LAB 5

DOCKER, SAMBA, DNS và Firewall

Họ tên và MSSV: Huỳnh Quốc Dinh B2110009

Nhóm học phần: 03

- Các sinh viên bị phát hiện sao chép bài của nhau sẽ nhận 0đ cho tất cả bài thực hành của môn này.

- Bài nộp phải ở dạng PDF, hình minh họa phải rõ ràng chi tiết.

1. **Triển khai dịch vụ WEB sử dụng Docker**

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

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

```
[b2110009@localhost ~]$ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.63.20  netmask 255.255.255.0  broadcast 192.168.63.255
        inet6 fe80::a00:27ff:fe70:8c69  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:70:8c:69  txqueuelen 1000  (Ethernet)
        RX packets 127197  bytes 185778246 (177.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25595  bytes 1732107 (1.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 23  bytes 2464 (2.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 2464 (2.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
[b2110009@localhost ~]$ ping 192.168.63.102
PING 192.168.63.102 (192.168.63.102) 56(84) bytes of data.
64 bytes from 192.168.63.102: icmp_seq=1 ttl=128 time=0.306 ms
64 bytes from 192.168.63.102: icmp_seq=2 ttl=128 time=0.918 ms
64 bytes from 192.168.63.102: icmp_seq=3 ttl=128 time=1.53 ms
64 bytes from 192.168.63.102: icmp_seq=4 ttl=128 time=1.16 ms
^C
--- 192.168.63.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3020ms
rtt min/avg/max/mdev = 0.306/0.978/1.533/0.445 ms
```

```
[b2110009@localhost ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=44.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=36.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=41.1 ms
^C
--- 8.8.8.8 ping statistics ---
```

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
```

```
[b2110009@localhost ~]$ 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>
```

```
[b2110009@localhost ~]$ sudo systemctl stop firewalld
```

```
[b2110009@localhost ~]$ sudo systemctl status firewalld
[sudo] password for b2110009:
○ firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset>
     Active: inactive (dead) since Sat 2024-04-06 23:27:36 +07; 16min ago
   Duration: 33min 13.368s
       Docs: man:firewalld(1)
    Process: 777 ExecStart=/usr/sbin/firewalld --nofork --nopid $FIREWALLD_ARGS>
   Main PID: 777 (code=exited, status=0/SUCCESS)
        CPU: 2.000s

Apr 06 22:54:20 localhost.localdomain systemd[1]: Starting firewalld - dynamic >
Apr 06 22:54:23 localhost.localdomain systemd[1]: Started firewalld - dynamic f>
Apr 06 23:27:36 localhost.localdomain systemd[1]: Stopping firewalld - dynamic >
Apr 06 23:27:36 localhost.localdomain systemd[1]: firewalld.service: Deactivate>
Apr 06 23:27:36 localhost.localdomain systemd[1]: Stopped firewalld - dynamic f>
Apr 06 23:27:36 localhost.localdomain systemd[1]: firewalld.service: Consumed 2>
```

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
```

```
  Running scriptlet: shadow-utils-subid-2:4.9-8.el9.x86_64                  4/4
  Verifying        : cockpit-podman-84.1-1.el9.noarch                       1/4
  Verifying        : conmon-2:2.1.10-1.el9.x86_64                           2/4
  Verifying        : podman-2:4.9.2-1.el9.x86_64                            3/4
  Verifying        : shadow-utils-subid-2:4.9-8.el9.x86_64                  4/4

Removed:
  cockpit-podman-84.1-1.el9.noarch     conmon-2:2.1.10-1.el9.x86_64
  podman-2:4.9.2-1.el9.x86_64          shadow-utils-subid-2:4.9-8.el9.x86_64

Complete!
```

- Cài đặt công cụ yum-utils

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

```
[b2110009@localhost ~]$ sudo dnf install -y yum-utils
Last metadata expiration check: 0:00:43 ago on Sat 06 Apr 2024 11:58:53 PM +07.
Dependencies resolved.
================================================================================
 Package              Architecture          Version                Repository  Size
================================================================================
Installing:
 yum-utils            noarch                4.3.0-13.el9           baseos      40 k

Transaction Summary
```

```
--------------------------------------------------------------------------------
Total                                           24 kB/s |  40 kB     00:01
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                        1/1
  Installing       : yum-utils-4.3.0-13.el9.noarch                          1/1
  Running scriptlet: yum-utils-4.3.0-13.el9.noarch                          1/1
  Verifying        : yum-utils-4.3.0-13.el9.noarch                          1/1

Installed:
  yum-utils-4.3.0-13.el9.noarch

Complete!
[b2110009@localhost ~]$
```

- Thêm địa chỉ repo của Docker vào công cụ yum

```
$sudo yum-config-manager \
--add-repo \
https://download.docker.com/linux/centos/docker-ce.repo
#Viết liên tục lệnh trên hoặc xuống hàng bằng enter.
```

```
[b2110009@localhost ~]$ 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
```

- Cài đặt Docker

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

```
  Running scriptlet: docker-ce-3:26.0.0-1.el9.x86_64                        6/6
  Verifying        : containerd.io-1.6.28-3.2.el9.x86_64                    1/6
  Verifying        : docker-buildx-plugin-0.13.1-1.el9.x86_64               2/6
  Verifying        : docker-ce-3:26.0.0-1.el9.x86_64                        3/6
  Verifying        : docker-ce-cli-1:26.0.0-1.el9.x86_64                    4/6
  Verifying        : docker-ce-rootless-extras-26.0.0-1.el9.x86_64          5/6
  Verifying        : docker-compose-plugin-2.25.0-1.el9.x86_64              6/6

Installed:
  containerd.io-1.6.28-3.2.el9.x86_64    docker-buildx-plugin-0.13.1-1.el9.x86_64    docker-ce-3:26.0.0-1.el9.x86_64
  docker-ce-cli-1:26.0.0-1.el9.x86_64    docker-ce-rootless-extras-26.0.0-1.el9.x86_64    docker-compose-plugin-2.25.0-1.el9.x86_64

Complete!
[b2110009@localhost ~]$
```

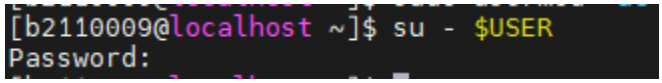
- Thêm người dùng hiện tại vào nhóm docker để sử dụng các lệnh của Docker mà không cần quyền sudo

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

```
[b2110009@localhost ~]$ sudo usermod -aG docker $USER
```

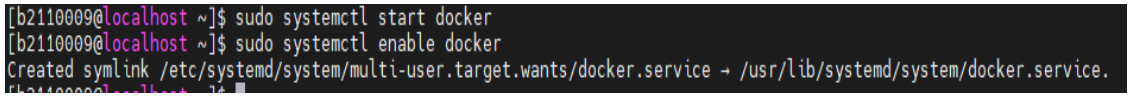
- Login lại vào shell để việc thêm người dùng vào nhóm có tác dụng

```
$su - $USER
```



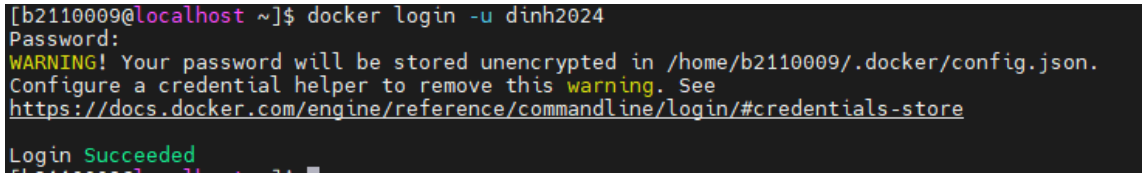
- Chạy dịch vụ Docker

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



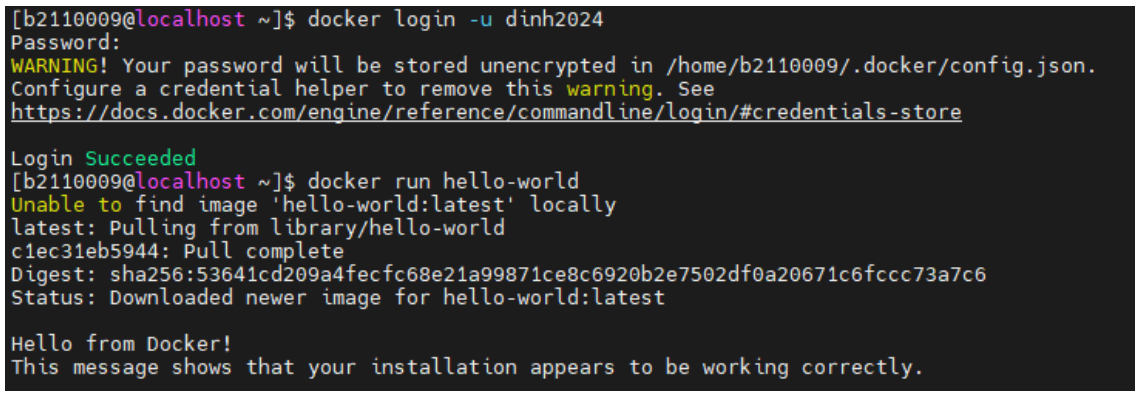
- Tạo 1 tài khoản trên DockerHub (https://hub.docker.com/), sau đó đăng nhập sử dụng lệnh sau:

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



- 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
```



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
```

```
[b2110009@localhost ~]$ docker search httpd
NAME                              DESCRIPTION                                     STARS     OFFICIAL
httpd                             The Apache HTTP Server Project                  4689      [OK]
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 …   12
wodby/httpd                                                                       0
dockette/httpdump                                                                 0
betterweb/httpd                                                                   0
dockette/apache                   Apache / HTTPD                                  1
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
centos/httpd-24-centos8                                                           3
dockerpinata/httpd                                                                1
19022021/httpd-connection_test    This httpd image will test the connectivity …   0
httpdocker/kubia                                                                  0
publici/httpd                     httpd:latest                                    1
centos/httpd                                                                      36
httpdss/archerysec                ArcherySec repository                           0
e2eteam/httpd                                                                     0
manasip/httpd                                                                     0
solsson/httpd-openidc             mod_auth_openidc on official httpd image, ve…   2
patrickha/httpd-err                                                               0
```

- 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

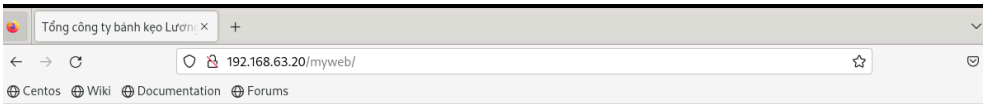
  `-p 8080:80` gắn cổng 8080 của máy CentOS vào cổng 80 của container.

```
[b2110009@localhost ~]$ docker run -d -it -p 8080:80 --name webserver httpd
Unable to find image 'httpd:latest' locally
latest: Pulling from library/httpd
8a1e25ce7c4f: Pull complete
9d6bc7327bff: Pull complete
4f4fb700ef54: Pull complete
32da760aec63: Pull complete
b8bd53c7eb2b: Pull complete
fafe44e4648e: Pull complete
Digest: sha256:ef6014cbbd99808811831bd36a596f36918847d3f6cb6b3f63874a92daee8d6b
Status: Downloaded newer image for httpd:latest
2de3b71cfcfe50a7459bed38aae1e83cb0690c2a1079f0d4f7eb66b562c8eef1
```

- 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/`

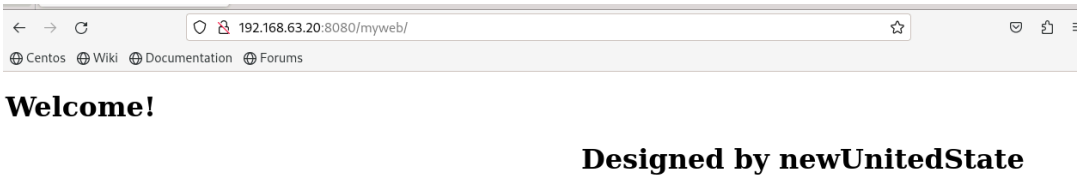
```
[b2110009@localhost ~]$ docker cp /var/www/html/myweb/ webserver:/usr/local/apache2/htdocs/
Successfully copied 2.56kB to webserver:/usr/local/apache2/htdocs/
```



Welcome!

Designed by B12345678

- 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.



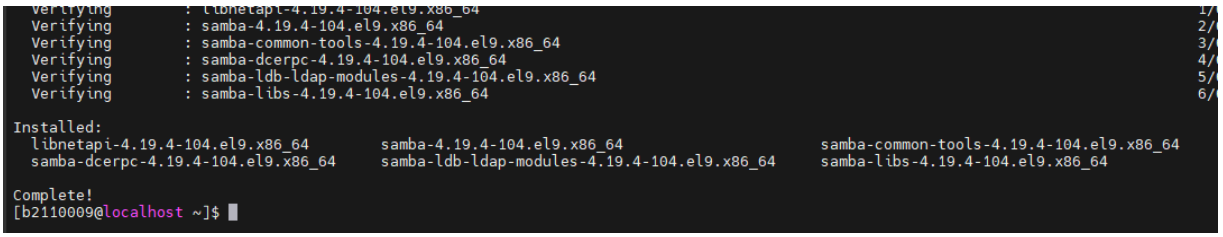
2. Cài đặt và cấu hình dịch vụ SAMBA

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):

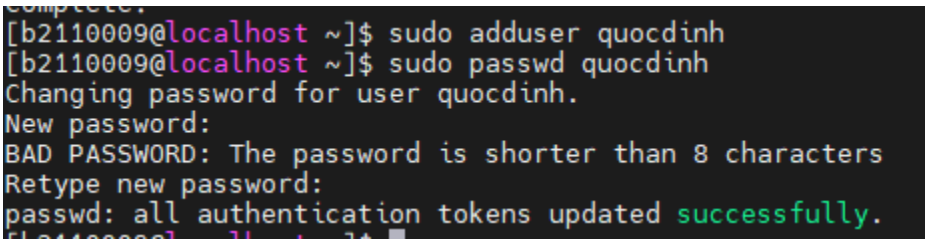
- Cài đặt dịch vụ Samba:

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

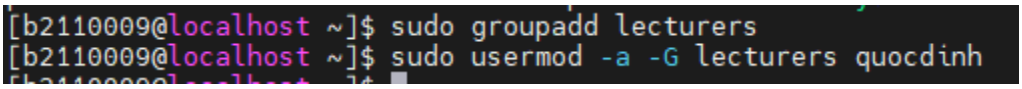


- Tạo người dùng và nhóm người dùng chia sẻ dữ liệu:

```
$sudo adduser baole
$sudo passwd baole
```




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



- Tạo thư mục cần chia sẻ và phân quyền:

```
$sudo mkdir /data
```

```
[b2110009@localhost ~]$ sudo mkdir /data1
[sudo] password for b2110009:
[b2110009@localhost ~]$ ls -l /
total 32
dr-xr-xr-x.   2 root root        6 Aug 10  2021 afs
drwxr-xr-x.   2 root root       28 Mar 12 00:42 backup
lrwxrwxrwx.   1 root root        7 Aug 10  2021 bin -> usr/bin
dr-xr-xr-x.   5 root root     4096 Mar 29 22:32 boot
drwxr-x---.   2 root nhanvien 4096 Apr  7 00:51 data
drwxr-xr-x.   2 root root        6 Apr  7 11:23 data1
```

$sudo chown :lecturers /data

```
[b2110009@localhost ~]$ sudo chown :lecturers /data1
[b2110009@localhost ~]$ ls -l /
```

```
drwxr-xr-x.   2 root lecturers    6 Apr  7 11:23 data1
```

$sudo chmod -R 775 /data

```
drwxrwxr-x.   2 root lecturers    6 Apr  7 11:23 data1
```

- 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

```
[b2110009@localhost ~]$ sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.orig
[b2110009@localhost ~]$ sudo nano /etc/samba/smb.conf
```

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

```
2. 192.168.63.20 (1)
  GNU nano 5.6.1                                  /etc/samba/smb.conf
[printers]
        comment = All Printers
        path = /var/tmp
        printable = Yes
        create mask = 0600
        browseable = No

[print$]
        comment = Printer Drivers
        path = /var/lib/samba/drivers
        write list = @printadmin root
        force group = @printadmin
        create mask = 0664
        directory mask = 0775
[data1]
        comment = Shared folder for lecturers
        path = /data1
        browsable = yes
        writable = yes
        read only = no
        valid users = @lecturers
```

- Thêm người dùng cho dịch vụ Samba:

  `$sudo smbpasswd -a baole`

  `#Đặt mật khẩu Samba cho người dùng`

```
[b2110009@localhost ~]$ sudo smbpasswd -a quocdinh
New SMB password:
Retype new SMB password:
Added user quocdinh.
```

- Cấu hình SELINUX cho phép Samba

  `$sudo setsebool -P samba_export_all_rw on`

  `$sudo setsebool -P samba_enable_home_dirs on`

```
[b2110009@localhost ~]$ sudo setsebool -P samba_export_all_rw on
[b2110009@localhost ~]$ sudo setsebool -P samba_enable_home_dirs on
```

- Tắt tường lửa:

  `$sudo systemctl stop firewalld`

```
[b2110009@localhost ~]$ sudo systemctl stop firewalld
```

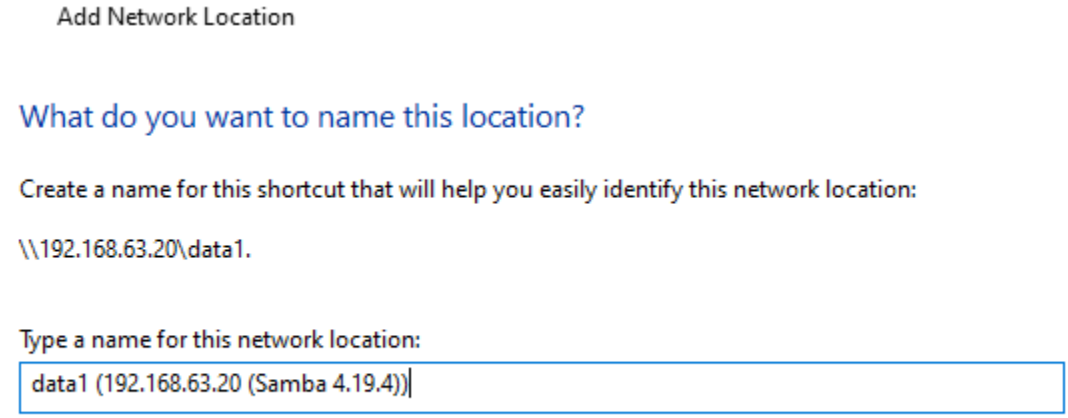
- Khởi động cho phép Samba tự động thực thi khi khởi động hệ điều hành:

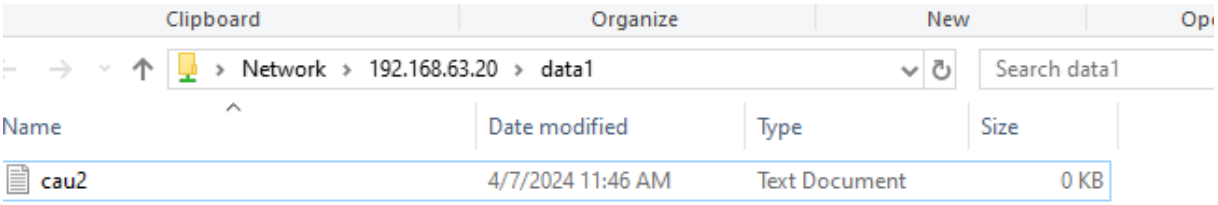
  `$sudo systemctl start smb`

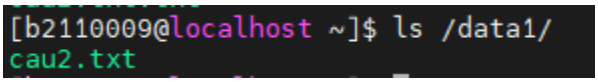
  `$sudo systemctl enable smb`

```
[b2110009@localhost ~]$ sudo systemctl start smb
[b2110009@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`







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
```

```
[b2110009@localhost ~]$ sudo dnf install bind bind-utils -y
[sudo] password for b2110009:
Last metadata expiration check: 0:15:32 ago on Sun 07 Apr 2024 11:42:15 AM +07.
Package bind-utils-32:9.16.23-15.el9.x86_64 is already installed.
Dependencies resolved.
================================================================================
 Package                    Architecture          Version
================================================================================
Installing:
 bind                       x86_64                32:9.16.23-15.el9
Installing dependencies:
 bind-dnssec-doc            noarch                32:9.16.23-15.el9
 python3-bind               noarch                32:9.16.23-15.el9
 python3-ply                noarch                3.11-14.el9
Installing weak dependencies:
 bind-dnssec-utils          x86_64                32:9.16.23-15.el9

Transaction Summary
================================================================================
```

```
  Verifying        : python3-ply-3.11-14.el9.noarch
  Verifying        : bind-32:9.16.23-15.el9.x86_64
  Verifying        : bind-dnssec-doc-32:9.16.23-15.el9.noarch
  Verifying        : bind-dnssec-utils-32:9.16.23-15.el9.x86_64
  Verifying        : python3-bind-32:9.16.23-15.el9.noarch

Installed:
  bind-32:9.16.23-15.el9.x86_64            bind-dnssec-doc-32:9.16.23-15.el9.noarch     bind-dnss
  python3-bind-32:9.16.23-15.el9.noarch    python3-ply-3.11-14.el9.noarch

Complete!
[b2110009@localhost ~]$
```

3.2. Cấu hình DNS server:

$sudo nano /etc/named.conf

```
  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; };
        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; };

        /*
```

```
#(tham khảo file mẫu)
...
options {
      listen-on port 53 { 127.0.0.1; any;};
      ...
      allow-query     { localhost; any; };
      recursion yes;
      forwarders {8.8.8.8; };
      ..
```

```
};

logging {
        ..
        };
};

zone "." IN {
      ...
};

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

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

…

```
options {
        listen-on port 53 { 127.0.0.1; any; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        secroots-file   "/var/named/data/named.secroots";
        recursing-file  "/var/named/data/named.recursing";
        allow-query     { localhost; any; };

        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;
        forwarders {8.8.8.8; };
        dnssec-validation yes;

        managed-keys-directory "/var/named/dynamic";
        geoip-directory "/usr/share/GeoIP";
```

```
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

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

zone "63.168.192.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:

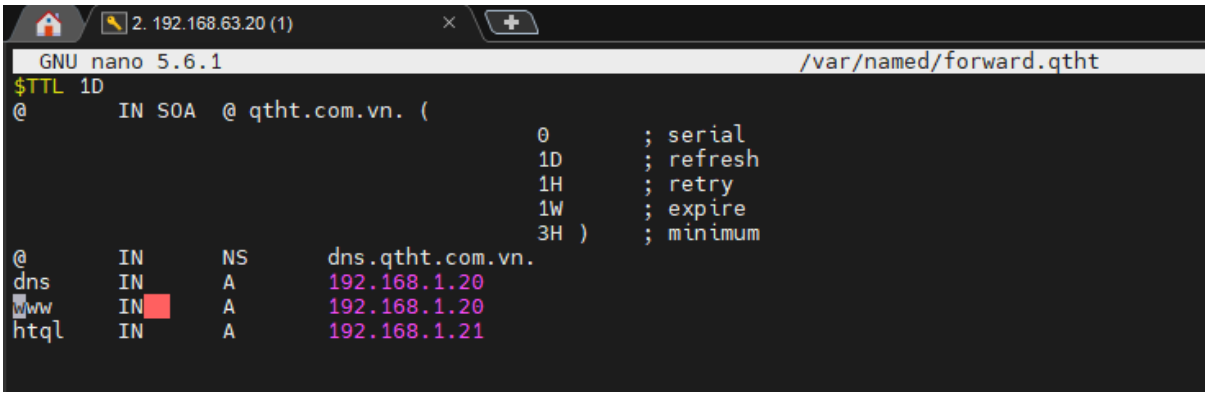
```
$sudo cp /var/named/named.localhost /var/named/forward.qtht
$sudo chgrp named /var/named/forward.qtht
$sudo nano /var/named/forward.qtht
```

```
[b2110009@localhost ~]$ sudo ls /var/named/
data  dynamic  named.ca  named.empty  named.localhost  named.loopback  slaves
```

```
[b2110009@localhost ~]$ sudo cp /var/named/named.localhost /var/named/forward.qtht
[b2110009@localhost ~]$ sudo chgrp named /var/named/forward.qtht
[b2110009@localhost ~]$ sudo ls -l /var/named/
total 20
drwxrwx---. 2 named named    6 Feb 12 23:32 data
drwxrwx---. 2 named named    6 Feb 12 23:32 dynamic
-rw-r-----. 1 root  named  152 Apr  7 12:15 forward.qtht
-rw-r-----. 1 root  named 2112 Feb 12 23:32 named.ca
-rw-r-----. 1 root  named  152 Feb 12 23:32 named.empty
-rw-r-----. 1 root  named  152 Feb 12 23:32 named.localhost
-rw-r-----. 1 root  named  168 Feb 12 23:32 named.loopback
drwxrwx---. 2 named named    6 Feb 12 23:32 slaves
```

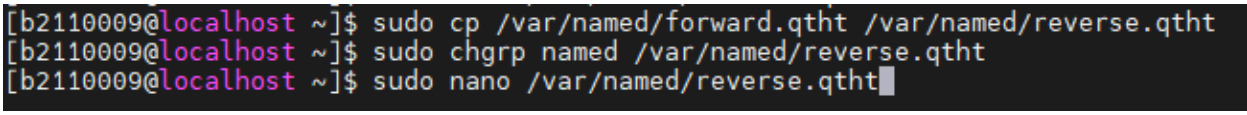
```
#(tham khảo file mẫu)
$TTL 1D
```

```
@    IN   SOA @ qtht.com.vn. (
                  0     ;Serial
                  1D    ;Refresh
                  1H    ;Retry
                  1W    ;Expire
                  3H    ;Minimum TTL
)
@      IN    NS    dns.qtht.com.vn.
dns    IN    A     192.168.1.20
www    IN    A     192.168.1.20
htql   IN    A     192.168.1.21
```



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

```
 GNU nano 5.6.1                                          /var/named/reverse.qtht
$TTL 1D
@       IN SOA  @ qtht.com.vn. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@       IN      NS      dns.qtht.com.vn.
dns     IN      A       192.168.1.20
20      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
```

```
[b2110009@localhost ~]$ sudo systemctl start named
[b2110009@localhost ~]$
```

```
[b2110009@localhost ~]$ sudo systemctl status named
● named.service - Berkeley Internet Name Domain (DNS)
     Loaded: loaded (/usr/lib/systemd/system/named.service; disabled; preset: disabled)
     Active: active (running) since Sun 2024-04-07 12:30:31 +07; 43s ago
    Process: 5732 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" == "yes" ]; then /usr/sbin/named-checkconf -z "$NAMEDCONF"; >
    Process: 5734 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 5735 (named)
      Tasks: 5 (limit: 23039)
     Memory: 22.6M
        CPU: 117ms
     CGroup: /system.slice/named.service
             └─5735 /usr/sbin/named -u named -c /etc/named.conf

Apr 07 12:30:31 localhost.localdomain named[5735]: zone 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa/IN: loa>
Apr 07 12:30:31 localhost.localdomain named[5735]: zone 63.168.192.in-addr.arpa/IN: loaded serial 0
Apr 07 12:30:31 localhost.localdomain named[5735]: zone localhost.localdomain/IN: loaded serial 0
Apr 07 12:30:31 localhost.localdomain named[5735]: zone 63.168.192.in-addr.arpa/IN: sending notifies (serial 0)
Apr 07 12:30:31 localhost.localdomain named[5735]: all zones loaded
Apr 07 12:30:31 localhost.localdomain systemd[1]: Started Berkeley Internet Name Domain (DNS).
Apr 07 12:30:31 localhost.localdomain named[5735]: running
Apr 07 12:30:31 localhost.localdomain named[5735]: zone qtht.com.vn/IN: sending notifies (serial 0)
Apr 07 12:30:31 localhost.localdomain named[5735]: managed-keys-zone: Initializing automatic trust anchor management for zone '.'; DNSKE>
Apr 07 12:30:31 localhost.localdomain named[5735]: resolver priming query complete
lines 1-22/22 (END)
```

- Kiểm tra kết quả:

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

```
[b2110009@localhost ~]$ nslookup www.qtht.com.vn 192.168.63.20
Server:         192.168.63.20
Address:        192.168.63.20#53

Name:   www.qtht.com.vn
Address: 192.168.1.20
```

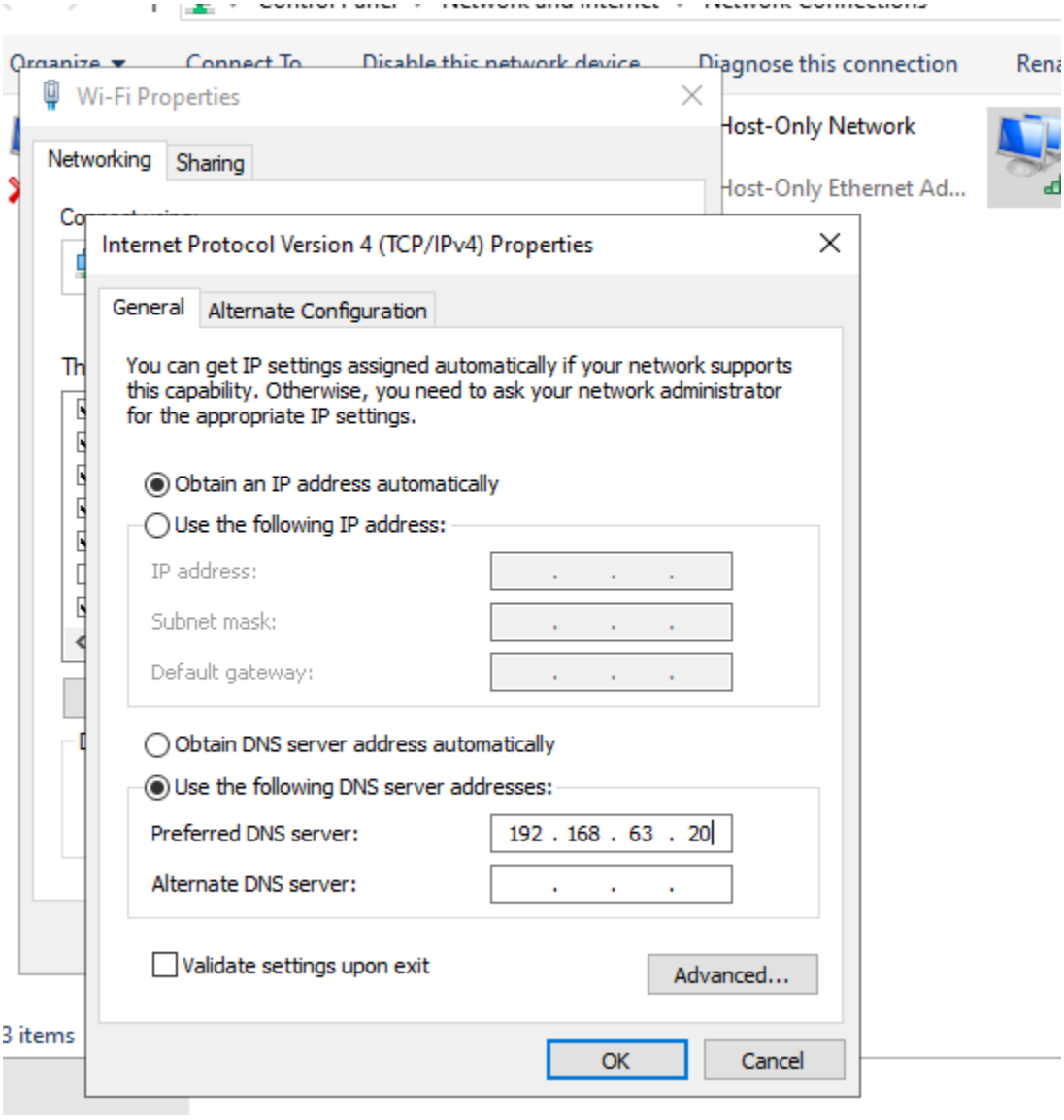
```
nslookup htql.qtht.com.vn <địa chỉ IP máy ảo>
```

```
[b2110009@localhost ~]$ nslookup htql.qtht.com.vn 192.168.63.20
Server:         192.168.63.20
Address:        192.168.63.20#53

Name:   htql.qtht.com.vn
Address: 192.168.1.21
```

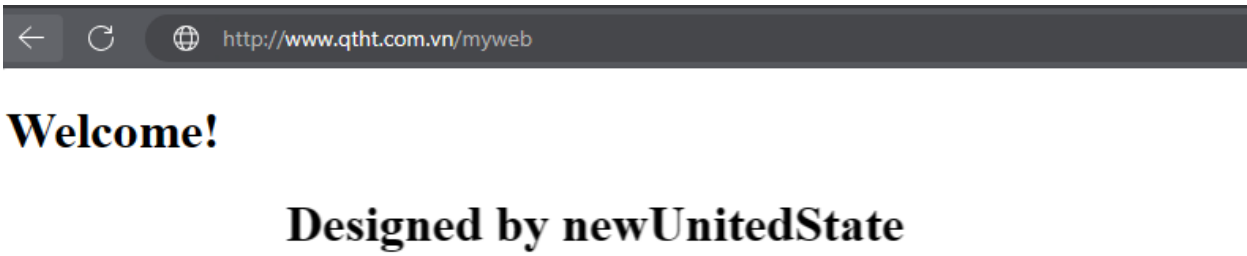
```
nslookup www.ctu.edu.vn <địa chỉ IP máy ảo>
```

```
[b2110009@localhost ~]$ nslookup www.ctu.edu.vn 192.168.63.20
Server:         192.168.63.20
Address:        192.168.63.20#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**(DNS Server). Sau đó, mở trình duyệt web và truy cập vào địa chỉ http://www.qtht.com.vn/myweb



-



–

4. Cấu hình tường lửa 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
```

```
[b2110009@localhost ~]$ sudo systemctl start firewalld
[b2110009@localhost ~]$ sudo systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
     Active: active (running) since Sun 2024-04-07 13:35:02 +07; 2s ago
       Docs: man:firewalld(1)
   Main PID: 7465 (firewalld)
      Tasks: 2 (limit: 23039)
     Memory: 24.1M
        CPU: 1.322s
     CGroup: /system.slice/firewalld.service
             └─7465 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid

Apr 07 13:35:01 localhost.localdomain systemd[1]: Starting firewalld - dynamic firewall daemon...
Apr 07 13:35:02 localhost.localdomain systemd[1]: Started firewalld - dynamic firewall daemon.
```

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

  `$firewall-cmd --get-zones`

```
[b2110009@localhost ~]$ firewall-cmd --get-zones
block dmz docker drop external home internal nm-shared public trusted work
```

- Kiểm tra zone mặc định

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

```
[b2110009@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`

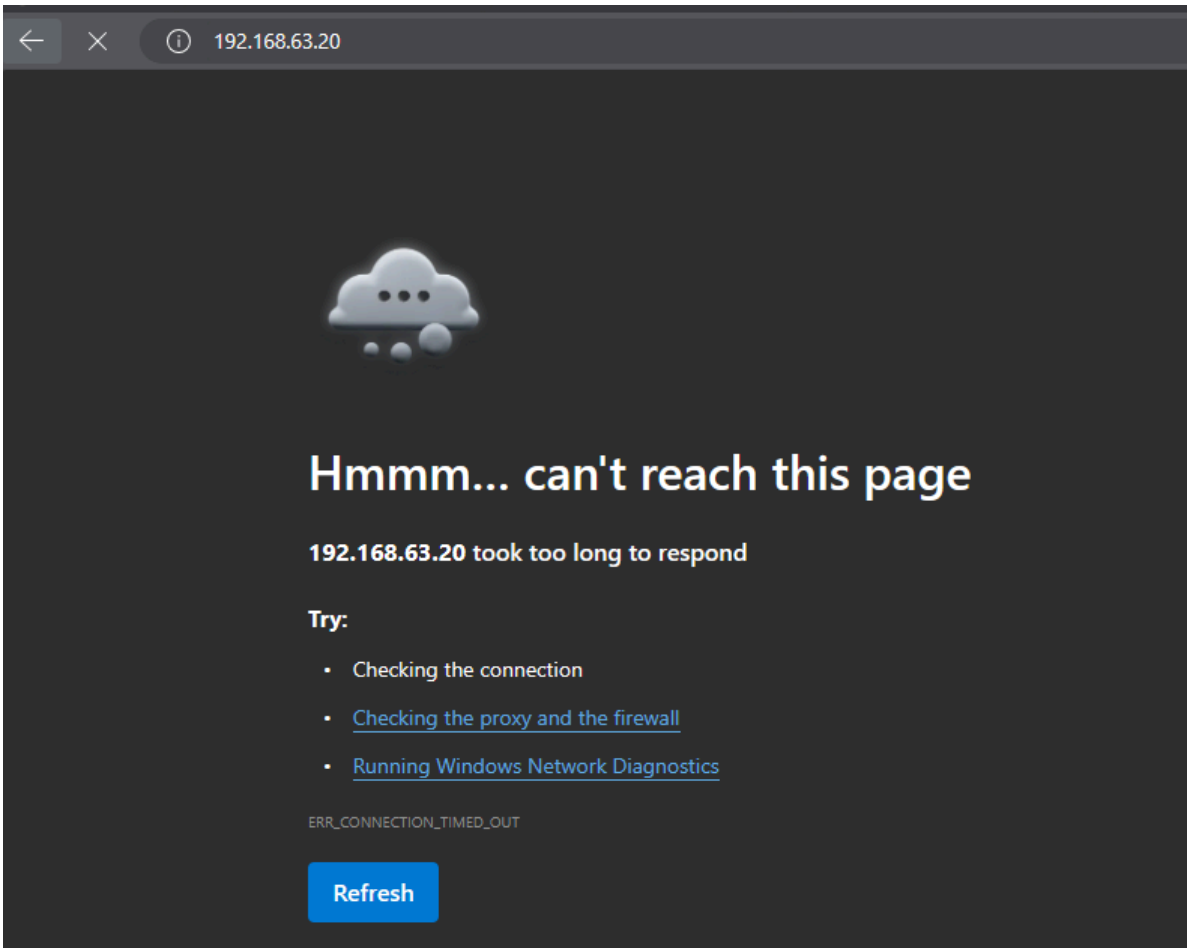
```
[b2110009@localhost ~]$ firewall-cmd --get-active-zones
docker
  interfaces: docker0
public
  interfaces: enp0s3
```

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

```
[b2110009@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:
```

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

```
Pinging 192.168.63.20 with 32 bytes of data:
Reply from 192.168.63.20: bytes=32 time<1ms TTL=64
Reply from 192.168.63.20: bytes=32 time=1ms TTL=64
Reply from 192.168.63.20: bytes=32 time=1ms TTL=64
Reply from 192.168.63.20: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.63.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```



- 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
```

```
[b2110009@localhost ~]$ sudo firewall-cmd --zone=drop --change-interface=enp0s3
success
[b2110009@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:
```

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

```
C:\Users\HP>ping 192.168.63.20

Pinging 192.168.63.20 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.63.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\HP>
```

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

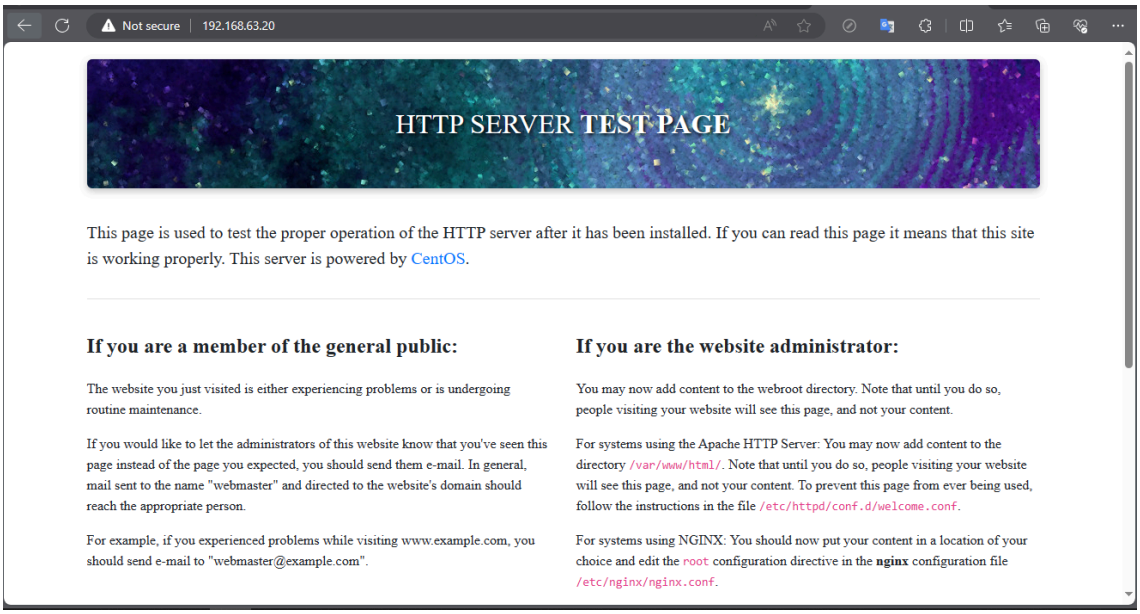
$sudo firewall-cmd --zone=trusted --change-interface=enp0s3

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

```
[b2110009@localhost ~]$ sudo firewall-cmd --zone=trusted --change-interface=enp0s3
success
[b2110009@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:
```

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

```
C:\Users\HP>ping 192.168.63.20

Pinging 192.168.63.20 with 32 bytes of data:
Reply from 192.168.63.20: bytes=32 time<1ms TTL=64
Reply from 192.168.63.20: bytes=32 time=1ms TTL=64
Reply from 192.168.63.20: bytes=32 time=1ms TTL=64
Reply from 192.168.63.20: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.63.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```



- 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 (ng dùng tự định nghĩa)
```

```
[b2110009@localhost ~]$ sudo firewall-cmd --permanent --new-zone=qthtserver
success
[b2110009@localhost ~]$ sudo systemctl restart firewalld
[b2110009@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:
```

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

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

```
[b2110009@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=http
success
[b2110009@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=dns
success
[b2110009@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=samba
success
[b2110009@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=ftp
success
[b2110009@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=ssh
success
[b2110009@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-port=9999/tcp
success
```

- Khởi động lại tường lửa firewalld

```
$sudo systemctl restart firewalld
```

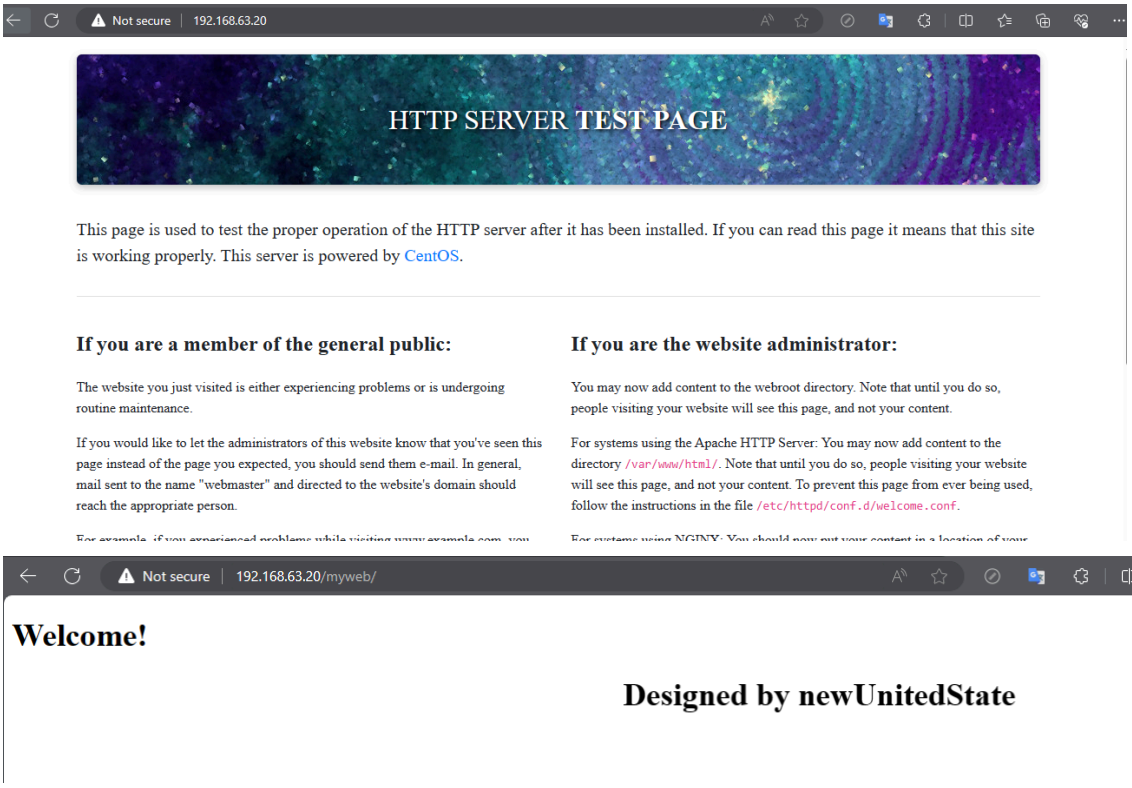
```
[b2110009@localhost ~]$ sudo systemctl restart firewalld
```

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

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

```
[b2110009@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --change-interface=enp0s3
The interface is under control of NetworkManager, setting zone to 'qthtserver'.
success
[b2110009@localhost ~]$ sudo firewall-cmd --list-all --zone=qthtserver
qthtserver (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: dns ftp http samba ssh
  ports: 9999/tcp
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

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



--- Hết ---