



LAB 5

SAMBA, DNS và Firewall

Họ tên và MSSV: Nguyễn Thanh Nghĩa B1908341

Nhóm học phần: Nhóm 3

- 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`

```
[root@localhost B1908341]# yum install samba
Loaded plugins: fastestmirror, refresh-packagekit, security
Setting up Install Process
Loading mirror speeds from cached hostfile
Package samba-3.6.23-53.el6_10.x86_64 already installed and latest version
Nothing to do
[root@localhost B1908341]#
```

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

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

```
B1908341@localhost:/home/B1908341
File Edit View Search Terminal Help
[root@localhost B1908341]# adduser tuanthai
[root@localhost B1908341]# passwd tuanthai
Changing password for user tuanthai.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost B1908341]# groupadd lecturers
[root@localhost B1908341]# usermod -a -G lecturers tuanthai
[root@localhost B1908341]# █
```

```
[root@localhost B1908341]# groups tuanthai
tuanthai : tuanthai lecturers
[root@localhost B1908341]# █
```

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

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

```
[root@localhost B1908341]# mkdir /data
[root@localhost B1908341]# chgrp lecturers /data
[root@localhost B1908341]# chmod -R 775 /data
[root@localhost B1908341]# █
```

```
dr-xr-xr-x.  5 root root      1024 May 20 07:44 boot
drwxrwxr-x.  2 root lecturers 4096 May 20 08:27 data
drwxr-xr-x. 21 root root      3700 May 20 07:49 dev
```

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
```

```
[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 B1908341]# smbpasswd -a tuanthai
New SMB password:
Retype new SMB password:
Added user tuanthai.
[root@localhost B1908341]#
```

- 2.6. Cấu hình SELINUX cho phép Samba

```
setsebool -P samba_export_all_rw on
setsebool -P samba_enable_home_dirs on
[root@localhost B1908341]# setsebool -P samba_export_all_rw on
[root@localhost B1908341]# setsebool -P samba_enable_home_dirs on
[root@localhost B1908341]#
```

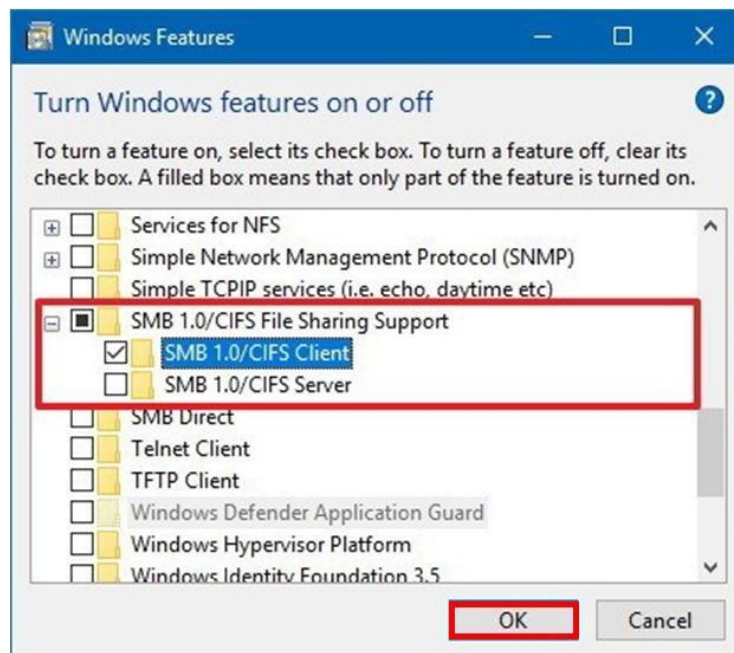
- 2.7. Tắt tường lửa: `service iptables stop`

```
[root@localhost B1908341]# service iptables stop
[root@localhost B1908341]#
```

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

```
[root@localhost B1908341]# service smb start
Starting SMB services:
[root@localhost B1908341]# [ OK ]
```

- 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

- 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
- Em sử dụng ubuntu nên bỏ qua 2.9 & 2.10 nha thầy
- ...

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`

```
Installed:
  bind.x86_64 32:9.8.2-0.68.rc1.el6_10.8

Updated:
  bind-utils.x86_64 32:9.8.2-0.68.rc1.el6_10.8

Dependency Updated:
  bind-libs.x86_64 32:9.8.2-0.68.rc1.el6_10.8

Complete!
[root@localhost B1908341]#
```

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; };
};
...
```

```
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";
    allow-query     { localhost; any; };
    recursion yes;
}
```

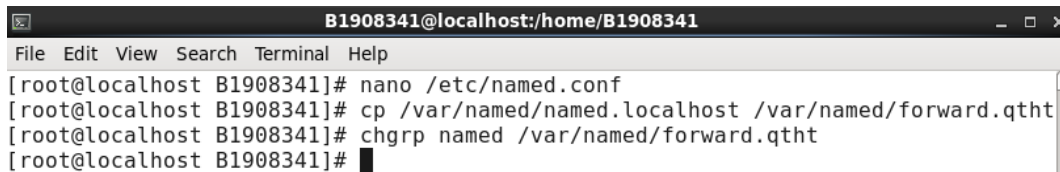
```
zone "qtht.com.vn" IN {
    type master;
    file "forward.qtht";
    allow-update { none; };
};

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

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
```



```
B1908341@localhost:/home/B1908341
File Edit View Search Terminal Help
[root@localhost B1908341]# nano /etc/named.conf
[root@localhost B1908341]# cp /var/named/named.localhost /var/named/forward.qtht
[root@localhost B1908341]# chgrp named /var/named/forward.qtht
[root@localhost B1908341]#
```

```
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

$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       192.168.1.8
www     IN      A       192.168.1.8
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
[root@localhost B1908341]# nano /etc/named.conf
[root@localhost B1908341]# cp /var/named/forward.qtht /var/named/reverse.qtht
[root@localhost B1908341]# chgrp named /var/named/reverse.qtht
[root@localhost B1908341]# █

```

```
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       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
@      IN      NS      dns.qtht.com.vn.
dns     IN      A       192.168.1.8
8       IN      PTR     www.qtht.com.vn

```

3.5. Tắt tường lửa: `service iptables stop`

```
[root@localhost B1908341]# service iptables stop
```

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

```
[root@localhost B1908341]# service iptables stop
[root@localhost B1908341]# service named start
Starting named: named: already running [ OK ]
[root@localhost B1908341]# █
```

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

```
[root@localhost B1908341]# nslookup www.qtht.com.vn 192.168.1.8
Server:          192.168.1.8
Address:         192.168.1.8#53

Name:   www.qtht.com.vn
Address: 192.168.1.8

[root@localhost B1908341]# █
```

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`

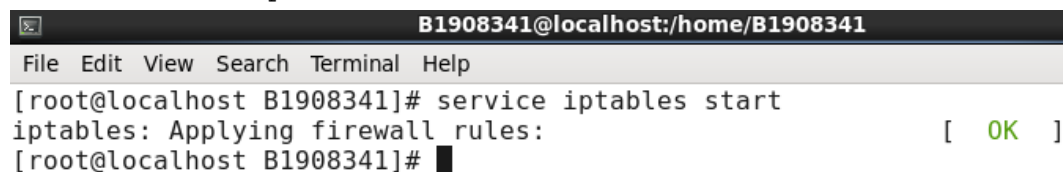
4. Cấu hình tường lửa iptables

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
```



```
B1908341@localhost:/home/B1908341
File Edit View Search Terminal Help
[root@localhost B1908341]# service iptables start
iptables: Applying firewall rules: [ OK ]
[root@localhost B1908341]# █
```

4.2. Hiển thị các rules hiện có trên iptables

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

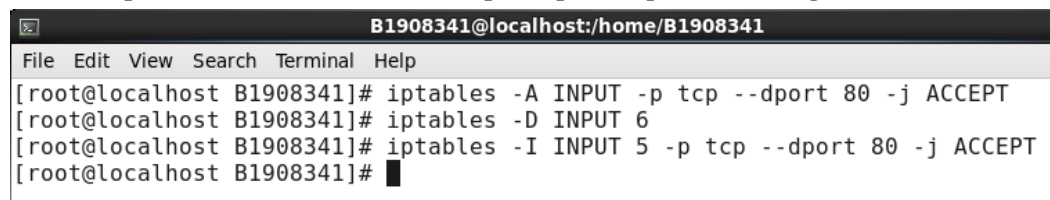


```
[root@localhost B1908341]# iptables -v -L --line-numbers
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target     prot opt in     out     source         destination
1      45  4595 ACCEPT     all  --  any    any     anywhere       anywhere
    state RELATED,ESTABLISHED
2       0     0 ACCEPT     icmp --  any    any     anywhere       anywhere
3       0     0 ACCEPT     all  --  lo     any     anywhere       anywhere
4       0     0 ACCEPT     tcp  --  any    any     anywhere       anywhere
    state NEW tcp dpt:ssh
5       0     0 REJECT     all  --  any    any     anywhere       anywhere
    reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target     prot opt in     out     source         destination
1       0     0 REJECT     all  --  any    any     anywhere       anywhere
```

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
```



```
B1908341@localhost:/home/B1908341
File Edit View Search Terminal Help
[root@localhost B1908341]# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
[root@localhost B1908341]# iptables -D INPUT 6
[root@localhost B1908341]# iptables -I INPUT 5 -p tcp --dport 80 -j ACCEPT
[root@localhost B1908341]#
```

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
[root@localhost B1908341]# iptables -D INPUT 2
[root@localhost B1908341]# iptables -I INPUT 2 -p icmp -s 192.168.1.8 -j ACCEPT
[root@localhost B1908341]#
```

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 B1908341]# iptables -A OUTPUT -p tcp -m string --string facebook
iptables v1.4.7: STRING match: You must specify '--algo'
Try 'iptables -h' or 'iptables --help' for more information.
[root@localhost B1908341]# iptables -A OUTPUT -p tcp -m string --string facebook --algo kmp -j REJECT
[root@localhost B1908341]#
```

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
```

```
B1908341@localhost:/home/B1908341
File Edit View Search Terminal Help
[root@localhost B1908341]# iptables-save > /etc/sysconfig/iptables
[root@localhost B1908341]# iptables-restore < /etc/sysconfig/iptables
[root@localhost B1908341]# █
```

--- Hết ---