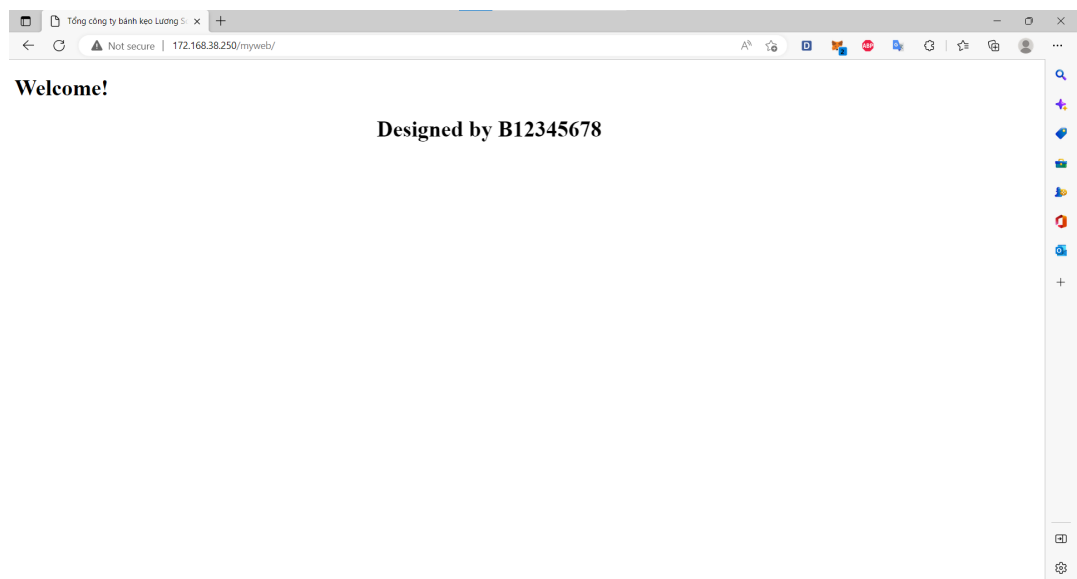
```
[B2012045@localhost ~]$ docker run -d -it -p 8080:80 --name webserver httpd
Unable to find image 'httpd:latest' locally
latest: Pulling from library/httpd
a603fa5e3b41: Pull complete
4691bd33efec: Pull complete
ff7b0b8c417a: Pull complete
9df1012343c7: Pull complete
b1c114085b25: Pull complete
Digest: sha256:f2e89def4c032b02c83e162c1819ccfcbd4ea6bdbc5ff784bbc68cba940a9046
Status: Downloaded newer image for httpd:latest
bdf72c22844659112e88717b5105099d41ca1dc5c518a940954aeaf25adf0d32
[B2012045@localhost ~]$
```

- 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/
```

- 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.



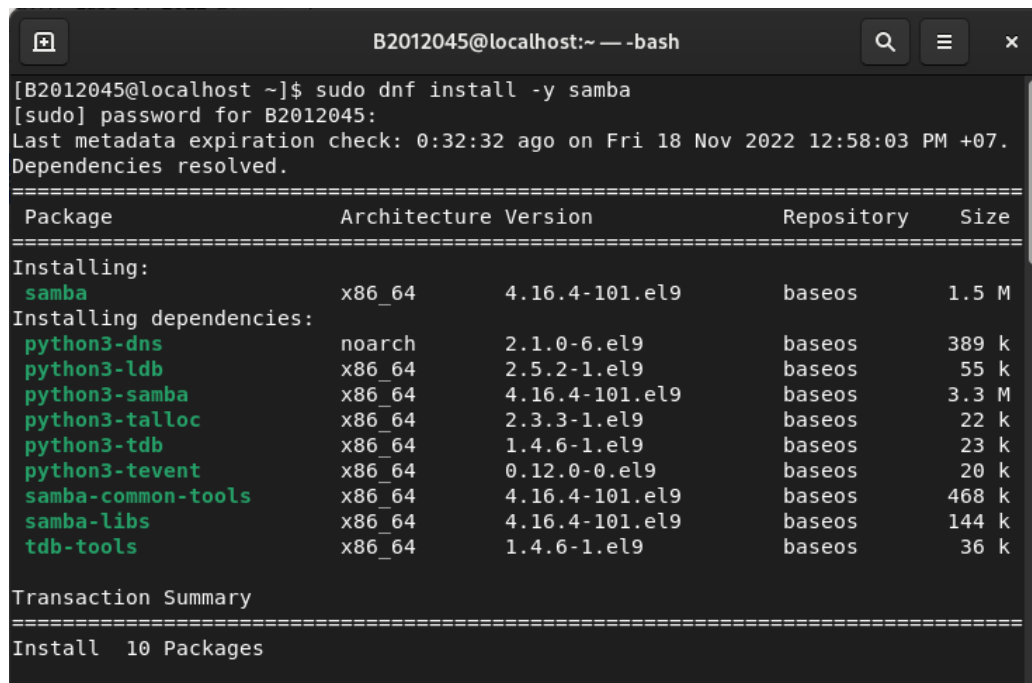
2. Cài đặt và cấu hình dịch vụ SAMBA

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
```

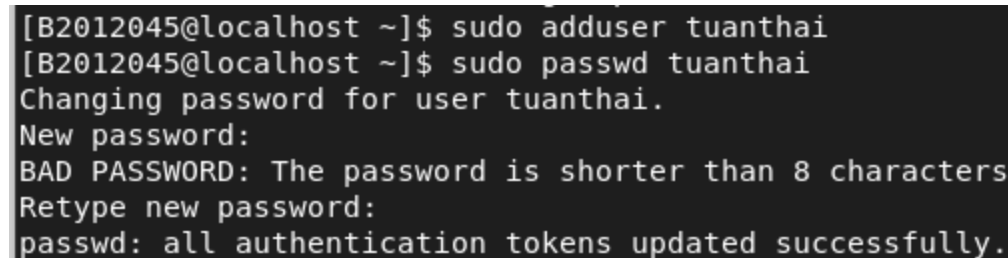


```
[B2012045@localhost ~] $ sudo dnf install -y samba
[sudo] password for B2012045:
Last metadata expiration check: 0:32:32 ago on Fri 18 Nov 2022 12:58:03 PM +07.
Dependencies resolved.
=====
Package                        Architecture Version           Repository         Size
=====
Installing:
samba                          x86_64           4.16.4-101.el9    baseos             1.5 M
Installing dependencies:
python3-dns                    noarch           2.1.0-6.el9       baseos             389 k
python3-ldb                    x86_64           2.5.2-1.el9       baseos             55 k
python3-samba                  x86_64           4.16.4-101.el9    baseos             3.3 M
python3-talloc                 x86_64           2.3.3-1.el9       baseos             22 k
python3-tdb                    x86_64           1.4.6-1.el9       baseos             23 k
python3-tevent                 x86_64           0.12.0-0.el9      baseos             20 k
samba-common-tools             x86_64           4.16.4-101.el9    baseos             468 k
samba-libs                     x86_64           4.16.4-101.el9    baseos             144 k
tdb-tools                      x86_64           1.4.6-1.el9       baseos             36 k
=====
Transaction Summary
=====
Install 10 Packages
```

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

```
$sudo adduser tuanthai
```

```
$sudo passwd tuanthai
```



```
[B2012045@localhost ~]$ sudo adduser tuanthai
[B2012045@localhost ~]$ sudo passwd tuanthai
Changing password for user tuanthai.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
```

```
$sudo groupadd lecturers
```



```
[B2012045@localhost ~]$ sudo groupadd lecturers
```

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



```
[B2012045@localhost ~]$ sudo usermod -a -G lecturers tuanthai
```

- Tạo thư mục cần chia sẻ và phân quyền:

```
$sudo mkdir /data
```

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

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

```
[B2012045@localhost ~]$ sudo mkdir /data
[B2012045@localhost ~]$ sudo chown :lecturers /data
[B2012045@localhost ~]$ sudo chmod -R 775 /data
```

- Cấu hình dịch vụ Samba:

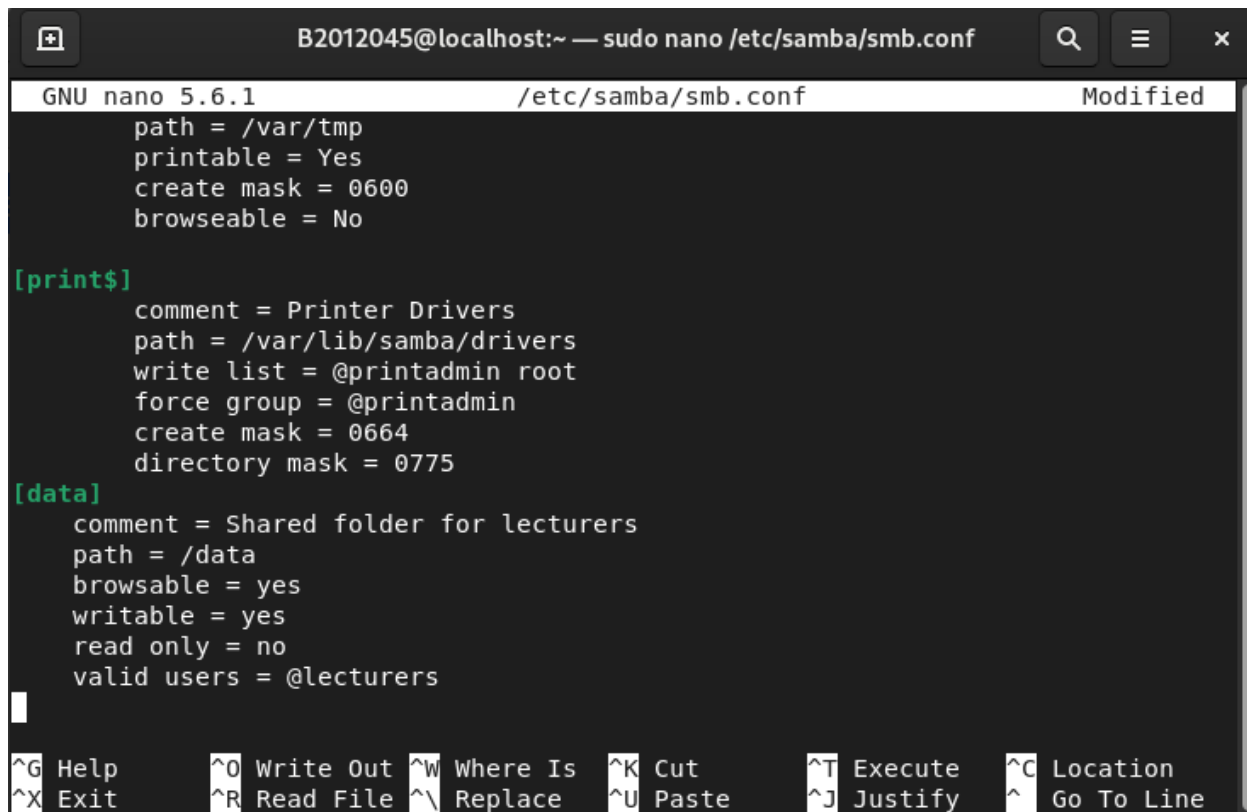
```
$sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.orig
```

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

```
[B2012045@localhost ~]$ sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.orig
[B2012045@localhost ~]$ 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
```



```
B2012045@localhost:~ — sudo nano /etc/samba/smb.conf
GNU nano 5.6.1 /etc/samba/smb.conf Modified
    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

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

- Thêm người dùng cho dịch vụ Samba:

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

#Đặt mật khẩu Samba cho người dùng

```
[B2012045@localhost ~]$ sudo smbpasswd -a tuanthai
New SMB password:
Retype new SMB password:
Added user tuanthai.
```

- Cấu hình SELINUX cho phép Samba

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

```
[B2012045@localhost ~]$ sudo setsebool -P samba_export_all_rw on
[B2012045@localhost ~]$ sudo setsebool -P samba_enable_home_dirs on
```

- Tắt tường lửa:

```
$sudo systemctl stop firewalld
```

```
[B2012045@localhost ~]$ sudo systemctl stop firewalld
```

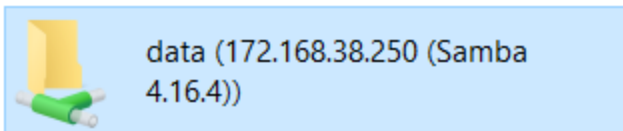
- Khởi động cho phép Samba tự động thực thi khi khởi động hệ điều hành:

```
$sudo systemctl start smb
$sudo systemctl enable smb
```

```
[B2012045@localhost ~]$ sudo systemctl start smb
[B2012045@localhost ~]$ sudo systemctl enable smb
Created symlink /etc/systemd/system/multi-user.target.wants/smb.service → /usr/lib/systemd/system/smb.service.
```

- 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

▼ Network locations (1)



```
[B2012045@localhost ~]$ ls /data
hello.txt  'New folder'
[B2012045@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:

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

```
[B2012045@localhost ~]$ sudo dnf install bind bind-utils -y
```

```
[sudo] password for B2012045:
```

```
Last metadata expiration check: 0:58:17 ago on Fri 18 Nov 2022 12:58:03 PM +07.
```

```
Package bind-utils-32:9.16.23-4.el9.x86_64 is already installed.
```

```
Dependencies resolved.
```

Package	Arch	Version	Repository	Size
Installing:				
bind	x86_64	32:9.16.23-4.el9	appstream	504 k
Installing dependencies:				
bind-dnssec-doc	noarch	32:9.16.23-4.el9	appstream	47 k
python3-bind	noarch	32:9.16.23-4.el9	appstream	69 k
python3-ply	noarch	3.11-14.el9	appstream	106 k
Installing weak dependencies:				
bind-dnssec-utils	x86_64	32:9.16.23-4.el9	appstream	118 k
Transaction Summary				
Install 5 Packages				
Total download size: 845 k				
Installed size: 2.5 M				
Downloading Packages:				

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; };
};
...

```

```

GNU nano 5.6.1 /etc/named.conf
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
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; };
}

```

[Read 73 lines]

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



```
B2012045@localhost:~ — sudo nano /etc/named.conf
GNU nano 5.6.1 /etc/named.conf
    file "named.ca";
};

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

zone "0.168.172.in-addr.arpa" IN {
    type master;
    file "reverse.qtht";
    allow-update { none; };
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

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

3.3. Tạo tập tin cấu hình phân giải xuôi:

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

```
[B2012045@localhost ~]$ sudo cp /var/named/named.localhost /var/named/forward.qtht
```

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

```
[B2012045@localhost ~]$ sudo chgrp named /var/named/forward.qtht
```

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

```
[B2012045@localhost ~]$ 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
htql   IN    A      8.8.8.8
```



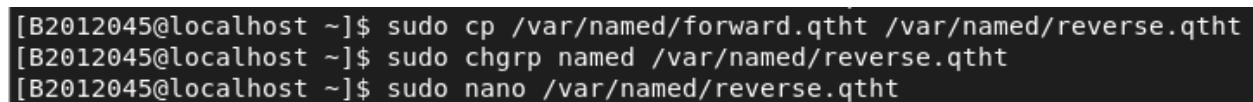
```
B2012045@localhost:~ — sudo nano /var/named/forward.qtht
GNU nano 5.6.1 /var/named/forward.qtht
$TTL 1D
@      IN SOA  @ qtht.com.vn. (
                                0      ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )    ; minimum

@      IN     NS      dns.qtht.com.vn.
dns    IN     A       172.168.38.250
www    IN     A       172.168.38.250
htql   IN     A       8.8.8.8

[ Read 11 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

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
```



```
[B2012045@localhost ~]$ sudo cp /var/named/forward.qtht /var/named/reverse.qtht
[B2012045@localhost ~]$ sudo chgrp named /var/named/reverse.qtht
[B2012045@localhost ~]$ 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.
```

```
B2012045@localhost:~ — sudo nano /var/named/reverse.qtht
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       172.168.38.250
250     IN     PTR     www.qtht.com.vn.

[ Wrote 10 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

3.5. Kiểm tra và sử dụng dịch vụ DNS

- Tắt tường lửa:

```
$sudo systemctl stop firewalld
```

```
[B2012045@localhost ~]$ sudo systemctl stop firewalld
```

- Khởi động dịch vụ DNS:

```
$sudo systemctl start named
```

```
[B2012045@localhost ~]$ sudo systemctl start named
```

```
[B2012045@localhost ~]$ sudo systemctl status named
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; disabled; vendor pr>
   Active: active (running) since Fri 2022-11-18 14:22:57 +07; 8s ago
     Process: 38274 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" ==>
     Process: 38276 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS >
   Main PID: 38277 (named)
     Tasks: 4 (limit: 10944)
    Memory: 18.6M
       CPU: 63ms
    CGroup: /system.slice/named.service
           └─38277 /usr/sbin/named -u named -c /etc/named.conf

Nov 18 14:22:57 localhost.localdomain named[38277]: zone 1.0.0.0.0.0.0.0.0.0.>
Nov 18 14:22:57 localhost.localdomain named[38277]: zone localhost.localdomain/>
Nov 18 14:22:57 localhost.localdomain named[38277]: zone 1.0.0.127.in-addr.arp>
Nov 18 14:22:57 localhost.localdomain named[38277]: zone qtht.com.vn/IN: loaded>
Nov 18 14:22:57 localhost.localdomain named[38277]: zone qtht.com.vn/IN: sendin>
Nov 18 14:22:57 localhost.localdomain named[38277]: all zones loaded
Nov 18 14:22:57 localhost.localdomain systemd[1]: Started Berkeley Internet Nam>
Nov 18 14:22:57 localhost.localdomain named[38277]: running
Nov 18 14:22:57 localhost.localdomain named[38277]: managed-keys-zone: Initiali>
Nov 18 14:22:57 localhost.localdomain named[38277]: resolver priming query comp>
[B2012045@localhost ~]$
```

- Kiểm tra kết quả:

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

```
[B2012045@localhost ~]$ nslookup www.qtht.com.vn 172.168.38.250
Server:          172.168.38.250
Address:         172.168.38.250#53

Name:   www.qtht.com.vn
Address: 172.168.38.250
```

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

```
[B2012045@localhost ~]$ nslookup htql.qtht.com.vn 172.168.38.250
Server:          172.168.38.250
Address:         172.168.38.250#53

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

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

```
[B2012045@localhost ~]$ nslookup www.ctu.edu.vn 172.168.38.250
Server:          172.168.38.250
Address:         172.168.38.250#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>

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
`$sudo systemctl start firewalld`

```
B2012045@localhost:~ — -bash
[B2012045@localhost ~]$ sudo systemctl start firewalld
[B2012045@localhost ~]$ sudo systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor>
   Active: active (running) since Fri 2022-11-18 15:35:31 +07; 35s ago
     Docs: man:firewalld(1)
  Main PID: 39443 (firewalld)
    Tasks: 2 (limit: 10944)
   Memory: 31.1M
      CPU: 545ms
   CGroup: /system.slice/firewalld.service
           └─39443 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid

Nov 18 15:35:31 localhost.localdomain systemd[1]: Starting firewalld - dynamic >
Nov 18 15:35:31 localhost.localdomain systemd[1]: Started firewalld - dynamic f>
```

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

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

```
[B2012045@localhost ~]$ firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
```

- Kiểm tra zone mặc định

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

```
[B2012045@localhost ~]$ firewall-cmd --get-default-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
```

```
[B2012045@localhost ~]$ firewall-cmd --get-active-zones
public
interfaces: enp0s3
```

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

```
[B2012045@localhost ~]$ 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:
[B2012045@localhost ~]$
```

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

The screenshot shows a Google Docs document titled "B2012045_QTHT_Lab5_01_2022_2023" with a list of tasks. A Windows Command Prompt window is open, displaying the output of the firewall-cmd command and the results of a ping test to 172.168.38.250.

Command Prompt Output:

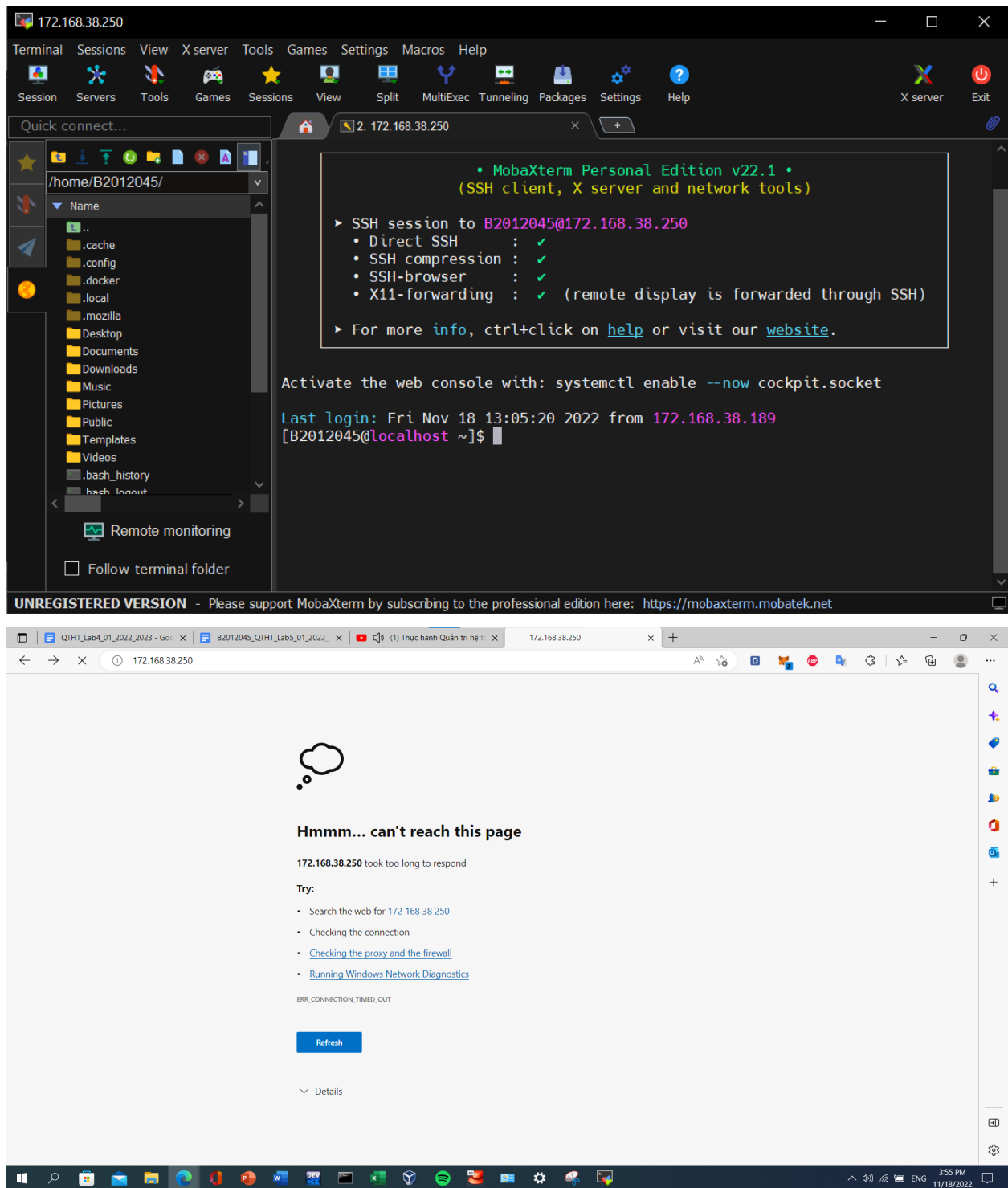
```
C:\Users\DELL>ping 172.168.38.250

Pinging 172.168.38.250 with 32 bytes of data:
Reply from 172.168.38.250: bytes=32 time=1ms TTL=64
Reply from 172.168.38.250: bytes=32 time=1ms TTL=64
Reply from 172.168.38.250: bytes=32 time=1ms TTL=64
Reply from 172.168.38.250: bytes=32 time=1ms TTL=64

Ping statistics for 172.168.38.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Google Docs List:

- Từ máy vật lý, ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS. Cho biết kết quả.
- Chuyển giao diện
- \$sudo firewall-cmd --list-all
- \$sudo firewall-cmd --list-all
- Từ máy vật lý, ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS. Cho biết kết quả.
- Chuyển giao diện
- \$sudo firewall-cmd --list-all
- \$sudo firewall-cmd --list-all
- Từ máy vật lý, ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS. Cho biết kết quả.
- Tạo zone mới có tên gthtserver
- \$sudo firewall-cmd --permanent --new-zone=gthtserver
- \$sudo systemctl restart firewalld
- \$sudo firewall-cmd --list-all --zone=gthtserver
- Cho phép các dịch vụ HTTP, DNS, SAMBA, FTP và cổng 9999/tcp hoạt động



Không truy cập được đến web server CentOS vì zone publish không cho phép dịch vụ http, dịch vụ web


```
[B2012045@localhost ~]$ 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:
```

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

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

```
[B2012045@localhost ~]$ sudo firewall-cmd --zone=drop --change-interface=enp0s3
success
```

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

```
[B2012045@localhost ~]$ 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:
[B2012045@localhost ~]$
```

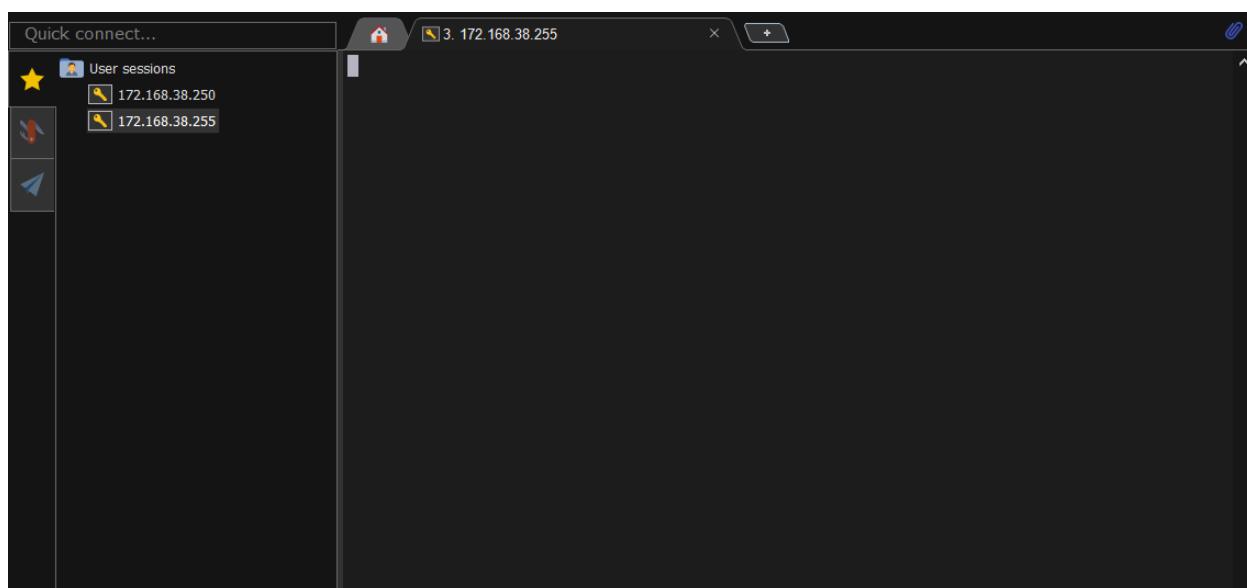
- Từ máy vật lý, ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS. Cho biết kết quả.

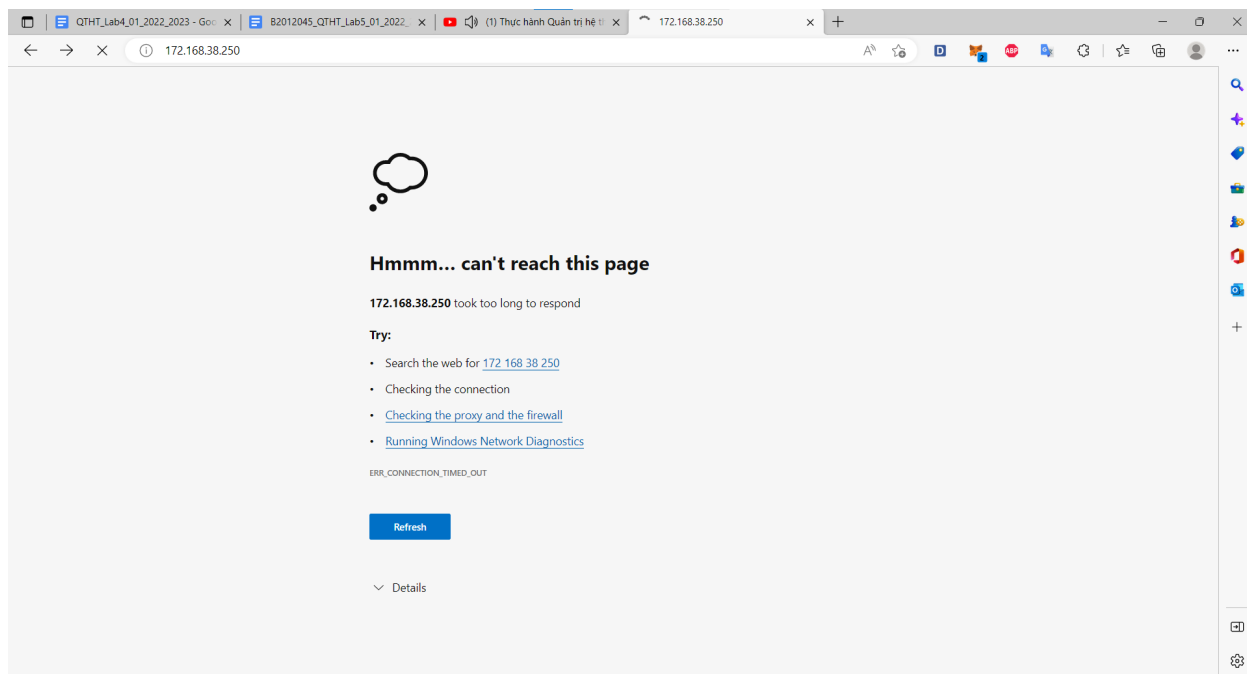
```
C:\Users\DELL>ping 172.168.38.250

Pinging 172.168.38.250 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.168.38.250:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\DELL>
```





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

```
[B2012045@localhost ~]$ $sudo firewall-cmd --zone=trusted --change-interface=enp0s3
success
```

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

```
[B2012045@localhost ~]$ $sudo firewall-cmd --list-all --zone=trusted
trusted (active)
  target: ACCEPT
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services:
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[B2012045@localhost ~]$
```

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

```
C:\Users\DELL>ping 172.168.38.250

Pinging 172.168.38.250 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

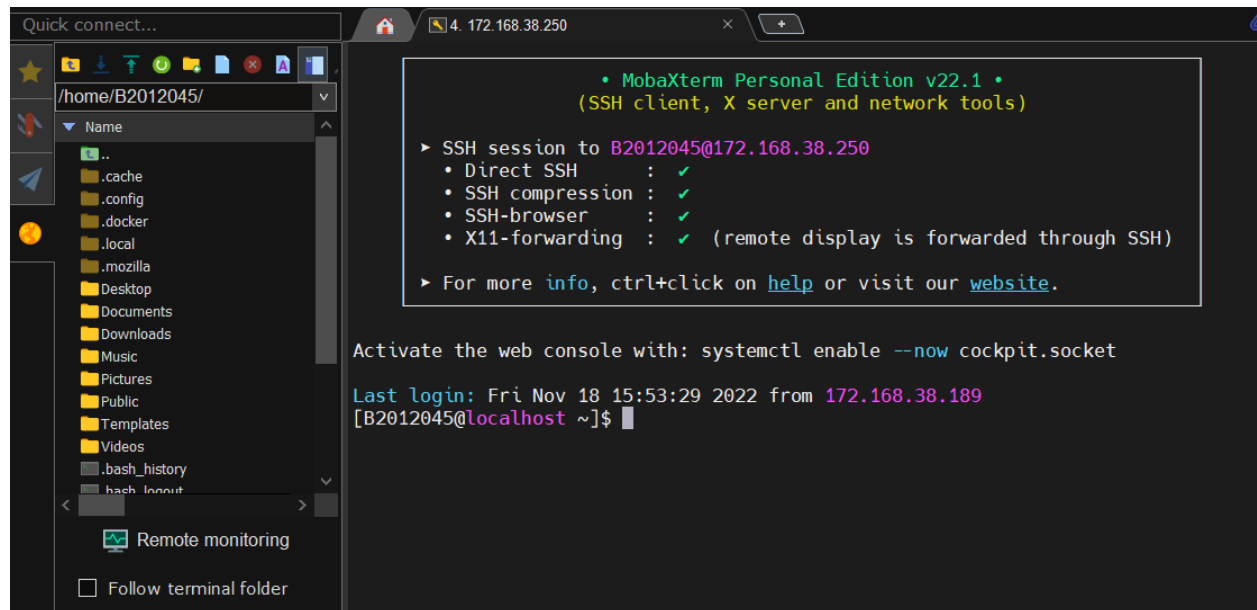
Ping statistics for 172.168.38.250:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

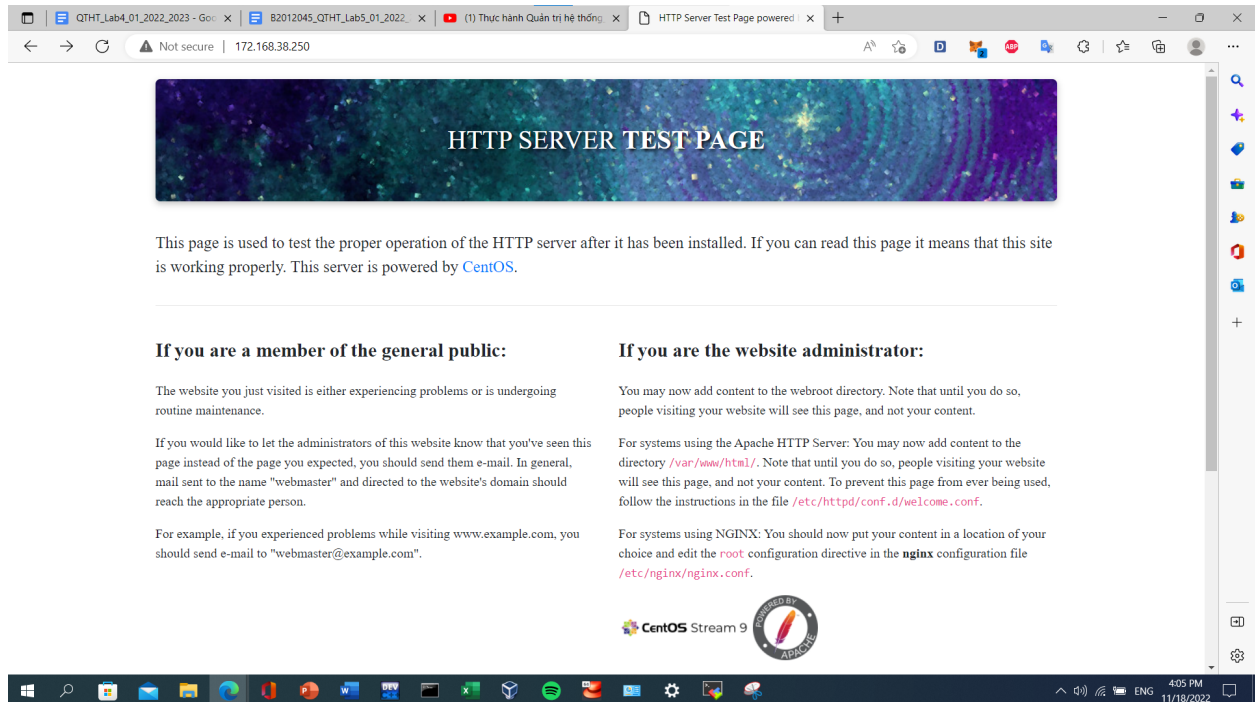
C:\Users\DELL>ping 172.168.38.250

Pinging 172.168.38.250 with 32 bytes of data:
Reply from 172.168.38.250: bytes=32 time<1ms TTL=64
Reply from 172.168.38.250: bytes=32 time=2ms TTL=64
Reply from 172.168.38.250: bytes=32 time=2ms TTL=64
Reply from 172.168.38.250: bytes=32 time=1ms TTL=64

Ping statistics for 172.168.38.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\Users\DELL>
```





- 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
```

```
[B2012045@localhost ~]$ sudo firewall-cmd --permanent --new-zone=qthtserver
[sudo] password for B2012045:
Sorry, try again.
[sudo] password for B2012045:
success
[B2012045@localhost ~]$ sudo systemctl restart firewalld
[B2012045@localhost ~]$ 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:
[B2012045@localhost ~]$
```

- 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
```

```
[B2012045@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=http
success
[B2012045@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=dns
success
[B2012045@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=ftp
success
[B2012045@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=samba
success
[B2012045@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-port=9999/tcp
success
[B2012045@localhost ~]$
```

- 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'
```

```
[B2012045@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-rich-rule='rule family=ipv4 source address=172.168.38.189/32 port port=22 protocol=tcp accept'
success
[B2012045@localhost ~]$
```

- Khởi động lại tường lửa firewalld

```
$sudo systemctl restart firewalld
```

```
[B2012045@localhost ~]$ sudo systemctl restart firewalld
```

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

```
$sudo firewall-cmd --permanent --zone=qthtserver --change-interface=enp0s3
```

```
[B2012045@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --change-interface=enp0s3
The interface is under control of NetworkManager, setting zone to 'qthtserver'.
success
```

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

```
[B2012045@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="172.168.38.189/32" port port="22" protocol="tcp" accept
[B2012045@localhost ~]$
```

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

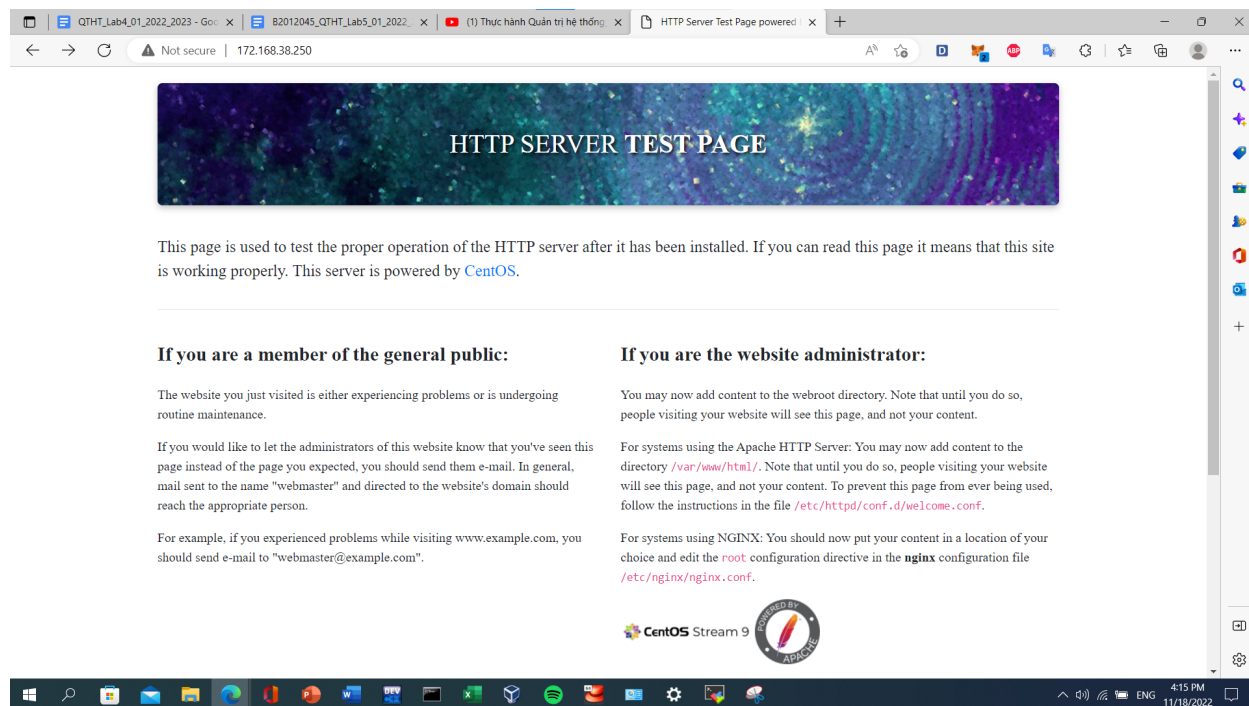
```
• MobaXterm Personal Edition v22.1 •
(SSH client, X server and network tools)

► SSH session to B2012045@172.168.38.250
  • 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 18 16:05:35 2022 from 172.168.38.189
[B2012045@localhost ~]$
```

--- Hết ---