**LAB 5**

**DOCKER, SAMBA, DNS và Firewall**

| Họ tên và MSSV: |
| --- |
| Nhóm học phần: |

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

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

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

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

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

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

Tắt tường lửa:

```
$sudo systemctl stop firewalld
```

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
```

- Cài đặt công cụ yum-utils

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

- Thêm địa repo của Docker vào công cụ yum

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

- Cài đặt Docker

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

- 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
```

- 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
```

- 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.

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

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

- Trên máy vật lý, mở trình duyệt web và truy cập vào địa chỉ `http://<Địa chỉ IP máy ảo CentOS>:8080/myweb` để kiểm chứng trang web vừa tạo.

## 2. Cài đặt và cấu hình dịch vụ SAMBA

Samba là dịch vụ chia sẻ file giữa các hệ điều hành khác nhau như Windows và Linux bằng cách sử dụng giao thức SMB/CIFS. Trong bài thực hành sinh viên sẽ cài đặt và cấu hình dịch vụ Samba trên máy chủ CentOS và sử dụng máy Windows để truy cập tới dịch vụ.

Tìm hiểu và thực hiện các yêu cầu sau (kèm hình minh họa cho từng bước):

- Cài đặt dịch vụ Samba:

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

- 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
```

- Tạo thư mục cần chia sẻ và phân quyền:

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

- Cấu hình dịch vụ Samba:

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

```
#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
```

- Thêm người dùng cho dịch vụ Samba:

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

- 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
```

- 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
```

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; };
};
...
```

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
```

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.
```

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
```

- 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>
```

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

## 4. Cấu hình tường lửa Firewalld

Công cụ Firewalld (dynamic firewall daemon) cung cấp dịch vụ tường lửa mạnh mẽ, toàn diện; được cài đặt mặc định cho nhiều bản phân phối Linux. Từ CentOS 7 trở về sau, tường lửa Firewalld được thay thế cho tường lửa iptables với những khác biệt cơ bản:

- Firewalld sử dụng "zone" như là một nhóm các quy tắc (rule) áp đặt lên những luồng dữ liệu. Một số zone có sẵn thường dùng:
  - *drop*: ít tin cậy nhất – toàn bộ các kết nối đến sẽ bị từ chối.
  - *public*: đại diện cho mạng công cộng, không đáng tin cậy. Các máy tính/services khác không được tin tưởng trong hệ thống nhưng vẫn cho phép các kết nối đến tùy từng trường hợp cụ thể.

    - *trusted*: đáng tin cậy nhất – tin tưởng toàn bộ thiết bị trong hệ thống.
- Firewalld quản lý các quy tắc được thiết lập tự động, có tác dụng ngay lập tức mà không làm mất đi các kết nối và session hiện có.
    - *Runtime* (mặc định): có tác dụng ngay lập tức nhưng mất hiệu lực khi reboot hệ thống.
    - *Permanent*: không áp dụng cho hệ thống đang chạy, cần reload mới có hiệu lực, tác dụng vĩnh viễn cả khi reboot hệ thống.

Tìm hiểu và thực hiện các yêu cầu sau (kèm hình minh họa cho từng bước):

- Khởi động tường lửa firewalld

  ```
  $sudo systemctl start firewalld
  ```
- Liệt kê tất cả các zone đang có trong hệ thống

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

  ```
  $firewall-cmd --get-default-zone
  ```
- 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
  ```
- Từ máy vật lý, ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS. Cho biết kết quả.
- 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
  ```
- Từ máy vật lý, ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS. Cho biết kết quả.
- 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.
- 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
  ```
- 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
```

- 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'
```

- 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
```

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

--- Hết ---