LAB 5

SAMBA, DNS và Firewall

Họ tên và MSSV: **Nguyễn Quang Thụy B1910306**

Nhóm học phần: **03**

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

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

1. **Cài đặt CentOS**

(KHÔNG cần hình minh họa):

1.1. Thực hiện cài đặt CentOS 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`

```
[root@localhost b1910306]# yum install samba
```

```
Installed:
  samba-4.14.5-2.el8.x86_64          samba-common-tools-4.14.5-2.el8.x86_64
  samba-libs-4.14.5-2.el8.x86_64

Complete!
[root@localhost b1910306]#
```

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@localhost b1910306]# adduser tuanthai
[root@localhost b1910306]# passwd tuanthai
Changing password for user tuanthai.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost b1910306]# groupadd lecturers
[root@localhost b1910306]# usermod -a -G lecturers tuanthai
[root@localhost b1910306]# groups tuanthai
tuanthai : tuanthai lecturers
[root@localhost b1910306]#
```

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

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

```
[root@localhost b1910306]# mkdir /data
mkdir: cannot create directory ‘/data’: File exists
[root@localhost b1910306]# chgrp lecturers /data
[root@localhost b1910306]# chmod -R 775 /data
[root@localhost b1910306]#
```

```
drwxrwxr-x.   2 root lecturers    6 Sep 23 23:13 data
```

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@localhost b1910306]# cp /etc/samba/smb.conf /etc/samba/smb.conf.orig
```

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

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

```
[root@localhost b1910306]# smbpasswd -a tuanthai
New SMB password:
Retype new SMB password:
Added user tuanthai.
[root@localhost b1910306]#
```

2.6. Cấu hình SELINUX cho phép Samba

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

```
[root@localhost b1910306]# setsebool -P samba_export_all_rw on
[root@localhost b1910306]# setsebool -P samba_enable_home_dirs on
```

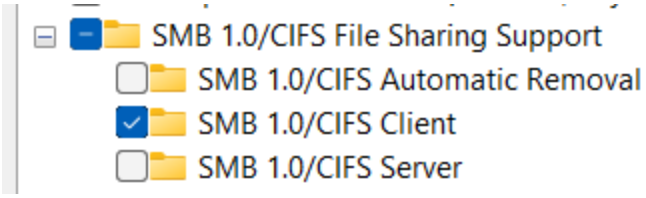
2.7. Tắt tường lửa: `systemctl stop firewalld`

```
[root@localhost b1910306]# systemctl stop firewalld
[root@localhost b1910306]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor>
   Active: inactive (dead) since Wed 2021-11-17 02:53:11 EST; 31min ago
     Docs: man:firewalld(1)
 Main PID: 900 (code=exited, status=0/SUCCESS)

Nov 17 02:33:31 localhost.localdomain systemd[1]: Starting firewalld - dynami>
Nov 17 02:33:34 localhost.localdomain systemd[1]: Started firewalld - dynamic>
Nov 17 02:33:35 localhost.localdomain firewalld[900]: WARNING: AllowZoneDrift>
Nov 17 02:52:56 localhost.localdomain systemd[1]: Stopping firewalld - dynami>
Nov 17 02:53:11 localhost.localdomain systemd[1]: firewalld.service: Succeede>
Nov 17 02:53:11 localhost.localdomain systemd[1]: Stopped firewalld - dynamic>
lines 1-12/12 (END)
```

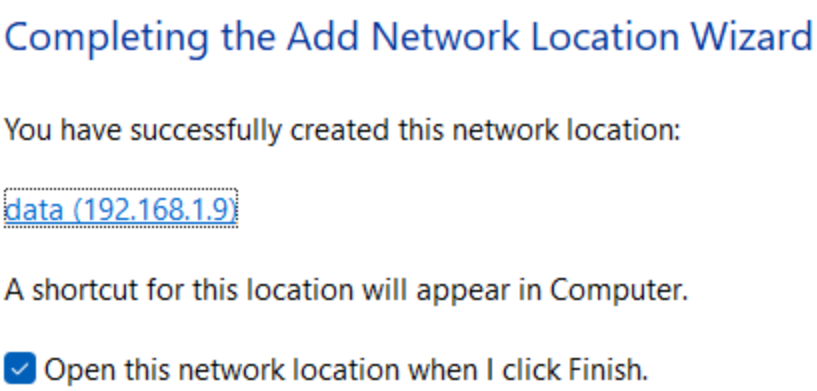
2.8. Khởi động dịch vụ Samba: `service smb start`

```
[root@localhost b1910306]# service smb start
Redirecting to /bin/systemctl start smb.service
[root@localhost b1910306]#
```

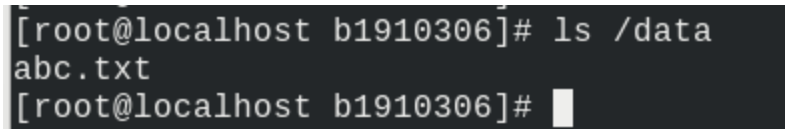
2.9. Trên máy Windows, bật tính năng hỗ trợ SMB1: mở Control Panel -> Programs -> Turn Windows features on or off -> SMB 1.0/CIFS File Sharing Support -> chọn SMB 1.0/CIFS Client



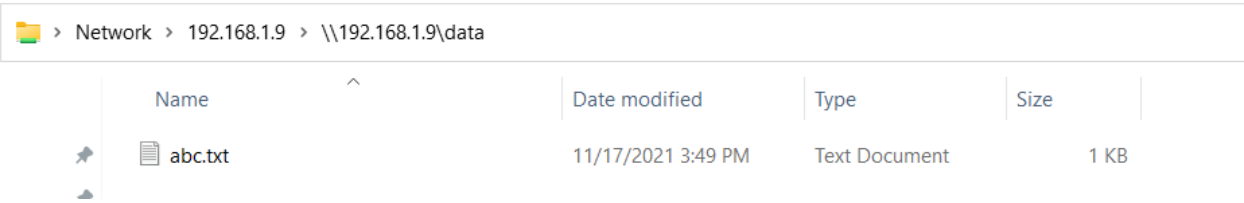
2.10. Trên File Explorer, chọn tính năng Add a network location để nối kết tới Samba server sử dụng địa chỉ `\\192.168.1.9\data` (Em đã đổi địa chỉ ip trên máy ảo thành 192.168.1.9)



- File abc.txt được tạo trên máy ảo CentOS



- File abc.txt được tạo trên máy ảo CentOS đã xuất hiện trên máy Windows, trong thư mục data có địa chỉ là: `\\192.168.1.9\data`



3. Cài đặt và cấu hình dịch vụ DNS

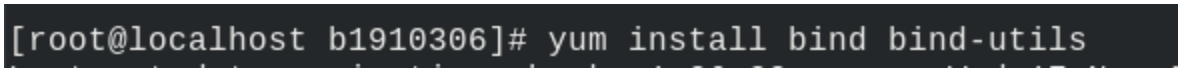
DNS (Domain Name System) là giải pháp dùng tên miền thay cho địa chỉ IP khó nhớ khi sử dụng các dịch vụ trên mạng. Truy cập đến website của Khoa CNTT-ĐH Cần thơ bằng địa chỉ nào dễ nhớ hơn ?

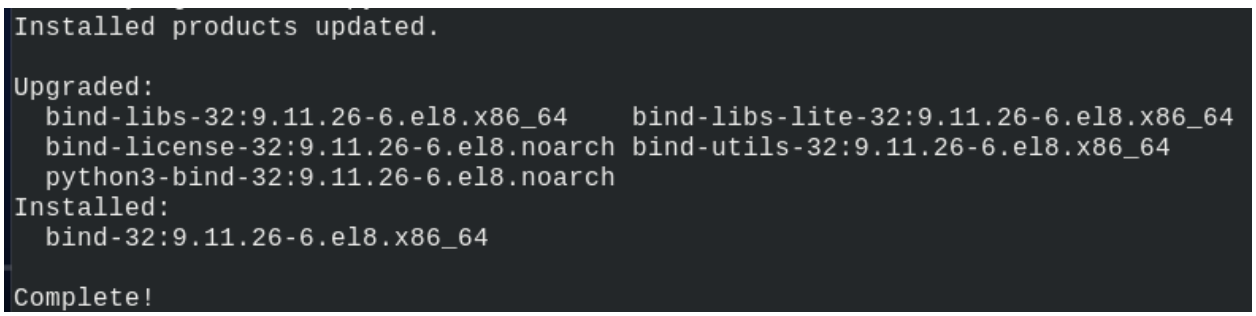
http://203.162.36.146 hay http://www.cit.ctu.edu.vn

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`





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

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

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

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

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     192.168.1.9
www   IN    A     192.168.1.9
htql  IN    A     8.8.8.8
```

```
[root@localhost b1910306]# cp /var/named/named.localhost /var/named/forward.qt
ht
[root@localhost b1910306]# cat /var/named/forward.qtht
$TTL 1D
@       IN SOA  @ rname.invalid. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       127.0.0.1
        AAAA    ::1
```

```
[root@localhost b1910306]# chgrp named /var/named/forward.qtht
[root@localhost b1910306]# ls -l /var/named
total 20
drwxrwx---. 2 named named    6 Aug 24 19:20 data
drwxrwx---. 2 named named    6 Aug 24 19:20 dynamic
-rw-r-----. 1 root  named  152 Nov 17 04:47 forward.qtht
-rw-r-----. 1 root  named 2253 Aug 24 19:20 named.ca
-rw-r-----. 1 root  named  152 Aug 24 19:20 named.empty
-rw-r-----. 1 root  named  152 Aug 24 19:20 named.localhost
-rw-r-----. 1 root  named  168 Aug 24 19:20 named.loopback
drwxrwx---. 2 named named    6 Aug 24 19:20 slaves
[root@localhost b1910306]#
```

```
$TTL 1D
@       IN SOA  @ qtht.com.vn. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@       IN      NS      dns.qtht.com.vn.
dns     IN      A       192.168.1.9
www     IN      A       192.168.1.9
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     192.168.1.9
9     IN    PTR   www.qtht.com.vn.
```

```
[root@localhost b1910306]# cp /var/named/forward.qtht /var/named/reverse.qtht
[root@localhost b1910306]# chgrp named /var/named/reverse.qtht
```

```
[root@localhost b1910306]# ls -l /var/named
total 24
drwxrwx---. 2 named named   23 Nov 17 04:54 data
drwxrwx---. 2 named named   60 Nov 17 04:55 dynamic
-rw-r-----. 1 root  named  207 Nov 17 04:53 forward.qtht
-rw-r-----. 1 root  named 2253 Aug 24 19:20 named.ca
-rw-r-----. 1 root  named  152 Aug 24 19:20 named.empty
-rw-r-----. 1 root  named  152 Aug 24 19:20 named.localhost
-rw-r-----. 1 root  named  168 Aug 24 19:20 named.loopback
-rw-r-----. 1 root  named  207 Nov 17 06:10 reverse.qtht
drwxrwx---. 2 named named    6 Aug 24 19:20 slaves
[root@localhost b1910306]#
```

```
$TTL 1D
@       IN SOA  @ qtht.com.vn. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@       IN      NS      dns.qtht.com.vn.
dns     IN      A       192.168.1.9
9       IN      PTR     www.qtht.com.vn.
```

3.5. Tắt tường lửa: `systemctl stop firewalld`

```
[root@localhost b1910306]# systemctl stop firewalld
[root@localhost b1910306]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor>
   Active: inactive (dead) since Wed 2021-11-17 02:53:11 EST; 2h 0min ago
     Docs: man:firewalld(1)
 Main PID: 900 (code=exited, status=0/SUCCESS)

Nov 17 02:33:31 localhost.localdomain systemd[1]: Starting firewalld - dynami>
Nov 17 02:33:34 localhost.localdomain systemd[1]: Started firewalld - dynamic>
Nov 17 02:33:35 localhost.localdomain firewalld[900]: WARNING: AllowZoneDrift>
Nov 17 02:52:56 localhost.localdomain systemd[1]: Stopping firewalld - dynami>
Nov 17 02:53:11 localhost.localdomain systemd[1]: firewalld.service: Succeede>
Nov 17 02:53:11 localhost.localdomain systemd[1]: Stopped firewalld - dynamic>
lines 1-12/12 (END)
```

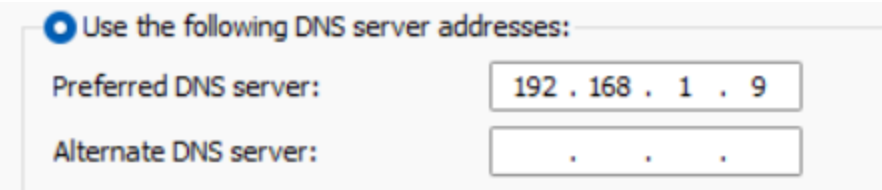
3.6. Khởi động dịch vụ DNS: `service named start`

```
[root@localhost b1910306]# service named start
Redirecting to /bin/systemctl start named.service
[root@localhost b1910306]# service named status
Redirecting to /bin/systemctl status named.service
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; disabled; vendor pr>
   Active: active (running) since Wed 2021-11-17 04:54:47 EST; 4s ago
  Process: 43845 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS >
  Process: 43843 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" ==>
 Main PID: 43847 (named)
    Tasks: 4 (limit: 4812)
   Memory: 59.6M
   CGroup: /system.slice/named.service
           └─43847 /usr/sbin/named -u named -c /etc/named.conf
```

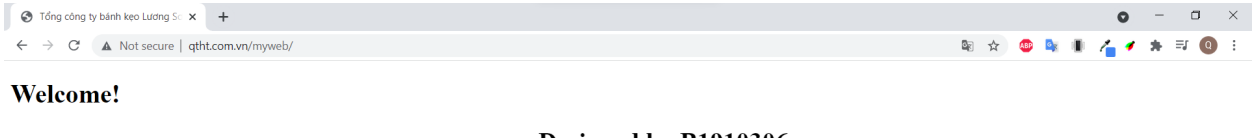
3.7. Kiểm tra kết quả: `nslookup www.qtht.com.vn 192.168.1.9`

```
[root@localhost b1910306]# nslookup www.qtht.com.vn 192.168.1.9
Server:         192.168.1.9
Address:        192.168.1.9#53

Name:   www.qtht.com.vn
Address: 192.168.1.9

[root@localhost b1910306]#
```

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`



- Máy Windows đã có thể truy cập được trang web có địa chỉ `http://www.qtht.com.vn/myweb`



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@localhost b1910306]# service iptables start
Redirecting to /bin/systemctl start iptables.service
[root@localhost b1910306]# 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>
   Active: active (exited) since Wed 2021-11-17 08:20:05 EST; 3s ago
  Process: 11014 ExecStart=/usr/libexec/iptables/iptables.init start (code=ex>
 Main PID: 11014 (code=exited, status=0/SUCCESS)

Nov 17 08:20:05 localhost.localdomain systemd[1]: Starting IPv4 firewall with>
Nov 17 08:20:05 localhost.localdomain iptables.init[11014]: iptables: Applyin>
Nov 17 08:20:05 localhost.localdomain systemd[1]: Started IPv4 firewall with >
lines 1-9/9 (END)
```

4.2. Hiển thị các rules hiện có trên iptables

```
iptables -v -L --line-numbers
```

```
[root@localhost b1910306]# iptables -v -L --line-number
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               desti
nation
1        0     0 ACCEPT     all  --  any    any     anywhere             anywh
ere             state RELATED,ESTABLISHED
2        0     0 ACCEPT     icmp --  any    any     anywhere             anywh
ere
3        0     0 ACCEPT     all  --  lo     any     anywhere             anywh
ere
4        0     0 ACCEPT     tcp  --  any    any     anywhere             anywh
ere             state NEW tcp dpt:ssh
5       20  4724 REJECT     all  --  any    any     anywhere             anywh
ere             reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               desti
nation
1        0     0 REJECT     all  --  any    any     anywhere             anywh
ere             reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT 20 packets, 3088 bytes)
num   pkts bytes target     prot opt in     out     source               desti
nation
[root@localhost b1910306]#
```

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
```

(thêm 1 rule vào iptables, rule này có vị trí là 6)

```
[root@localhost b1910306]# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
[root@localhost b1910306]# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  anywhere             anywhere             state RELAT
ED,ESTABLISHED
2    ACCEPT     icmp --  anywhere             anywhere
3    ACCEPT     all  --  anywhere             anywhere
4    ACCEPT     tcp  --  anywhere             anywhere             state NEW t
cp dpt:ssh
5    REJECT     all  --  anywhere             anywhere             reject-with
 icmp-host-prohibited
6    ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:htt
p

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    REJECT     all  --  anywhere             anywhere             reject-with
 icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
```

`iptables -D INPUT 6` (xóa rule số 6 là rule vừa tạo)

```
[root@localhost b1910306]# iptables -D INPUT 6
[root@localhost b1910306]# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  anywhere             anywhere             state RELAT
ED,ESTABLISHED
2    ACCEPT     icmp --  anywhere             anywhere
3    ACCEPT     all  --  anywhere             anywhere
4    ACCEPT     tcp  --  anywhere             anywhere             state NEW t
cp dpt:ssh
5    REJECT     all  --  anywhere             anywhere             reject-with
 icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    REJECT     all  --  anywhere             anywhere             reject-with
 icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
[root@localhost b1910306]#
```

`iptables -I INPUT 5 -p tcp --dport 80 -j ACCEPT`
(thêm 1 rule vào vị trí thứ 5 trong iptables và đẩy rule đang ở vị trí thứ 5 xuống vị trí thứ 6)

```
[root@localhost b1910306]# iptables -I INPUT 5 -p tcp --dport 80 -j ACCEPT
[root@localhost b1910306]# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  anywhere             anywhere             state RELAT
ED,ESTABLISHED
2    ACCEPT     icmp --  anywhere             anywhere
3    ACCEPT     all  --  anywhere             anywhere
4    ACCEPT     tcp  --  anywhere             anywhere             state NEW t
cp dpt:ssh
5    ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:htt
p
6    REJECT     all  --  anywhere             anywhere             reject-with
 icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    REJECT     all  --  anywhere             anywhere             reject-with
 icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
[root@localhost b1910306]#
```

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

`iptables -D INPUT 2` (xóa rule số 2 icmp)

```
[root@localhost b1910306]# iptables -D INPUT 2
[root@localhost b1910306]# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  anywhere             anywhere             state RELAT
ED,ESTABLISHED
2    ACCEPT     all  --  anywhere             anywhere
3    ACCEPT     tcp  --  anywhere             anywhere             state NEW t
cp dpt:ssh
4    ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:htt
p
5    REJECT     all  --  anywhere             anywhere             reject-with
 icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    REJECT     all  --  anywhere             anywhere             reject-with
 icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
[root@localhost b1910306]#
```

`iptables -I INPUT 2 -p icmp -s 192.168.1.8 -j ACCEPT`
(thay đổi rule để chấp nhận địa chỉ ip trên có thể gửi icmp tới máy CentOS)

```
[root@localhost b1910306]# iptables -I INPUT 2 -p icmp -s 192.168.1.8 -j ACCEP
T
[root@localhost b1910306]# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  anywhere             anywhere             state RELAT
ED,ESTABLISHED
2    ACCEPT     icmp --  192.168.1.8          anywhere
3    ACCEPT     all  --  anywhere             anywhere
4    ACCEPT     tcp  --  anywhere             anywhere             state NEW t
cp dpt:ssh
5    ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:htt
p
6    REJECT     all  --  anywhere             anywhere             reject-with
 icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    REJECT     all  --  anywhere             anywhere             reject-with
 icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
[root@localhost b1910306]#
```

- Máy Windows có thể gửi icmp tới máy CentOS

```
C:\Users\qthuy>ping 192.168.1.9

Pinging 192.168.1.9 with 32 bytes of data:
Reply from 192.168.1.9: bytes=32 time=1ms TTL=64
Reply from 192.168.1.9: bytes=32 time<1ms TTL=64
Reply from 192.168.1.9: bytes=32 time<1ms TTL=64
Reply from 192.168.1.9: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\qthuy>
```

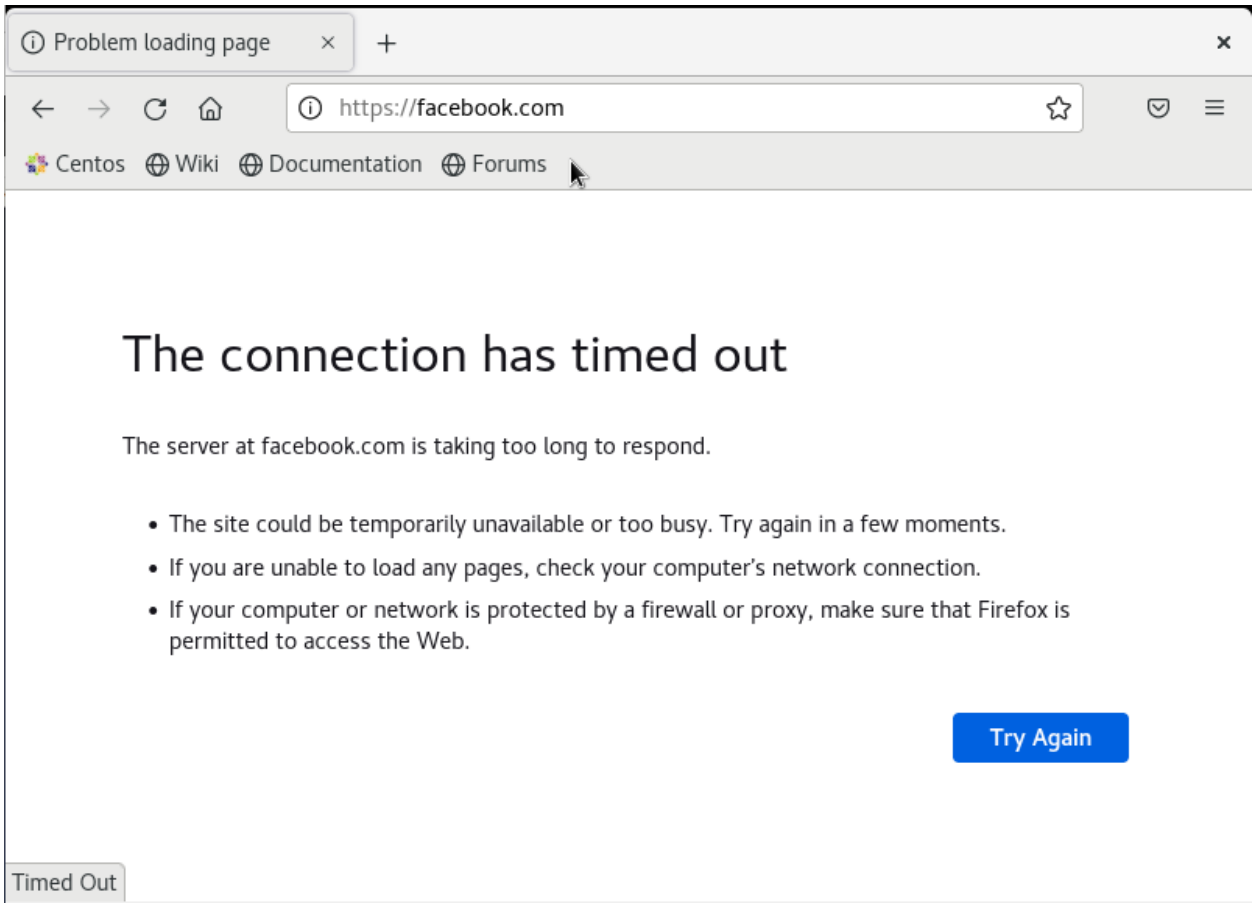
4.5. Tạo rules để KHÔNG cho người dùng trên máy CentOS truy cập tới địa chỉ facebook.com

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

```
[root@localhost b1910306]# iptables -A OUTPUT -p tcp -m string --string facebo
ok --algo kmp -j REJECT
```

```
Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
1    REJECT     tcp  --  anywhere             anywhere             STRING matc
h  "facebook" ALGO name kmp TO 65535 reject-with icmp-port-unreachable
```

- Không thể truy cập được facebook.com



4.6. Lưu và phục hồi các luật của iptables

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

```
[root@localhost b1910306]# cp /etc/sysconfig/iptables /etc/sysconfig/iptables.
orig
[root@localhost b1910306]# iptables-save > /etc/sysconfig/iptables
```

- Các rules vẫn giữ nguyên sau khi bị restart

```
[root@localhost b1910306]# service iptables restart
Redirecting to /bin/systemctl restart iptables.service
[root@localhost b1910306]# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  anywhere             anywhere             state RELAT
ED,ESTABLISHED
2    ACCEPT     icmp --  192.168.1.8          anywhere
3    ACCEPT     all  --  anywhere             anywhere
4    ACCEPT     tcp  --  anywhere             anywhere             state NEW t
cp dpt:ssh
5    ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:htt
p
6    REJECT     all  --  anywhere             anywhere             reject-with
 icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    REJECT     all  --  anywhere             anywhere             reject-with
 icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
1    REJECT     tcp  --  anywhere             anywhere             STRING matc
h  "facebook" ALGO name kmp TO 65535 reject-with icmp-port-unreachable
[root@localhost b1910306]#
```

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

- Xóa rule số 1 bằng lệnh

```
iptables -D INPUT 1
```

```
[root@localhost b1910306]# iptables -D INPUT 1
[root@localhost b1910306]# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     icmp --  192.168.1.8          anywhere
2    ACCEPT     all  --  anywhere             anywhere
3    ACCEPT     tcp  --  anywhere             anywhere             state NEW t
cp dpt:ssh
4    ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:htt
p
5    REJECT     all  --  anywhere             anywhere             reject-with
 icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    REJECT     all  --  anywhere             anywhere             reject-with
 icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
1    REJECT     tcp  --  anywhere             anywhere             STRING matc
h  "facebook" ALGO name kmp TO 65535 reject-with icmp-port-unreachable
[root@localhost b1910306]#
```

- Sau khi restore, các rules của iptables đã xuất hiện lại

```
[root@localhost b1910306]# iptables-restore < /etc/sysconfig/iptables
[root@localhost b1910306]# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  anywhere             anywhere             state RELAT
ED,ESTABLISHED
2    ACCEPT     icmp --  192.168.1.8          anywhere
3    ACCEPT     all  --  anywhere             anywhere
4    ACCEPT     tcp  --  anywhere             anywhere             state NEW t
cp dpt:ssh
5    ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:htt
p
6    REJECT     all  --  anywhere             anywhere             reject-with
 icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    REJECT     all  --  anywhere             anywhere             reject-with
 icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
1    REJECT     tcp  --  anywhere             anywhere             STRING matc
h  "facebook" ALGO name kmp TO 65535 reject-with icmp-port-unreachable
[root@localhost b1910306]#
```

--- Hết ---