



LAB 5

SAMBA, DNS và Firewall

Họ tên và MSSV: Lê Tuấn Kiệt - B1909935

Nhóm học phần: 2

- 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. Cài đặt CentOS

(KHÔNG cần hình minh họa):

- 1.1. Thực hiện cài đặt CentOS 6 (hoặc CentOS 7/8) 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.
- 1.3. Cài đặt dịch vụ Web server trên máy ảo. Tạo một trang web đơn giản `index.html` lưu vào thư mục `/var/www/html/myweb`
- 1.4. Nếu sử dụng CentOS 6 thì cần thay đổi file cấu hình của yum theo hướng dẫn [ở đây](#).

2. Cài đặt và cấu hình dịch vụ SAMBA

Samba là dịch vụ chia sẻ file giữa các nền tảng 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):

- 2.1. Cài đặt dịch vụ Samba: `yum install samba`

```
Installed:
samba-4.12.3-12.el8.3.x86_64      samba-common-tools-4.12.3-12.el8.3.x86_64
samba-libs-4.12.3-12.el8.3.x86_64

Complete!
```

==> Bạn có thể gõ `samba --version` để kiểm tra đã cài đặt chưa.

2.2. Tạo người dùng và nhóm người dùng chia sẻ dữ liệu:

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

```
[root@zen b1909935]# adduser tuanthai
[root@zen b1909935]# passwd tuanthai
Changing password for user tuanthai.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@zen b1909935]# groupadd lecturers
[root@zen b1909935]# usermod -aG lecturers tuanthai
[root@zen b1909935]# groups tuanthai
tuanthai : tuanthai lecturers
```

2.3. Tạo thư mục cần chia sẻ và phân quyền:

```
mkdir /data
chgrp lecturers /data
chmod -R 775 /data
```

```
[root@zen ~]# mkdir /data
[root@zen ~]# chgrp lecturers /data
[root@zen ~]# chmod -R 775 /data
[root@zen ~]# ls -l /
total 76
lrwxrwxrwx. 1 root root 7 Nov 3 2020 bin -> usr/bin
dr-xr-xr-x. 5 root root 4096 May 9 03:52 boot
drwxrwxr-x. 2 root lecturers 4096 May 9 11:12 data
drwxr-xr-x. 21 root root 3500 May 9 03:52 dev
drwxr-xr-x. 147 root root 12288 May 9 11:06 etc
drwxr-xr-x. 6 root root 4096 May 9 11:04 home
-rw-r--r--. 1 root root 221 May 3 20:35 index.html
lrwxrwxrwx. 1 root root 7 Nov 3 2020 lib -> usr/lib
lrwxrwxrwx. 1 root root 9 Nov 3 2020 lib64 -> usr/lib64
drwx-----. 2 root root 16384 Mar 14 20:41 lost+found
drwxr-xr-x. 2 root root 4096 Nov 3 2020 media
drwxr-xr-x. 2 root root 4096 Nov 3 2020 mnt
drwxr-xr-x. 3 root root 4096 May 3 19:52 opt
dr-xr-xr-x. 282 root root 0 May 9 10:51 proc
dr-xr-x---. 7 root root 4096 May 3 18:47 root
drwxr-xr-x. 44 root root 1300 May 9 10:59 run
lrwxrwxrwx. 1 root root 8 Nov 3 2020 sbin -> usr/sbin
drwxr-xr-x. 2 root root 4096 Nov 3 2020 srv
dr-xr-xr-x. 13 root root 0 May 9 03:51 sys
drwxrwxrwt. 21 root root 4096 May 9 11:11 tmp
drwxr-xr-x. 12 root root 4096 Mar 14 20:43 usr
drwxr-xr-x. 22 root root 4096 Mar 27 13:38 var
```

2.4. Cấu hình dịch vụ Samba:

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

...

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

```
[root@zen ~]# cp /etc/samba/smb.conf /etc/samba/smb.conf.orig
[root@zen ~]# gedit /etc/samba/smb.conf
```

Open  smb.conf /etc/samba Save  

```
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
```

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

Plain Text ▾ Tab Width: 8 ▾ Ln 42, Col 21 ▾ INS

💡 Giải thích chi tiết :

- `comment` : chú thích
- `path` : đường dẫn đến thư mục cần kết nối Samba
- `browseable` : kiểm soát việc chia sẻ file có được nhìn thấy trong chế độ thực
- `writable` : Cho phép ghi file (đảo ngược với `read only`)
- `read only` : Chỉ cho phép đọc (đảo ngược với `read only`)
- `valid users` : người dùng có hiệu lực

=> Tham khảo cách **config** [tại đây](#)

- 2.5. Thêm người dùng cho dịch vụ Samba: `smbpasswd -a tuanthai`

```
[root@zen ~]# smbpasswd -a tuanthai
New SMB password:
Retype new SMB password:
Added user tuanthai.
```

- 2.6. Cấu hình SELINUX cho phép Samba

```
setsebool -P samba_export_all_rw on
setsebool -P samba_enable_home_dirs on
```

- `samba_export_all_rw` : cho phép xuất bất kỳ files hay directories nào, cho phép quyền đọc và ghi
- `samba_enable_home_dirs on` : cho phép chia sẻ thư mục chính của người dùng

==> Tham khảo [tại đây](#)

- 2.7. Tắt tường lửa: `service iptables stop`

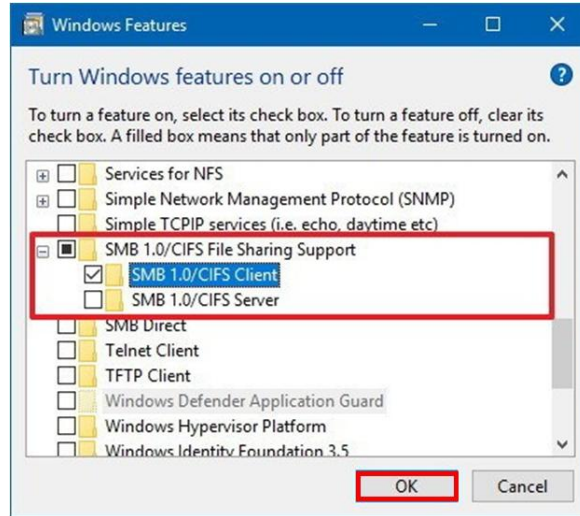
```
[root@zen ~]# service iptables stop
Redirecting to /bin/systemctl stop iptables.service
[root@zen ~]# service iptables status
Redirecting to /bin/systemctl status iptables.service
● iptables.service - IPv4 firewall with iptables
   Loaded: loaded (/usr/lib/systemd/system/iptables.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
```

- 2.8. Khởi động dịch vụ Samba: `service smb start`

```
[root@zen ~]# service smb start
Redirecting to /bin/systemctl start smb.service
[root@zen ~]# service smb status
Redirecting to /bin/systemctl status smb.service
● smb.service - Samba SMB Daemon
   Loaded: loaded (/usr/lib/systemd/system/smb.service; disabled; vendor preset: disabled)
   Active: active (running) since Sun 2021-05-09 11:19:45 +07; 5s ago
     Docs: man:smbd(8)
           man:samba(7)
           man:smb.conf(5)
  Main PID: 12651 (smbd)
    Status: "smbd: ready to serve connections..."
     Tasks: 4 (limit: 74046)
  Memory: 16.9M
   CGroup: /system.slice/smb.service
           └─12651 /usr/sbin/smbd --foreground --no-process-group
             └─12653 /usr/sbin/smbd --foreground --no-process-group
               └─12654 /usr/sbin/smbd --foreground --no-process-group
                 └─12655 /usr/sbin/smbd --foreground --no-process-group

May 09 11:19:45 zen systemd[1]: Starting Samba SMB Daemon...
May 09 11:19:45 zen systemd[1]: Started Samba SMB Daemon.
May 09 11:19:45 zen smbd[12651]: [2021/05/09 11:19:45.661284, 0] ../../lib/util/bec
May 09 11:19:45 zen smbd[12651]: daemon_ready: daemon 'smbd' finished starting up
```

- 2.9. Trên máy Windows, bật tính năng hỗ trợ SMB1: mở Control Panel -> Programs -> Turn Windows features on or off -> SMB 1.0/CIFS File Sharing Support -> chọn SMB 1.0/CIFS Client



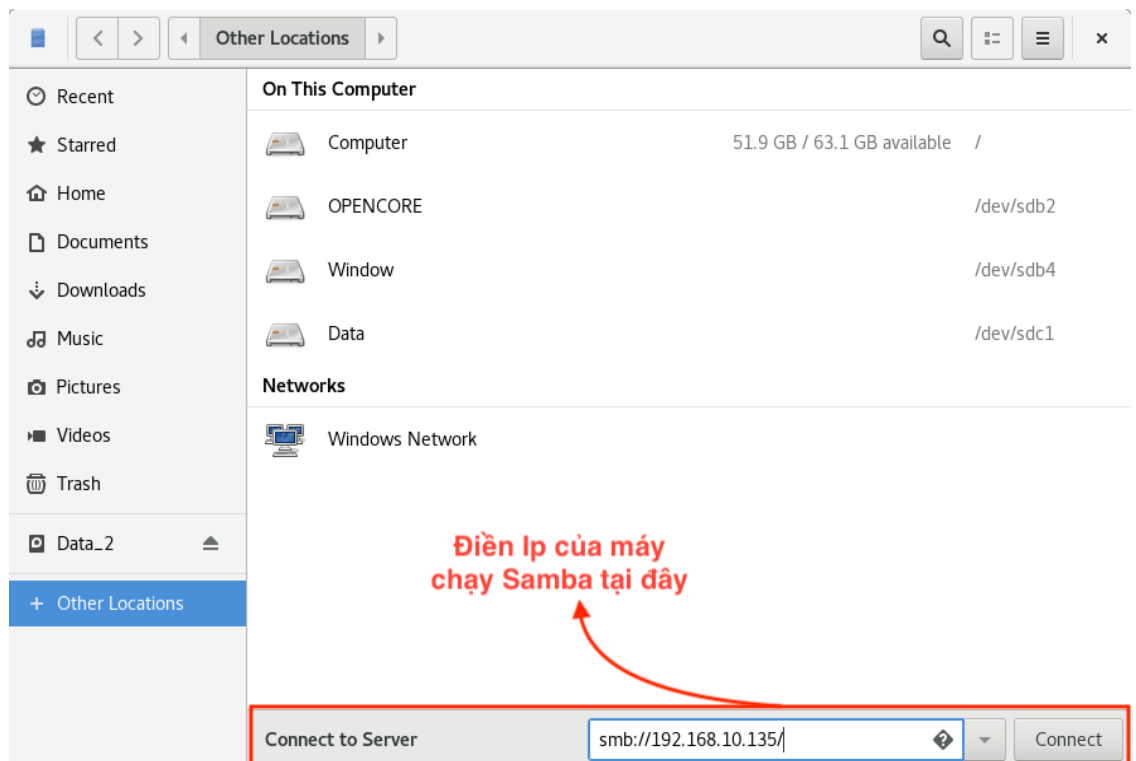
Nếu thực hành trong phòng máy của Khoa CNTT & TT có thể phải khởi động lại máy Windows. Trong trường hợp này sinh viên có thể qua bước 2.10

Cài CentOS trên ổ cứng, không sử dụng máy ảo, nên không làm bước này

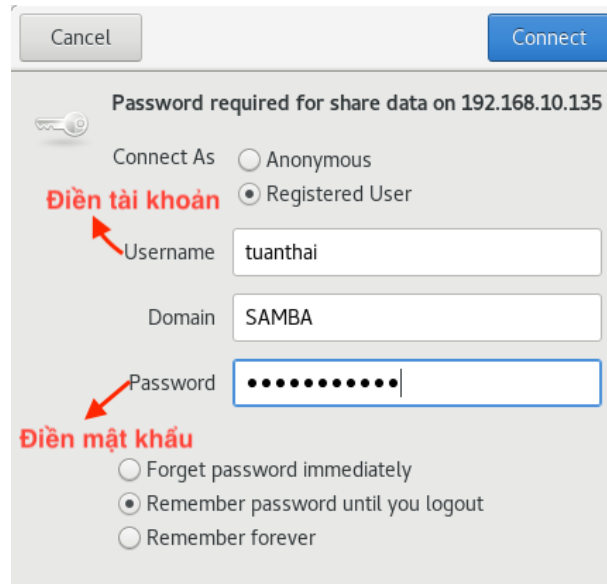
- 2.10. Trên File Explorer, chọn tính năng Add a network location để nối kết tới Samba server sử dụng địa chỉ \\<IP máy CentOS>\data

Thực hiện các bước sau để kết nối giao thức Samba trên CentOS :

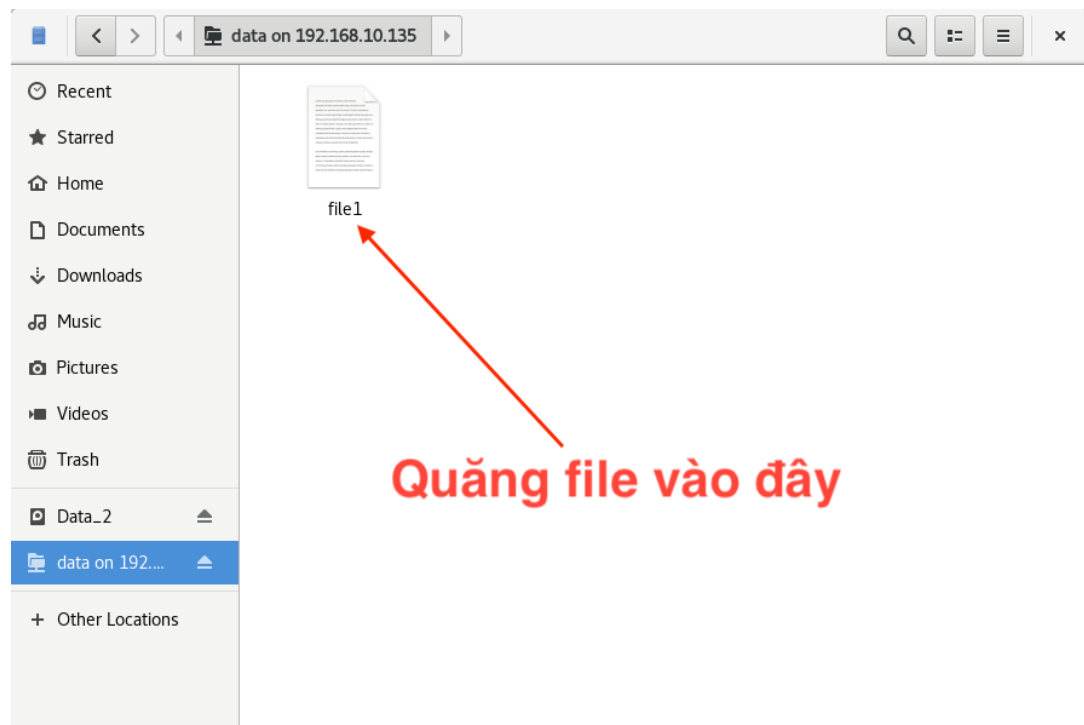
- B1: Vào Nautilus (hay còn gọi là Finder) ⇒ Chọn Other Locations ⇒ Điền IP của máy chạy Samba ⇒ Chọn Connect



- **B2:** Chọn **Registered User** và điền **tài khoản** và **mật khẩu** đăng ký **Samba** ở trên ⇒ Chọn **Connect**



- **B3:** Bạn có thể tạo **file** (ví dụ tạo **file1** như sau)



💡 Vào máy kết nối **Samba** kiểm tra như sau :

```
[root@zen Desktop]# ls -l /data
total 8
-rwxr--r--. 1 tuanthai tuanthai 49 May  9 12:07 file1
```

==> Như đã thấy **file1** đã xuất hiện

3. Cài đặt và cấu hình dịch vụ DNS

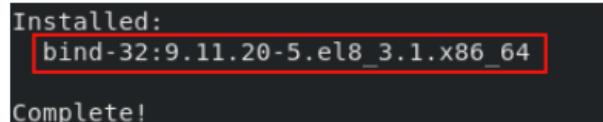
DNS (Domain Name System) là giải pháp dùng tên miền thay cho địa chỉ IP khó nhớ khi sử dụng các dịch vụ trên mạng. Truy cập đến website của Khoa CNTT-ĐH Cần thơ bằng địa chỉ nào để nhớ hơn ?

<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):

3.1. Cài đặt BIND và các công cụ cần thiết: `yum install bind bind-utils`



```
Installed:
bind-32:9.11.20-5.el8_3.1.x86_64
Complete!
```

==> Bạn có thể gõ `named -v` để kiểm tra `bind-utils` đã cài chưa.

3.2. Cấu hình DNS server: `nano /etc/named.conf` (tham khảo file mẫu)

```
...
options {
    listen-on port 53 { 127.0.0.1; any; };
    ...
    allow-query      { localhost; any; };
    recursion yes;
    ..
};

logging {
    ..
};

zone "." IN {
    ...
};

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

zone "33.30.172.in-addr.arpa" IN {
    type master;
    file "reverse.qtht";
```

```
allow-update { none; };

};

...
```

```
named.conf
/etc

//
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;

dnsssec-enable yes;
dnsssec-validation yes;
```

```
named.conf
/etc

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; };
};

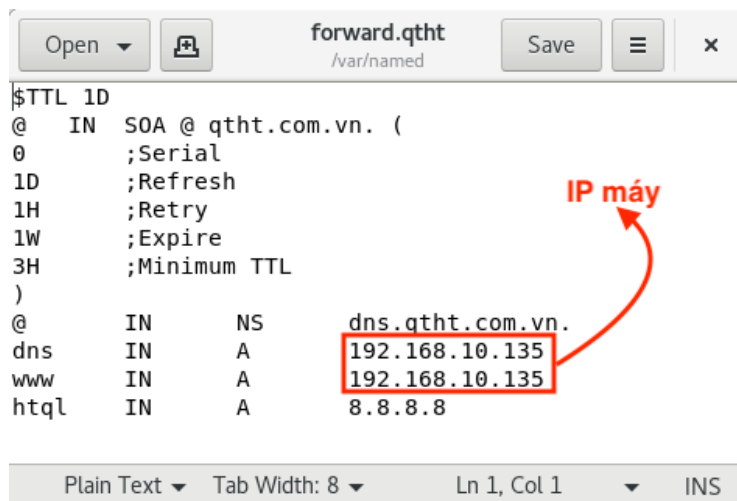
zone "10.168.192.in-addr.arpa" IN {
type master;
file "reverse.qtht";
allow-update { none; };
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```


3.3. Tạo tập tin cấu hình phân giải xuôi:

```
cp /var/named/named.localhost /var/named/forward.qtht
chgrp named /var/named/forward.qtht
nano /var/named/forward.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    172.30.33.245
www    IN      A    172.30.33.245
htql   IN      A    8.8.8.8
```



3.4. Tạo tập tin cấu hình phân giải ngược:

```
cp /var/named/forward.qtht /var/named/reverse.qtht
chgrp named /var/named/reverse.qtht
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    192.168.10.135
www    IN      A    192.168.10.135
htql   IN      A    8.8.8.8
```

```
@      IN      NS      dns.qtht.com.vn.
dns     IN      A       172.30.33.245
245     IN      PTR     www.qtht.com.vn.
```



```
$TTL 1D
@      IN      SOA     @ qtht.com.vn. (
0          ;Serial
1D         ;Refresh
1H         ;Retry
1W         ;Expire
3H         ;Minimum TTL
)
@      IN      NS      dns.qtht.com.vn.
@      IN      PTR     qtht.com.vn.
dns     IN      A       192.168.10.135
135     IN      PTR     ns1.qtht.com.vn.
```

3.5. Tắt tường lửa: service iptables stop

```
[root@zen ~]# service iptables stop
Redirecting to /bin/systemctl stop iptables.service
[root@zen ~]# service iptables status
Redirecting to /bin/systemctl status iptables.service
● iptables.service - IPv4 firewall with iptables
   Loaded: loaded (/usr/lib/systemd/system/iptables.service; disabled; vendor preset:
   Active: inactive (dead)
```

3.6. Khởi động dịch vụ DNS: service named start

```
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; disabled; vendor preset:
   Active: active (running) since Sun 2021-05-09 13:09:15 +07; 4s ago
     Process: 55486 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS (code=
     Process: 55483 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" == "yes"
   Main PID: 55487 (named)
      Tasks: 7 (limit: 74046)
     Memory: 63.7M
    CGroup: /system.slice/named.service
            └─55487 /usr/sbin/named -u named -c /etc/named.conf
```

3.7. Kiểm tra kết quả: nslookup www.qtht.com.vn <địa chỉ IP máy ảo>

- Phân giải xuôi

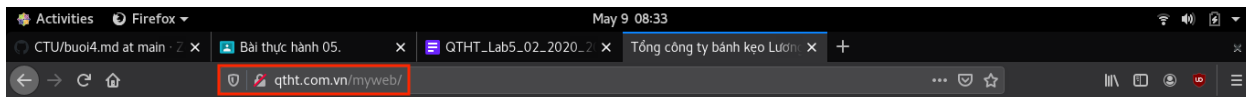
```
[root@zen b1909935]# nslookup www.qtht.com.vn 192.168.10.135
Server:      192.168.10.135
Address:     192.168.10.135#53

Name:   www.qtht.com.vn
Address: 192.168.10.135
```

- Phân giải ngược

```
[root@zen b1909935]# nslookup 192.168.10.135 192.168.10.135
135.10.168.192.in-addr.arpa    name = ns1.qtht.com.vn.
```

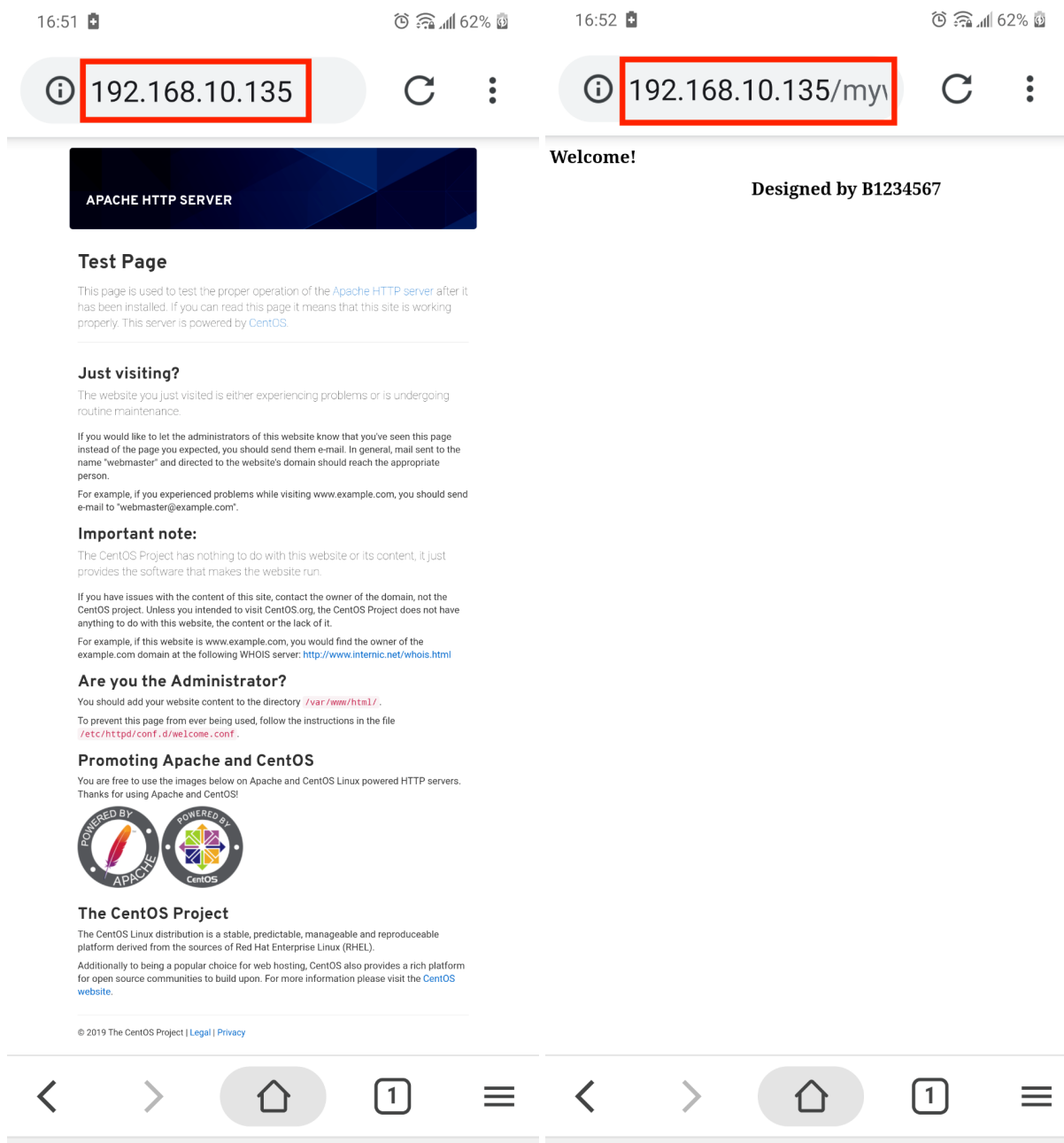
- 3.8. Trên máy vật lý, cấu hình DNS server là IP của máy ảo CentOS. Sau đó, mở trình duyệt web và truy cập vào địa chỉ `http://www.qtht.com.vn/myweb`



Welcome!

Designed by B1234567

💡 Cũng có thể dùng điện thoại để kết nối (Yêu cầu xài chung Wifi và thiết lập DNS custom)



4. Cấu hình tường lửa iptables

iptables là một bộ công cụ được tích hợp trên hệ điều hành Linux để thực hiện chức năng tường lửa theo cơ chế lọc gói tin (packet filtering). iptables theo dõi lưu lượng mạng đến và đi ở một máy tính và lọc nó dựa trên dựa trên các luật (rules) do người dùng định nghĩa trước.

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

4.1. Thực thi tường lửa iptables:

service iptables start

```
[root@zen b1909935]# service iptables start
Redirecting to /bin/systemctl start iptables.service
[root@zen b1909935]# service iptables status
Redirecting to /bin/systemctl status iptables.service
● iptables.service - IPv4 firewall with iptables
   Loaded: loaded (/usr/lib/systemd/system/iptables.service; disabled; vendor preset: disabled)
   Active: active (exited) since Sun 2021-05-09 09:12:23 +07; 20s ago
     Process: 12860 ExecStart=/usr/libexec/iptables/iptables.init start (code=exited, status=0/SUCCESS)
    Main PID: 12860 (code=exited, status=0/SUCCESS)

May 09 09:12:23 zen systemd[1]: Starting IPv4 firewall with iptables...
May 09 09:12:23 zen iptables.init[12860]: iptables: Applying firewall rules: [ OK ]
May 09 09:12:23 zen systemd[1]: Started IPv4 firewall with iptables.
```

4.2. Hiển thị các rules hiện có trên iptables

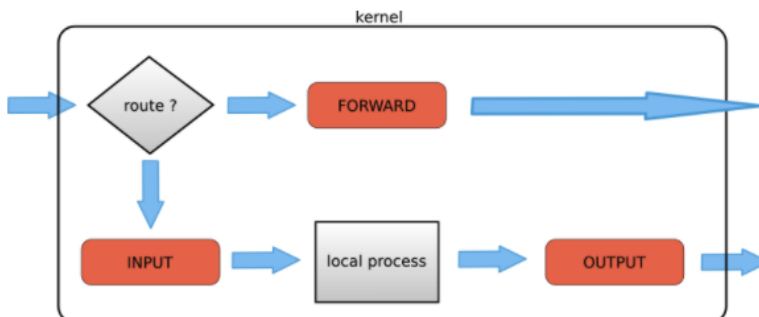
iptables -v -L --line-numbers

```
[root@zen b1909935]# iptables -v -L --line-numbers
Chain INPUT (policy ACCEPT 8391 packets, 19M bytes)
num  pkts bytes target    prot opt in      out     source         destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in      out     source         destination

Chain OUTPUT (policy ACCEPT 7558 packets, 1197K bytes)
num  pkts bytes target    prot opt in      out     source         destination
```

💡 Giải thích cụ thể :



Giải thích	INPUT	FORWARD	OUTPUT
Trừu tượng	Kiểm soát các gói đến từ <code>route</code> đến <code>server</code> của bạn	Kiểm soát các gói bắt nguồn từ <code>server</code> của bạn đến <code>nhà mạng</code>	Kiểm soát các gói được chuyển tiếp bởi <code>server</code> của bạn
Dễ hiểu	Lọc các gói dành cho <code>server</code> của bạn	Lọc các gói đến <code>server</code> của bạn mà <code>card wifi</code> khác có thể truy cập	Lọc các gói có nguồn gốc từ <code>server</code> của bạn

4.3. Tạo rules để cho phép các máy khác truy cập tới dịch vụ Web trên server

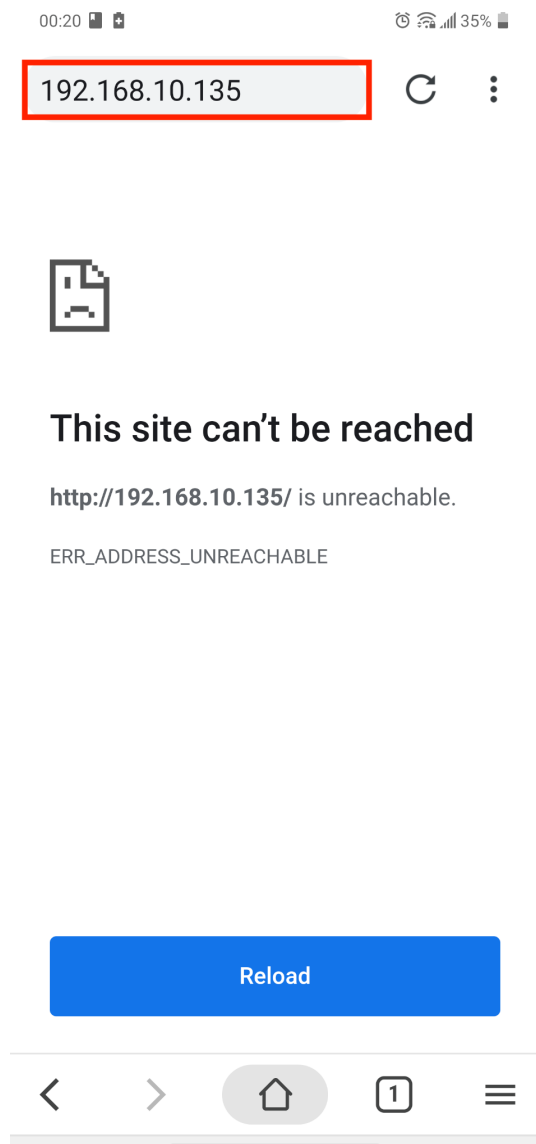
```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

```
iptables -D INPUT 6
```

```
iptables -I INPUT 5 -p tcp --dport 80 -j ACCEPT
```

Tham khảo cách dùng **iptables** căn bản [tại đây](#)

- Trước khi cho máy khác truy cập với dịch vụ Web Server :



- Sau khi cho máy khác truy cập tới dịch vụ Web Server bằng lệnh trên :

```
[root@zen b1909935]# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
[root@zen b1909935]# iptables -v -L --line-numbers
Chain INPUT (policy ACCEPT 54069 packets, 105M bytes)
  num  pkts bytes target     prot opt in     out     source    destination
  1      0      0 ACCEPT     tcp  --  any    any    anywhere  anywhere    tcp dpt:http
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  num  pkts bytes target     prot opt in     out     source    destination
Chain OUTPUT (policy ACCEPT 42030 packets, 6173K bytes)
  num  pkts bytes target     prot opt in     out     source    destination
```

16:51

62%



192.168.10.135



APACHE HTTP SERVER

Test Page

This page is used to test the proper operation of the [Apache HTTP server](#) after it has been installed. If you can read this page it means that this site is working properly. This server is powered by [CentOS](#).

Just visiting?

The website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting [www.example.com](#), you should send e-mail to "webmaster@example.com".

Important note:

The CentOS Project has nothing to do with this website or its content, it just provides the software that makes the website run.

If you have issues with the content of this site, contact the owner of the domain, not the CentOS project. Unless you intended to visit [CentOS.org](#), the CentOS Project does not have anything to do with this website, the content or the lack of it.

For example, if this website is [www.example.com](#), you would find the owner of the example.com domain at the following WHOIS server: <http://www.internic.net/whois.html>

Are you the Administrator?

You should add your website content to the directory `/var/www/html/`.

To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

Promoting Apache and CentOS

You are free to use the images below on Apache and CentOS Linux powered HTTP servers. Thanks for using Apache and CentOS!



The CentOS Project

The CentOS Linux distribution is a stable, predictable, manageable and reproducible platform derived from the sources of Red Hat Enterprise Linux (RHEL).

Additionally to being a popular choice for web hosting, CentOS also provides a rich platform for open source communities to build upon. For more information please visit the [CentOS website](#).


© 2019 The CentOS Project | [Legal](#) | [Privacy](#)




- 4.4. Tạo rules để cho máy vật lý có thể ping tới server, các máy khác KHÔNG ping được.


```
iptables -D INPUT 2
```

```
iptables -I INPUT 2 -p icmp -s 172.30.33.96 -j ACCEPT
```

Sử dụng  **Termux** của **Android** để thao tác các lệnh

 **Android** đang sử dụng chung mạng **Wifi** của máy dùng **iptables** và có IP như sau :
192.168.10.101 (riêng máy này thôi !)

- Trước khi thiết lập **rules** chặn **ping** :

-  **Android** sử dụng **ping**

```
17:12 >_
$ ping -c 5 192.168.10.135
PING 192.168.10.135 (192.168.10.135) 56(84) bytes of data.
64 bytes from 192.168.10.135: icmp_seq=1 ttl=64 time=2.86 ms
64 bytes from 192.168.10.135: icmp_seq=2 ttl=64 time=6.08 ms
64 bytes from 192.168.10.135: icmp_seq=3 ttl=64 time=17.8 ms
64 bytes from 192.168.10.135: icmp_seq=4 ttl=64 time=171 ms
64 bytes from 192.168.10.135: icmp_seq=5 ttl=64 time=9.68 ms

--- 192.168.10.135 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 2.865/41.577/171.405/65.106 ms
$ 0
```

-  **CentOS** sử dụng **ping**


```
[root@zen b1909935]# ping 192.168.10.135
PING 192.168.10.135 (192.168.10.135) 56(84) bytes of data.
64 bytes from 192.168.10.135: icmp_seq=1 ttl=64 time=0.026 ms
64 bytes from 192.168.10.135: icmp_seq=2 ttl=64 time=0.039 ms
64 bytes from 192.168.10.135: icmp_seq=3 ttl=64 time=0.040 ms
64 bytes from 192.168.10.135: icmp_seq=4 ttl=64 time=0.067 ms
64 bytes from 192.168.10.135: icmp_seq=5 ttl=64 time=0.058 ms
64 bytes from 192.168.10.135: icmp_seq=6 ttl=64 time=0.056 ms
```

==> Cả hai vẫn **ping** được

- Sau khi thiết lập rules chặn ping bằng lệnh trên :

```
[root@zen b1909935]# iptables -I INPUT 2 -p icmp -s 192.168.10.135 -j ACCEPT
[root@zen b1909935]# iptables -v -L --line-numbers
Chain INPUT (policy ACCEPT 54648 packets, 105M bytes)
num  pkts bytes target    prot opt in     out     source            destination
1      282 21413 ACCEPT    tcp  --  any    any    anywhere          anywhere          tcp dpt:http
2        0    0 ACCEPT    icmp --  any    any    qtht.com.vn       anywhere
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source            destination
Chain OUTPUT (policy ACCEPT 42726 packets, 6641K bytes)
num  pkts bytes target    prot opt in     out     source            destination
```

🤔 qtht.com.vn tương đương 192.168.10.135 vì đã cấu hình DNS bên trên

- o  Android sử dụng ping

```
17:09 >_
uelen 1000 (UNSPEC)

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.101 netmask 255.255.255.0 broadcast 192.168.10.255
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txque
uelen 3000 (UNSPEC)

$ ping 192.168.10.135
PING 192.168.10.135 (192.168.10.135) 56(84) bytes of data.
From 192.168.10.135: icmp_seq=4 Destination Port Unreachable
From 192.168.10.135: icmp_seq=9 Destination Port Unreachable
```

- o  CentOS sử dụng ping

```
[root@zen b1909935]# ping 192.168.10.135
PING 192.168.10.135 (192.168.10.135) 56(84) bytes of data.
64 bytes from 192.168.10.135: icmp_seq=1 ttl=64 time=0.026 ms
64 bytes from 192.168.10.135: icmp_seq=2 ttl=64 time=0.039 ms
64 bytes from 192.168.10.135: icmp_seq=3 ttl=64 time=0.040 ms
64 bytes from 192.168.10.135: icmp_seq=4 ttl=64 time=0.067 ms
64 bytes from 192.168.10.135: icmp_seq=5 ttl=64 time=0.058 ms
64 bytes from 192.168.10.135: icmp_seq=6 ttl=64 time=0.056 ms
```

==> Sau khi thiết lập rules chỉ có máy có IP:192.168.10.135 là ping được đến server .

4.5. Tạo rules để KHÔNG cho người dùng trên máy CentOS truy cập tới địa chỉ facebook.com

```
iptables -A OUTPUT -p tcp -m string --string facebook
--algo kmp -j REJECT
```

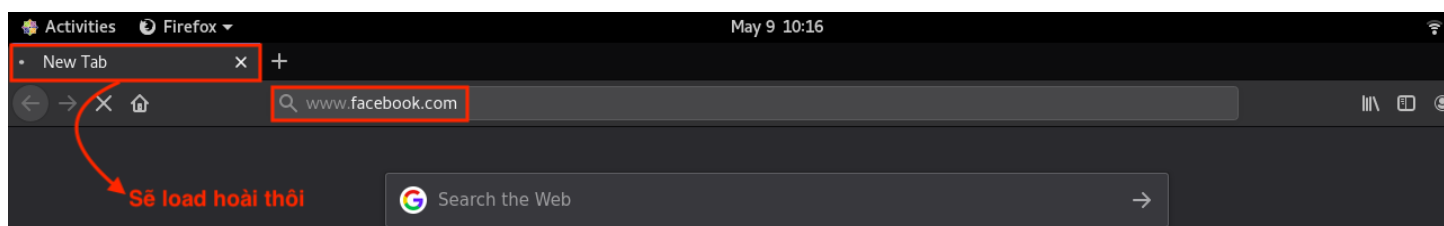
Sử dụng lệnh trên để gửi gói truy cập đến server của Facebook :

```
[root@zen b1909935]# iptables -A OUTPUT -p tcp -m string --string facebook --algo kmp -j REJECT
[root@zen b1909935]# iptables -v -L --line-numbers
Chain INPUT (policy ACCEPT 59537 packets, 107M bytes)
num  pkts bytes target    prot opt in     out     source               destination
1    314 23856 ACCEPT    tcp  --  any    any    anywhere             anywhere
2     46  4508 REJECT    icmp --  any    any    qtht.com.vn          anywhere
icmp-port-unreachable

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 48511 packets, 7343K bytes)
num  pkts bytes target    prot opt in     out     source               destination
1     0     0 REJECT    tcp  --  any    any    anywhere             anywhere
"facebook" ALGO name kmp TO 65535 reject-with icmp-port-unreachable
```

==> Sau khi đã áp dụng rules thì chúng ta không thể truy cập facebook được nữa :



4.6. Lưu và phục hồi các luật của iptables

```
cp /etc/sysconfig/iptables /etc/sysconfig/iptables.orig
iptables-save > /etc/sysconfig/iptables
iptables-restore < /etc/sysconfig/iptables
```

Trước khi tắt iptables, ta nên sao lưu (backup) lại rules bằng lệnh :

```
$ iptables-save > /etc/sysconfig/iptables
```

🤔 Vì sau khi tắt iptables và khởi động lại, các rules thiết lập trước đó sẽ reset như sau :

```
[root@zen b1909935]# iptables -v -L --line-numbers
Chain INPUT (policy ACCEPT 1214 packets, 626K bytes)
num  pkts bytes target    prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 1166 packets, 112K bytes)
num  pkts bytes target    prot opt in     out     source               destination
```

=> Khi đó ta có thể khôi phục (restore) lại `rules` đã sao lưu (backup) bằng lệnh sau:

```
$ iptables-restore < /etc/sysconfig/iptables
```

🌸 Kết quả như sau :

```
[root@zen b1909935]# iptables-restore < /etc/sysconfig/iptables
[root@zen b1909935]# iptables -v -L --line-numbers
Chain INPUT (policy ACCEPT 13 packets, 1060 bytes)
num  pkts bytes target    prot opt in     out     source               destination
1      0      0 ACCEPT    tcp  --  any    any    anywhere             tcp dpt:http
2      0      0 REJECT    icmp --  any    any    qtht.com.vn          anywhere             reject-with icmp-port-un
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source               destination
Chain OUTPUT (policy ACCEPT 13 packets, 1060 bytes)
num  pkts bytes target    prot opt in     out     source               destination
```

(Vì mình đã xóa `rules` chặn `facebook` trước đó nên không còn ở OUTPUT nữa)

--- Hết ---