



LAB 5

DOCKER, SAMBA, DNS và Firewall

Họ tên và MSSV: Nguyễn Hoàng Huy - B2011967

Nhóm học phần: Quản trị hệ thống - 01

- 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)
 - Cấu hình mạng máy ảo

```
b2011967@myserver:~  
[b2011967@myserver ~]$ nmcli -f ipv4.dns,ipv4.addresses,ipv4.gateway con show en  
p0s3  
ipv4.dns: 123.23.23.23,123.26.26.26  
ipv4.addresses: 192.168.1.245/24  
ipv4.gateway: 192.168.1.1  
[b2011967@myserver ~]$
```

- Kiểm tra bằng cách ping từ máy vật lý sang máy ảo => máy window (đã ping được sang máy ảo).

```
Command Prompt  
C:\Users\PC>ping 192.168.1.245  
  
Pinging 192.168.1.245 with 32 bytes of data:  
Reply from 192.168.1.245: bytes=32 time<1ms TTL=64  
Reply from 192.168.1.245: bytes=32 time<1ms TTL=64  
Reply from 192.168.1.245: bytes=32 time<1ms TTL=64  
Reply from 192.168.1.245: bytes=32 time<1ms TTL=64  
  
Ping statistics for 192.168.1.245:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 0ms, Average = 0ms  
  
C:\Users\PC>
```

- Kiểm tra bằng cách ping google.com (ping thành công google.com)

```
b2011967@myserver:~  
[b2011967@myserver ~]$ 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=116 time=60.7 ms  
64 bytes from hkg07s40-in-f14.1e100.net (142.250.204.110): icmp_seq=2 ttl=116 time=61.7 ms  
64 bytes from hkg07s40-in-f14.1e100.net (142.250.204.110): icmp_seq=3 ttl=116 time=61.5 ms  
  
--- google.com ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2002ms  
rtt min/avg/max/mdev = 60.723/61.305/61.672/0.416 ms  
[b2011967@myserver ~]$
```

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

```
b2011967@myserver:~  
[b2011967@myserver ~]$ cat ./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>  
[b2011967@myserver ~]$
```

Tắt tường lửa:

```
$sudo systemctl stop firewalld  
(Tắt tường lửa và kiểm tra trạng thái)
```

```
b2011967@myserver:~ — sudo systemctl status firewalld
[b2011967@myserver ~]$ sudo systemctl stop firewalld
[sudo] password for b2011967:
[b2011967@myserver ~]$ sudo systemctl status firewalld
○ firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor
   Active: inactive (dead) since Thu 2023-04-13 21:33:01 +07; 7s ago
   Duration: 27min 50.299s
   Docs: man:firewalld(1)
   Process: 6415 ExecStart=/usr/sbin/firewalld --nofork --nopid $FIREWALLD_ARG
   Main PID: 6415 (code=exited, status=0/SUCCESS)
   CPU: 913ms

Apr 13 21:05:10 myserver systemd[1]: Starting firewalld - dynamic firewall daem
Apr 13 21:05:11 myserver systemd[1]: Started firewalld - dynamic firewall daemo
Apr 13 21:33:01 myserver systemd[1]: Stopping firewalld - dynamic firewall daem
Apr 13 21:33:01 myserver systemd[1]: firewalld.service: Deactivated successfull
Apr 13 21:33:01 myserver systemd[1]: Stopped firewalld - dynamic firewall daemo
lines 1-14/14 (END)
```

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 dùng độ với Docker)

\$sudo dnf -y remove podman runc

```
b2011967@myserver:~
[b2011967@myserver ~]$ sudo dnf -y remove podman runc
[sudo] password for b2011967:
Dependencies resolved.
=====
Package                Arch      Version      Repository      Size
=====
Removing:
podman                  x86_64    2:4.1.1-1.el9 @AppStream      45 M
runc                    x86_64    4:1.1.3-1.el9 @AppStream       9.5 M
Removing dependent packages:
```

```

b2011967@myserver:~
Verifying      : libnet-1.2-6.el9.x86_64      11/19
Verifying      : libslirp-4.4.0-4.el9.x86_64  12/19
Verifying      : netavark-2:1.0.1-39.el9.x86_64 13/19
Verifying      : podman-2:4.1.1-1.el9.x86_64  14/19
Verifying      : podman-catatonit-2:4.1.1-1.el9.x86_64 15/19
Verifying      : runc-4:1.1.3-1.el9.x86_64    16/19
Verifying      : shadow-utils-subid-2:4.9-4.el9.x86_64 17/19
Verifying      : slirp4netns-1.2.0-2.el9.x86_64 18/19
Verifying      : yajl-2.1.0-20.el9.x86_64     19/19

Removed:
aardvark-dns-2:1.0.1-39.el9.x86_64      buildah-1:1.26.1-4.el9.x86_64
cockpit-podman-48-1.el9.noarch           common-2:2.1.2-2.el9.x86_64
container-selinux-3:2.188.0-1.el9.noarch containers-common-2:1-39.el9.x86_64
criu-3.17-2.el9.x86_64                  criu-libs-3.17-2.el9.x86_64
crun-1.4.5-2.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-2:1.0.1-39.el9.x86_64          podman-2:4.1.1-1.el9.x86_64
podman-catatonit-2:4.1.1-1.el9.x86_64   runc-4:1.1.3-1.el9.x86_64
shadow-utils-subid-2:4.9-4.el9.x86_64   slirp4netns-1.2.0-2.el9.x86_64
yajl-2.1.0-20.el9.x86_64

Complete!
[b2011967@myserver ~]$

```

- Cài đặt công cụ yum-utils

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

```

b2011967@myserver:~
[b2011967@myserver ~]$ sudo dnf install -y yum-utils
Last metadata expiration check: 0:16:33 ago on Thu 13 Apr 2023 09:25:07 PM +07.
Dependencies resolved.
=====
Package                Arch      Version      Repository    Size
=====
Installing:
yum-utils              noarch    4.3.0-4.el9  baseos        41 k
Upgrading:
dnf-plugins-core       noarch    4.3.0-4.el9  baseos        38 k
python3-dnf-plugins-core noarch    4.3.0-4.el9  baseos       260 k
=====

```

```
b2011967@myserver:~  
Running transaction test  
Transaction test succeeded.  
Running transaction  
  Preparing           :                               1/1  
  Upgrading           : python3-dnf-plugins-core-4.3.0-4.el9.noarch 1/5  
  Upgrading           : dnf-plugins-core-4.3.0-4.el9.noarch        2/5  
  Installing          : yum-utils-4.3.0-4.el9.noarch               3/5  
  Cleanup             : dnf-plugins-core-4.1.0-1.el9.noarch        4/5  
  Cleanup             : python3-dnf-plugins-core-4.1.0-1.el9.noarch 5/5  
  Running scriptlet: python3-dnf-plugins-core-4.1.0-1.el9.noarch 5/5  
  Verifying           : yum-utils-4.3.0-4.el9.noarch               1/5  
  Verifying           : dnf-plugins-core-4.3.0-4.el9.noarch        2/5  
  Verifying           : dnf-plugins-core-4.1.0-1.el9.noarch        3/5  
  Verifying           : python3-dnf-plugins-core-4.3.0-4.el9.noarch 4/5  
  Verifying           : python3-dnf-plugins-core-4.1.0-1.el9.noarch 5/5  
  
Upgraded:  
  dnf-plugins-core-4.3.0-4.el9.noarch  
  python3-dnf-plugins-core-4.3.0-4.el9.noarch  
Installed:  
  yum-utils-4.3.0-4.el9.noarch  
  
Complete!  
[b2011967@myserver ~]$
```

- Thêm địa repo của Docker vào công cụ yum

```
$sudo yum-config-manager \  
--add-repo \  

```

<https://download.docker.com/linux/centos/docker-ce.repo>

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

```
b2011967@myserver:~  
[b2011967@myserver ~]$ sudo yum-config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo  
Adding repo from: https://download.docker.com/linux/centos/docker-ce.repo  
[b2011967@myserver ~]$
```

- Cài đặt Docker

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

```
b2011967@myserver:~  
[b2011967@myserver ~]$ sudo dnf install docker-ce -y  
Docker CE Stable - x86_64                23 kB/s | 21 kB    00:00  
Dependencies resolved.  
=====
```

Package	Arch	Version	Repository	Size
Installing:				
docker-ce	x86_64	3:23.0.2-1.el9	docker-ce-stable	23 M

```
=====
```

```
b2011967@myserver:~  
Verifying      : docker-scan-plugin-0.23.0-3.el9.x86_64      11/15  
Verifying      : selinux-policy-38.1.11-2.el9.noarch        12/15  
Verifying      : selinux-policy-34.1.37-1.el9.noarch        13/15  
Verifying      : selinux-policy-targeted-38.1.11-2.el9.noarch 14/15  
Verifying      : selinux-policy-targeted-34.1.37-1.el9.noarch 15/15  
  
Upgraded:  
  selinux-policy-38.1.11-2.el9.noarch  
  selinux-policy-targeted-38.1.11-2.el9.noarch  
Installed:  
  container-selinux-3:2.209.0-1.el9.noarch  
  containerd.io-1.6.20-3.1.el9.x86_64  
  docker-buildx-plugin-0.10.4-1.el9.x86_64  
  docker-ce-3:23.0.2-1.el9.x86_64  
  docker-ce-cli-1:23.0.2-1.el9.x86_64  
  docker-ce-rootless-extras-23.0.2-1.el9.x86_64  
  docker-compose-plugin-2.17.2-1.el9.x86_64  
  docker-scan-plugin-0.23.0-3.el9.x86_64  
  fuse-overlayfs-1.11-1.el9.x86_64  
  libslirp-4.4.0-7.el9.x86_64  
  slirp4netns-1.2.0-3.el9.x86_64  
  
Complete!  
[b2011967@myserver ~]$
```

- 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
```

```
b2011967@myserver:~  
[b2011967@myserver ~]$ sudo usermod -aG docker $USER  
[sudo] password for b2011967:  
[b2011967@myserver ~]$
```

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

```
$su - $USER
```

```
b2011967@myserver:~ -- -bash  
[b2011967@myserver ~]$ su - $USER  
Password:  
[b2011967@myserver ~]$
```

- Chạy dịch vụ Docker

```
$sudo systemctl start docker
```

```
$sudo systemctl enable docker
```

```
b2011967@myserver:~ — sudo systemctl status docker

[b2011967@myserver ~]$ sudo systemctl start docker
[b2011967@myserver ~]$ sudo systemctl enable docker
Created symlink /etc/systemd/system/multi-user.target.wants/docker.service → /usr/lib/systemd/system/docker.service.
[b2011967@myserver ~]$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
   Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2023-04-16 16:14:57 +07; 29s ago
     TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
      Main PID: 9372 (dockerd)
         Tasks: 7
        Memory: 28.5M
          CPU: 391ms
         CGroup: /system.slice/docker.service
                └─9372 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock

Apr 16 16:14:56 myserver dockerd[9372]: time="2023-04-16T16:14:56.694985009+07:00" level=info msg="Starting dockerd"
Apr 16 16:14:56 myserver dockerd[9372]: time="2023-04-16T16:14:56.695101323+07:00" level=info msg="API listen on /var/run/docker.sock"
Apr 16 16:14:56 myserver dockerd[9372]: time="2023-04-16T16:14:56.826115178+07:00" level=info msg="Listening for events on /var/run/docker.sock"
Apr 16 16:14:57 myserver dockerd[9372]: time="2023-04-16T16:14:57.294245668+07:00" level=info msg="Listening for events on /var/run/docker.sock"
Apr 16 16:14:57 myserver dockerd[9372]: time="2023-04-16T16:14:57.546720950+07:00" level=info msg="Listening for events on /var/run/docker.sock"
Apr 16 16:14:57 myserver dockerd[9372]: time="2023-04-16T16:14:57.617342792+07:00" level=info msg="Listening for events on /var/run/docker.sock"
Apr 16 16:14:57 myserver dockerd[9372]: time="2023-04-16T16:14:57.617771866+07:00" level=info msg="Listening for events on /var/run/docker.sock"
```

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

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

```
b2011967@myserver:~ — -bash

[b2011967@myserver ~]$ docker login -u b2011967
Password:
WARNING! Your password will be stored unencrypted in /home/b2011967/.docker/config.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credentials-store

Login Succeeded
[b2011967@myserver ~]$
```

- 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
```



```

b2011967@myserver:~ — -bash
[b2011967@myserver ~]$ docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
2db29710123e: Pull complete
Digest: sha256:4e83453afed1b4fala3500525091dbfca6ce1e66903fd4c01ff015dbcb1ba33e
Status: Downloaded newer image for hello-world:latest

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

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

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

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

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

[b2011967@myserver ~]$

```

- 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

```

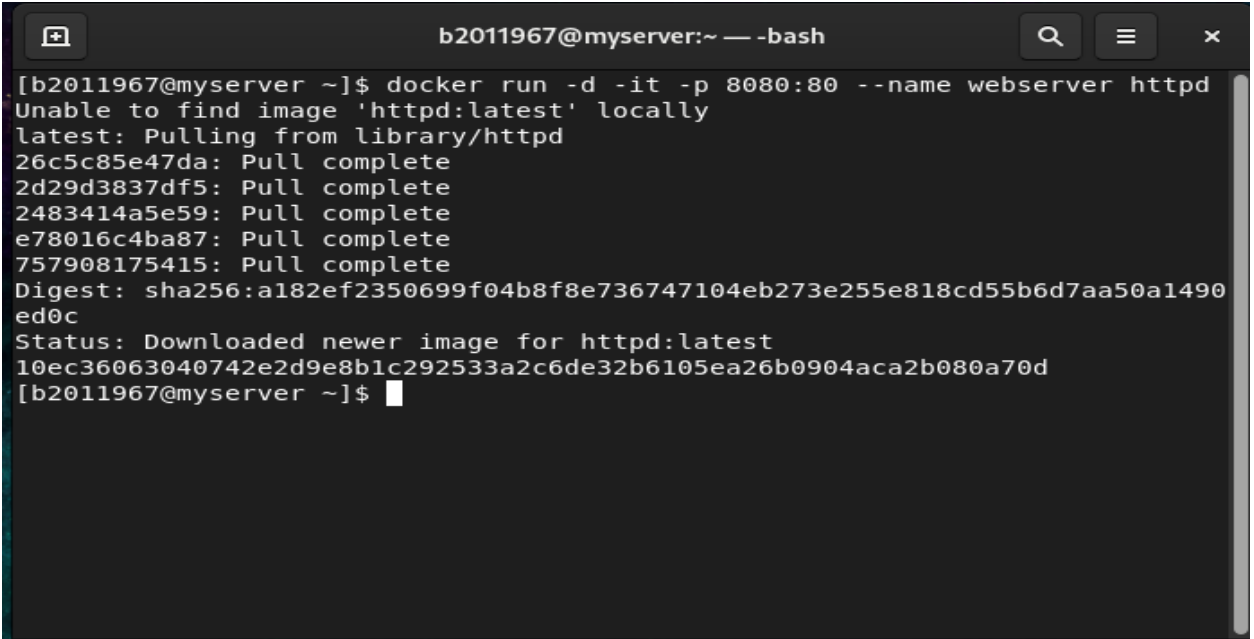
b2011967@myserver:~ — -bash
[b2011967@myserver ~]$ docker search httpd
NAME                DESCRIPTION                                     STARS
ARS    OFFICIAL    AUTOMATED
httpd              The Apache HTTP Server Project                43
98      [OK]
clearlinux/httpd   httpd HyperText Transfer Protocol (HTTP) ser...  2
paketobuildpacks/httpd
vulhub/httpd
jitesoft/httpd     Apache httpd on Alpine linux.                 0
avenga/httpd-static
betterweb/httpd
centos/httpd-24-centos7   Platform for running Apache httpd 2.4 or bui...  45
manageiq/httpd         Container with httpd, built on CentOS for Ma...  1
[OK]
centos/httpd-24-centos8
dockerpinata/httpd
19022021/httpd-connection_test   This httpd image will test the connectivity ...  0
centos/httpd          [OK]                                           36

```

- Tạo container từ image httpd


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

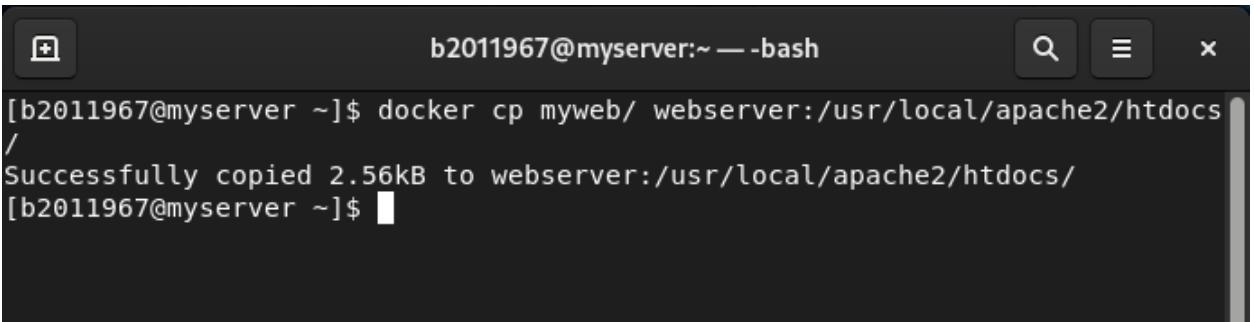
- d: chạy container ở chế độ background
- it: tạo shell để tương tác với container
- name webserver: đặt tên container là webserver
- p 8080:80 gắn cổng 8080 của máy CentOS vào cổng 80 của container.



```
b2011967@myserver:~ — -bash
[b2011967@myserver ~]$ docker run -d -it -p 8080:80 --name webserver httpd
Unable to find image 'httpd:latest' locally
latest: Pulling from library/httpd
26c5c85e47da: Pull complete
2d29d3837df5: Pull complete
2483414a5e59: Pull complete
e78016c4ba87: Pull complete
757908175415: Pull complete
Digest: sha256:a182ef2350699f04b8f8e736747104eb273e255e818cd55b6d7aa50a1490ed0c
Status: Downloaded newer image for httpd:latest
10ec36063040742e2d9e8b1c292533a2c6de32b6105ea26b0904aca2b080a70d
[b2011967@myserver ~]$
```

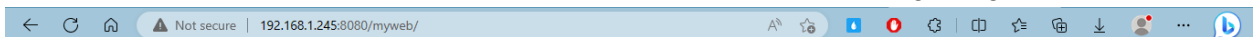
- Sao chép thư mục ~/myweb vào thư mục gốc của dịch vụ của web trên Docker container.

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



```
b2011967@myserver:~ — -bash
[b2011967@myserver ~]$ docker cp myweb/ webserver:/usr/local/apache2/htdocs/
Successfully copied 2.56kB to webserver:/usr/local/apache2/htdocs/
[b2011967@myserver ~]$
```

- 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 B987654321

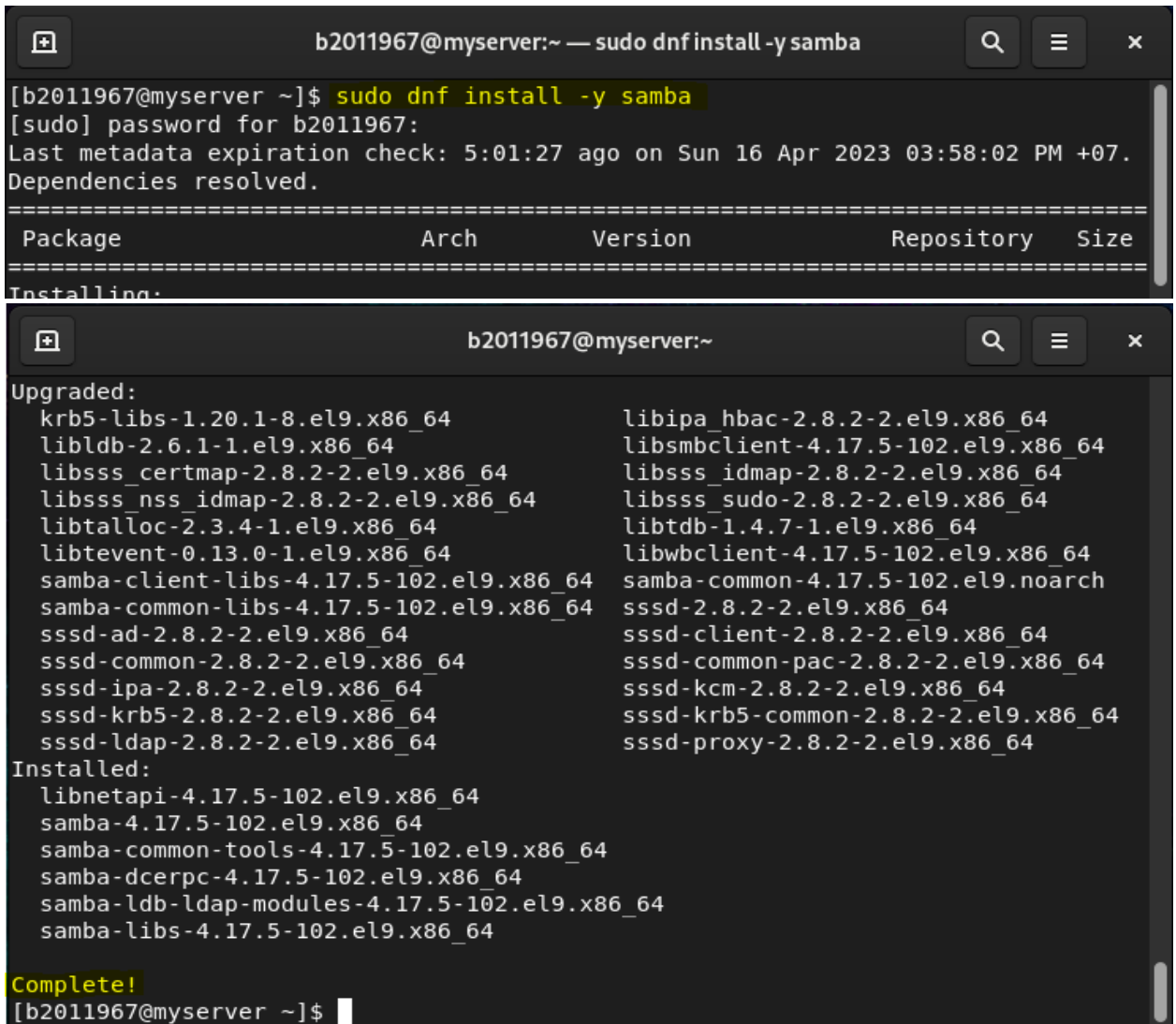
2. Cài đặt và cấu hình dịch vụ SAMBA

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
```



```
b2011967@myserver:~ — sudo dnf install -y samba
[b2011967@myserver ~]$ sudo dnf install -y samba
[sudo] password for b2011967:
Last metadata expiration check: 5:01:27 ago on Sun 16 Apr 2023 03:58:02 PM +07.
Dependencies resolved.
=====
Package                                Arch      Version                               Repository      Size
=====
Installing:
Upgraded:
krb5-libs-1.20.1-8.el9.x86_64          libipa_hbac-2.8.2-2.el9.x86_64
libldb-2.6.1-1.el9.x86_64              libsmbclient-4.17.5-102.el9.x86_64
libsss_certmap-2.8.2-2.el9.x86_64      libsss_idmap-2.8.2-2.el9.x86_64
libsss_nss_idmap-2.8.2-2.el9.x86_64    libsss_sudo-2.8.2-2.el9.x86_64
libtalloc-2.3.4-1.el9.x86_64           libtdb-1.4.7-1.el9.x86_64
libtevent-0.13.0-1.el9.x86_64          libwbclient-4.17.5-102.el9.x86_64
samba-client-libs-4.17.5-102.el9.x86_64 samba-common-4.17.5-102.el9.noarch
samba-common-libs-4.17.5-102.el9.x86_64 sssd-2.8.2-2.el9.x86_64
sssd-ad-2.8.2-2.el9.x86_64             sssd-client-2.8.2-2.el9.x86_64
sssd-common-2.8.2-2.el9.x86_64         sssd-common-pac-2.8.2-2.el9.x86_64
sssd-ipa-2.8.2-2.el9.x86_64            sssd-kcm-2.8.2-2.el9.x86_64
sssd-krb5-2.8.2-2.el9.x86_64           sssd-krb5-common-2.8.2-2.el9.x86_64
sssd-ldap-2.8.2-2.el9.x86_64           sssd-proxy-2.8.2-2.el9.x86_64
Installed:
libnetapi-4.17.5-102.el9.x86_64
samba-4.17.5-102.el9.x86_64
samba-common-tools-4.17.5-102.el9.x86_64
samba-dcerpc-4.17.5-102.el9.x86_64
samba-ldb-ldap-modules-4.17.5-102.el9.x86_64
samba-libs-4.17.5-102.el9.x86_64
Complete!
[b2011967@myserver ~]$
```

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

```
$sudo adduser tuanthai
$sudo passwd tuanthai
```

```
b2011967@myserver:~  
[b2011967@myserver ~]$ sudo adduser hoanghuy  
[sudo] password for b2011967:  
[b2011967@myserver ~]$ sudo passwd hoanghuy  
Changing password for user hoanghuy.  
New password:  
BAD PASSWORD: The password contains the user name in some form  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[b2011967@myserver ~]$
```

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

```
b2011967@myserver:~  
[b2011967@myserver ~]$ sudo groupadd lecturers  
[b2011967@myserver ~]$ sudo usermod -a -G lecturers hoanghuy  
[b2011967@myserver ~]$
```

- Tạo thư mục cần chia sẻ và phân quyền:

```
$sudo mkdir /data  
(Vì thư mục /data đã tạo rồi nên k cần tạo nữa)
```

```
b2011967@myserver:~  
[b2011967@myserver ~]$ sudo mkdir /data  
mkdir: cannot create directory '/data': File exists  
[b2011967@myserver ~]$ ls /  
afs boot dev home lib64 mnt proc root sbin sys usr  
bin data etc lib media opt report run srv tmp var  
[b2011967@myserver ~]$
```

```
$sudo chown :lecturers /data  
$sudo chmod -R 775 /data
```

```
b2011967@myserver:~  
[b2011967@myserver ~]$ sudo chown :lecturers /data  
[b2011967@myserver ~]$ sudo chmod -R 775 /data  
[b2011967@myserver ~]$
```

- Kiểm tra lại :

```
b2011967@myserver:~  
[b2011967@myserver ~]$ ls -l /  
total 24  
dr-xr-xr-x.  2 root root      6 Aug 10  2021 afs  
lrwxrwxrwx.  1 root root      7 Aug 10  2021 bin -> usr/bin  
dr-xr-xr-x.  5 root root    4096 Feb 14  09:07 boot  
drwxrwxr-x.  2 root lecturers 23 Mar  2  20:40 data  
drwxr-xr-x. 20 root root   3340 Apr 16  20:57 dev  
drwxr-xr-x.133 root root   8192 Apr 16  21:06 etc  
drwxr-xr-x.  8 root root    109 Apr 16  21:04 home  
lrwxrwxrwx.  1 root root      7 Aug 10  2021 lib -> usr/lib
```

- Cấu hình dịch vụ Samba:

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

```
b2011967@myserver:~  
[b2011967@myserver ~]$ sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.orig  
[b2011967@myserver ~]$
```

```
$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
```

```
b2011967@myserver:~ — sudo nano /etc/samba/smb.conf  
GNU nano 5.6.1 /etc/samba/smb.conf  
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

```
b2011967@myserver:~  
[b2011967@myserver ~]$ sudo smbpasswd -a hoanghuy  
New SMB password:  
Retype new SMB password:  
Added user hoanghuy.  
[b2011967@myserver ~]$
```

- Cấu hình SELINUX cho phép Samba

\$sudo setsebool -P samba_export_all_rw on

\$sudo setsebool -P samba_enable_home_dirs on

```
b2011967@myserver:~  
[b2011967@myserver ~]$ sudo setsebool -P samba_export_all_rw on  
[b2011967@myserver ~]$ sudo setsebool -P samba_enable_home_dirs on  
[b2011967@myserver ~]$
```

- Tắt tường lửa:

\$sudo systemctl stop firewalld

```
b2011967@myserver:~  
[b2011967@myserver ~]$ sudo systemctl stop firewalld  
[b2011967@myserver ~]$
```

(Kiểm tra trạng thái hoạt động của tường lửa đã tắt chưa)

```
b2011967@myserver:~ — sudo systemctl status firewalld  
[b2011967@myserver ~]$ sudo systemctl stop firewalld  
[b2011967@myserver ~]$ sudo systemctl status firewalld  
○ firewalld.service - firewalld - dynamic firewall daemon  
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor>  
   Active: inactive (dead) since Sun 2023-04-16 21:21:55 +07; 1min 2s ago  
   Duration: 25min 35.231s  
   Docs: man:firewalld(1)  
   Process: 824 ExecStart=/usr/sbin/firewalld --nofork --nopid $FIREWALLD_ARGS>  
   Main PID: 824 (code=exited, status=0/SUCCESS)  
   CPU: 2.784s
```

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

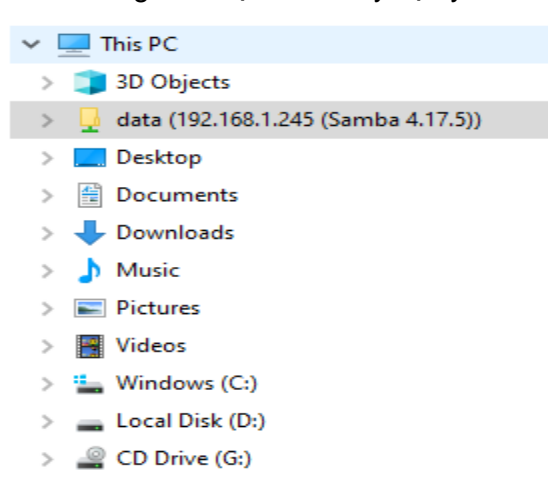
\$sudo systemctl start smb

\$sudo systemctl enable smb

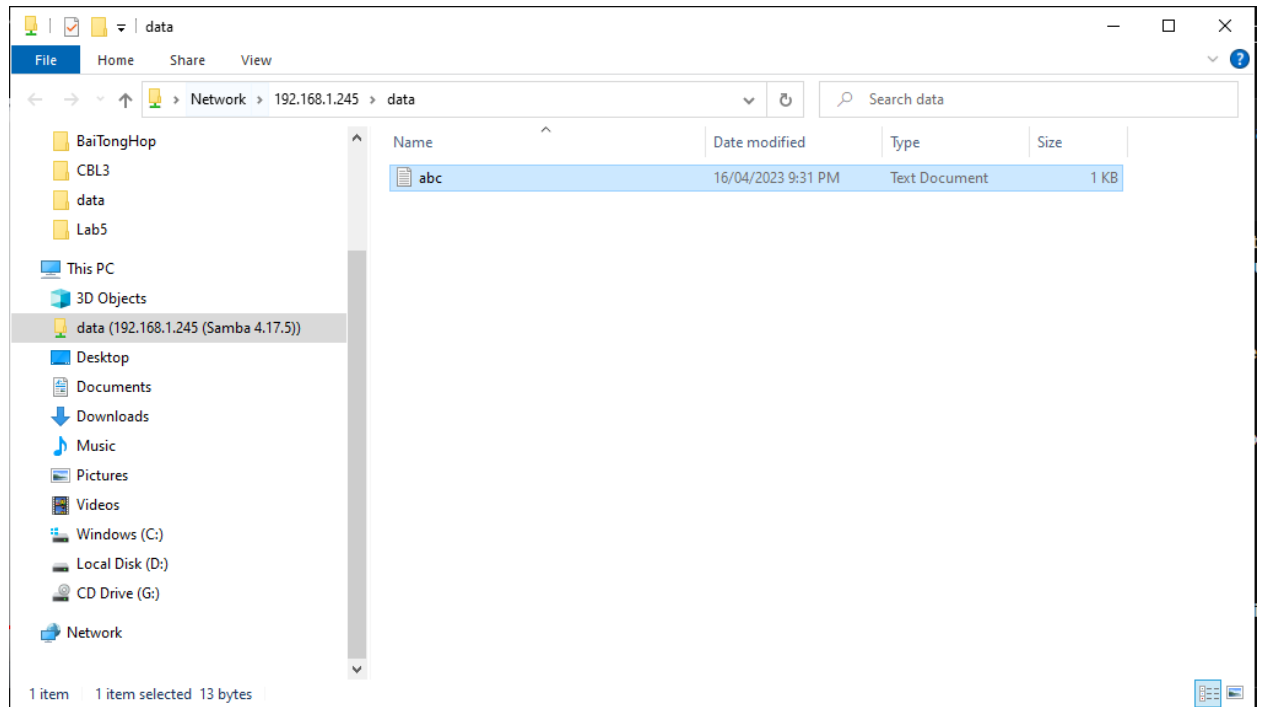
```
b2011967@myserver:~  
[b2011967@myserver ~]$ sudo systemctl start smb  
[b2011967@myserver ~]$ sudo systemctl enable smb  
Created symlink /etc/systemd/system/multi-user.target.wants/smb.service → /usr/lib/systemd/system/smb.service.  
[b2011967@myserver ~]$
```

- 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

(Tạo thành công thư mục trên máy vật lý kết nối samba)



(Tạo 1 file abc.txt với nội dung là Hello Samba)



(Kiểm tra lại tên máy ảo và đã thành công)



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 ?

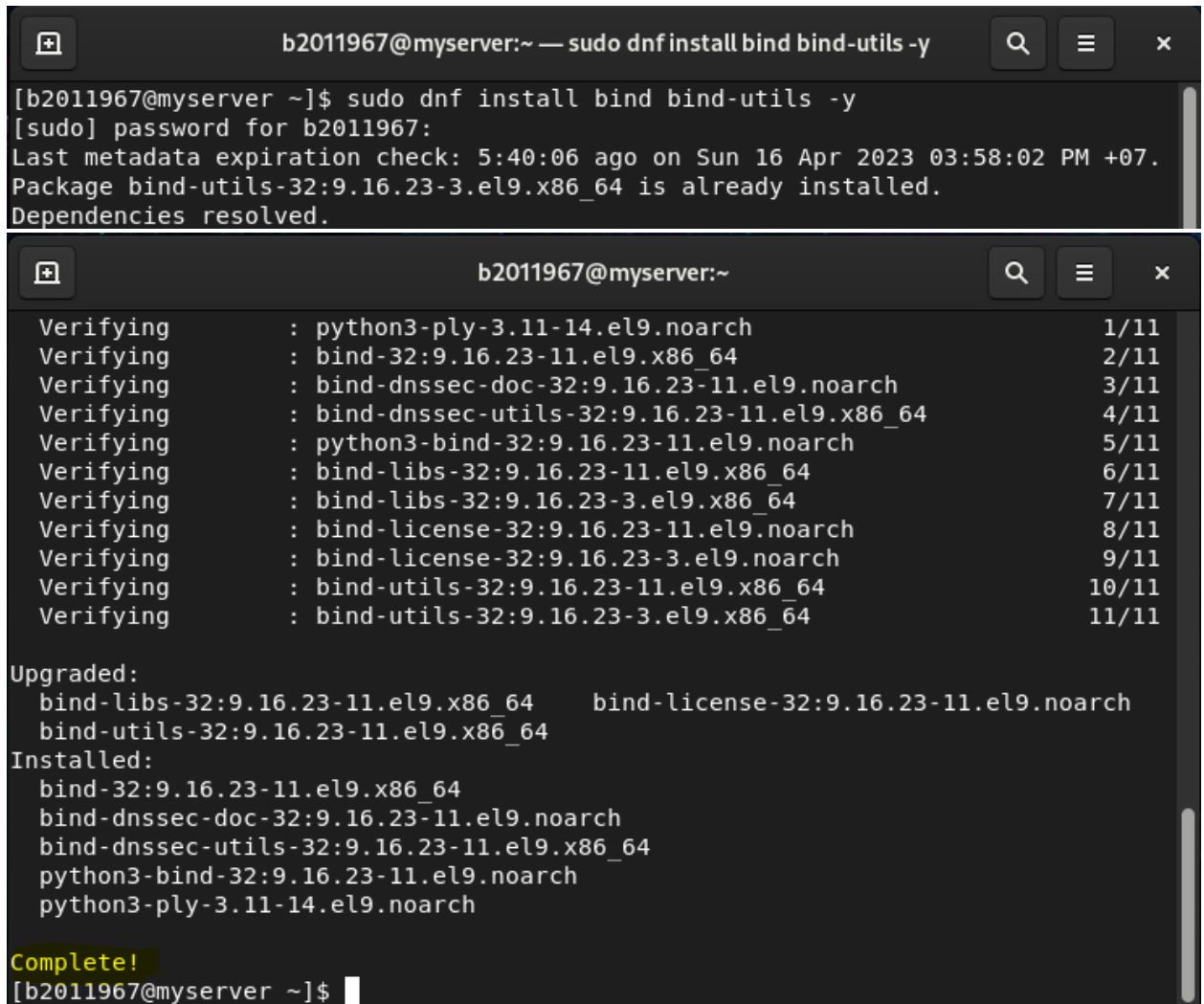
<http://123.30.143.202> hay <http://www.cit.ctu.edu.vn>

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
```



```
b2011967@myserver:~ — sudo dnf install bind bind-utils -y
[b2011967@myserver ~]$ sudo dnf install bind bind-utils -y
[sudo] password for b2011967:
Last metadata expiration check: 5:40:06 ago on Sun 16 Apr 2023 03:58:02 PM +07.
Package bind-utils-32:9.16.23-3.el9.x86_64 is already installed.
Dependencies resolved.

Verifying      : python3-ply-3.11-14.el9.noarch                1/11
Verifying      : bind-32:9.16.23-11.el9.x86_64                2/11
Verifying      : bind-dnssec-doc-32:9.16.23-11.el9.noarch      3/11
Verifying      : bind-dnssec-utils-32:9.16.23-11.el9.x86_64   4/11
Verifying      : python3-bind-32:9.16.23-11.el9.noarch         5/11
Verifying      : bind-libs-32:9.16.23-11.el9.x86_64            6/11
Verifying      : bind-libs-32:9.16.23-3.el9.x86_64             7/11
Verifying      : bind-license-32:9.16.23-11.el9.noarch         8/11
Verifying      : bind-license-32:9.16.23-3.el9.noarch          9/11
Verifying      : bind-utils-32:9.16.23-11.el9.x86_64          10/11
Verifying      : bind-utils-32:9.16.23-3.el9.x86_64           11/11

Upgraded:
  bind-libs-32:9.16.23-11.el9.x86_64    bind-license-32:9.16.23-11.el9.noarch
  bind-utils-32:9.16.23-11.el9.x86_64

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

Complete!
[b2011967@myserver ~]$
```

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; };
};
...

```

```

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; };
}

```

```
*/
recursion yes;
forwarders {123.23.23.23; };

dnssec-validation yes;

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

zone "23.23.123.in-addr.arpa" IN {
    type master;
    file "reverse.qtht";
    allow-update { none; };
};
include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

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
```

#(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
```

```
b2011967@myserver:~
[b2011967@myserver ~]$ sudo cp /var/named/named.localhost /var/named/forward.qth
t
[b2011967@myserver ~]$ sudo chgrp named /var/named/forward.qtht
[b2011967@myserver ~]$ sudo nano /var/named/forward.qtht
[b2011967@myserver ~]$
```

```

b2011967@myserver:~ — 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       123.23.23.23
www    IN     A       123.23.23.23
htqtl  IN     A       8.8.8.8

```

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

```

```

$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.

```

```

b2011967@myserver:~
[b2011967@myserver ~]$ sudo cp /var/named/forward.qtht /var/named/reverse.qtht
[sudo] password for b2011967:
[b2011967@myserver ~]$ sudo chgrp named /var/named/reverse.qtht
[b2011967@myserver ~]$ sudo nano /var/named/reverse.qtht
[b2011967@myserver ~]$

```

```
b2011967@myserver:~ — 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       123.23.23.23
23     IN     PTR     www.qtht.com.vn.
```

3.5. Kiểm tra và sử dụng dịch vụ DNS

- Tắt tường lửa:

```
$sudo systemctl stop firewalld
```

(Tắt tường lửa và kiểm tra trạng thái hoạt động)

```
b2011967@myserver:~ — sudo systemctl status firewalld
[b2011967@myserver ~]$ sudo systemctl stop firewalld
[b2011967@myserver ~]$ sudo systemctl status firewalld
○ firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor
   Active: inactive (dead) since Sun 2023-04-16 21:21:55 +07; 43min ago
   Duration: 25min 35.231s
   Docs: man:firewalld(1)
   Main PID: 824 (code=exited, status=0/SUCCESS)
   CPU: 2.784s
```

- Khởi động dịch vụ DNS:

```
$sudo systemctl start named
```

```
b2011967@myserver:~
[b2011967@myserver ~]$ sudo systemctl start named
[b2011967@myserver ~]$
```

```
$sudo systemctl enable named
```

```
b2011967@myserver:~
[b2011967@myserver ~]$ sudo systemctl enable named
[b2011967@myserver ~]$
```

- Kiểm tra kết quả:

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

```
b2011967@myserver:~  
[b2011967@myserver ~]$ nslookup www.qtht.com.vn 192.168.1.245  
Server:          192.168.1.245  
Address:         192.168.1.245#53  
  
Name:   www.qtht.com.vn  
Address: 123.23.23.23  
  
[b2011967@myserver ~]$
```

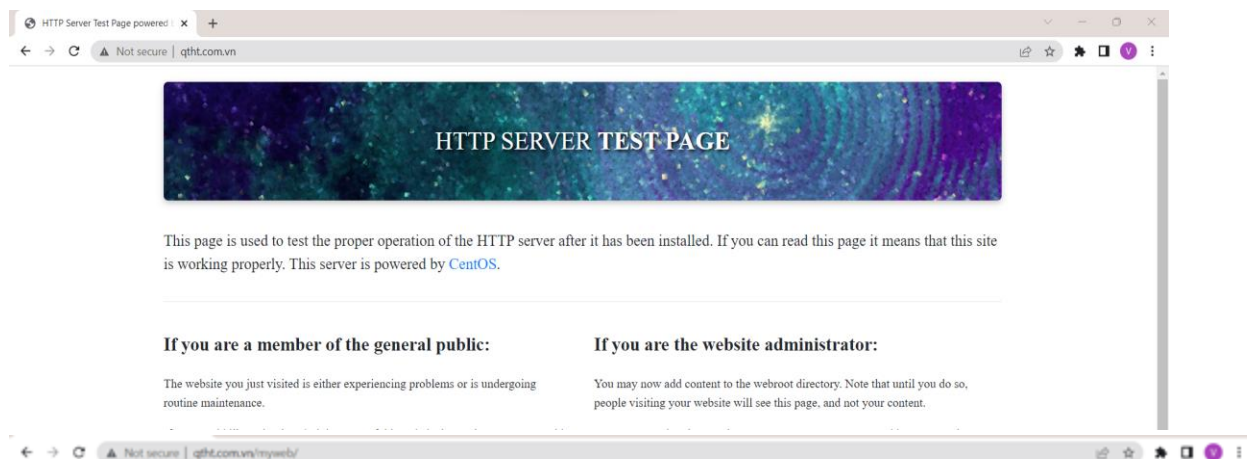
nslookup htql.qtht.com.vn <địa chỉ IP máy ảo>

```
b2011967@myserver:~  
[b2011967@myserver ~]$ nslookup htql.qtht.com.vn 192.168.1.245  
Server:          192.168.1.245  
Address:         192.168.1.245#53  
  
Name:   htql.qtht.com.vn  
Address: 8.8.8.8  
  
[b2011967@myserver ~]$
```

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

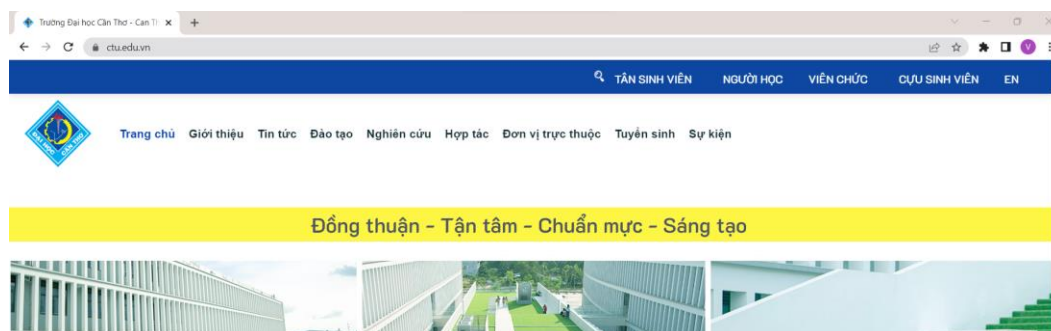
```
b2011967@myserver:~  
[b2011967@myserver ~]$ nslookup www.ctu.edu.vn 192.168.1.245  
Server:          192.168.1.245  
Address:         192.168.1.245#53  
  
Non-authoritative answer:  
Name:   www.ctu.edu.vn  
Address: 123.30.143.225  
  
[b2011967@myserver ~]$
```

- 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>



Welcome!

Designed by b2011967



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

```
b2011967@localhost:~ — sudo systemctl status firewalld

[b2011967@myserver ~]$ sudo systemctl start firewalld
[sudo] password for b2011967:
[b2011967@myserver ~]$ sudo systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2023-04-22 15:39:58 +07; 22s ago
     Docs: man:firewalld(1)
   Main PID: 41385 (firewalld)
    Tasks: 2 (limit: 10946)
   Memory: 28.1M
      CPU: 1.155s
   CGroup: /system.slice/firewalld.service
           └─41385 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid

Apr 22 15:39:57 myserver systemd[1]: Starting firewalld - dynamic firewall daemon:
Apr 22 15:39:58 myserver systemd[1]: Started firewalld - dynamic firewall daemon:
lines 1-13/13 (END)
```

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

\$firewall-cmd --get-zones

```
b2011967@localhost:~

[b2011967@myserver ~]$ firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
[b2011967@myserver ~]$
```

- Kiểm tra zone mặc định

\$firewall-cmd --get-default-zone

```
b2011967@localhost:~

[b2011967@myserver ~]$ firewall-cmd --get-default-zone
public
[b2011967@myserver ~]$
```

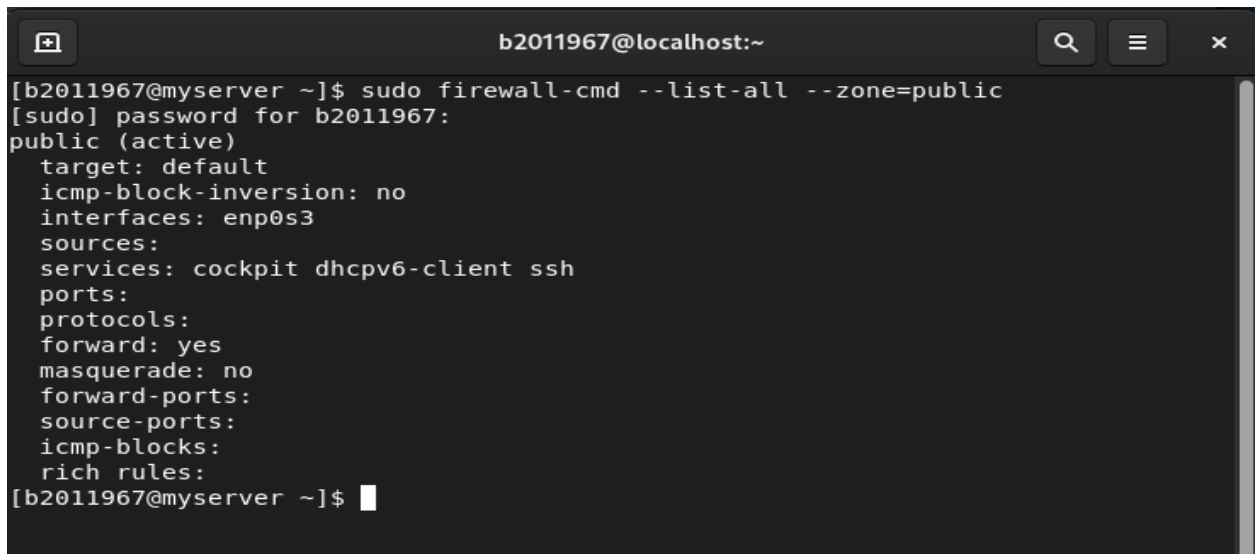
- Kiểm tra zone đang được sử dụng bởi giao diện mạng (thường là *public*); và xem các rules của zone

\$firewall-cmd --get-active-zones

```
b2011967@localhost:~

[b2011967@myserver ~]$ firewall-cmd --get-active-zones
public
   interfaces: enp0s3
[b2011967@myserver ~]$
```

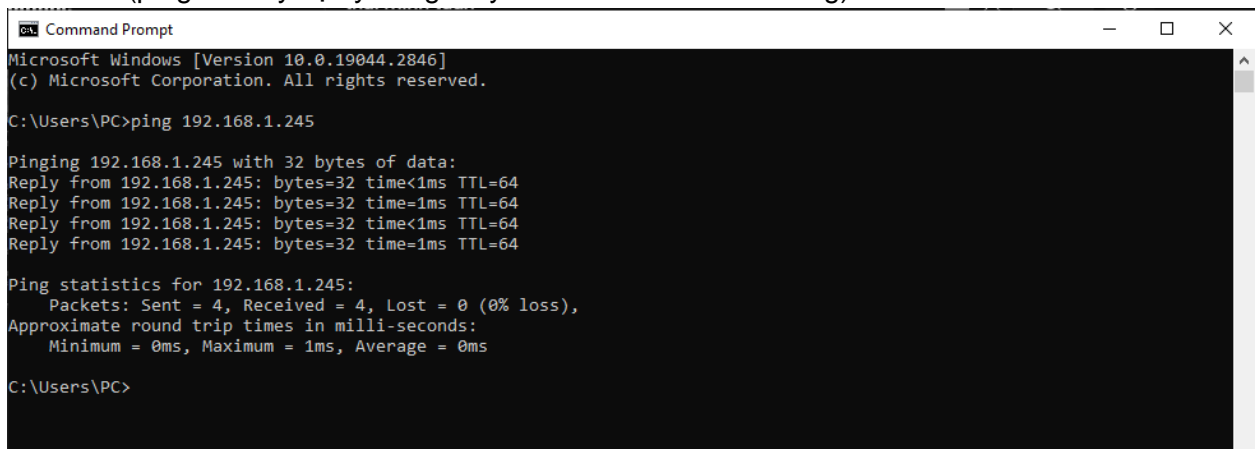
```
$sudo firewall-cmd --list-all --zone=public
```

A terminal window titled 'b2011967@localhost:~' showing the output of the command 'sudo firewall-cmd --list-all --zone=public'. The output lists various firewall settings for the 'public' zone, including target, icmp-block-inversion, interfaces, sources, services, ports, protocols, forward, masquerade, forward-ports, source-ports, icmp-blocks, and rich rules.

```
[b2011967@myserver ~]$ sudo firewall-cmd --list-all --zone=public
[sudo] password for b2011967:
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:
```

- 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 centos -> Thành công)

A Windows Command Prompt window titled 'Command Prompt' showing the results of a ping command to 192.168.1.245. The output shows four successful replies with 0% loss and round trip times of less than 1ms.

```
Microsoft Windows [Version 10.0.19044.2846]
(c) Microsoft Corporation. All rights reserved.

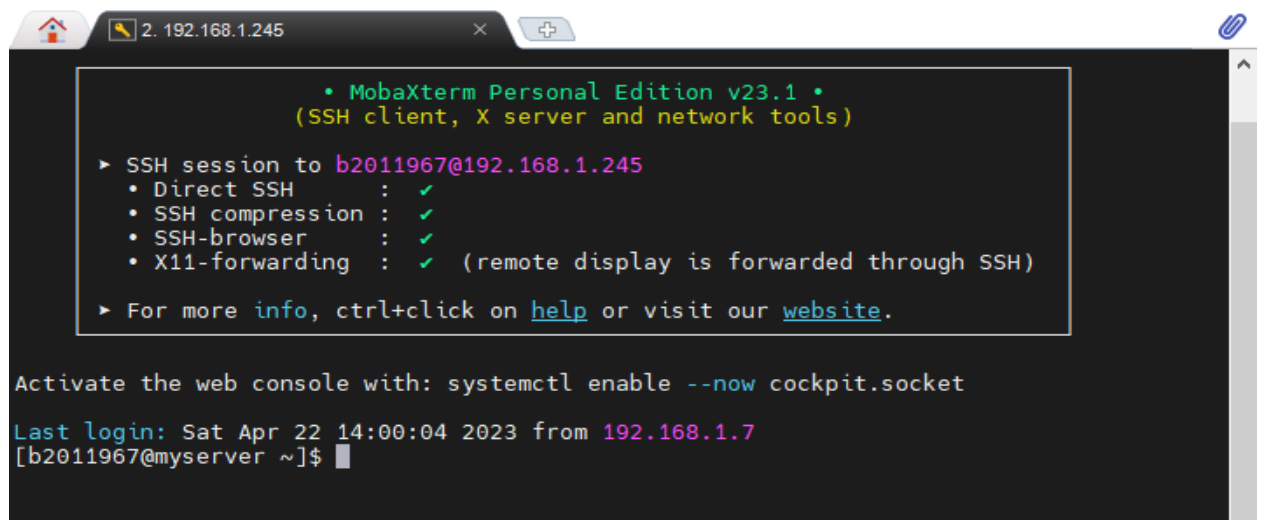
C:\Users\PC>ping 192.168.1.245

Pinging 192.168.1.245 with 32 bytes of data:
Reply from 192.168.1.245: bytes=32 time<1ms TTL=64
Reply from 192.168.1.245: bytes=32 time=1ms TTL=64
Reply from 192.168.1.245: bytes=32 time<1ms TTL=64
Reply from 192.168.1.245: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.245:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\PC>
```

(Kết nối dịch vụ ssh -> Thành công)



```
• MobaXterm Personal Edition v23.1 •
(SSH client, X server and network tools)

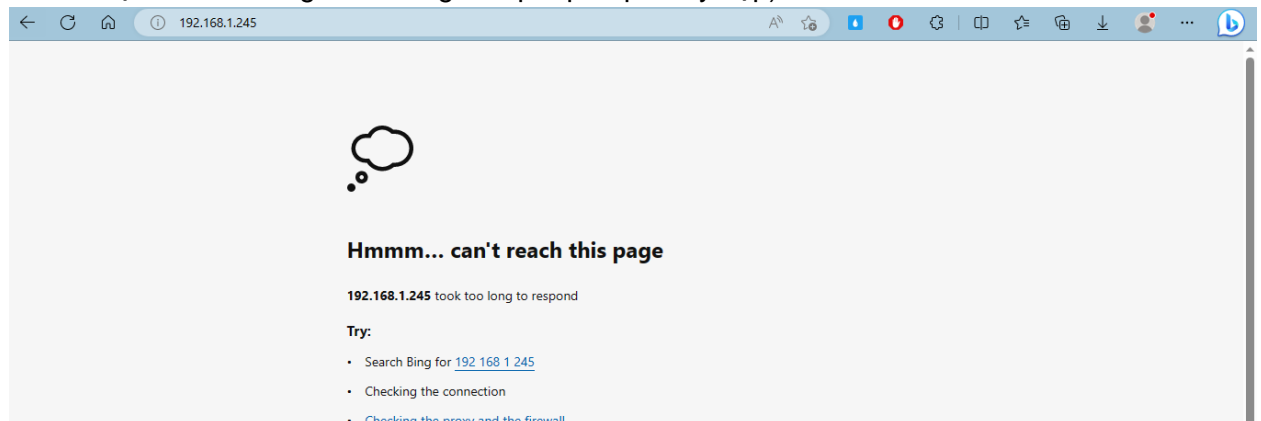
▶ SSH session to b2011967@192.168.1.245
  • Direct SSH      : ✓
  • SSH compression : ✓
  • SSH-browser     : ✓
  • X11-forwarding  : ✓ (remote display is forwarded through SSH)

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

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

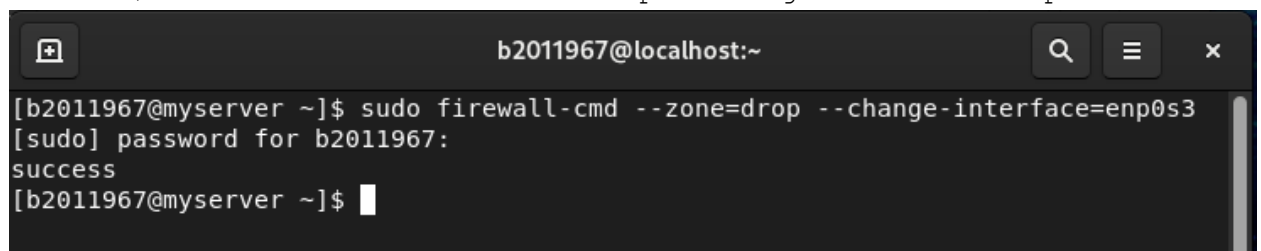
Last login: Sat Apr 22 14:00:04 2023 from 192.168.1.7
[b2011967@myserver ~]$
```

(Truy cập dịch vụ web -> Dịch vụ web chưa thể truy cập được vì lúc này tường lửa đã bật lên và tường lửa không cho phép httpd truy cập).



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

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



```
b2011967@localhost:~
[b2011967@myserver ~]$ sudo firewall-cmd --zone=drop --change-interface=enp0s3
[sudo] password for b2011967:
success
[b2011967@myserver ~]$
```

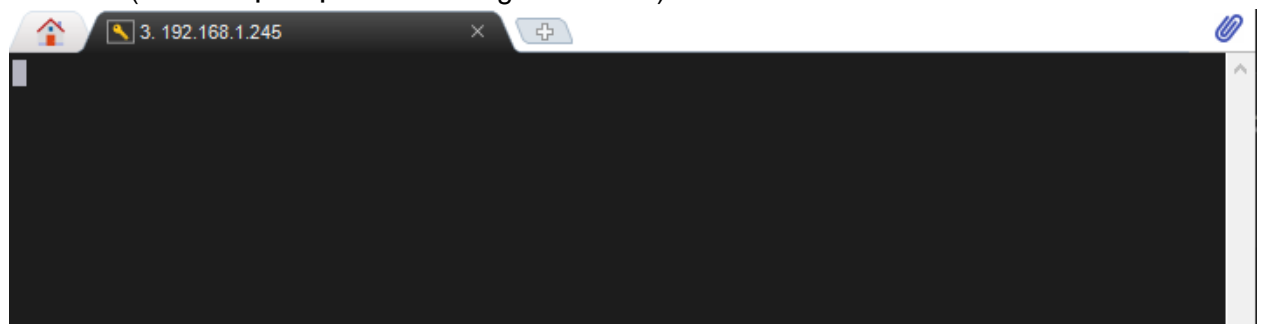
```
$sudo firewall-cmd --list-all --zone=drop
```

```
b2011967@localhost:~  
[b2011967@myserver ~]$ sudo firewall-cmd --list-all --zone=drop  
drop (active)  
target: DROP  
icmp-block-inversion: no  
interfaces: enp0s3  
sources:  
services:  
ports:  
protocols:  
forward: yes  
masquerade: no  
forward-ports:  
source-ports:  
icmp-blocks:  
rich rules:  
[b2011967@myserver ~]$
```

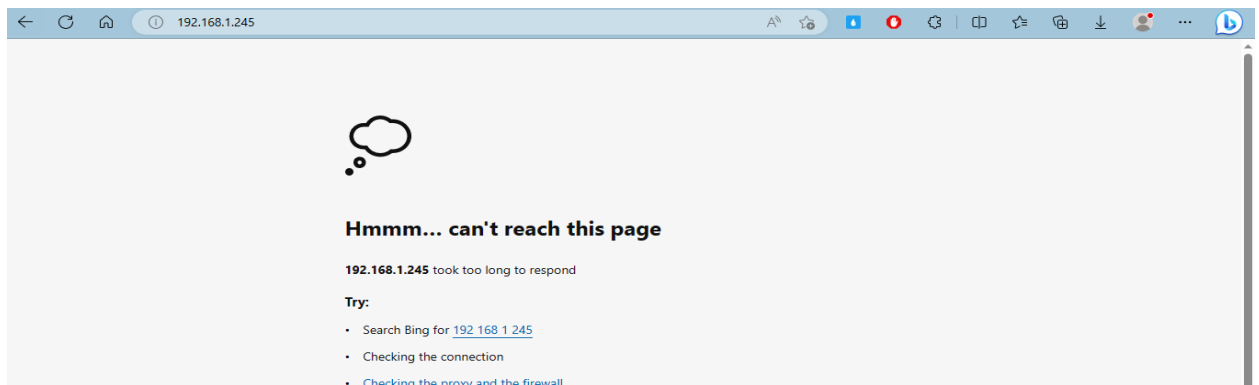
- Từ máy vật lý, ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS. Cho biết kết quả.
(ping từ máy vật lý sang máy ảo centos -> Không có phản hồi)

```
Command Prompt  
C:\Users\PC>ping 192.168.1.245  
  
Pinging 192.168.1.245 with 32 bytes of data:  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
  
Ping statistics for 192.168.1.245:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
  
C:\Users\PC>
```

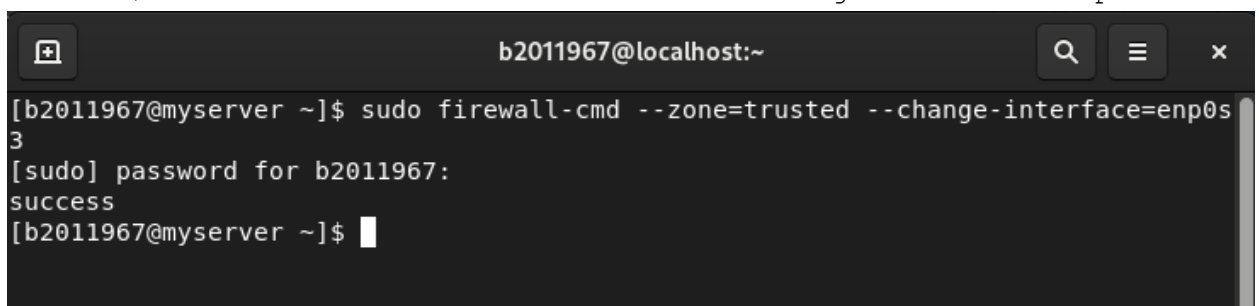
(Kết nối dịch vụ ssh -> Không thể nối kết)



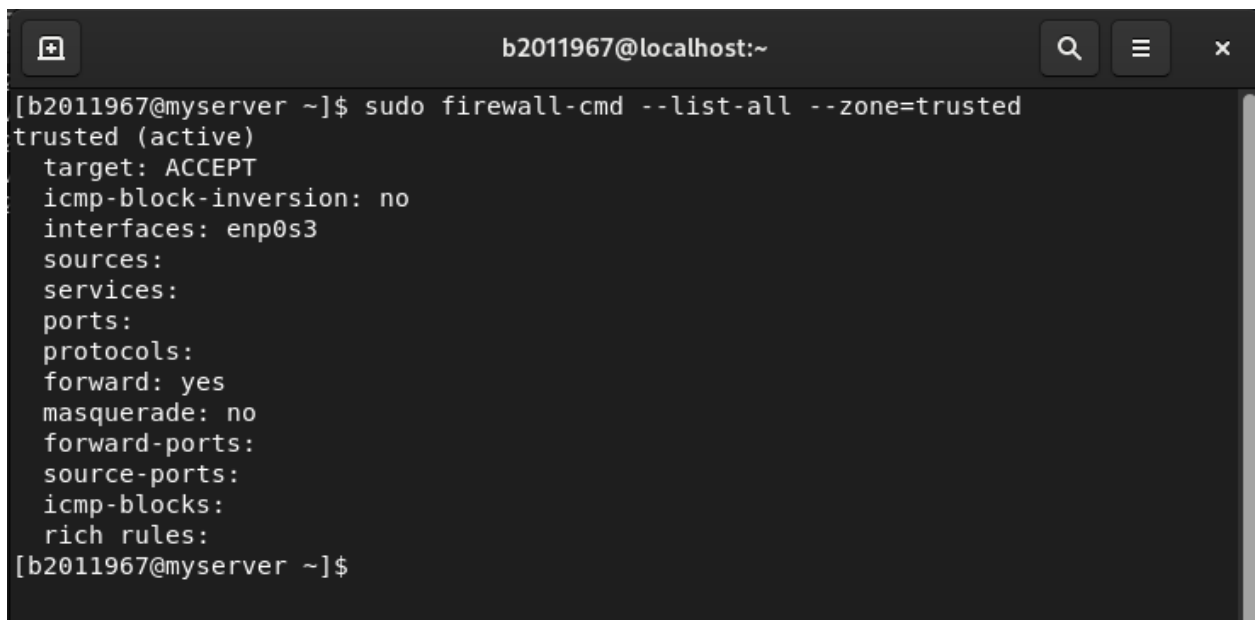
(Kết nối dịch vụ web -> Vẫn không nối kết được)



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



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



- 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 -> Thành công)

```
Command Prompt
C:\Users\PC>ping 192.168.1.245

Pinging 192.168.1.245 with 32 bytes of data:
Reply from 192.168.1.245: bytes=32 time<1ms TTL=64
Reply from 192.168.1.245: bytes=32 time=1ms TTL=64
Reply from 192.168.1.245: bytes=32 time=1ms TTL=64
Reply from 192.168.1.245: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.245:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\PC>
```

(Kết nối dịch vụ ssh -> Kết nối thành công)

```
4. 192.168.1.245
• MobaXterm Personal Edition v23.1 •
  (SSH client, X server and network tools)

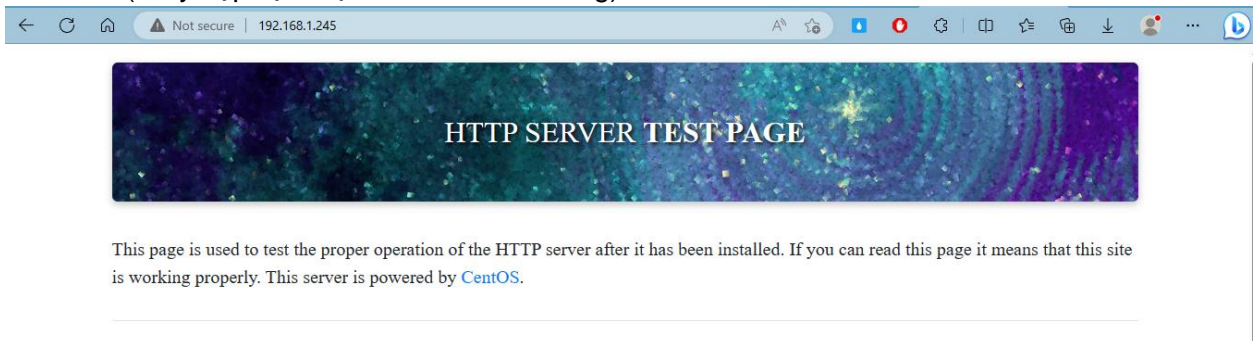
► SSH session to b2011967@192.168.1.245
  • Direct SSH      : ✓
  • SSH compression : ✓
  • SSH-browser     : ✓
  • X11-forwarding  : ✓ (remote display is forwarded through SSH)

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

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

Last login: Sat Apr 22 15:52:50 2023 from 192.168.1.7
[b2011967@myserver ~]$
```

(Truy cập dịch vụ web -> Thành công)

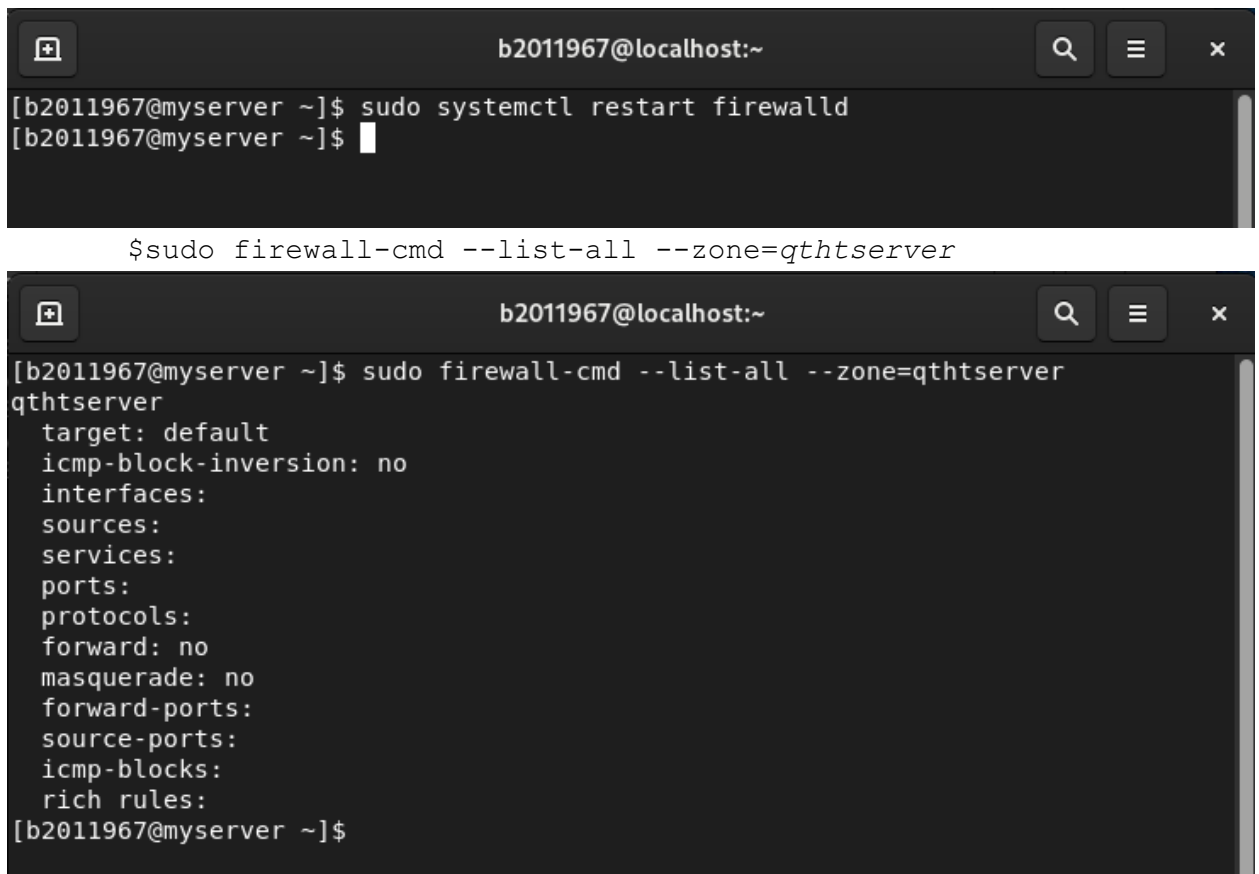


- Tạo zone mới có tên là *qthtserver*

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

```
b2011967@localhost:~
[b2011967@myserver ~]$ sudo firewall-cmd --permanent --new-zone=qthtserver
success
[b2011967@myserver ~]$
```

```
$sudo systemctl restart firewalld
```



The image contains two terminal window screenshots. The top window shows a user running `sudo systemctl restart firewalld` and then `$sudo firewall-cmd --list-all --zone=qthtserver`. The bottom window shows the output of the second command, displaying the current firewall configuration for the `qthtserver` zone.

```
b2011967@localhost:~  
[b2011967@myserver ~]$ sudo systemctl restart firewalld  
[b2011967@myserver ~]$  
  
$sudo firewall-cmd --list-all --zone=qthtserver  
  
b2011967@localhost:~  
[b2011967@myserver ~]$ 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:  
[b2011967@myserver ~]$
```

- 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`


```
b2011967@localhost:~  
[b2011967@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=http  
Warning: ALREADY_ENABLED: http  
success  
[b2011967@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=dns  
Warning: ALREADY_ENABLED: dns  
success  
[b2011967@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=samba  
Warning: ALREADY_ENABLED: samba  
success  
[b2011967@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=ftp  
Warning: ALREADY_ENABLED: ftp  
success  
[b2011967@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-port=9999/tcp  
success  
[b2011967@myserver ~]$
```

- 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'

```
b2011967@localhost:~  
[b2011967@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-rich-rule='rule family=ipv4 source address=192.168.1.7/32 port port=22 protocol=tcp accept'  
success  
[b2011967@myserver ~]$
```

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

```
b2011967@localhost:~  
[b2011967@myserver ~]$ sudo systemctl restart firewalld  
[b2011967@myserver ~]$
```

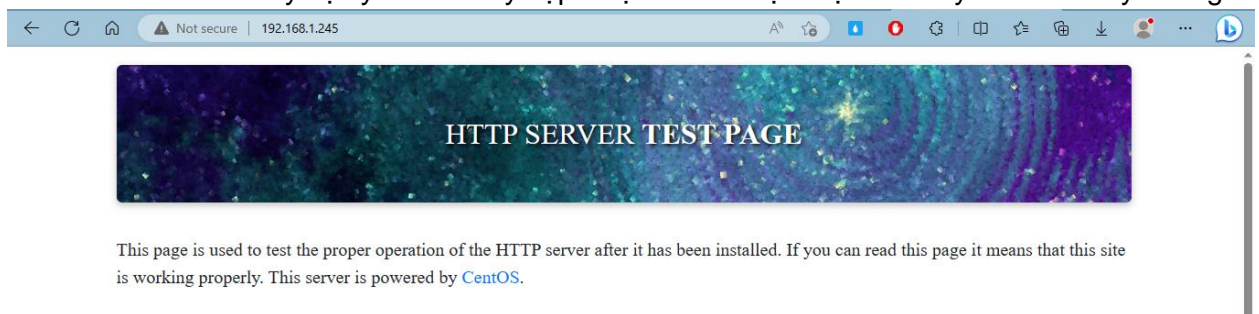
- Chuyển giao diện mạng sang zone qthtserver; và xem các rules của zone
\$sudo firewall-cmd --permanent --zone=qthtserver --change-interface=enp0s3

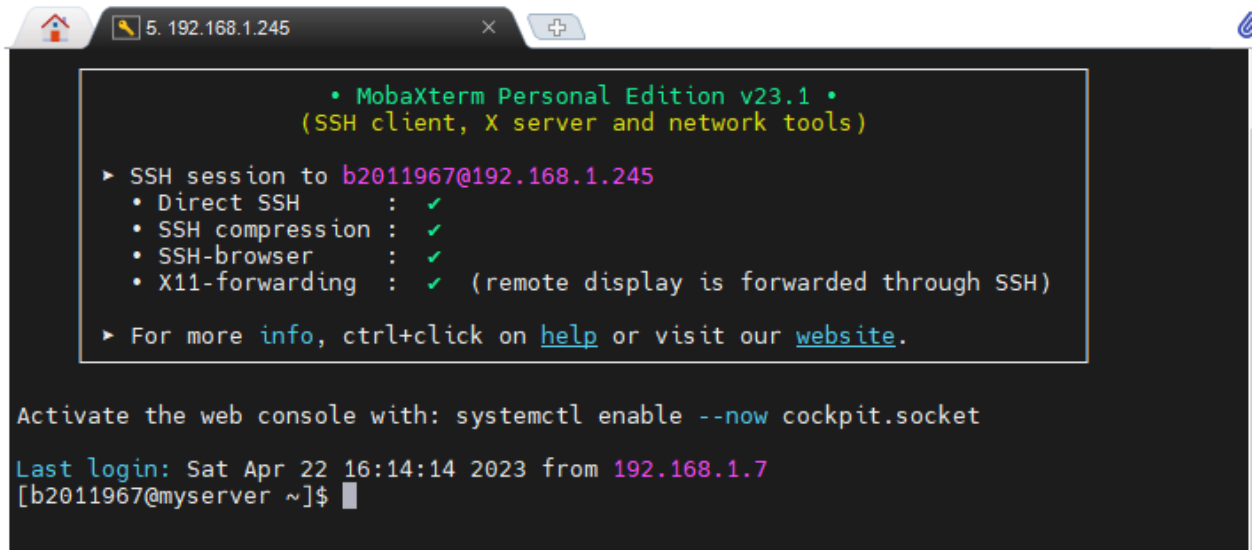
```
b2011967@localhost:~  
[b2011967@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --change-interface=enp0s3  
The interface is under control of NetworkManager, setting zone to 'qthtserver'.  
success  
[b2011967@myserver ~]$
```

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

```
b2011967@localhost:~  
[b2011967@myserver ~]$ sudo firewall-cmd --list-all --zone=qthtserver  
qthtserver (active)  
  target: default  
  icmp-block-inversion: no  
  interfaces: enp0s3  
  sources:  
  services: dns ftp http samba  
  ports: 9999/tcp  
  protocols:  
  forward: no  
  masquerade: no  
  forward-ports:  
  source-ports:  
  icmp-blocks:  
  rich rules:  
    rule family="ipv4" source address="192.168.1.7/32" port port="22" protocol="tcp" accept  
[b2011967@myserver ~]$
```

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





```
• MobaXterm Personal Edition v23.1 •  
(SSH client, X server and network tools)  
  
► SSH session to b2011967@192.168.1.245  
• 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 Apr 22 16:14:14 2023 from 192.168.1.7  
[b2011967@myserver ~]$
```

--- Hết ---