LAB 5

DOCKER, SAMBA, DNS và Firewall

Họ tên và MSSV: Lê Trương Ngọc Duyên - B2105569

Nhóm học phần: CT179-06

- *Các sinh viên bị phát hiện sao chép bài của nhau sẽ nhận 0đ cho tất cả bài thực hành của môn này.*
- *Bài nộp phải ở dạng PDF, hình minh họa phải rõ ràng chi tiết.* Hình minh hoạ chỉ cần chụp ở nội dung thực hiện, không chụp toàn màn hình.
- *Video hướng dẫn ở cuối bài.*

1. Triển khai dịch vụ WEB sử dụng Docker

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

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

```
[B2105569@myserver ~]$ nmcli -f ipv4.dns,ipv4.addresses,ipv4.gateway con show enp0s3
ipv4.dns:                               203.113.131.2,203.113.188.8
ipv4.addresses:                         192.168.1.250/24
ipv4.gateway:                           192.168.1.1
```

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

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

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

```
[B2105569@localhost ~]$ ping -c 3 google.com
PING google.com(hkg07s01-in-x0e.1e100.net (2404:6800:4005:80a::200e)) 56 data b
ytes
64 bytes from hkg07s48-in-x0e.1e100.net (2404:6800:4005:80a::200e): icmp_seq=1
ttl=58 time=41.1 ms
64 bytes from hkg07s48-in-x0e.1e100.net (2404:6800:4005:80a::200e): icmp_seq=2
ttl=58 time=43.1 ms
64 bytes from hkg07s34-in-x0e.1e100.net (2404:6800:4005:80a::200e): icmp_seq=3
ttl=58 time=38.0 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 38.048/40.755/43.134/2.089 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)

Tắt tường lửa:

```
$sudo systemctl stop firewalld
```

```
[B2105569@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>
```

```
[B2105569@myserver ~]$ sudo systemctl stop firewalld
[sudo] password for B2105569:
[B2105569@myserver ~]$ sudo systemctl status firewalld
○ firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled;
 preset: ena>
     Active: inactive (dead) since Sun 2023-11-05 18:22:14 +07; 13s ago
   Duration: 22min 6.498s
```

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
```

```
Removed:
  cockpit-podman-75-1.el9.noarch  conmon-2:2.1.8-1.el9.x86_64
  podman-2:4.6.1-5.el9.x86_64     shadow-utils-subid-2:4.9-8.el9.x86_64

Complete!
[B2105569@myserver ~]$
```

- Cài đặt công cụ yum-utils

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

```
Installed:
  yum-utils-4.3.0-11.el9.noarch

Complete!
[B2105569@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.
```

```
[B2105569@myserver ~]$ sudo yum-config-manager --add-repo https://download.docker.com
/linux/centos/docker-ce.repo
[sudo] password for B2105569:
Adding repo from: https://download.docker.com/linux/centos/docker-ce.repo
```

- Cài đặt Docker

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

```
Installed:
  containerd.io-1.6.24-3.1.el9.x86_64
  docker-buildx-plugin-0.11.2-1.el9.x86_64
  docker-ce-3:24.0.7-1.el9.x86_64
  docker-ce-cli-1:24.0.7-1.el9.x86_64
  docker-ce-rootless-extras-24.0.7-1.el9.x86_64
  docker-compose-plugin-2.21.0-1.el9.x86_64

Complete!
[B2105569@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
```

```
[B2105569@myserver ~]$ sudo usermod -aG docker $USER
```

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

```
$su - $USER
```

```
[B2105569@myserver ~]$ su - $USER
```

- Chạy dịch vụ Docker

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

```
[B2105569@myserver ~]$ sudo systemctl start docker
[B2105569@myserver ~]$ sudo systemctl enable docker
Created symlink /etc/systemd/system/multi-user.target.wants/docker.service → /usr/lib
/systemd/system/docker.service.
[B2105569@myserver ~]$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
     Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; preset: disabl>
     Active: active (running) since Sun 2023-11-05 19:33:14 +07; 23s ago
```

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

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

```
[B2105569@myserver ~]$ docker login -u ltnduyen
Password:
WARNING! Your password will be stored unencrypted in /home/B2105569/.docker/config.js
on.
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`

```
[B2105569@myserver ~]$ docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
719385e32844: Pull complete

Digest: sha256:88ec0acaa3ec199d3b7eaf73588f4518c25f9d34f58ce9a0df68429c5af48e8d
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/
```

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
```

Hiện nay, có rất nhiều image có tên httpd → Sẽ tải image httpd mặc nhiên được cung cấp bởi hệ điều hành CentOS:

```
[B2105569@myserver ~]$ docker search httpd
NAME                              DESCRIPTION                                     STARS
AUTOMATED
httpd                             The Apache HTTP Server Project                  4582
clearlinux/httpd                  httpd HyperText Transfer Protocol (HTTP) ser…   5
paketobuildpacks/httpd                                                            0
vulhub/httpd                                                                      0
jitesoft/httpd                    Apache httpd on Alpine linux.                   0
openquantumsafe/httpd             Demo of post-quantum cryptography in Apache …   2
wodby/httpd                                                                       0
avenga/httpd-static                                                               0
dockette/httpdump                                                                 0
betterweb/httpd                                                                   0
dockette/apache                   Apache / HTTPD                                  1
[OK]
centos/httpd-24-centos7           Platform for running Apache httpd 2.4 or bui…   46
manageiq/httpd                    Container with httpd, built on CentOS for Ma…   1
[OK]
centos/httpd-24-centos8                                                           3
dockerpinata/httpd                                                                1
19022021/httpd-connection_test    This httpd image will test the connectivity …   0
publici/httpd                     httpd:latest                                    1
[OK]
centos/httpd                                                                      36
[OK]
```

- Tạo container từ image httpd

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

  `-d`: chạy container ở chế độ background

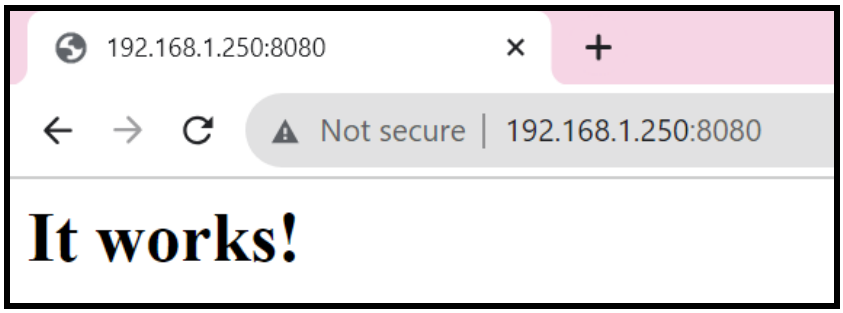
  `-it`: tạo shell để tương tác với container

  `--name webserver`: đặt tên container là webserver

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

```
[B2105569@myserver ~]$ docker run -d -it -p 8080:80 --name webserver httpd
Unable to find image 'httpd:latest' locally
latest: Pulling from library/httpd
578acb154839: Pull complete

c1a8c8567b78: Pull complete

10b9ab03bf45: Pull complete

74dbedf7ddc0: Pull complete

6a3b76b70f73: Pull complete

Digest: sha256:4e24356b4b0aa7a961e7dfb9e1e5025ca3874c532fa5d999f13f8fc33c09d1b7
Status: Downloaded newer image for httpd:latest
367b8257bc3794b8d466f572b45046c95abff7966dbb57d4186e2ba300664318
```

⇒ Kiểm tra bằng cách truy cập đến cổng 8080 của máy ảo CentOS:



- 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/`

```
[B2105569@myserver ~]$ docker cp myweb/ webserver:/usr/local/apache2/htdocs/
Successfully copied 2.56kB to 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.

- Lệnh $`docker container ls -a` dùng để xem lại danh sách các container có ở trên máy
- Lệnh `$docker container stop <tên container>` dùng để dừng một container.
- Lệnh `$docker container start <tên container>` dùng để chạy lại một container.

```
[B2105569@myserver ~]$ docker container ls -a
CONTAINER ID   IMAGE         COMMAND              CREATED          STATUS
PORTS                                   NAMES
367b8257bc37   httpd         "httpd-foreground"   9 minutes ago    Up 9 minutes
0.0.0.0:8080->80/tcp, :::8080->80/tcp   webserver
f879f8e6853f   hello-world   "/hello"             19 minutes ago   Exited (0) 19 minutes ago
                                        dreamy_poincare
[B2105569@myserver ~]$ docker container stop webserver
webserver
[B2105569@myserver ~]$ docker container start webserver
webserver
```

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
```

```
Installed:
  libnetapi-4.18.6-100.el9.x86_64                    samba-4.18.6-100.el9.x86_64
  samba-common-tools-4.18.6-100.el9.x86_64           samba-dcerpc-4.18.6-100.el9.x86_64
  samba-ldb-ldap-modules-4.18.6-100.el9.x86_64       samba-libs-4.18.6-100.el9.x86_64

Complete!
```

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

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

```
[B2105569@myserver ~]$ sudo adduser tuanthai
[sudo] password for B2105569:
[B2105569@myserver ~]$ sudo passwd tuanthai
Changing password for user tuanthai.
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: all authentication tokens updated successfully.
[B2105569@myserver ~]$ sudo groupadd lectures
[B2105569@myserver ~]$ sudo usermod -aG lectures tuanthai
```

- Tạo thư mục cần chia sẻ và phân quyền:

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

Do thư mục `data` đã được tạo ở Lab2, nên em sẽ tạo thư mục `data1`

```
[B2105569@myserver ~]$ sudo mkdir /data1
[B2105569@myserver ~]$ sudo chown :lectures /data1
[B2105569@myserver ~]$ sudo chmod -R 775 /data1
[B2105569@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 Sep  6 10:09 boot
drwxr-x---.   2 root nhanvien   23 Sep 21 20:22 data
drwxrwxr-x.   2 root lectures    6 Nov  5 20:47 data1
drwxr-xr-x.  20 root root     3380 Nov  5 18:00 dev
```

- Cấu hình dịch vụ Samba:

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

[data1]
        comment = Shared folder for lectures
        path = /data1
        browsable = yes
        writable = yes
        read only = no
        valid users = @lectures
```

- Thêm người dùng cho dịch vụ Samba:

```
$sudo smbpasswd -a tuanthai
#Đặt mật khẩu Samba cho người dùng
```

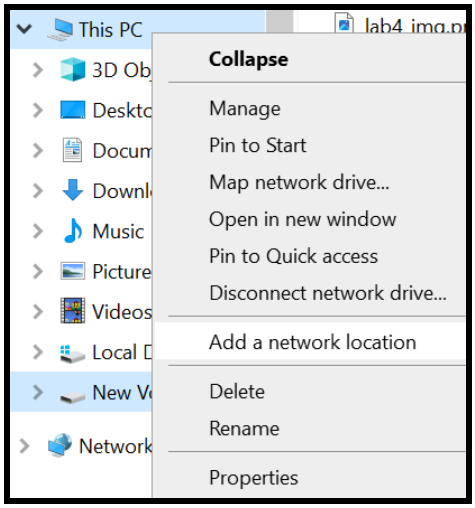
```
[B2105569@myserver ~]$ sudo smbpasswd -a tuanthai
New SMB password:
Retype new SMB password:
Added user tuanthai.
```

- Cấu hình SELINUX cho phép Samba
  `$sudo setsebool -P samba_export_all_rw on`
  `$sudo setsebool -P samba_enable_home_dirs on`
- Tắt tường lửa:
  `$sudo systemctl stop firewalld`
- Khởi động cho phép Samba tự động thực thi khi khởi động hệ điều hành:
  `$sudo systemctl start smb`
  `$sudo systemctl enable smb`

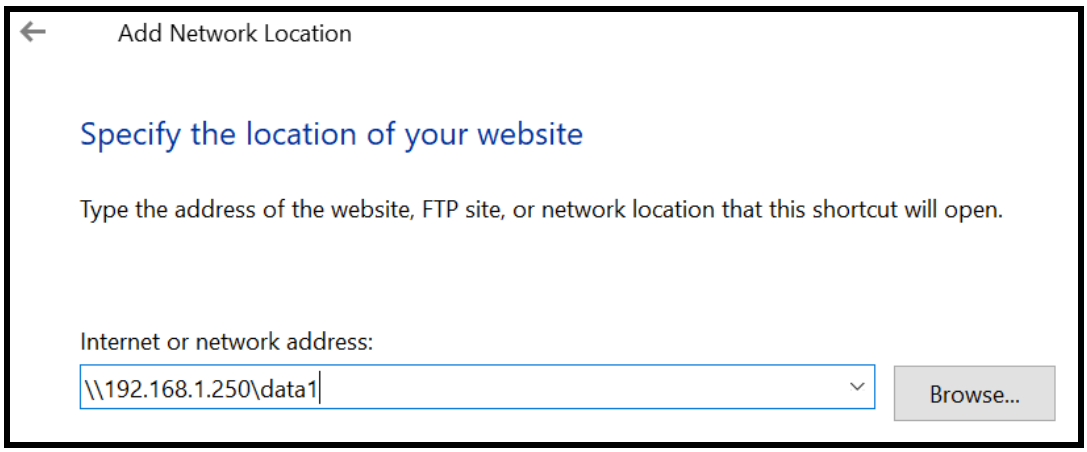
```
[B2105569@myserver ~]$ sudo setsebool -P samba_export_all_rw on
[B2105569@myserver ~]$ sudo setsebool -P samba_enable_home_dirs on
[B2105569@myserver ~]$ sudo systemctl stop firewalld
[B2105569@myserver ~]$ sudo systemctl start smb
[B2105569@myserver ~]$ sudo systemctl enable smb
Created symlink /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`

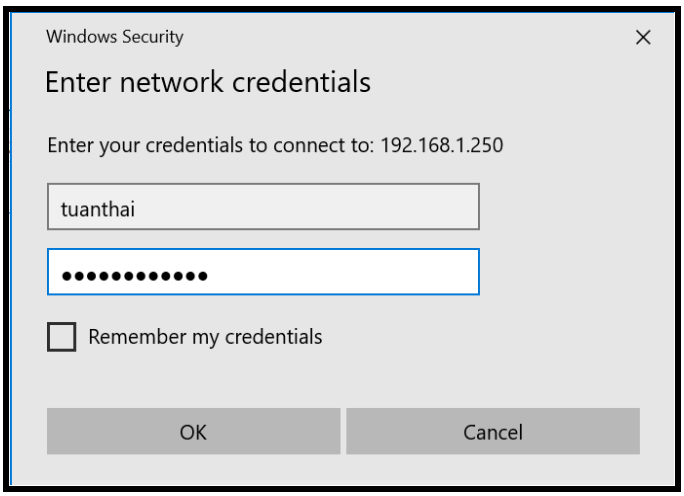
-Tại File Explorer của máy Windows, click chuột phải tại This PC và chọn “Add a network location”



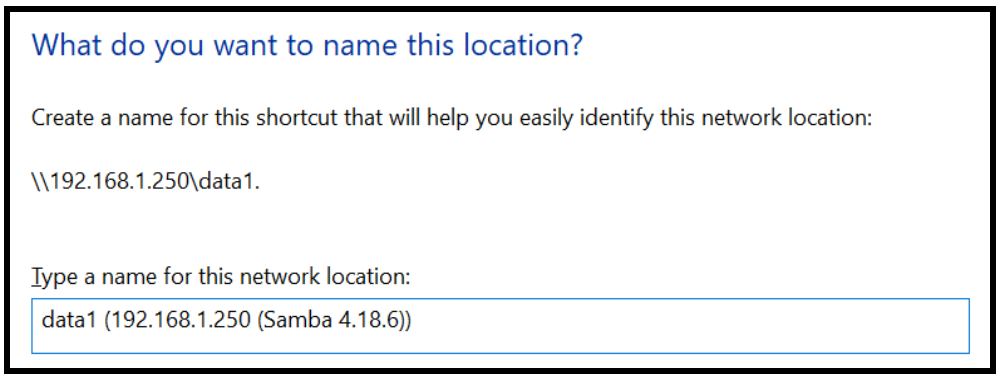
-Tiếp tục, chọn vào “Choose a custom network location” thì sẽ hiện ra như dưới đây, ta sẽ nhập vào địa chỉ `\\<IP máy CentOS>\data1`:



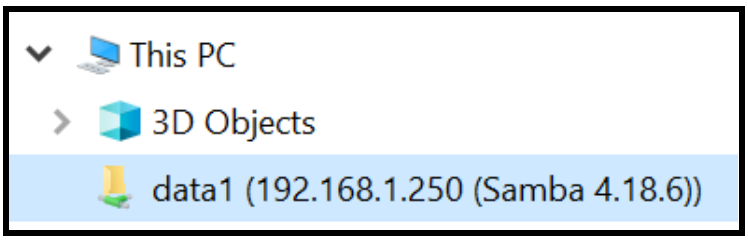
-Lúc này, dịch vụ Samba sẽ yêu cầu ta nhập vào username và mật khẩu để kết nối đến thư mục chia sẻ, chọn OK:



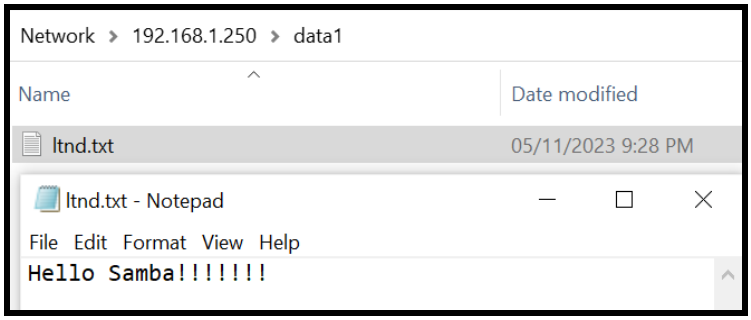
-Sau khi chọn OK, từ máy Windows ta đã kết nối được với thư mục data1 của dịch vụ Samba trên máy CentOS:



-Khi đó trên máy Windows đã tạo ra một thư mục ảo:



-Tạo một tập tin văn bản mới trong ổ ảo của thư mục data1:



-Quay lại với máy CentOS, kiểm tra:

```
[B2105569@myserver ~]$ ls /data1
ltnd.txt
[B2105569@myserver ~]$ cat /data1/ltnd.txt
Hello Samba!!!!!!!
```

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
```

```
Installed:
  bind-32:9.16.23-13.el9.x86_64
  bind-dnssec-doc-32:9.16.23-13.el9.noarch
  bind-dnssec-utils-32:9.16.23-13.el9.x86_64
  python3-bind-32:9.16.23-13.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 {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                    Modified
//
// 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; };
```

```
forwarders {192.168.1.1; };

dnssec-validation no;
```

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

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

3.3. Tạo tập tin cấu hình phân giải xuôi:

```
$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
```

```
[B2105569@myserver ~]$ sudo ls -l /var/named
[sudo] password for B2105569:
total 24
drwxrwx---. 2 named named   23 Nov 11 10:55 data
drwxrwx---. 2 named named   60 Nov 11 10:55 dynamic
-rw-r-----. 1 root  named  210 Nov 11 10:54 forward.qtht
-rw-r-----. 1 root  named 2253 Jul 20 01:18 named.ca
-rw-r-----. 1 root  named  152 Jul 20 01:18 named.empty
-rw-r-----. 1 root  named  152 Jul 20 01:18 named.localhost
-rw-r-----. 1 root  named  168 Jul 20 01:18 named.loopback
-rw-r-----. 1 root  named  197 Nov 11 20:43 reverse.qtht
drwxrwx---. 2 named named    6 Jul 20 01:18 slaves
```

```
  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       192.168.1.250
www     IN      A       192.168.1.250
htql    IN      A       8.8.8.8
```

3.4. Tạo tập tin cấu hình phân giải ngược:

```
$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.
```

```
[B2105569@myserver ~]$ sudo cp /var/named/forward.qtht /var/named/reverse.qtht
[B2105569@myserver ~]$ sudo chgrp named /var/named/reverse.qtht
[B2105569@myserver ~]$ sudo ls -l /var/named/
total 24
drwxrwx---. 2 named named    6 Jul 20 01:18 data
drwxrwx---. 2 named named    6 Jul 20 01:18 dynamic
-rw-r-----. 1 root  named  209 Nov 11 10:48 forward.qtht
-rw-r-----. 1 root  named 2253 Jul 20 01:18 named.ca
-rw-r-----. 1 root  named  152 Jul 20 01:18 named.empty
-rw-r-----. 1 root  named  152 Jul 20 01:18 named.localhost
-rw-r-----. 1 root  named  168 Jul 20 01:18 named.loopback
-rw-r-----. 1 root  named  209 Nov 11 10:49 reverse.qtht
drwxrwx---. 2 named named    6 Jul 20 01:18 slaves
```

```
  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       192.168.1.250
250     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`

```
[B2105569@myserver ~]$ sudo systemctl stop firewalld
[B2105569@myserver ~]$ sudo systemctl start named
[B2105569@myserver ~]$ sudo systemctl status named
● named.service - Berkeley Internet Name Domain (DNS)
     Loaded: loaded (/usr/lib/systemd/system/named.service; disabled; pre
     Active: active (running) since Sat 2023-11-11 10:55:19 +07; 16s ago
```

- Kiểm tra kết quả:

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

```
[B2105569@myserver ~]$ nslookup www.qtht.com.vn 192.168.1.250
Server:         192.168.1.250
Address:        192.168.1.250#53

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

[B2105569@myserver ~]$ nslookup htql.qtht.com.vn 192.168.1.250
Server:         192.168.1.250
Address:        192.168.1.250#53

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

[B2105569@myserver ~]$ nslookup www.ctu.edu.vn 192.168.1.250
Server:         192.168.1.250
Address:        192.168.1.250#53

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

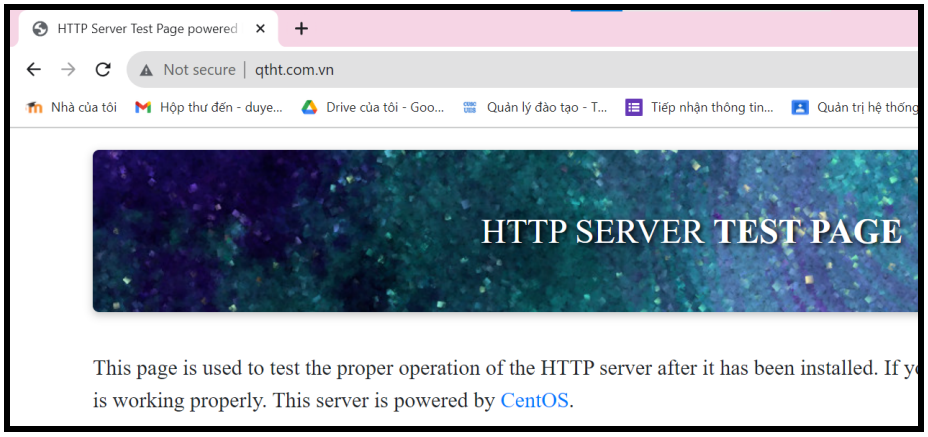
Có thể kiểm tra trên máy Windows bằng Terminal:

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

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


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

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


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

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

⇒Kết quả trả về trên máy Windows cũng giống như kết quả trên máy CentOS

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

Cấu hình DNS server là 192.168.1.250:



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
```

```
[B2105569@myserver ~]$ sudo systemctl start  firewalld
[sudo] password for B2105569:
[B2105569@myserver ~]$ sudo systemctl status  firewalld
● firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.serv
     Active: active (running) since Sat 2023-11-11 11:31:15
```

- Liệt kê tất cả các zone đang có trong hệ thống
  `$firewall-cmd --get-zones`

```
[B2105569@myserver ~]$ firewall-cmd --get-zones
block dmz docker drop external home internal nm-shared public trusted work
[B2105569@myserver ~]$
```

- Kiểm tra zone mặc định
  `$firewall-cmd --get-default-zone`

```
[B2105569@myserver ~]$ firewall-cmd --get-default-zone
public
```

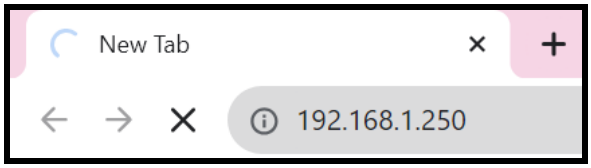
- Kiểm tra zone đang được sử dụng bởi giao diện mạng (thường là *`public`*); và xem các rules của zone
  `$firewall-cmd --get-active-zones`
  `$sudo firewall-cmd --list-all --zone=public`

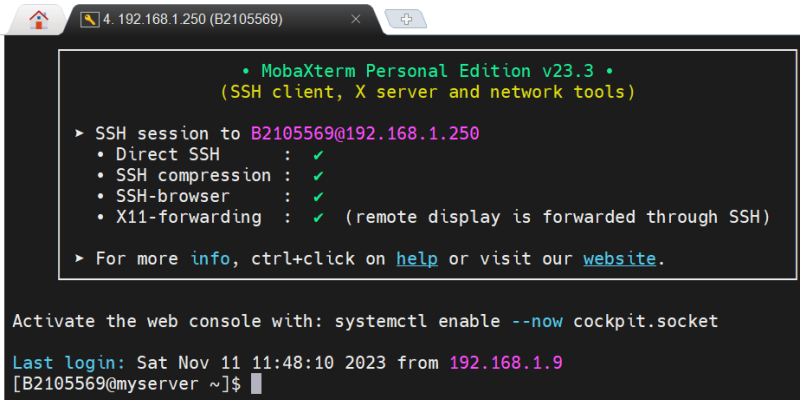
```
[B2105569@myserver ~]$ sudo firewall-cmd --zone=public --change-interface=enp0s3
[sudo] password for B2105569:
success
[B2105569@myserver ~]$ sudo firewall-cmd --list-all --zone=public
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

⇒Zone này có `target: default` nên sẽ chặn hết các dữ liệu mạng ngoại trừ những dịch vụ được liệt kê ở `services`

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

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

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

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





⇒**Kết quả:** Ping và kết nối SSH tới máy CentOS thành công. Nhưng không truy cập dịch vụ web được vì zone public không cho phép dịch vụ web.

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

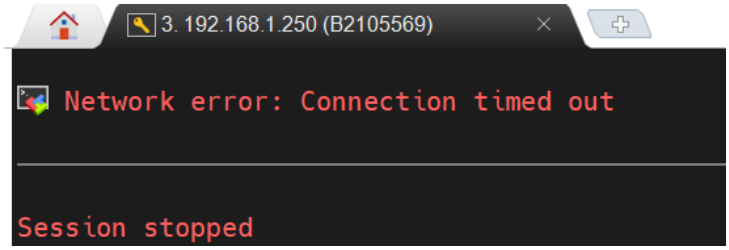
```
$sudo firewall-cmd --zone=drop --change-interface=enp0s3
$sudo firewall-cmd --list-all --zone=drop
```

```
[B2105569@myserver ~]$ sudo firewall-cmd --zone=drop --change-interface=enp0s3
[sudo] password for B2105569:
success
[B2105569@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:
```

⇒Zone này có `target: DROP` nên toàn bộ cac kết nối sẽ bị từ chối

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

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

Pinging 192.168.1.250 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.250:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



⇒**Kết quả:** Cả 3 công việc ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS đều không thực hiện được vì tất cả các dịch vụ bị chặn lại

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

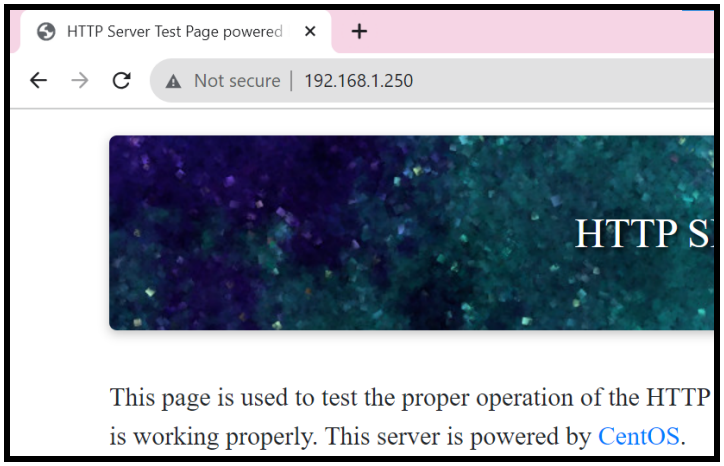
```
$sudo firewall-cmd --zone=trusted --change-interface=enp0s3
$sudo firewall-cmd --list-all --zone=trusted
```

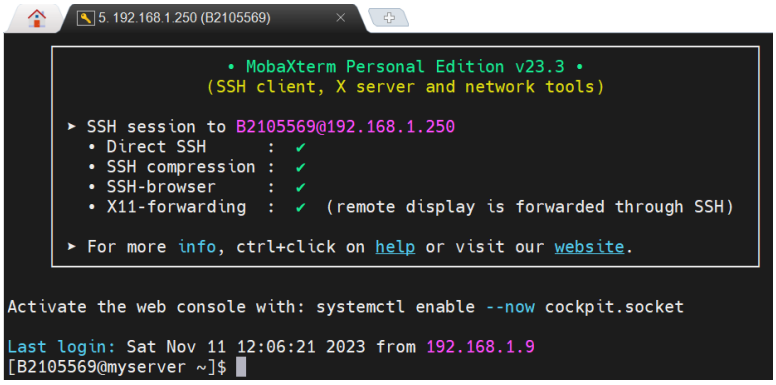
```
[B2105569@myserver ~]$ sudo firewall-cmd --zone=trusted --change-interface=enp0s3
[sudo] password for B2105569:
success
[B2105569@myserver ~]$ sudo firewall-cmd --list-all --zone=trusted
trusted (active)
  target: ACCEPT
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services:
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

⇒Zone này có `target: ACCEPT` nên cho phép tất cả các dịch vụ kết nối tới máy CentOS

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

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

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

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





⇒Cả 3 công việc ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS đều thực hiện thành công.

- 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
```

```
[B2105569@myserver ~]$ sudo firewall-cmd --permanent --new-zone=qthtserver
[sudo] password for B2105569:
success
[B2105569@myserver ~]$ sudo systemctl restart firewalld
[B2105569@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:
```

⇒⇒Zone này có `target: default` nên sẽ chặn hết các dữ liệu mạng ngoại trừ những dịch vụ được liệt kê ở `services`

- 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
```

```
[B2105569@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=http
[sudo] password for B2105569:
success
[B2105569@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=dns
success
[B2105569@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=samba
success
[B2105569@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=ftp
success
[B2105569@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=9999/t
cp
Error: INVALID_SERVICE: Zone 'qthtserver': '9999/tcp' not among existing services
[B2105569@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-port=9999/tcp
success
[B2105569@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'`

```
[B2105569@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-rich-rule=
'rule family=ipv4 source address=192.168.1.9/32 port port=22 protocol=tcp accept'
success
[B2105569@myserver ~]$
```

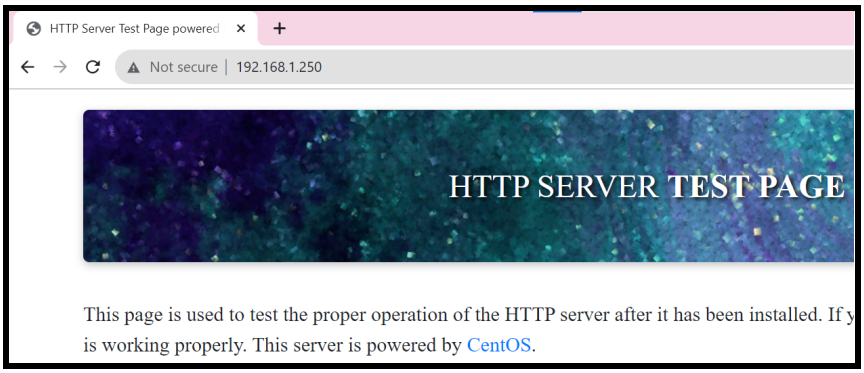
Toàn bộ rule này có nghĩa là: Cho phép dữ liệu mạng là giao thức ipv4, người gửi dữ liệu mạng có địa chỉ ip là 192.168.1.9 truy cập đến cổng 22 (cổng của dịch vụ SSH) thì cho phép.

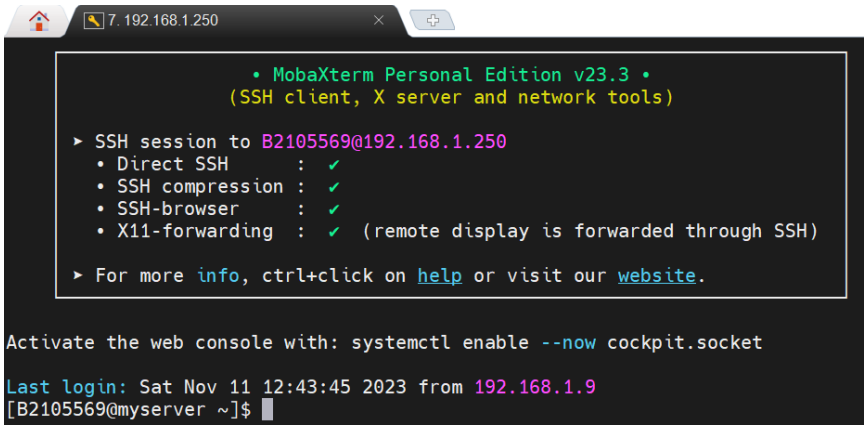
- Khởi động lại tường lửa firewalld
  `$sudo systemctl restart firewalld`
- Chuyển giao diện mạng sang zone `qthtserver`; và xem các rules của zone
  `$sudo firewall-cmd --permanent --zone=qthtserver --change-interface=enp0s3`
  `$sudo firewall-cmd --list-all --zone=qthtserver`

```
[B2105569@myserver ~]$ sudo systemctl restart firewalld
[B2105569@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="192.168.1.9/32" port port="22" protocol="tcp" accept
[B2105569@myserver ~]$
```

⇒Zone này có `target: default` nên sẽ chặn hết các dữ liệu mạng ngoại trừ những dịch vụ được liệt kê ở `services: dns ftp http samba` và truy cập đến `ports: 9999/tcp`. Ngoài ra, còn cho phép máy tính có địa chỉ 192.168.1.9 truy cập đến cổng 22 trên máy CentOS.

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





--- Hết ---

Video hướng dẫn làm bài:

+ Hướng dẫn làm bài: https://youtu.be/MgrW8zeh02E
+ Hướng dẫn câu 1: https://youtu.be/0oW0TF1iVQs
+ Hướng dẫn câu 2: https://youtu.be/ZuRg10OdtJQ
+ Hướng dẫn câu 3: https://youtu.be/89mAL_T_uuY
+ Hướng dẫn câu 4: https://youtu.be/cS3Qv90bBQ8