**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.*

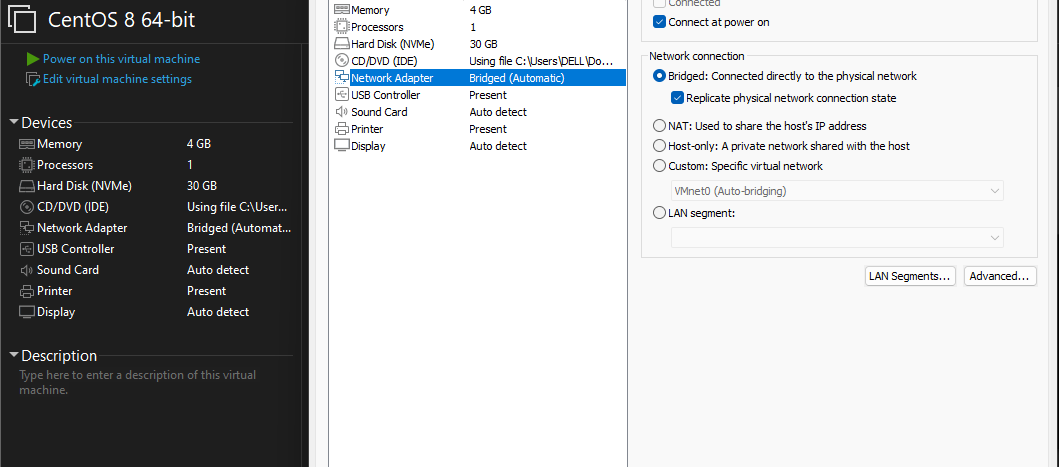
*- Bài nộp phải ở dạng PDF, hình minh họa phải rõ ràng chi tiết.*

1. **Triển khai dịch vụ WEB sử dụng Docker**
   1. Thực hiện cài đặt CentOS 9 vào máy tính cá nhân (hoặc máy ảo).
   2. Cấu hình mạng cho máy ảo giao tiếp được với máy vật lý và kết nối được vào Internet. (Câu 2 - Lab04)
      1. **Đổi cấu hình card mạng của máy ảo sang Bridged Adapter**

- Xem hướng dẫn để khắc phục lỗi card mạng chỉ hiện "not selected" + "no

bridged network adapter is currently selected" (nếu có lỗi).

Đổi cấu hình card mạng của máy ảo sang Bridged Adapter trên VMware



* + 1. **Cấu hình kết nối mạng**

- Hiện NetworkManager trên CentOS 9 đã chuyển sang dùng công cụ nmcli

để cấu hình mạng. Trong bài thực hành sinh viên sẽ sử dụng công cụ này để

cấu hình thay vì sử dụng tập tin ifcfg như trước đây.

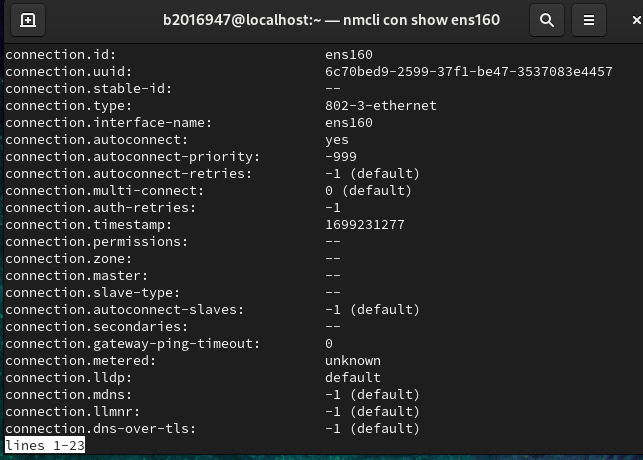
- Hiển thị danh sách các nối kết mạng

$nmcli dev status

****

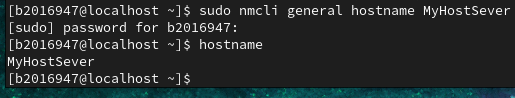
* Hiển thị thông tin của nối một nối kết mạng

$nmcli con show ens160

****

* Đổi tên máy

$sudo nmcli general hostname <tên máy>

****

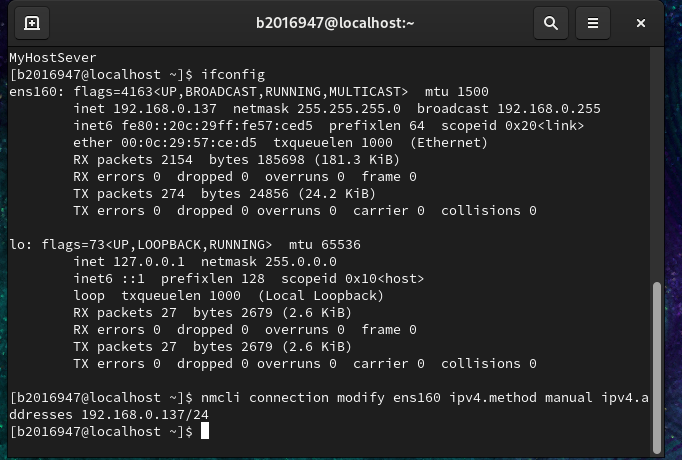
* Chuyển sang chế độ cấu hình tĩnh và cấu hình địa chỉ IPv4

$nmcli con mod <tên nối kết> ipv4.method manual ipv4.addresses <Địa chỉ

IP>/<Netmask>

$nmcli connection modify ens160 ipv4.method manual ipv4.addresses

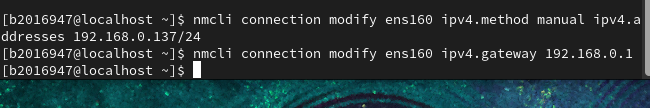
192.168.0.137/24

****

* Cấu hình gateway

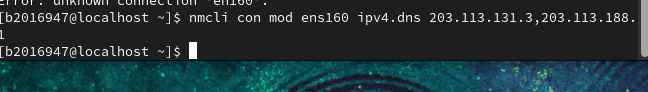
$nmcli con mod <tên nối kết> ipv4.gateway <Địa chỉ gateway>

$nmcli connection modify ens160 ipv4.gateway 192.168.0.1

****

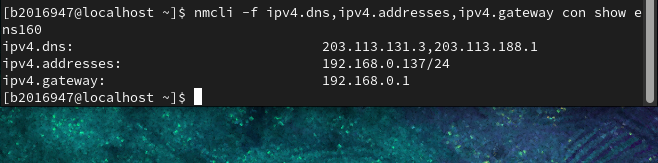
* Cấu hình DNS

$nmcli con mod én160 ipv4.dns 203.113.131.3,203.113.188.1

****

* Xem lại các thông tin đã cấu hình:

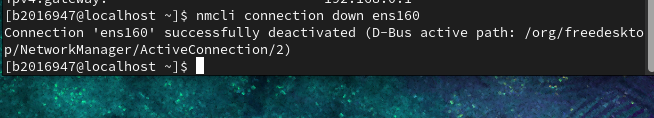
$nmcli -f ipv4.dns,ipv4.addresses,ipv4.gateway con show ens160



* Cập nhật các thay đổi

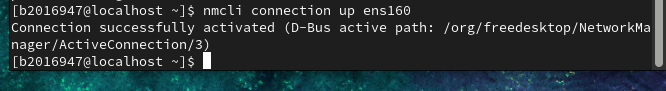
$nmcli con down <tên nối kết>

Tắt kết nối mạng: $nmcli connection down ens160



**$**nmcli con up <tên nối kết>

Bật kết nối mạng: $$nmcli connection up ens160

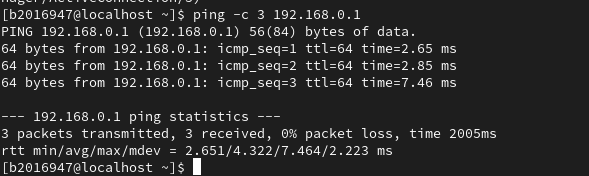


* Kiểm tra nối kết tới gateway, máy vật lý và Internet:

$ping -c 3 <IP của gateway>

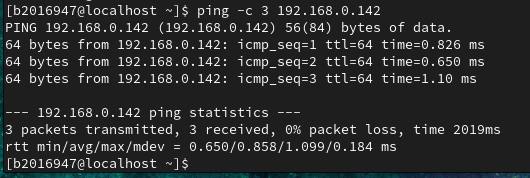
* Kiểm tra kết nối từ máy ảo sang Gateway của máy vật lý:

$ping -c 3 192.168.0.1

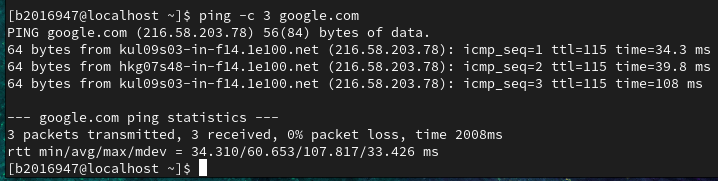
****

* Kiểm tra kết nối từ máy ảo sang địa chỉ IPV4 của máy vật lý:

$ping -c 3 192.168.0.142

****

Kiểm tra kết nối từ máy ảo đến google.com



* 1. 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:

$sudosystemctl stop firewalld

- Cài đặt Apache web server:

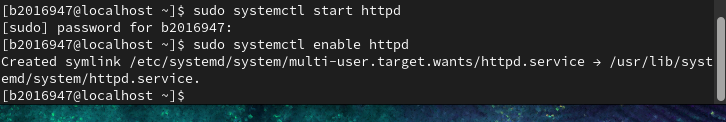
$sudo dnf -y install httpd



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

$sudo systemctl start httpd

$sudo systemctl enable httpd



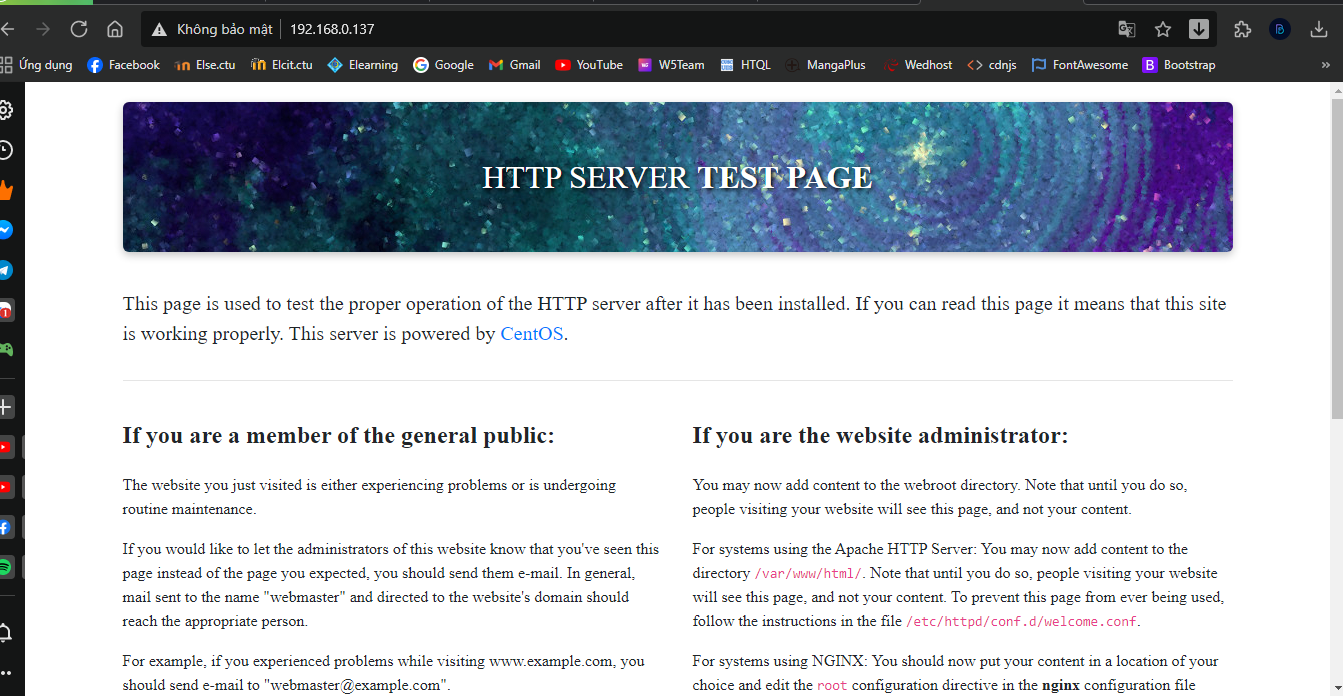
- Tắt tường lửa:

$sudo systemctl stop firewalld



- Trên máy vật lý, mở trình duyệt web và truy cập vào địa chỉ http://<Địa chỉ

IP máy ảo CentOS> để kiểm tra.



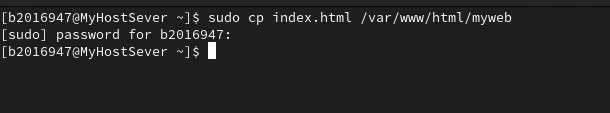
- Tạo thực mục /var/www/html/myweb, sao chép file index.html ở Câu 5 vào

thư mục /var/www/html/myweb

$sudo mkdir /var/www/html/myweb



$sudo cp index.html /var/www/html/myweb



- Trên máy vật lý, mở trình duyệt web và truy cập vào địa chỉ http://<Địa chỉ

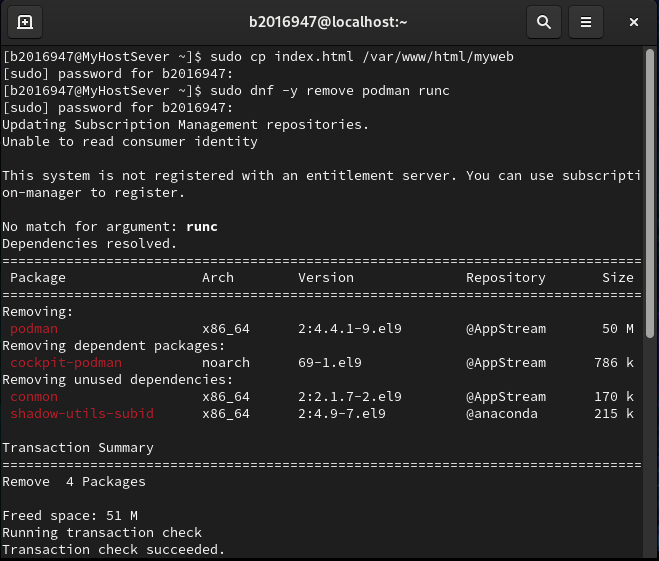
IP máy ảo CentOS>/myweb để kiểm chứng trang web vừa tạo.



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

* 1. Cài đặt Docker lên máy ảo CentOS 9
* Gỡ bỏ PodMan (do sẽ đụng độ với Docker)

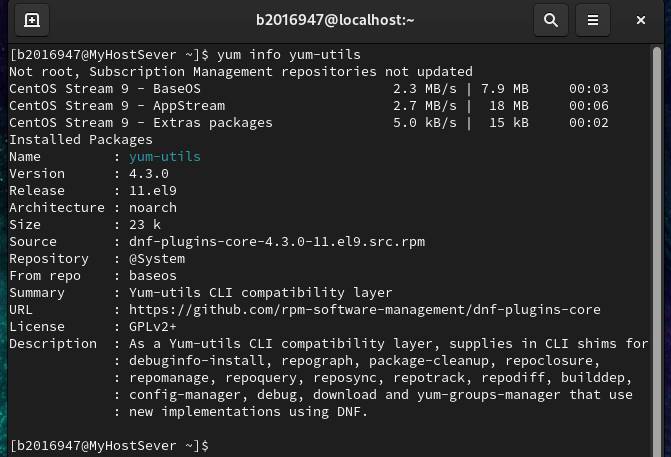
$sudo dnf -y remove podman runc



* Cài đặt công cụ yum-utils

$sudo dnf install -y yum-utils

Đã cài đặt công cụ yum-utils



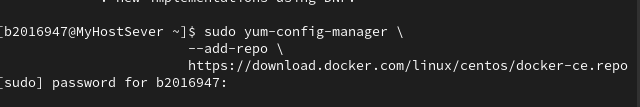
* Thêm địa chỉ repo của Docker vào công cụ yum

$sudo yum-config-manager \

--add-repo \

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

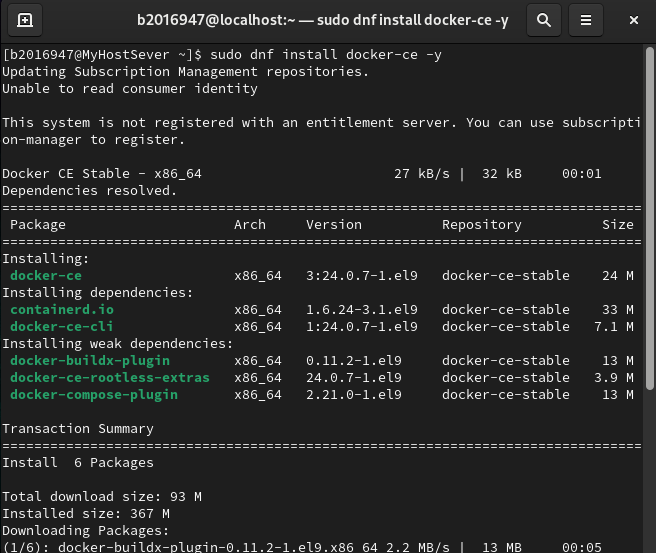
#Viết liên tục lệnh trên hoặc xuống hàng bằng enter.



* Cài đặt Docker

$sudo dnf install docker-ce -y

Đã thực hiện cài đặt docker trên centOS 9



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

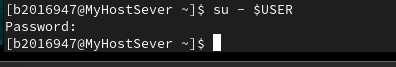
$sudo usermod -aG docker $USER

Đã thực hiện nhóm người dùng hiện tại vào trong group docker/



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

$su - $USER

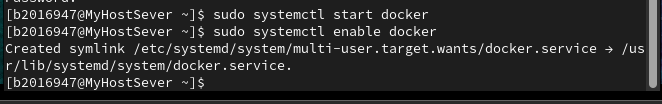


* Chạy dịch vụ Docker

Kích hoạt dịch vụ docker bằng câu lệnh ben dưới

$sudo systemctl start docker

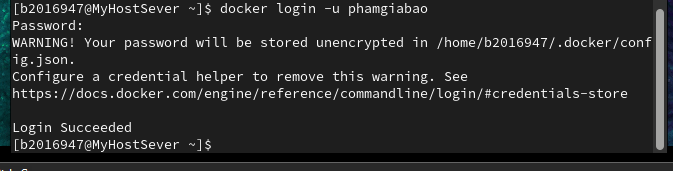
$sudo systemctl enable docker



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

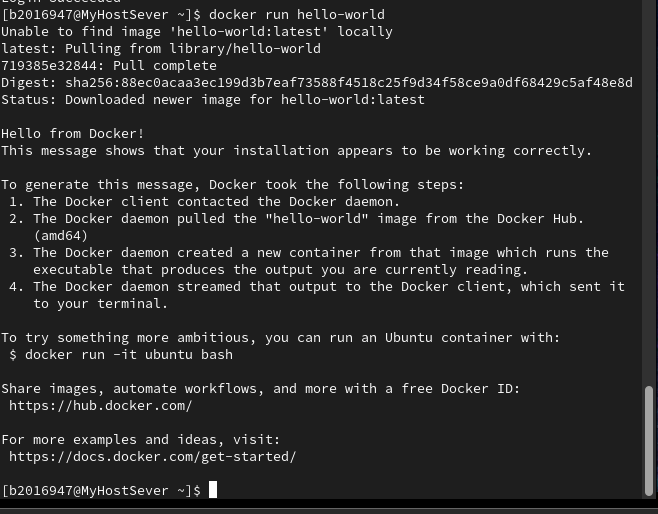
$docker login -u <docker-username>

Đăng nhập thành công trên DockerHub thông qua câu lệnh:**$docker login -u phamgiabao** .Trong terminal Trên centOS9.



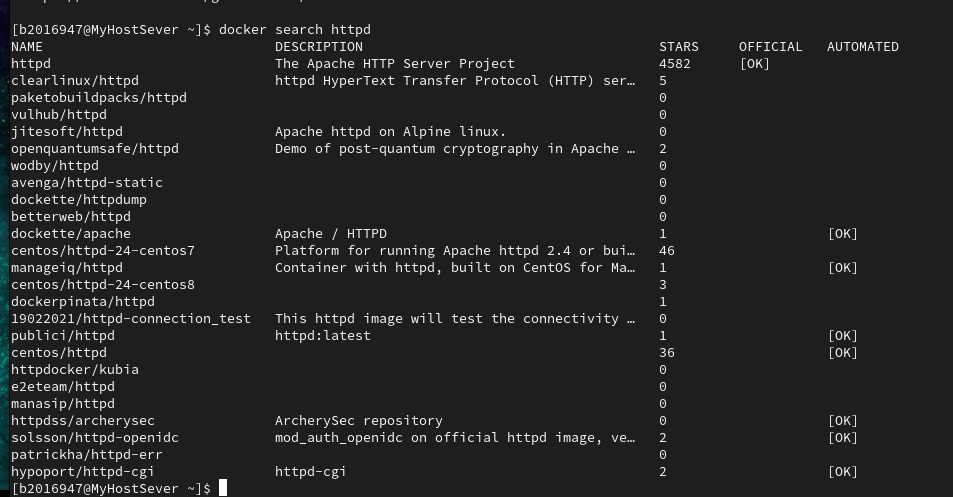
* Kiểm tra docker bằng cách tải image hello-world và tạo container tương ứng. Nếu xuất hiện thông điệp chào mừng từ Docker là cài đặt thành công.

$docker run hello-world



* 1. 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

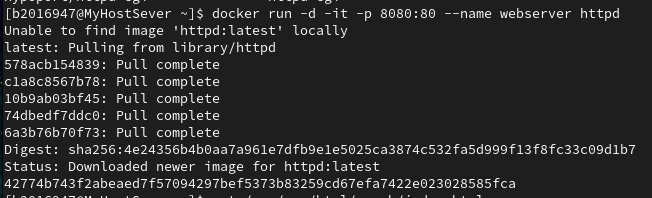
$docker run -d -it -p 8080:80 --name webserver httpd

-d: chạy container ở chế độ background

-it: tạo shell để tương tác với container

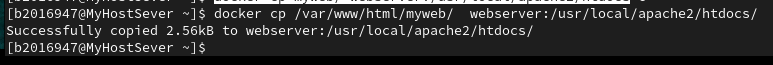
--name webserver: đặt tên container là webserver

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

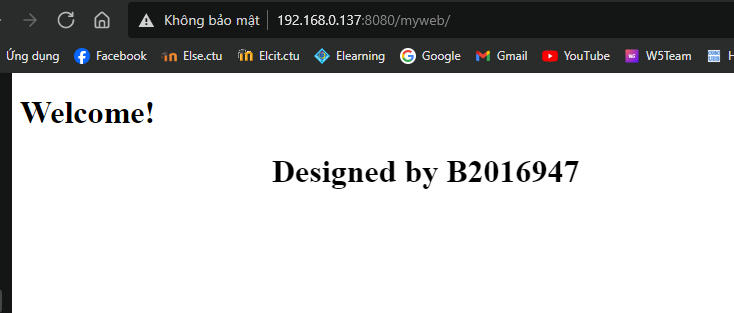


* Sao chép thư mục ~/myweb vào thư mục gốc của dịch vụ của web trên Docker container.

$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.



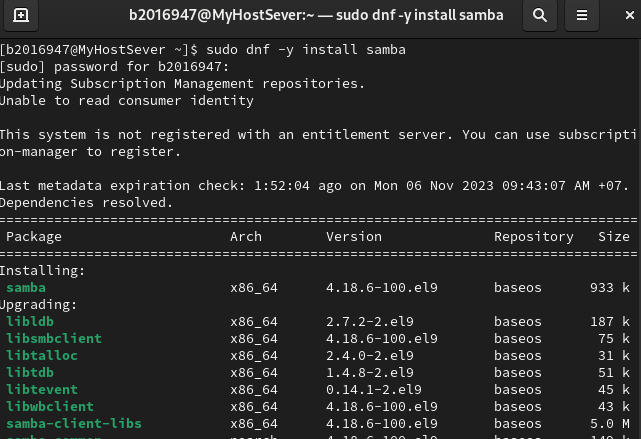
1. **Cài đặt và cấu hình dịch vụ SAMBA**

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:

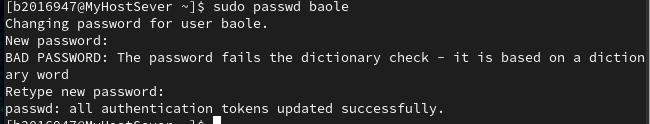
**$sudo adduser baole**

.Lệnh trên dùng để tạo người dùng baole



**$sudo passwd baole**

.Đặt mật khẩu cho người dùng baole



**$sudo groupadd lecturers**

Câu lệnh trên dùng để tạo nhóm tên là lecturers



**$sudo usermod -a -G lecturers baole**

Câu lệnh trên dùng để thêm người dùng baole vào nhóm lecturers



* Tạo thư mục cần chia sẻ và phân quyền:

**$sudo mkdir /data** >>Tạo thư mục data nằm trong thư mục gốc



**$sudo chown :lecturers /data** >> Cấp quyền nhóm sở hữu của thư mục data là lecturers



**$sudo chmod -R 775 /data**  >> Cấp quyền cho thư mục data, thì người sở hữu và nhóm người dùng có quyền đọc, ghi và thực thi. Còn người dùng khác hỉ có quyền đọc và thực thi. Được áp dụng cho toàn bộ thư mục bên trong data



* Cấu hình dịch vụ Samba:

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

Tạo tệp tin cấu hình smb.conf dự phòng mới và lưu tại /etc/samba/



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

Mờ tệp tin /etc/samba/smb.conf để cấu hình

#Thêm đoạn cấu hình bên dưới vào cuối tập tin

[data]

comment = Shared folder for lecturers

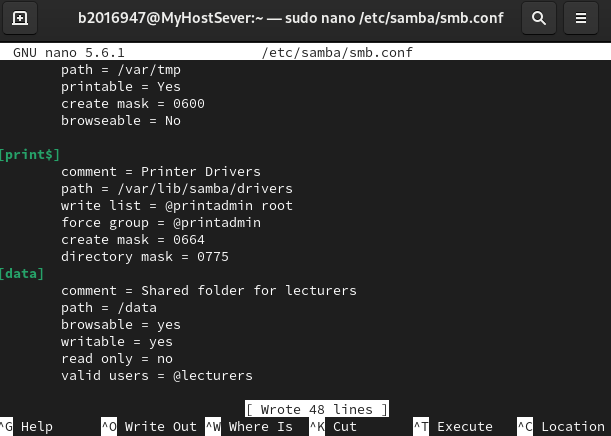
path = /data

browsable = yes

writable = yes

read only = no

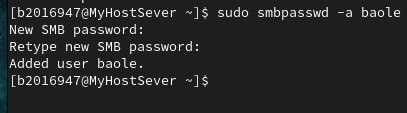
valid users = @lecturers



* Thêm người dùng cho dịch vụ Samba:

**$sudo smbpasswd -a baole** >>Thêm người dùng baole vào dịch vụ samba

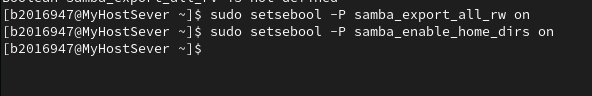
#Đặt mật khẩu Samba cho người dùng



* 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**  >> thực hiện tắt tường lửa

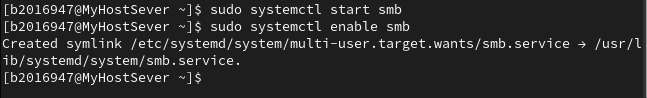


* Khởi động cho phép Samba tự động thực thi khi khởi động hệ điều hành:

**$sudo systemctl start smb**

**$sudo systemctl enable smb**

>> Khởi động dịch vụ samba

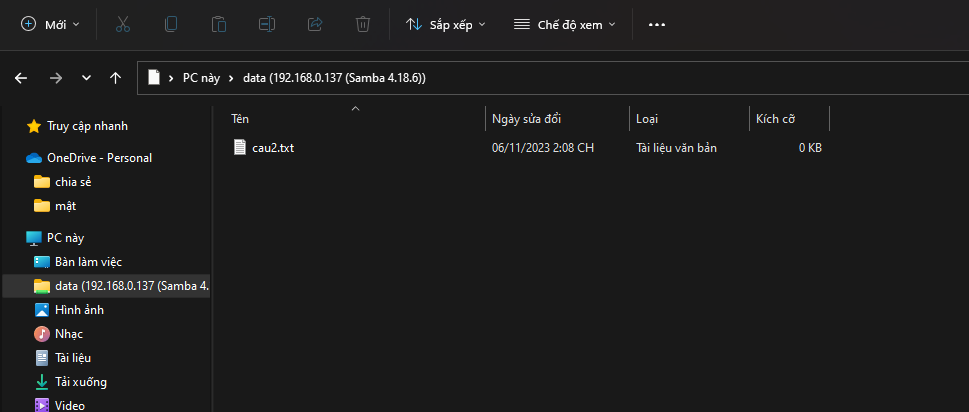


* Trên File Explorer của máy Windows, chọn tính năng “Add a network location” để nối kết tới Samba server sử dụng địa chỉ \\<IP máy CentOS>\data

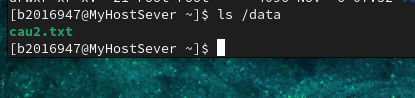
1. Chọn chức năng AddNetWorldLocation sau đó điển địa chỉ ip của máy ảo:

//192.168.0.137/data

1. Tạo tệp tin “cau2.txt” tại thư mục data trên máy vật lý



1. Qua bên máy ảo kiểm tra thấy tồn tại tệp tin “cau2.txt”. Vậy công việc chia sẻ dữ liệu giữa máy thực và máy ảo thành công



1. **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 ?

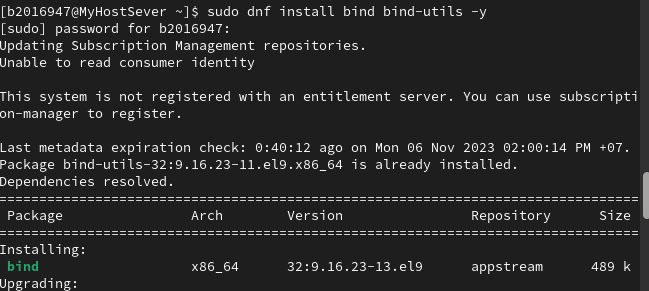
[http://123.30.143.202](http://203.162.36.146) hay <http://www.cit.ctu.edu.vn>

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):

* 1. Cài đặt BIND và các công cụ cần thiết:

$sudo dnf install bind bind-utils -y



* 1. Cấu hình DNS server:

Cấu hình tại tệp tin named.conftrong thư mục/etc

$**sudo nano /etc/named.conf**

#(tham khảo file mẫu)

...

options {

listen-on port 53 { 127.0.0.1; any;}; **#any**; **cho phép các máy tính khác có thể lắng nghe các yêu cầu được gửi đến từ các máy khác đến chúng ta .**..

allow-query { localhost; any; };**#any cho phép các máy tính khác truy vấn tới**

recursion yes;

forwarders {8.8.8.8; }; **#Khi chúng ta cài “**bind bind-utils” **thì nó biến centOS này thành DNS server. Khi DNS server phân giải yêu cầu người dùng , thỉnh thoảng DNS server không phân giải được. Khi đó chúng ta cấu hình** forwarders {8.8.8.8; }; **để chuyển thông tin đó đến máy chủ DNS khác để phân giải giùm, cụ thể là bên DNS vừa cài đặt nếu phân giải thông tin yêu cầu không được thì chuyển thông tin đó qua DNS của google**

..

};

logging {

..

};

};

zone "." IN {

...

};

zone "qtht.com.vn" IN {

type master;

file "forward.qtht";

allow-update { none; };

}; **#Zone là tên miền để dịch vụ DNS cung cấp phân giải cho tên này khi mà có các yêu cầu từ phía máy trạm [Phân giải xuôi: từ tên qua địa chỉ IP]**

zone "1.168.192.in-addr.arpa" IN {

type master;

file "reverse.qtht";

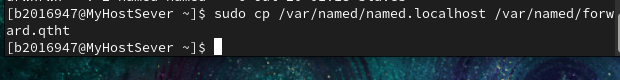
allow-update { none; };

};**[Phân giải Ngược: từ địa chỉ IP qua tên ]**

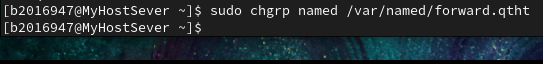
...

* 1. Tạo tập tin cấu hình phân giải xuôi:

**$sudo cp /var/named/named.localhost /var/named/forward.qtht** >> Sao chép tệp tin named.localhost từ /var/named/ và lấy tệp tin sao chép đổi tên thành forward.qtht và lưu tại /var/named/



**$sudo chgrp named /var/named/forward.qtht >>** Chuyển đổi nhóm người sở hữu sang **named**

****

**$sudo nano /var/named/forward.qtht >>** Mở tệp tin **forward.qtht**

#(tham khảo file mẫu)

$TTL 1D

@ IN SOA @ qtht.com.vn. (

0 ;Serial

1D ;Refresh

1H ;Retry

1W ;Expire

3H ;Minimum TTL

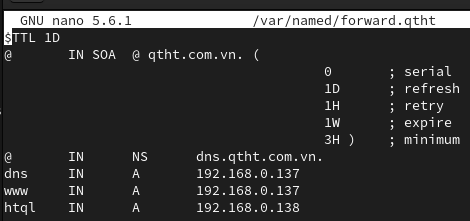
)

@ IN NS dns.qtht.com.vn.

dns IN A 192.168.1.20

www IN A 192.168.1.20

htql IN A 192.168.1.21



* 1. Tạo tập tin cấu hình phân giải ngược:

**$sudo cp /var/named/forward.qtht /var/named/reverse.qtht**

>> Sao chép tệp tin **forward.qtht** từ /var/named/ và lấy tệp tin sao chép đổi tên thành **reverse**.qtht và lưu tại /var/named/

****

**$sudo chgrp named /var/named/reverse.qtht**

**>>** Chuyển đổi nhóm người sở hữu sang **named**

****

**$sudo nano /var/named/reverse.qtht**

>>Mở tệp tin **reverse.qtht**

$TTL 1D

@ IN SOA @ qtht.com.vn. (

0 ;Serial

1D ;Refresh

1H ;Retry

1W ;Expire

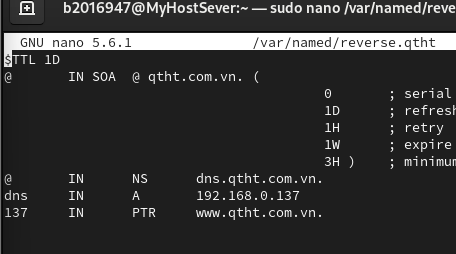
3H ;Minimum TTL

)

@ IN NS dns.qtht.com.vn.

dns IN A 192.168.1.20

20 IN PTR www.qtht.com.vn.



* 1. Kiểm tra và sử dụng dịch vụ DNS
* Tắt tường lửa:

**$sudo systemctl stop firewalld**



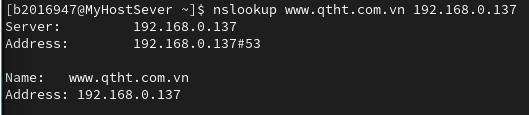
* Khởi động dịch vụ DNS:

**$sudo systemctl start named**



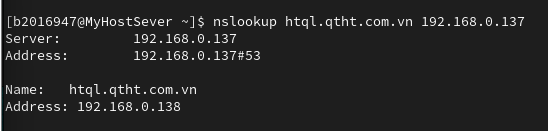
* Kiểm tra kết quả:

**nslookup www.qtht.com.vn 192.168.0.137**

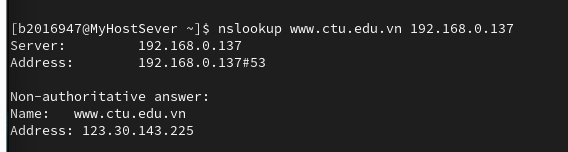
****

**->Phân giải xuôi**

**nslookup htql.qtht.com.vn 192.168.0.137**

****

**nslookup www.ctu.edu.vn 192.168.0.137**

****

* 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

1. **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):

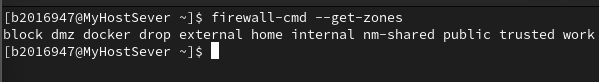
* Khởi động tường lửa firewalld

**$sudo systemctl start firewalld** >> Thực hiện thao tác kích hoạt tường lửa.



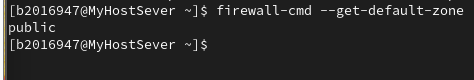
* Liệt kê tất cả các zone đang có trong hệ thống

**$firewall-cmd --get-zones** >> Xem tất cả zone trong hệ thống



* Kiểm tra zone mặc định

**$firewall-cmd --get-default-zone** >>Kiểm tra hiện tại đang thực hiện chạy zone nào

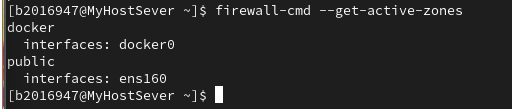


Hiện tại là đang áp dụng zone public.

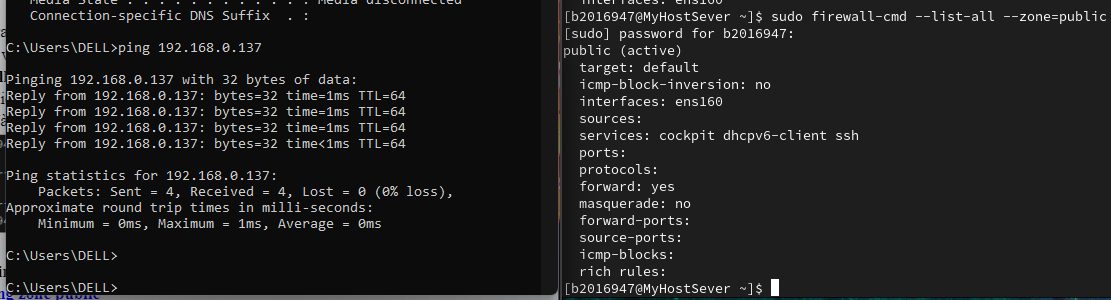
* Kiểm tra zone đang được sử dụng bởi giao diện mạng (thường là *public*); và xem các rules của zone

**$firewall-cmd --get-active-zones**

* Hiện tại zone public đang được sử dụng bởi card mạng ens160
* Và zone docker đang được sử dụng bởi giao diện docker0

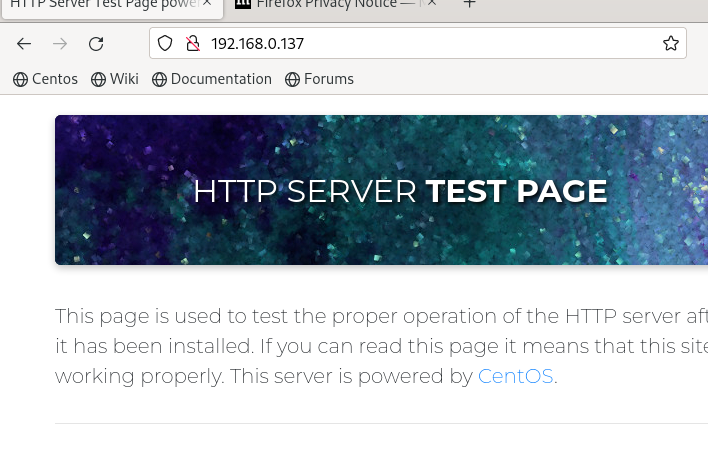


**$sudo firewall-cmd --list-all --zone=public >>Liệt kê các quy định bên trong zone public**

****

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

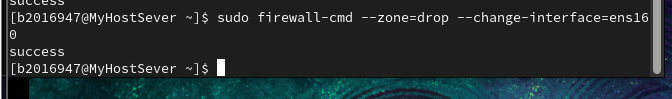
Vì dịch vụ từ zone public không có định nghĩa dịch vụ web. Nên không thể truy cập đến dịch vụ web httpd.



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

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

>> Zone drop này sẽ chặn hết không cho thiết bị nào có thể kết nối đến nó

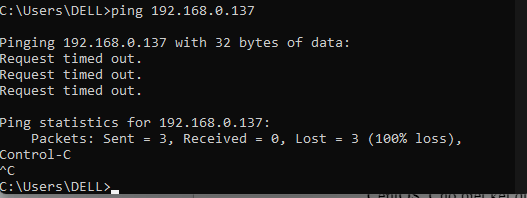


**$sudo firewall-cmd --list-all --zone=drop**

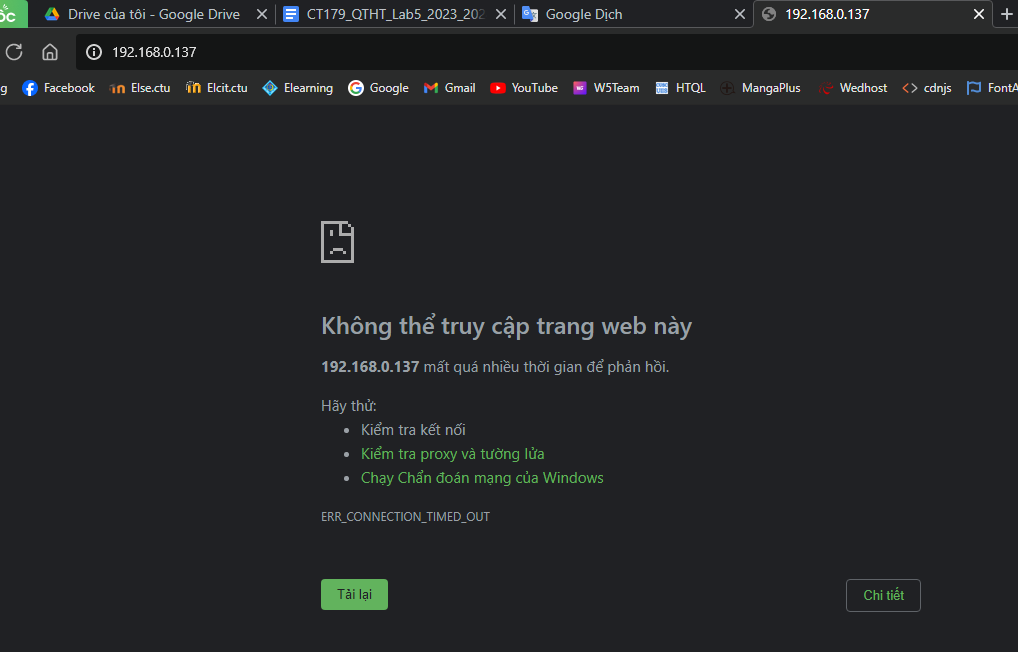
****

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

Từ máy vật lý ping tới IP máy ảo thì thấy không thể ping tới vì zone drop chặn không cho kết nối đến.

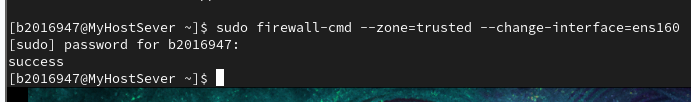


Từ web không thể kết nối đến địa chỉ IP máy ảo vì zone drop chặn không cho kết nối đến.



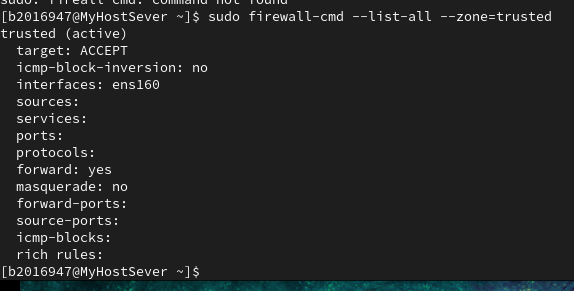
* Chuyển giao diện mạng sang zone *trusted*; và xem các rules của zone

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



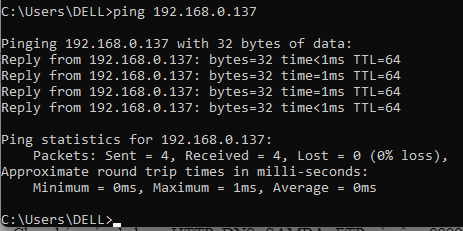
**$sudo firewall-cmd --list-all --zone=truste**d

Thấy phần target của zone trusted cho giá trị là ACCEPT có nghĩa là cho bất ký các thiết bị khác đến kết nối với nó.

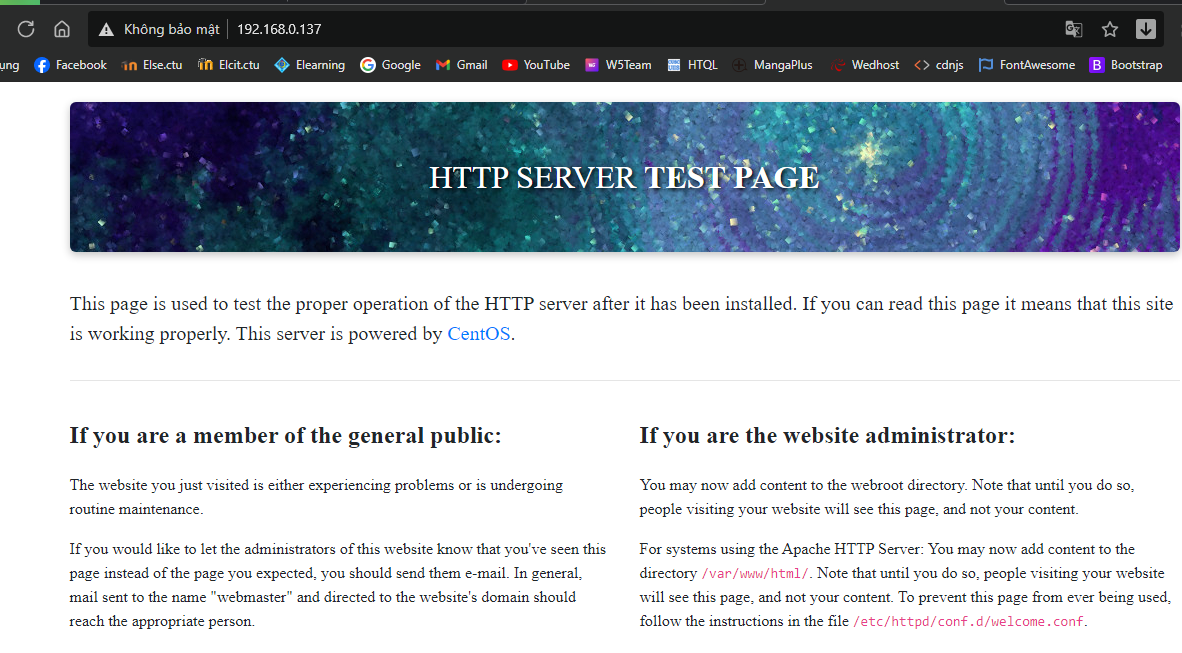


* Từ máy vật lý, ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS. Cho biết kết quả.

Từ máy vật lý thực hiện ping lại đến địa chỉ IP của máy ảo khi zone trong máy ảo là trusted thì cho phép máy vật ký ping tới.



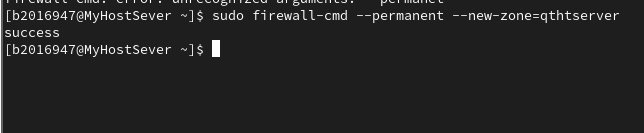
Từ ping đến dịch vụ web



* Tạo zone mới có tên là *qthtserver*

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

***Tạo ra một zone mới có tên là qthtserver và tự áp dụng các quy định cho tường lửa***

******

**$sudo systemctl restart firewalld**

Sau đó thực hiện khởi động lại dịch vụ tường lửa để cho Firewalld áp dụng các quy tắc lên hệ thống và có hiệu lực, tác dụng vĩnh viễn cả khi reboot hệ thống.

****

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

***Thực hiện chuyển đổi zone từ trusted sang 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**

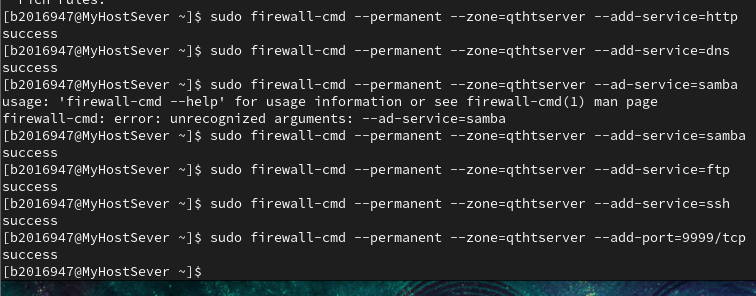
**$sudo firewall-cmd --permanent --zone=*qthtserver* --add-service=samba**

**$sudo firewall-cmd --permanent --zone=*qthtserver* --add-service=ftp**

**$sudo firewall-cmd --permanent --zone=*qthtserver* --add-service=ssh**

**$sudo firewall-cmd --permanent --zone=*qthtserver* --add-port=9999/tcp**

Thực hiện cấu hình cho phép các dịch vụ HTTP, DNS, SAMBA, FTP và bất kỳ cổng nào khác có thể đí qua tường lửa trên zone=*qthtserver*



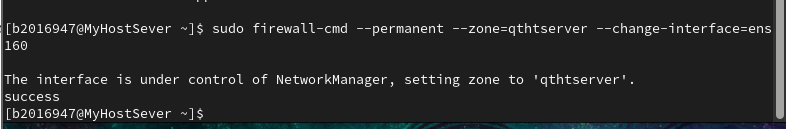
* Khởi động lại tường lửa firewalld

**$sudo systemctl restart firewalld**



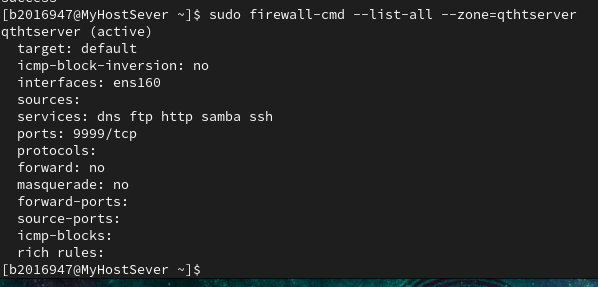
* Chuyển giao diện mạng sang zone qthtserver; và xem các rules của zone

**$sudo firewall-cmd --permanent --zone=qthtserver --change-interface=ens160**



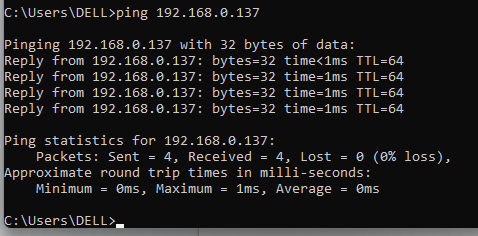
**$sudo firewall-cmd --list-all --zone=qthtserver**

**Xem các quy tâc được áp dụng trên zone=qthtserver**

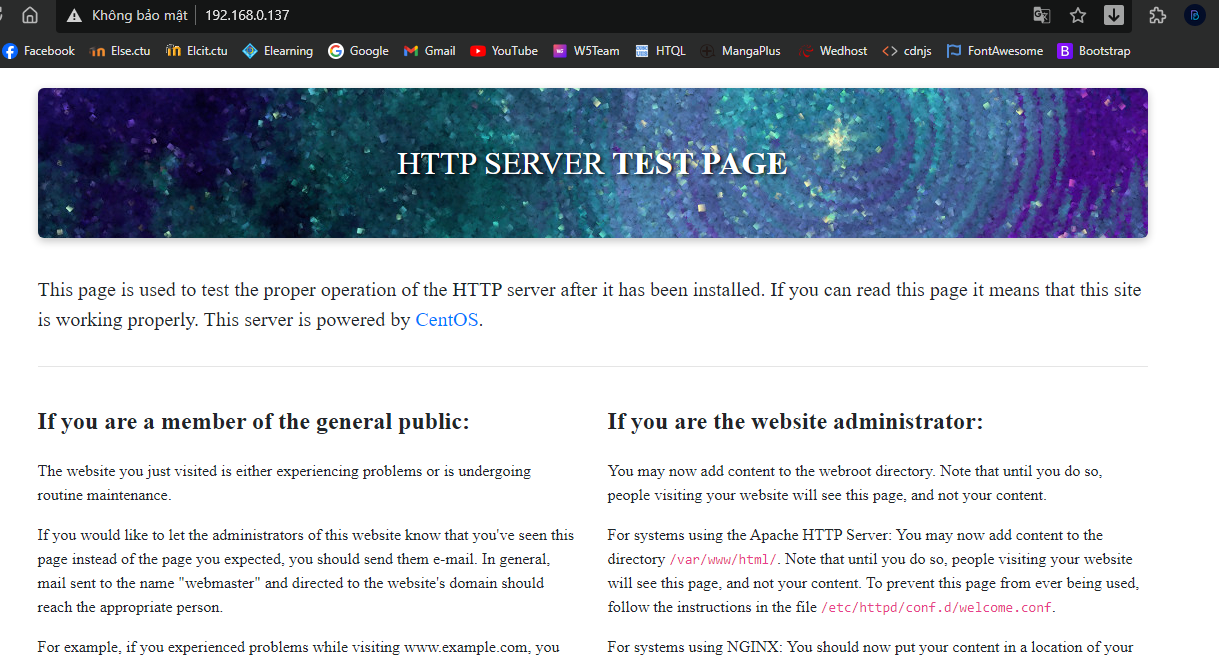
****

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

Từ máy vật lý thực hiện truy cập đến máy áo có thể truy cập được



Truy cập đến dịch vụ web có thể truy cập được



--- Hết ---