



## LAB 5

### DOCKER, SAMBA, DNS và Firewall

Họ tên và MSSV: **Lê Tuấn Đạt - B2113328**

Nhóm học phần: **CT17906**

- 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 họa 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)

- Thông tin cấu hình mạng của máy CentOS trong Câu 2 - Lab04:

```
[B2113328@myserver ~]$ nmcli -f ipv4.addresses,ipv4.gateway,ipv4.dns con show enp0s3
ipv4.addresses:          10.2.67.253/23
ipv4.gateway:            10.2.66.1
ipv4.dns:                203.162.4.190,8.8.8.8
[B2113328@myserver ~]$
```

- Ping đến google.com:

```
[B2113328@myserver ~]$ ping -c 3 google.com
PING google.com (142.250.197.46) 56(84) bytes of data:
64 bytes from nchkg-a-g-in-f14.1e100.net (142.250.197.46): icmp_seq=1 ttl=119 time=31.7 ms
64 bytes from nchkg-a-g-in-f14.1e100.net (142.250.197.46): icmp_seq=2 ttl=119 time=33.9 ms
64 bytes from nchkg-a-g-in-f14.1e100.net (142.250.197.46): icmp_seq=3 ttl=119 time=30.1 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 30.137/31.936/33.937/1.557 ms
[B2113328@myserver ~]$
```

- Ping đến máy vật lý:

```
[B2113328@myserver ~]$ ping -c 3 10.2.67.19
PING 10.2.67.19 (10.2.67.19) 56(84) bytes of data.
64 bytes from 10.2.67.19: icmp_seq=1 ttl=128 time=1.57 ms
64 bytes from 10.2.67.19: icmp_seq=2 ttl=128 time=0.464 ms
64 bytes from 10.2.67.19: icmp_seq=3 ttl=128 time=0.350 ms

--- 10.2.67.19 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.350/0.794/1.569/0.549 ms
[B2113328@myserver ~]$
```

- Ping từ máy vật lý:

```
PS C:\Users\LE TUAN DAT> ping 10.2.67.253

Pinging 10.2.67.253 with 32 bytes of data:
Reply from 10.2.67.253: bytes=32 time<1ms TTL=64
Reply from 10.2.67.253: bytes=32 time<1ms TTL=64
Reply from 10.2.67.253: bytes=32 time<1ms TTL=64
Reply from 10.2.67.253: bytes=32 time<1ms TTL=64

Ping statistics for 10.2.67.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\LE TUAN DAT>
```

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

```
[B2113328@myserver ~]$ ls -l
total 24
-rw-r--r--. 1 B2113328 B2113328 6508 Oct 16 22:10 370198946_195235066899021_3903443868681036681_n.jpg
-rwxr-xr-x. 1 B2113328 B2113328 317 Oct 7 20:55 backup.sh
drwxr-xr-x. 2 B2113328 B2113328 6 Aug 24 16:08 Desktop
drwxr-xr-x. 2 B2113328 B2113328 6 Sep 1 15:35 Documents
drwxr-xr-x. 2 B2113328 B2113328 52 Aug 24 16:11 Downloads
-rw-r--r--. 1 B2113328 B2113328 214 Oct 16 22:48 index.html
-rwxr-xr-x. 1 B2113328 B2113328 368 Oct 7 20:46 info.sh
drwxr-xr-x. 2 B2113328 B2113328 6 Aug 24 16:08 Music
drwxr-xr-x. 2 B2113328 B2113328 6 Aug 24 16:08 Pictures
drwxr-xr-x. 2 B2113328 B2113328 6 Aug 24 16:08 Public
drwxr-xr-x. 2 B2113328 B2113328 24 Oct 7 21:12 safe_rm_recycle
-rwxr-xr-x. 1 B2113328 B2113328 215 Oct 7 21:11 safe_rm.sh
drwxr-xr-x. 2 B2113328 B2113328 6 Aug 24 16:08 Templates
drwxr-xr-x. 2 B2113328 B2113328 6 Aug 24 16:08 Videos
[B2113328@myserver ~]$ mkdir myweb
[B2113328@myserver ~]$ mv index.html myweb/index.html
[B2113328@myserver ~]$ ls -l myweb
total 4
-rw-r--r--. 1 B2113328 B2113328 214 Oct 16 22:48 index.html
[B2113328@myserver ~]$
```

Tắt tường lửa:

```
$sudo systemctl stop firewalld
```

```
[B2113328@myserver ~]$ sudo systemctl stop firewalld
[sudo] password for B2113328:
[B2113328@myserver ~]$ sudo systemctl status firewalld
○ firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
   Active: inactive (dead) since Mon 2024-10-28 09:27:00 +07; 12s ago
```

**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 chạy với Docker)

```
$sudo dnf -y remove podman runc
```

```
[B2113328@myserver ~]$ sudo dnf -y remove podman runc
```

```
Removed:
  cockpit-podman-93.1-1.el9.noarch                common-3:2.1.12-1.el9.x86_64
  passt-0^20240806.gee36266-2.el9.x86_64         passt-selinux-0^20240806.gee36266-2.el9.noarch
  podman-4:5.2.3-6.el9.x86_64
Complete!
```

- Cài đặt công cụ yum-utils

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

```
[B2113328@myserver ~]$ sudo dnf install -y yum-utils
```

```
Upgraded:
  dnf-plugins-core-4.3.0-17.el9.noarch             python3-dnf-plugins-core-4.3.0-17.el9.noarch
Installed:
  yum-utils-4.3.0-17.el9.noarch
```

- 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.**

```
[B2113328@myserver ~]$ sudo yum-config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo
Adding repo from: https://download.docker.com/linux/centos/docker-ce.repo
[B2113328@myserver ~]$
```

- Cài đặt Docker

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

```
[B2113328@myserver ~]$ sudo dnf install docker-ce -y
```

```
Installed:
  containerd.io-1.7.22-3.1.el9.x86_64              docker-buildx-plugin-0.17.1-1.el9.x86_64
  docker-ce-3:27.3.1-1.el9.x86_64                 docker-ce-cli-1:27.3.1-1.el9.x86_64
  docker-ce-rootless-extras-27.3.1-1.el9.x86_64    docker-compose-plugin-2.29.7-1.el9.x86_64
```

- 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
```

```
[B2113328@myserver ~]$ sudo usermod -aG docker $USER  
[B2113328@myserver ~]$
```

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

```
$su - $USER
```

```
[B2113328@myserver ~]$ su - $USER  
Password:  
[B2113328@myserver ~]$
```

- Chạy dịch vụ Docker

```
$sudo systemctl start docker
```

```
$sudo systemctl enable docker
```

```
[B2113328@myserver ~]$ sudo systemctl start docker  
[B2113328@myserver ~]$ sudo systemctl enable docker  
Created symlink /etc/systemd/system/multi-user.target.wants/docker.service → /usr/lib/systemd/system/docker.service.  
[B2113328@myserver ~]$
```

```
[B2113328@myserver ~]$ sudo systemctl status docker  
● docker.service - Docker Application Container Engine  
   Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; preset: disabled)  
   Active: active (running) since Mon 2024-10-28 09:34:50 +07; 28s ago
```

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

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

```
[B2113328@myserver ~]$ docker login -u dattuanle  
Password:  
WARNING! Your password will be stored unencrypted in /home/B2113328/.docker/config.json.  
Configure a credential helper to remove this warning. See  
https://docs.docker.com/engine/reference/commandline/login/#credential-stores  
  
Login Succeeded  
[B2113328@myserver ~]$
```

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

```
$docker run hello-world
```



```
[B2113328@myserver ~]$ docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
c1ec31eb5944: Pull complete
Digest: sha256:d211f485f2dd1dee407a80973c8f129f00d54604d2c90732e8e320e5038a0348
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/

[B2113328@myserver ~]$
```

**1.5.** Triển khai dịch vụ web server lên máy ảo CentOS 9 sử dụng một Docker container

- Tìm kiếm image với từ khóa httpd, kết quả sẽ thấy 1 image tên httpd ở dòng đầu tiên.

\$docker search httpd

```
[B2113328@myserver ~]$ docker search httpd
```

NAME	DESCRIPTION	STARS	OFFICIAL
httpd	The Apache HTTP Server Project	4804	[OK]
manageiq/httpd	Container with httpd, built on CentOS for Ma...	1	
paketobuildpacks/httpd		0	
vulhub/httpd		0	
jitesoft/httpd	Apache httpd on Alpine linux.	0	
openquantumsafe/httpd	Demo of post-quantum cryptography in Apache ...	14	
openeuler/httpd		0	
betterweb/httpd		0	
dockerpinata/httpd		1	
centos/httpd		36	

- Tạo container từ image httpd

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

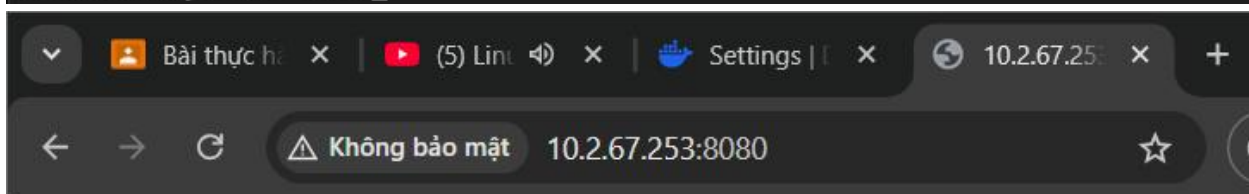
-d: chạy container ở chế độ background

-it: tạo shell để tương tác với container

--name webserver: đặt tên container là webserver

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

```
[B2113328@myserver ~]$ docker run -d -it -p 8080:80 --name webserver httpd
Unable to find image 'httpd:latest' locally
latest: Pulling from library/httpd
a480a496ba95: Pull complete
3a2663e66670: Pull complete
4f4fb700ef54: Pull complete
dbde712f81fb: Pull complete
867b2ea3628d: Pull complete
6bd9d3710aae: Pull complete
Digest: sha256:bbea29057f25d9543e6a96a8e3cc7c7c937206d20eab2323f478fdb2469d536d
Status: Downloaded newer image for httpd:latest
13b66d7b55cb4ea862db57cf636cb0e58ff594c00d0d5d53337d109c4d3b511a
[B2113328@myserver ~]$
```



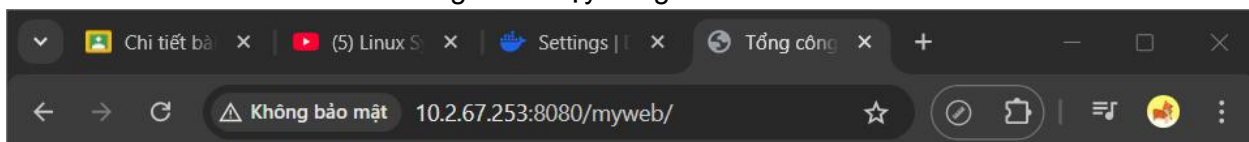
## It works!

- 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/
```

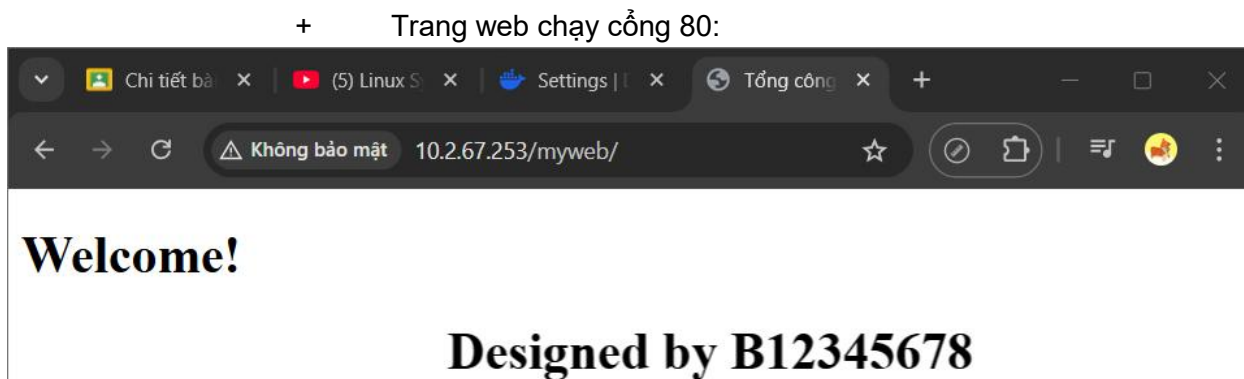
```
[B2113328@myserver ~]$ docker cp myweb/ webserver:/usr/local/apache2/htdocs/
Successfully copied 2.56kB to webserver:/usr/local/apache2/htdocs/
[B2113328@myserver ~]$
```

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



## Welcome!

Designed by B2113328



## 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.

**Tim 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
```

```
[B2113328@myserver ~]$ sudo dnf install -y samba
```

Installed:

libnetapi-4.20.2-2.el9.x86\_64

samba-common-tools-4.20.2-2.el9.x86\_64

samba-ldb-ldap-modules-4.20.2-2.el9.x86\_64

samba-4.20.2-2.el9.x86\_64

samba-dcerpc-4.20.2-2.el9.x86\_64

samba-libs-4.20.2-2.el9.x86\_64

- 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
```

```
[B2113328@myserver ~]$ sudo adduser tuanthai
```

```
[B2113328@myserver ~]$ sudo passwd tuanthai
```

```
Changing password for user tuanthai.
```

```
New password:
```

```
BAD PASSWORD: The password is shorter than 8 characters
```

```
Retype new password:
```

```
passwd: all authentication tokens updated successfully.
```

```
[B2113328@myserver ~]$
```

```
[B2113328@myserver ~]$ sudo groupadd lecturers
```

```
[B2113328@myserver ~]$ sudo usermod -aG lecturers tuanthai
```

```
[B2113328@myserver ~]$
```

- Tạo thư mục cần chia sẻ và phân quyền:

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

(\*) Do đã tồn tại thư mục data, nên sẽ tạo data\_1.

```
[B2113328@myserver ~]$ sudo mkdir /data_1
[B2113328@myserver ~]$ sudo chown :lecturers /data_1
[B2113328@myserver ~]$ sudo chmod -R 775 /data_1
[B2113328@myserver ~]$ ls -l /
total 24
dr-xr-xr-x.  2 root root          6 Jun 25 21:23 afs
lrwxrwxrwx.  1 root root          7 Jun 25 21:23 bin -> usr/bin
dr-xr-xr-x.  5 root root    4096 Oct 28 09:13 boot
drwxr-xr-x.  2 root root          6 Sep 20 18:35 data
drwxrwxr-x.  2 root lecturers    6 Oct 28 10:05 data_1
```

- 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
```

```
[B2113328@myserver ~]$ sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.orig
[B2113328@myserver ~]$
```

```
[B2113328@myserver ~]$ sudo nano /etc/samba/smb.conf
[B2113328@myserver ~]$
```

```
[data_1]
    comment = Shared folder for lecturers
    path = /data_1
    browsable = yes
    writeable = 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
```



```
[B2113328@myserver ~]$ sudo smbpasswd -a tuanthai
New SMB password:
Retype new SMB password:
Added user tuanthai.
[B2113328@myserver ~]$
```

- Cấu hình SELINUX cho phép Samba

```
$sudo setsebool -P samba_export_all_rw on
$sudo setsebool -P samba_enable_home_dirs on
```

```
[B2113328@myserver ~]$ sudo setsebool -P samba_export_all_rw on
[B2113328@myserver ~]$ sudo setsebool -P samba_enable_home_dirs on
[B2113328@myserver ~]$
```

- Tắt tường lửa:

```
$sudo systemctl stop firewalld
```

```
[B2113328@myserver ~]$ sudo systemctl stop firewalld
[B2113328@myserver ~]$ sudo systemctl status firewalld
○ firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
   Active: inactive (dead) since Mon 2024-10-28 09:27:00 +07; 45min ago
```

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

```
$sudo systemctl start smb
$sudo systemctl enable smb
```

```
[B2113328@myserver ~]$ sudo systemctl start smb
[B2113328@myserver ~]$ sudo systemctl enable smb
Created symlink /etc/systemd/system/multi-user.target.wants/smb.service → /usr/lib/systemd/system/smb.service.
[B2113328@myserver ~]$ sudo systemctl status smb
● smb.service - Samba SMB Daemon
   Loaded: loaded (/usr/lib/systemd/system/smb.service; enabled; preset: disabled)
   Active: active (running) since Mon 2024-10-28 10:13:18 +07; 14s ago
```

- 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

← Add Network Location

### Specify the location of your website

Type the address of the website, FTP site, or network location that this shortcut will open.

Internet or network address:

\\10.2.67.253\data\_1

Browse...

[View examples](#)

```
▼ This PC
> data_1 (10.2.67.253 (Samba 4.20.2))

[B2113328@myserver ~]$ ls /data_1
abc.txt
[B2113328@myserver ~]$ cat /data_1/abc.txt
Hello Samba!
[B2113328@myserver ~]$
```

### 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
```

```
[B2113328@myserver ~]$ sudo dnf install bind bind-utils -y
```

```
Installed:
bind-32:9.16.23-24.el9.x86_64          bind-dnssec-doc-32:9.16.23-24.el9.noarch
bind-dnssec-utils-32:9.16.23-24.el9.x86_64  python3-bind-32:9.16.23-24.el9.noarch
python3-ply-3.11-14.el9.noarch
```

#### 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; };
};
...
```

```
[B2113328@myserver ~]$ sudo nano /etc/named.conf
[B2113328@myserver ~]$
```

```
options {
    listen-on port 53 { 127.0.0.1; any;};
```

```
allow-query { localhost; any;};
```

```
recursion yes;
forwarders {203.162.4.190; };
```

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

zone "67.2.10.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

```

```

[B2113328@myserver ~]$ sudo cp /var/named/named.localhost /var/named/forward.qtht
[B2113328@myserver ~]$ sudo ls -l /var/named/
total 20
drwxrwx---. 2 named named    6 Sep  5 21:12 data
drwxrwx---. 2 named named    6 Sep  5 21:12 dynamic
-rw-r-----. 1 root  root   152 Oct 28 10:44 forward.qtht
-rw-r-----. 1 root  named 2112 Sep  5 21:12 named.ca
-rw-r-----. 1 root  named  152 Sep  5 21:12 named.empty
-rw-r-----. 1 root  named  152 Sep  5 21:12 named.localhost
-rw-r-----. 1 root  named  168 Sep  5 21:12 named.loopback
drwxrwx---. 2 named named    6 Sep  5 21:12 slaves
[B2113328@myserver ~]$

```

```

[B2113328@myserver ~]$ sudo chgrp named /var/named/forward.qtht
[B2113328@myserver ~]$ sudo ls -l /var/named/
total 20
drwxrwx---. 2 named named    6 Sep  5 21:12 data
drwxrwx---. 2 named named    6 Sep  5 21:12 dynamic
-rw-r-----. 1 root  named  152 Oct 28 10:44 forward.qtht
-rw-r-----. 1 root  named 2112 Sep  5 21:12 named.ca
-rw-r-----. 1 root  named  152 Sep  5 21:12 named.empty
-rw-r-----. 1 root  named  152 Sep  5 21:12 named.localhost
-rw-r-----. 1 root  named  168 Sep  5 21:12 named.loopback
drwxrwx---. 2 named named    6 Sep  5 21:12 slaves
[B2113328@myserver ~]$

```

```

[B2113328@myserver ~]$ sudo nano /var/named/forward.qtht
[B2113328@myserver ~]$

```

```

$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      10.2.67.253
www     IN      A      10.2.67.253
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.
```

```
[B2113328@myserver ~]$ sudo cp /var/named/forward.qtht /var/named/reverse.qtht
[B2113328@myserver ~]$ sudo chgrp named /var/named/reverse.qtht
[B2113328@myserver ~]$
```

```
[B2113328@myserver ~]$ sudo nano /var/named/reverse.qtht
[B2113328@myserver ~]$
```

```
$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    10.2.67.253
253    IN      PTR  www.qtht.com.vn
```

### 3.5. Kiểm tra và sử dụng dịch vụ DNS

- Tắt tường lửa:

```
$sudo systemctl stop firewalld
```

```
[B2113328@myserver ~]$ sudo systemctl stop firewalld
[B2113328@myserver ~]$ sudo systemctl status firewalld
○ firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
   Active: inactive (dead) since Mon 2024-10-28 09:27:00 +07; 1h 25min ago
```



- Khởi động dịch vụ DNS:

```
$sudo systemctl start named
```

```
[B2113328@myserver ~]$ sudo systemctl start named
[B2113328@myserver ~]$ 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 Mon 2024-10-28 10:53:28 +07; 11s ago
```

- Kiểm tra kết quả:

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

```
[B2113328@myserver ~]$ nslookup www.qtht.com.vn 10.2.67.253
Server:          10.2.67.253
Address:         10.2.67.253#53

Name:   www.qtht.com.vn
Address: 10.2.67.253

[B2113328@myserver ~]$
```

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

```
[B2113328@myserver ~]$ nslookup htql.qtht.com.vn 10.2.67.253
Server:          10.2.67.253
Address:         10.2.67.253#53

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

[B2113328@myserver ~]$
```

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

```
[B2113328@myserver ~]$ nslookup www.ctu.edu.vn 10.2.67.253
Server:          10.2.67.253
Address:         10.2.67.253#53

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

[B2113328@myserver ~]$
```

```
PS C:\Users\LE TUAN DAT> nslookup www.qtht.com.vn 10.2.67.253
Server:      www.qtht.com.vn.67.2.10.in-addr.arpa
Address: 10.2.67.253

Name:   www.qtht.com.vn
Address: 10.2.67.253

PS C:\Users\LE TUAN DAT> nslookup htql.qtht.com.vn 10.2.67.253
Server:      www.qtht.com.vn.67.2.10.in-addr.arpa
Address: 10.2.67.253

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

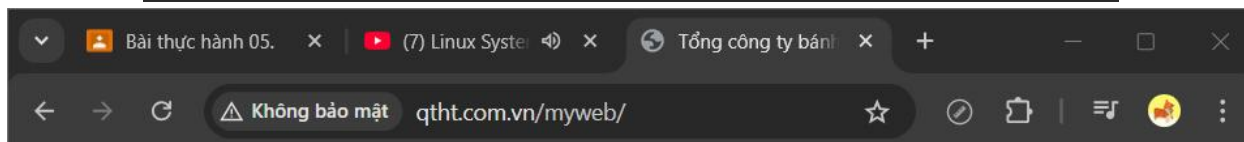
PS C:\Users\LE TUAN DAT> nslookup www.ctu.edu.vn 10.2.67.253
Server:      www.qtht.com.vn.67.2.10.in-addr.arpa
Address: 10.2.67.253

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

PS C:\Users\LE TUAN DAT>
```

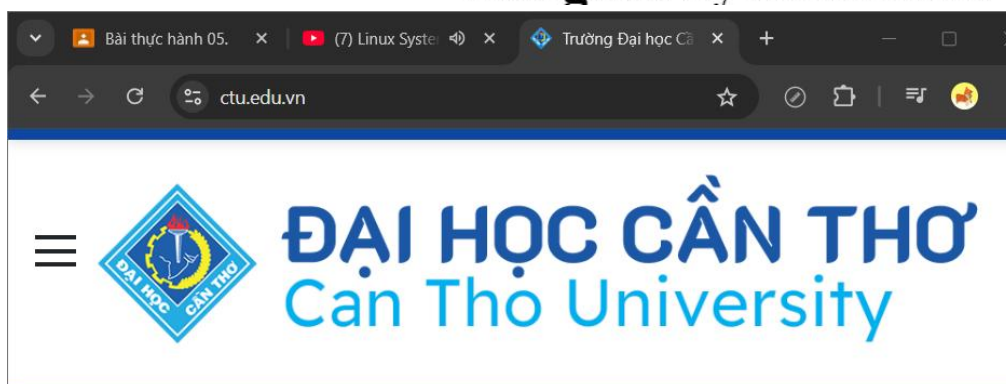
- Trên máy vật lý, cấu hình DNS server là IP của máy ảo CentOS. Sau đó, mở trình duyệt web và truy cập vào địa chỉ <http://www.qtht.com.vn/myweb>

```
DNS server assignment:      Manual
IPv4 DNS servers:          10.2.67.253 (Unencrypted)
```



**Welcome!**

**Designed by B12345678**



#### 4. Cấu hình tường lửa Firewallld

Công cụ Firewallld (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 Firewallld được thay thế cho tường lửa iptables với những khác biệt cơ bản:

- Firewallld 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.
- Firewallld 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.

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

- Khởi động tường lửa firewallld

```
$sudo systemctl start firewallld
```

```
[B2113328@myserver ~]$ sudo systemctl start firewallld
[B2113328@myserver ~]$ sudo systemctl status firewallld
● firewallld.service - firewallld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewallld.service; enabled; preset: enabled)
   Active: active (running) since Mon 2024-10-28 11:07:06 +07; 4s ago
```

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

```
$firewall-cmd --get-zones
```

```
[B2113328@myserver ~]$ firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
[B2113328@myserver ~]$
```

- Kiểm tra zone mặc định

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

```
[B2113328@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
```

```
[B2113328@myserver ~]$ firewall-cmd --get-active-zone
public
  interfaces: enp0s3
[B2113328@myserver ~]$
```

```
[B2113328@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:
[B2113328@myserver ~]$
```

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

```
PS C:\Users\LE TUAN DAT> ping 10.2.67.253

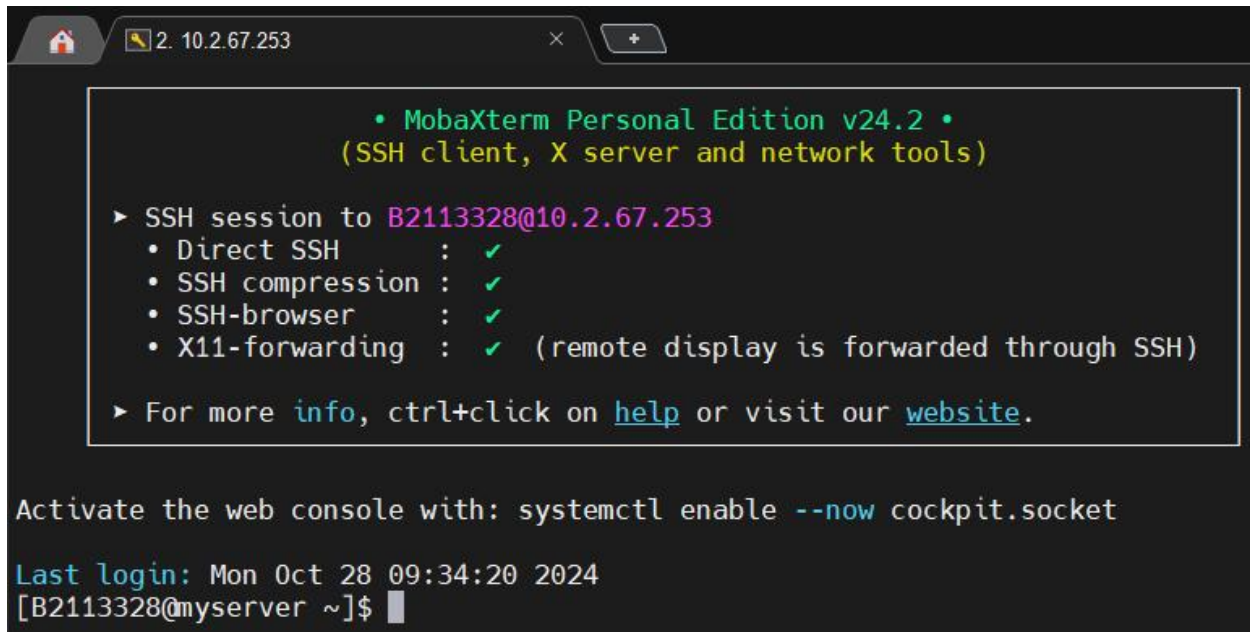
Pinging 10.2.67.253 with 32 bytes of data:
Reply from 10.2.67.253: bytes=32 time=1ms TTL=64
Reply from 10.2.67.253: bytes=32 time<1ms TTL=64
Reply from 10.2.67.253: bytes=32 time<1ms TTL=64
Reply from 10.2.67.253: bytes=32 time<1ms TTL=64

Ping statistics for 10.2.67.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\LE TUAN DAT>
```

```
[B2113328@myserver ~]$ sudo nano /etc/ssh/sshd_config
[B2113328@myserver ~]$
```

```
!PasswordAuthentication yes
```

```
[B2113328@myserver ~]$ sudo systemctl restart sshd
[B2113328@myserver ~]$
```



```
• MobaXterm Personal Edition v24.2 •
(SSH client, X server and network tools)

► SSH session to B2113328@10.2.67.253
  • Direct SSH      : ✓
  • SSH compression : ✓
  • SSH-browser     : ✓
  • X11-forwarding  : ✓ (remote display is forwarded through SSH)

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

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

Last login: Mon Oct 28 09:34:20 2024
[B2113328@myserver ~]$
```

=> Không sử dụng dịch vụ Web được do zone *public* không có dịch vụ http.

- 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

```
[B2113328@myserver ~]$ sudo firewall-cmd --zone=drop --change-interface=enp0s3
success
[B2113328@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:
[B2113328@myserver ~]$
```

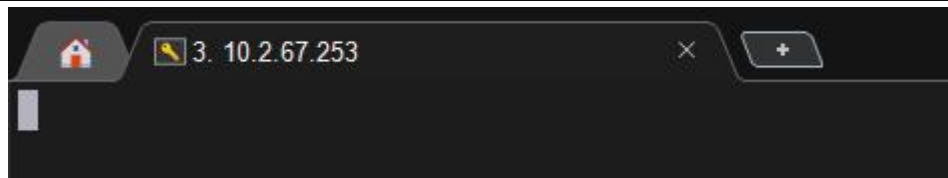
- Từ máy vật lý, ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS. Cho biết kết quả.



```
PS C:\Users\LE TUAN DAT> ping 10.2.67.253

Pinging 10.2.67.253 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 10.2.67.253:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
PS C:\Users\LE TUAN DAT>
```



- 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

```
[B2113328@myserver ~]$ sudo firewall-cmd --zone=trusted --change-interface=enp0s3
success
[B2113328@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:
[B2113328@myserver ~]$
```

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

```
PS C:\Users\LE TUAN DAT> ping 10.2.67.253
```

```
Pinging 10.2.67.253 with 32 bytes of data:
```

```
Reply from 10.2.67.253: bytes=32 time<1ms TTL=64
```

```
Reply from 10.2.67.253: bytes=32 time<1ms TTL=64
```

```
Reply from 10.2.67.253: bytes=32 time<1ms TTL=64
```

```
Reply from 10.2.67.253: bytes=32 time<1ms TTL=64
```


```
Ping statistics for 10.2.67.253:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
    Approximate round trip times in milli-seconds:
```

```
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
PS C:\Users\LE TUAN DAT> |
```


 4. 10.2.67.253

• MobaXterm Personal Edition v24.2 •  
(SSH client, X server and network tools)

- ▶ SSH session to **B2113328@10.2.67.253**
  - Direct SSH : ✓
  - SSH compression : ✓
  - SSH-browser : ✓
  - X11-forwarding : ✓ (remote display is forwarded through SSH)
- ▶ For more [info](#), ctrl+click on [help](#) or visit our [website](#).

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

Last login: Mon Oct 28 11:15:51 2024 from **10.2.67.19**  
[B2113328@myserver ~]\$

 CentOS

HTTP Server Test Page

- 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
```

```
[B2113328@myserver ~]$ sudo firewall-cmd --permanent --new-zone=qthtserver
success
[B2113328@myserver ~]$ sudo systemctl restart firewalld
[B2113328@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:
[B2113328@myserver ~]$
```

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

```
$sudo firewall-cmd --permanent --zone=qthtserver --add-service=http
```

```
$sudo firewall-cmd --permanent --zone=qthtserver --add-service=dns
```

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

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

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

```
[B2113328@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=http
success
[B2113328@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=dns
success
[B2113328@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=samba
success
[B2113328@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=ftp
success
[B2113328@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-port=9999/tcp
success
[B2113328@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'
```

```
[B2113328@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-rich-rule='rule family=ipv4 source ad
dress=10.2.67.19/32 port port=22 protocol=tcp accept'
success
[B2113328@myserver ~]$
```

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

```
[B2113328@myserver ~]$ sudo systemctl restart firewalld
[B2113328@myserver ~]$
```

- 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

```
[B2113328@myserver ~]$ sudo firewall-cmd --zone=qthtserver --change-interface=enp0s3
success
[B2113328@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="10.2.67.19/32" port port="22" protocol="tcp" accept
[B2113328@myserver ~]$
```

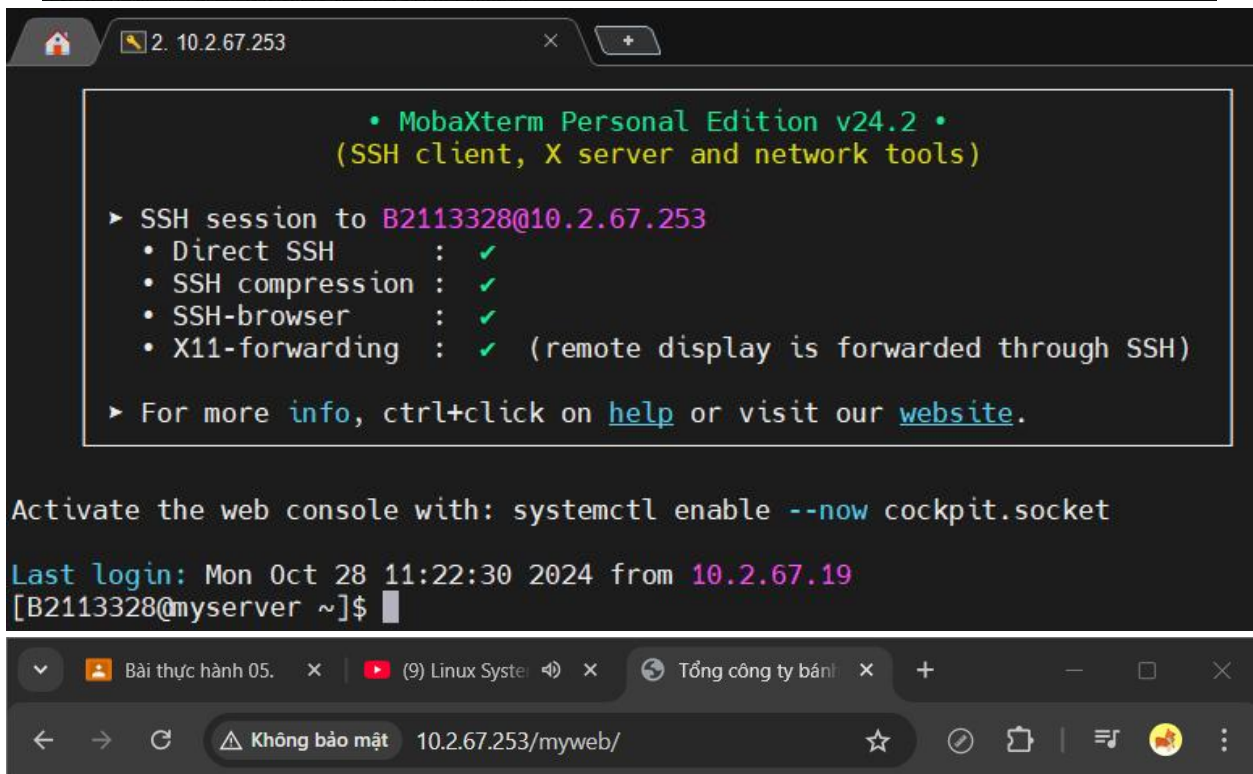
- Kiểm tra máy vật lý có thể truy cập được tới các dịch vụ trên máy CentOS hay không.



```
PS C:\Users\LE TUAN DAT> ping 10.2.67.253

Pinging 10.2.67.253 with 32 bytes of data:
Reply from 10.2.67.253: bytes=32 time<1ms TTL=64
Reply from 10.2.67.253: bytes=32 time<1ms TTL=64
Reply from 10.2.67.253: bytes=32 time<1ms TTL=64
Reply from 10.2.67.253: bytes=32 time<1ms TTL=64

Ping statistics for 10.2.67.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\LE TUAN DAT>
```



**Welcome!**

**Designed by B12345678**

+ Nếu đổi địa chỉ IP máy vật lý thành:



IP address

10.2.67.20

Subnet mask

255.255.254.0

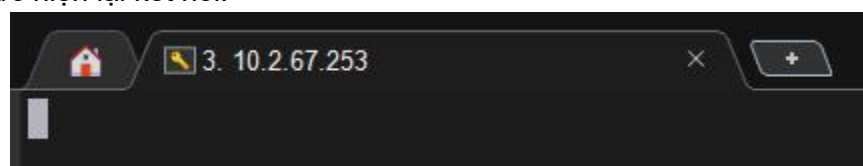
Gateway

10.2.66.1

Preferred DNS

10.2.66.1

=> Thực hiện lại kết nối:



=> Không kết nối được

--- Hết ---