

Phần IV: Internet Services

Bài Lab 1: FTP

Bài Lab 2: The Secure Shell(SSH)

Bài Lab 3: DNS

Bài Lab 4: Web Server

Bài Lab 5: Squid Server

Bài Lab 6: Mail Server

Bài Lab 7: Firewall Server

Bài Lab 8: IDS Server

Bài Lab 1: FTP

I/ Cài đặt FTP:

FTP là dịch vụ cung cấp cơ chế truyền tin dưới dạng file thông qua mạng tcp. Có nhiều chương trình ftp server sử dụng trên Linux như: Vsftpd, Wu-ftp, PureFTPd, ProFTPD,... Trong giáo trình này sẽ trình bày Vsftpd

- Kiểm tra vsftpd đã được cài đặt hay chưa:

```
[root@testsrv /]# rpm -qa | grep vsftpd
```

- Cài đặt (nếu chưa được cài đặt):

```
[root@testsrv /]# rpm -ivh vsftpd-2.0.5-10.el5.i386.rpm
```

```
Preparing... ##### [100%]
```

```
1:vsftpd _ ##### [100%]
```

- Kiểm tra vsftpd đã được cài đặt trên hệ thống:

```
[root@testsrv /]# rpm -qa | grep vsftpd
```

```
vsftpd-2.0.5-10.el5
```

II/ Cấu hình vsftpd server:

file dùng để cấu hình vsftpd server là /etc/vsftpd/vsftpd.conf

- Sửa file cấu hình vsftpd.conf như sau:

```
[root@testsrv /]# vi /etc/vsftpd/vsftpd.conf
```

```
anonymous_enable=NO # không cho phép anonymous login vào
local_enable=YES      # Cho phép người dùng cục bộ login vào
write_enable=YES      # Cung cấp quyền ghi cho người dùng
xferlog_enable=YES    # Cho phép ghi log
xferlog_file=/var/log/vsftpd.log # Vị trí file log
connect_from_port_20=YES # Sử dụng cổng 20 cho FTP-Data
ftpd_banner=Trung Tam Dao Tao Mang May Tinh Athena
userlist_enable=YES   # Những người dùng trong user_list bị cấm truy cập
```

Chú ý: Khi chạy vsftpd trên CentOS5. Nếu bật chức năng SELinux = enforcing (/etc/sysconfig/selinux) thì ta cần phải set biến ftp_home_dir = on

- Kiểm tra biến ftp_home_dir:

```
[root@testsrv vsftpd]# getsebool ftp_home_dir
```

```
ftp_home_dir --> off
```

- Set biến ftp_home_dir = on:

```
[root@testsrv vsftpd]# setsebool -P ftp_home_dir 1
```

- Kiểm tra lại biến ftp_home_dir:

```
[root@testsrv vsftpd]# getsebool ftp_home_dir
```

```
ftp_home_dir --> on
```

- Tạo FTP Home Dir

```
[root@testsrv /]# mkdir /home_ftp
```

- Tạo User cho phép truy cập FTP server:

```
[root@testsrv vsftpd]# useradd -d /home_ftp/ftpuser ftpuser
```

- Tạo Password cho user ftpuser

```
[root@testsrv /]# passwd ftpuser
Changing password for user ftpuser.
New UNIX password:
BAD PASSWORD: it is based on a dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```
- Tạo file test.txt

```
[root@testsrv vsftpd]# touch /home ftp/ftpuser/test.txt
```
- FTP server khi chạy cần mở port (20,21) nên ta phải mở 2 port này trên firewall hay tắt firewall.

```
[root@testsrv /]# service iptables stop
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
```
- Start vsftpd daemon:

```
[root@testsrv /]# service vsftpd start
Starting vsftpd for vsftpd: [ OK ]
```

III/ FTP client:

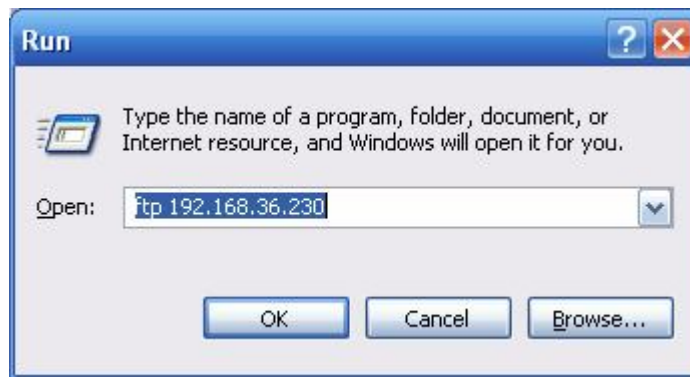
- Truy cập từ Linux:

```
[root@testsrv vsftpd]# ftp 192.168.36.230
Connected to 192.168.36.230.
220 Trung Tam Dao Tao Mang May Tinh Athena
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (192.168.36.230:root): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Kiểm tra

```
ftp> ls
227 Entering Passive Mode (192,168,36,230,207,244)
150 Here comes the directory listing.
-rw-r--r--  1 0      0          0 Feb 12 04:53 test.txt
226 Directory send OK.
```

- Truy cập từ windows:



```
Connected to 192.168.36.230.
220 Trung Tam Dao Tao Mang Tinh Athena
User (192.168.36.230:(none)): ftpuser
331 Please specify the password.
Password:
230 Login successful.
ftp>
```

Kiểm tra

```
ftp> ls -l
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 0 Feb 12 04:53 test.txt
226 Directory send OK.
ftp: 66 bytes received in 0.00Seconds 66000.00Kbytes/sec.
ftp>
```

Bài Lab 2: The Secure Shell(SSH)

I/ Cài đặt SSH:

Chương trình telnet cho phép người dùng đăng nhập từ xa vào hệ thống. Nhưng khuyết điểm của chương trình này là tên người dùng và mật khẩu gửi qua mạng không được mã hoá. Do đó, rất dễ bị tấn công. Phần mềm ssh là một sự hỗ trợ mới của linux nhằm khắc phục nhược điểm của telnet. Nó cho phép bạn đăng nhập từ xa vào hệ thống linux và mật khẩu sẽ được mã hoá.

Mặc định khi cài đặt linux thì ssh đã được cài đặt

- Kiểm tra ssh đã được cài đặt hay chưa:

```
[root@testsrv /]# rpm -qa | grep openssh
openssh-4.3p2-16.el5
openssh-clients-4.3p2-16.el5
openssh-askpass-4.3p2-16.el5
openssh-server-4.3p2-16.el5
```

II/ Cấu hình SSH server:

file dùng để cấu hình ssh server là `/etc/ssh/sshd_config`

- Xem file cấu hình sshd_config với các option mặc định:

```
[root@testsrv /]# vi /etc/ssh/sshd_config
```

- ssh server khi chạy cần mở port (22) nên ta phải mở port này trên firewall hay tắt firewall.

```
[root@testsrv /]# service iptables stop
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
```

- Start sshd daemon:

```
[root@testsrv /]# service sshd start
Starting sshd: [ OK ]
```

III/ SSH client:

- Truy cập ssh server từ Linux:

```
[root@testsrv /]# ssh 192.168.36.230
The authenticity of host '192.168.36.230 (192.168.36.230)' can't be established.
RSA key fingerprint is 6f:9c:a0:92:7f:61:e7:18:0e:58:97:eb:07:a6:51:3a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.36.230' (RSA) to the list of known hosts.
root@192.168.36.230's password:
```

Nhập vào password của root.

Để thoát khỏi ssh server gõ `exit`

Nếu muốn ssh với account khác root thì thêm vào option `-l` như sau:

```
[root@testsrv /]# ssh -l usera 192.168.36.230
usera@192.168.36.230's password:
[usera@testsrv ~]$
```

- Sử dụng lệnh scp để thực hiện sao chép qua ssh:

```
[root@testsrv /]# scp /var/log/maillog 192.168.36.230:/tmp
root@192.168.36.230's password:
maillog
```

100% 1083 1.1KB/s 00:00

=> Sao chép file maillog từ localhost sang thư mục /tmp của server 192.168.36.230

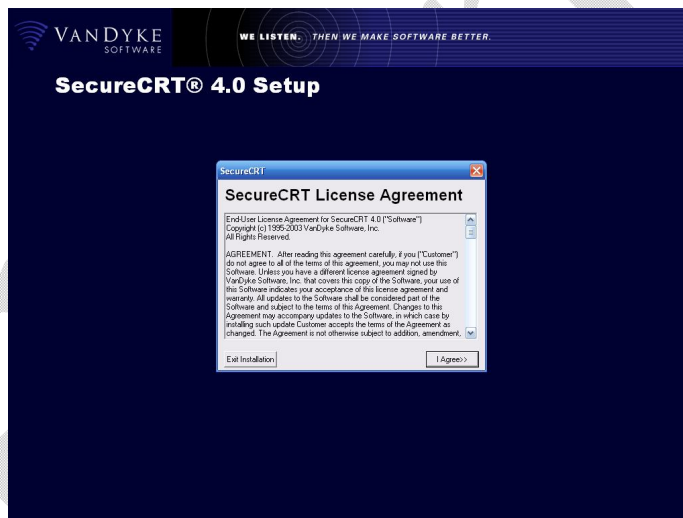
Nếu muốn copy cả thư mục thì thêm vào option -r như sau:

```
[root@testsrv /]# scp -r /var/log 192.168.36.230:/tmp
root@192.168.36.230's password:
anaconda.log          100% 471KB 470.9KB/s 00:00
:0.log                100% 892    0.9KB/s 00:00
:0.log.2              100% 892    0.9KB/s 00:00
:0.log.1              100% 892    0.9KB/s 00:00
yum.log               100% 52     0.1KB/s 00:00
secure                100% 3723   3.6KB/s 00:00
```

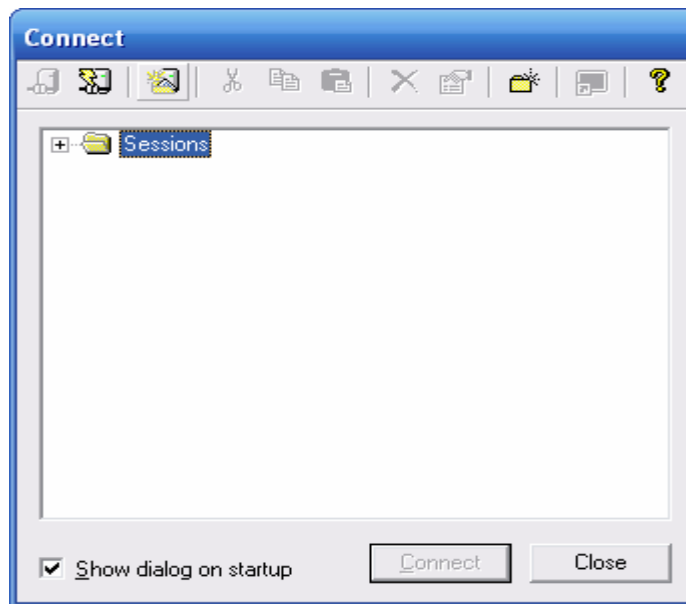
=> Sao chép thư mục log sang thư mục /tmp của server 192.168.36.230


- Truy cập ssh server từ windows:

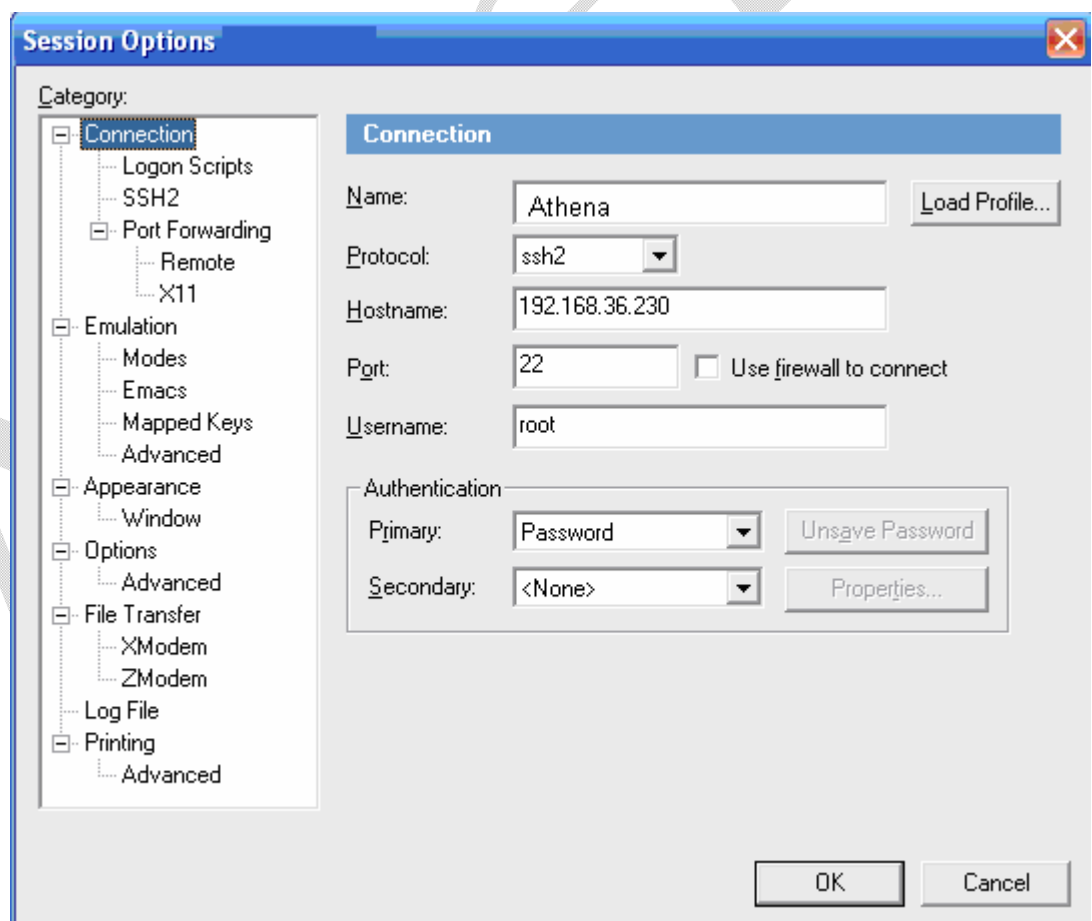
Trên windows cài chương trình *SCRT 4.0.5.exe*



Sau khi cài đặt xong, chạy chương trình trong *Start => programs => SecureCRT 4.0 => SecureCRT 4.0.exe*



Chọn  (New Session), khai báo các thông số sau:

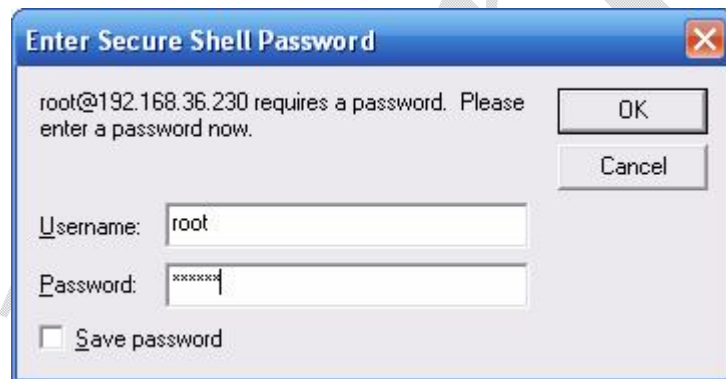


Chọn *OK*

Chọn connection *Ahtena* => chọn *Connect*



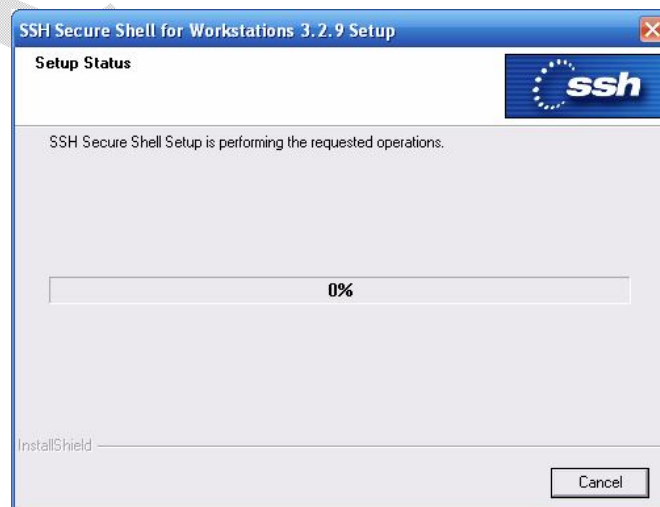
Chọn *Accept & Save*



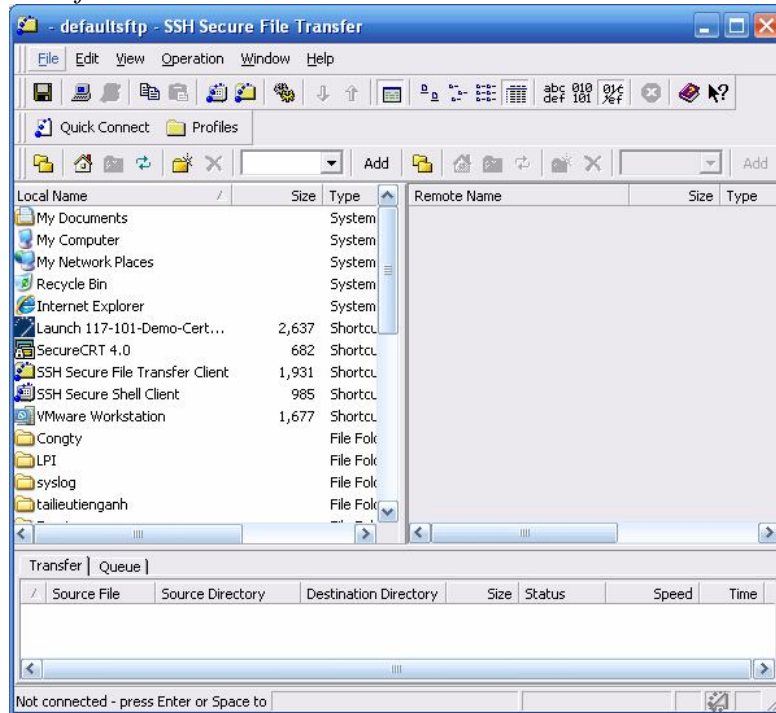
Nhập vào password cho account root, chọn *OK*


- Secure Transfer File từ windows:

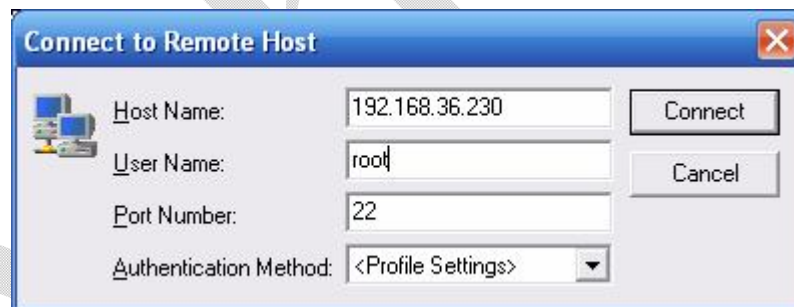
Trên windows cài chương trình *SSHSecureShellClient-3.2.9.exe*



Sau khi cài đặt xong, chạy chương trình trong *Start => programs => SSH Secure Shell => Secure File Transfer Client*



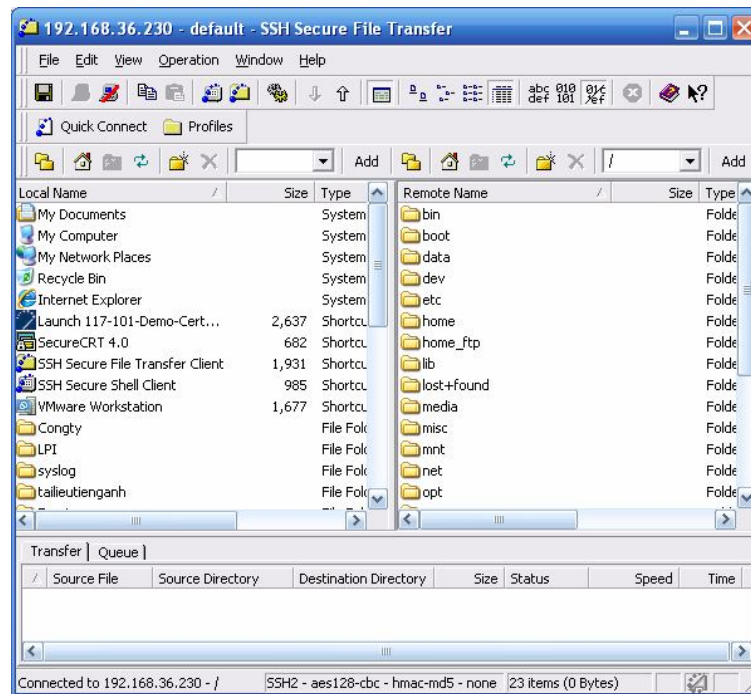
Chọn  Quick Connect, nhập vào các thông số



Chọn *Connect*



Nhập vào password của account root, chọn *OK*



IV/ Cấu hình cho phép truy cập SSH server không yêu cầu nhập password:

- Sửa file cấu hình trên server thiết lập 2 thuộc tính sau:

```
[root@testsrv /]# vi /etc/ssh/sshd_config
.....
PubkeyAuthentication yes
AuthorizedKeysFile      .ssh/authorized_keys
.....
```

- Tạo key tại máy Client:

```
[root@testsrv /]# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
c7:76:bb:14:a6:93:34:2a:4d:c0:d9:e0:32:29:f8:5e root@testsrv.athena.edu.vn
```

- Copy key của Client lên Server:

```
[root@testsrv /]# scp -r /root/.ssh 192.168.36.230:/root/
root@192.168.36.230's password:
known_hosts          100% 396    0.4KB/s   00:00
id_rsa.pub           100% 407    0.4KB/s   00:00
id_rsa               100% 1675    1.6KB/s   00:00
```

IP Server

- Trên server copy file id_rsa.pub thành file mới đổi tên thành authorized_keys:

```
[root@testsrv /]# cp /root/.ssh/id_rsa.pub /root/.ssh/authorized_keys
```

- Restart lại sshd daemon trên server:

```
[root@testsrv /]# service sshd restart
```

```
Stopping sshd:
```

```
[ OK ]
```

```
Starting sshd:
```

```
[ OK ]
```

- Truy cập SSH từ Client:

```
[root@testsrv /]# ssh 192.168.36.230
```

```
Last login: Tue Feb 26 12:50:13 2008 from 192.168.36.233
```

```
[root@testsrv ~]# █
```

Bài Lab 3: DNS

DNS là dịch vụ phân giải tên miền thành IP và ngược lại.

Có 3 loại Name Server: Primary Name Server, Secondary Name Server, Caching Name Server

I/ Cài đặt Primary Name Server:

- Kiểm tra DNS đã được cài đặt hay chưa:

```
[root@testsrv /]# rpm -qa | grep bind
```

- Cài đặt (nếu chưa được cài đặt):

```
[root@testsrv /]# rpm -ivh bind-libs-9.3.3-10.el5.i386.rpm
Preparing... ##### [100%]
1:bind-libs ##### [100%]
[root@testsrv /]# rpm -ivh bind-9.3.3-10.el5.i386.rpm
Preparing... ##### [100%]
1:bind ##### [100%]
[root@testsrv /]# rpm -ivh bind-utils-9.3.3-10.el5.i386.rpm
Preparing... ##### [100%]
1:bind-utils ##### [100%]
```

- Kiểm tra DNS đã được cài đặt trên hệ thống:

```
[root@testsrv /]# rpm -qa | grep bind
bind-utils-9.3.3-10.el5
bind-libs-9.3.3-10.el5
bind-9.3.3-10.el5
```

II/ Cấu hình Primary Name Server:

- Tạo file cấu hình /etc/named.conf như sau:

```
[root@testsrv /]# vi /etc/named.conf
options
{
    query-source      port 53;
    query-source-v6   port 53;
    directory          "/var/named"; // the default
    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";
    notify             yes;
};

zone "." in {
    type hint;
    file "named.root";
};

zone "localhost" in {
    type master;
    file "localhost.db";
};

zone "0.0.127.in-addr.arpa" in {
    type master;
    file "0.0.127.in-addr.arpa.db";
};
```



```
zone "athena.edu.vn" {
    type master;
    file "athena.edu.vn.db";
};

zone "36.168.192.in-addr.arpa" {
    type master;
    file "36.168.192.in-addr.arpa.db";
};
```

- Tạo file /var/named/named.root bằng cách download trên mạng như sau:

```
[root@testsrv /]# cd /var/named.
[root@testsrv named]# wget http://www.internic.net/zones/named.root
--08:29:53-- http://www.internic.net/zones/named.root
Resolving www.internic.net... 208.77.188.101
Connecting to www.internic.net|208.77.188.101|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2878 (2.8K) [text/plain]
Saving to: `named.root'

100%[=====>] 2,878      --.-K/s  in 0s

08:29:53 (38.6 MB/s) - `named.root' saved [2878/2878]
```

Chú ý: Server phải kết nối đến internet.

- Tạo file /var/named/localhost.db:

```
[root@testsrv named]# vi /var/named/localhost.db
$TTL 86400      ; 1 day
@              IN SOA  localhost root (
                                20080213 ; serial
                                10800     ; refresh (3 hours)
                                3600      ; retry (1 hour)
                                604800    ; expire (1 week)
                                86400     ; minimum (1 day)
                                )
IN              NS       @
IN              A        127.0.0.1
```

- Tạo file /var/named/0.0.127.in-addr.arpa.db:

```
[root@testsrv named]# vi /var/named/0.0.127.in-addr.arpa.db
$TTL 86400      ; 1 day
@              IN SOA  localhost. root.localhost. (
                                20080213 ; serial
                                10800     ; refresh (3 hours)
                                3600      ; retry (1 hour)
                                604800    ; expire (1 week)
                                86400     ; minimum (1 day)
                                )
IN              NS       localhost.
1               IN      PTR localhost.
```

- Tạo file /var/named/athena.edu.vn.db:

```
[root@testsrv named]# vi /var/named/athena.edu.vn.db
```



```
$TTL 86400      ; 1 day
@               IN SOA  dns1.athena.edu.vn. root (
                                20080213      ; serial
                                10800           ; refresh (3 hours)
                                3600            ; retry (1 hour)
                                604800          ; expire (1 week)
                                86400           ; minimum (1 day)
                                )
web             IN      NS      dns1.athena.edu.vn.
web             IN      A       192.168.36.230
www             IN      CNAME   web
```

- Tạo file /var/named/36.168.192.in-addr.arpa.db:

```
[root@testsrv named]# vi /var/named/36.168.192.in-addr.arpa.db
$TTL 86400      ; 1 day
@               IN SOA  dns1.athena.edu.vn. root (
                                20080213      ; serial
                                10800           ; refresh (3 hours)
                                3600            ; retry (1 hour)
                                604800          ; expire (1 week)
                                86400           ; minimum (1 day)
                                )
230            IN      NS      dns1.athena.edu.vn.
230            IN      PTR     athena.edu.vn.
```

- Start named daemon:

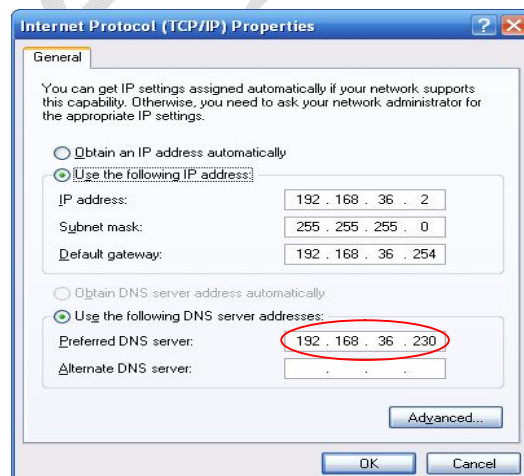
```
[root@testsrv named]# service named start
Starting named: [ OK ]
```

- Mở port 53 trên fireware hay stop firewall

```
[root@testsrv named]# service iptables stop
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
```

III/ Cấu hình DNS client:

- Từ windows: Khai báo Preferred DNS Server là IP của DNS Server



Dùng lệnh nslookup để kiểm tra: nslookup www.athena.edu.vn

- Từ linux:

Sửa file resolv.conf như sau:

```
[root@testsrv named]# vi /etc/resolv.conf
search athena.edu.vn
nameserver 192.168.36.230
```

Dùng lệnh nslookup để kiểm tra: nslookup www.athena.edu.vn

Dùng lệnh ping để kiểm tra: ping www.athena.edu.vn

IV/ Một số công cụ kiểm tra DNS:

- dig (domain information groper): dig @192.168.36.230 www.athena.edu.vn ANY

- nslookup: nslookup www.athena.edu.vn

- host: host -a www.athena.edu.vn 192.168.36.230

Bài Lab 4: Web Server

I/ Cài đặt Apache:

Apache là một phần mềm Web Server có nhiều tính năng như sau:

- Hỗ trợ đầy đủ những giao thức HTTP trước đây như HTTP/1.1.
- Có thể cấu hình và mở rộng với những module của công ty thứ ba.
- Cung cấp source code đầy đủ với license không hạn chế.
- Chạy được trên nhiều HĐH như Win 9x, Netware 5.x, OS/2, Unix, Linux

- Kiểm tra Apache đã được cài đặt hay chưa:

```
[root@testsrv /]# rpm -qa | grep httpd
```

- Cài đặt (nếu chưa được cài đặt):

```
[root@testsrv /]# rpm -ivh httpd-2.2.3-11.el5_1.centos.3.i386.rpm
Preparing... ##### [100%]
1:httpd ##### [100%]
```

- Kiểm tra Apache đã được cài đặt trên hệ thống:

```
[root@testsrv /]# rpm -qa | grep httpd
httpd-2.2.3-11.el5_1.centos.3
```

II/ Cấu hình Apache Web Server:

file dùng để cấu hình apache web server là `/etc/httpd/conf/httpd.conf`

- Tạo thư mục gốc cho web site:

```
[root@testsrv html]# mkdir /var/www/html/myweb
```

- Tạo một trang html như sau:

```
[root@testsrv html]# vi /var/www/html/myweb/index.html
<html>
    <head><title>Test Page</title></head>
    <body>
        <p>Trung Tam Athena Xin Chao Cac Ban !!! </p>
    </body>
</html>
```

- Sửa file cấu hình httpd.conf như sau:

```
[root@testsrv /]# vi /etc/httpd/conf/httpd.conf
ServerRoot "/etc/httpd"      # Vị trí cài đặt Apache
Timeout      120              # Thời gian sống của một kết nối (giây)
KeepAlive    On               # Cho phép client gửi nhiều y/c đến server qua 1 kết nối
MaxkeepAliveRequests 100      # Số request tối đa trên một kết nối
KeepAliveTimeout 15           # Thời gian timeout của một request (giây)
Listen       80               # Lắng nghe trên port 80
User         apache           # User và Group để chạy httpd
Group        apache
ServerAdmin  root@localhost   # Email của người quản trị
ServerName   www.athena.edu.vn # Khai báo địa chỉ URL
DocumentRoot "/var/www/html"  # Thư mục gốc của web server
```

```
<Directory "/var/www/html/myweb">
    Options Indexes FollowSymLinks
    Order deny,allow
    Deny from all
    Allow from 192.168.36.0/255.255.255.0
</Directory>
```

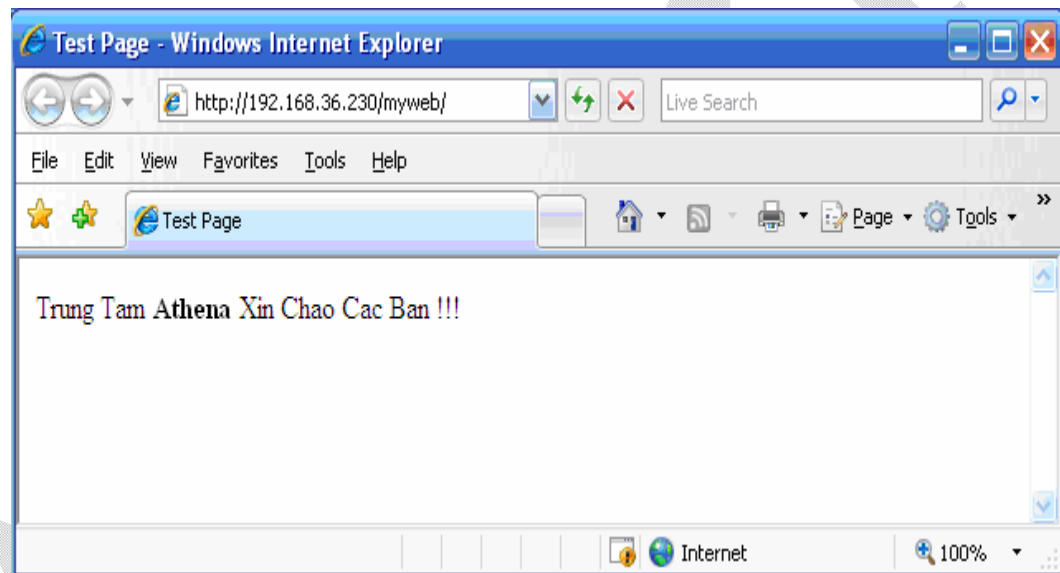
```
DirectoryIndex      index.html    # Tập tin mặc định khi chạy website
ErrorLog             logs/error_log # Lưu các Error log (/etc/httpd/logs/error_log)
CustomLog            log/access_log # Lưu các access log (/etc/httpd/logs/error_log)
```

- Start httpd daemon:

```
[root@testsrv conf]# service httpd start
Starting httpd:
```

[OK]

III/ Truy cập web server:



IV/ Chứng thực truy cập: (Base Authentication)

1/ Tạo tập tin passwords:

- Tạo 2 user truy cập như sau:

```
[root@testsrv /]# useradd user1
[root@testsrv /]# useradd user2
```

- Tạo tập tin passwords cho 2 user vừa tạo như sau:

```
[root@testsrv /]# useradd user2
[root@testsrv /]# htpasswd -c /etc/httpd/conf/passwords user1
New password:
Re-type new password:
Adding password for user user1
```

```
[root@testsrv /]# htpasswd /etc/httpd/conf/passwords user2
New password:
Re-type new password:
Adding password for user user2
```

Lưu ý: Tùy chọn -c sẽ tạo một tập tin passwords mới. Nếu tập tin này đã tồn tại thì nó sẽ xóa nội dung cũ và ghi vào nội dung mới. Khi tạo thêm một password cho người dùng khác thì ta không dùng tùy chọn -c.

- Kiểm tra tập tin passwords vừa tạo:

```
[root@testsrv /]# cat /etc/httpd/conf/passwords
user1:QYFSqDRTo8LNU
user2:PiixHD8C.pq16
```

2/ Tạo tập tin groups như sau:

```
[root@testsrv /]# vi /etc/httpd/conf/groups
web : user1 user2
```

3/ Sửa file cấu hình của apache như sau:

```
[root@testsrv /]# vi /etc/httpd/conf/httpd.conf
.....
<Directory "/var/www/html/myweb">
    Options Indexes FollowSymLinks
    Order deny,allow
    Deny from all
    Allow from 192.168.36.0/255.255.255.0
```

AuthType	Basic
AuthName	"Temporary"
AuthUserFile	/etc/httpd/conf/passwords
AuthGroupFile	/etc/httpd/conf/groups
Require group	web

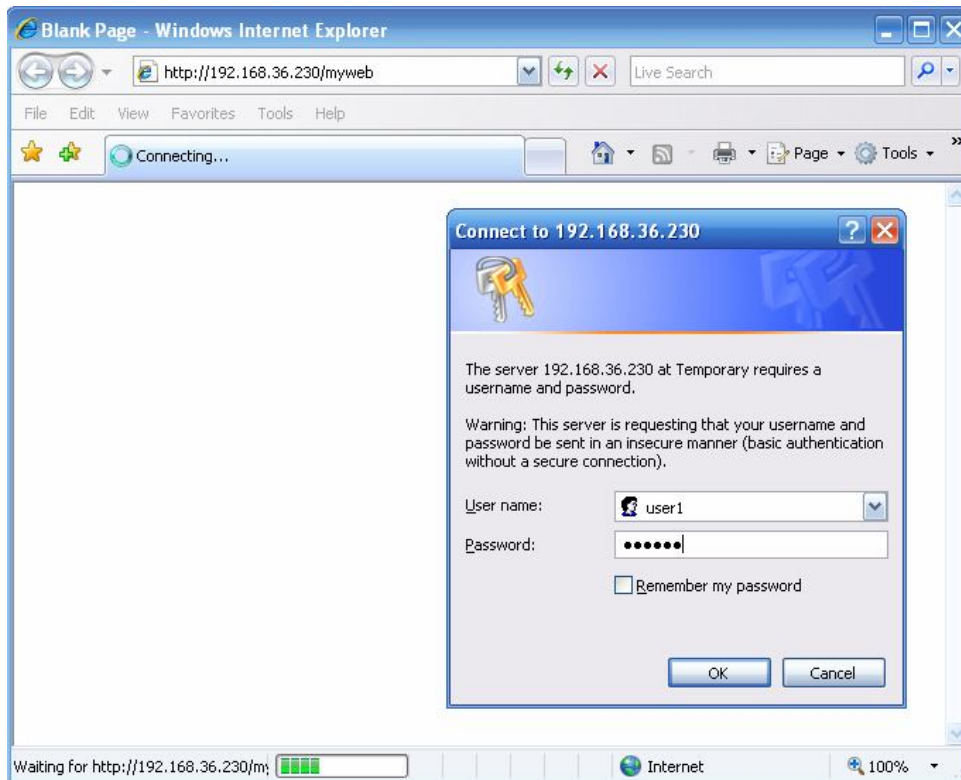
```
</Directory>
.....
```

4/ Restart httpd daemon:

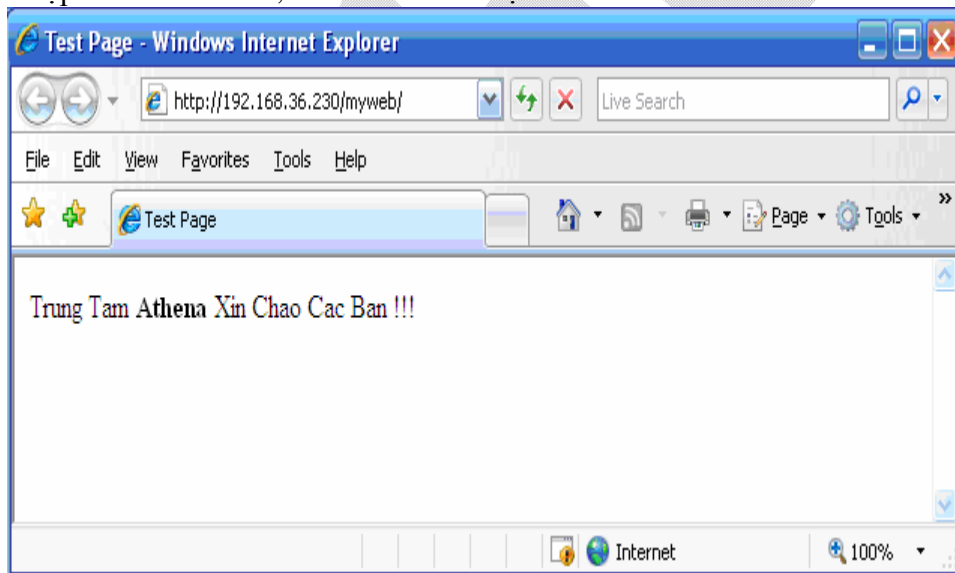
```
[root@testsrv /]# service httpd restart
Stopping httpd:
Starting httpd:
```

```
[ OK ]
[ OK ]
```

5/ Kiểm tra truy cập:



Nhập vào User name, Password => Chọn OK



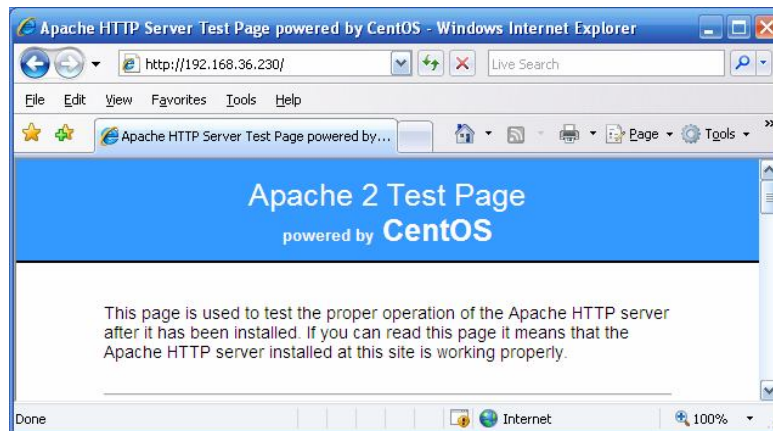
V/ VirtualHost:

là tính năng cho phép ta tạo nhiều hơn một website trên server.

Các cách tạo virtual host là: *IP-based virtual host* (một IP cho một website yêu cầu phải có nhiều IP) và *Named-based virtual host* (một IP cho nhiều tên khác nhau yêu cầu phải có DNS server).

Ở đây sẽ hướng dẫn các bạn tạo virtualhost bằng cách *IP-based virtual host*.

- Kiểm tra host trên card mạng eth0



- Tạo một IP khác trên card mạng eth0

```
[root@testsrv www]# ifconfig eth0:0 192.168.36.233 netmask 255.255.255.0 up
```

- Sửa file httpd.conf như sau:

```
[root@testsrv /]# vi /etc/httpd/conf/httpd.conf
<VirtualHost 192.168.36.233:80>
    ServerAdmin root@localhost
    DocumentRoot /var/www/html/myweb
    ServerName athena.edu.vn
    ErrorLog logs/dummy-host.example.com-error_log
    CustomLog logs/dummy-host.example.com-access_log common
</VirtualHost>
```

- Restart httpd daemon:

```
[root@testsrv /]# service httpd restart
```

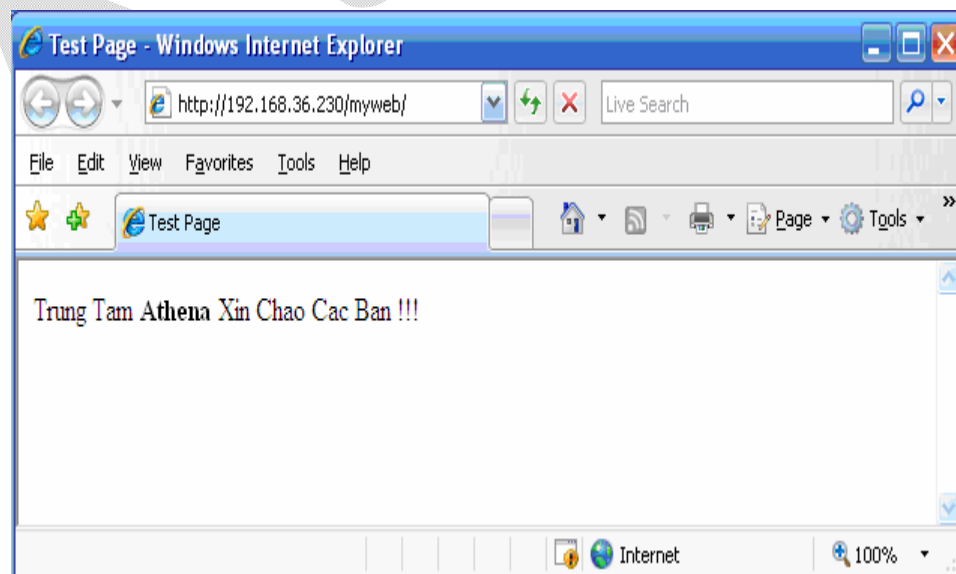
```
Stopping httpd:
```

```
[ OK ]
```

```
Starting httpd:
```

```
[ OK ]
```

- Kiểm tra:



VI/ Cài đặt php:

- Kiểm tra php đã được cài đặt hay chưa:

```
[root@testsrv /]# rpm -qa | grep php
```

- Cài đặt (nếu chưa được cài đặt):

```
[root@testsrv /]# rpm -ivh php-5.1.6-15.el5.i386.rpm
Preparing... ##### [100%]
1:php ##### [100%]
```

- Kiểm tra php đã được cài đặt trên hệ thống:

```
[root@testsrv /]# rpm -qa | grep php
php-cli-5.1.6-15.el5
php-common-5.1.6-15.el5
php-5.1.6-15.el5
```

VII/ Cấu hình Apache hỗ trợ php:

- Sửa file httpd.conf như sau:

```
[root@testsrv /]# vi /etc/httpd/conf/httpd.conf
DirectoryIndex index.html index.php index.html.var
LoadModule php5_module modules/libphp5.so
```

- Tạo trang web php như sau:

```
[root@testsrv /]# vi /var/www/html/index.php
<?php
phpinfo();
?>
```

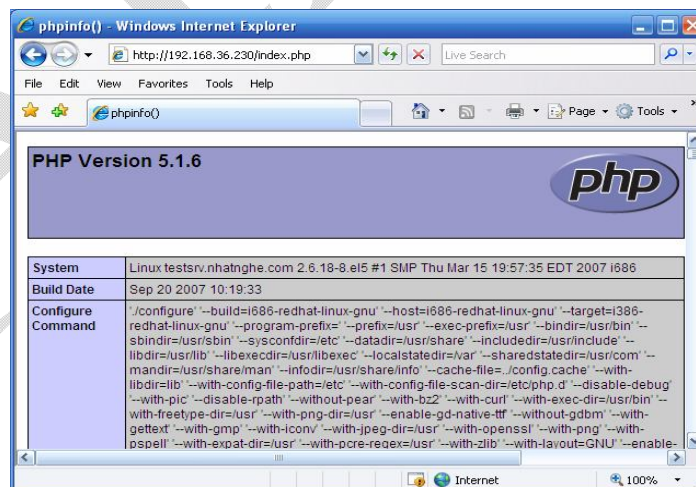
- Restart httpd daemon:

```
[root@testsrv /]# service httpd restart
Stopping httpd:
Starting httpd:
```

[OK]

[OK]

- Kiểm tra



Bài Lab 4 (tt): Apache + DNS

I/ Cài đặt Apache:

```
[root@testsrv /]# rpm -ivh httpd-2.2.3-11.el5_1.centos.3.i386.rpm
Preparing... ##### [100%]
1:httpd ##### [100%]
```

II/ Cấu hình web server cho domain webtest.com:

- Tạo thư mục web như sau:

```
[root@testsrv /]# mkdir /var/www/html/webtest
```

- Tạo một trang index.html như sau:

```
[root@testsrv /]# vi /var/www/html/webtest/index.html
<html>
    <head><title>Test Page</title></head>
    <body>
        <p>Trung Tam Athena Xin Chao Cac Ban !!! </p>
        <p>Bai Lap: Cai dat Apache va DNS</p>
    </body>
</html>
```

- Sửa file cấu hình httpd.conf như sau:

```
[root@testsrv /]# vi /etc/httpd/conf/httpd.conf
.....
<VirtualHost 192.168.36.230:80>
    ServerAdmin root@localhost
    DocumentRoot /var/www/html/webtest
    ServerName www.webtest.com
    ErrorLog logs/dummy-host.example.com-error_log
    CustomLog logs/dummy-host.example.com-access_log common
</VirtualHost>
```

- Start httpd daemon:

```
[root@testsrv /]# service httpd start
Starting httpd: [ OK ]
```

III/ Cài đặt DNS:

```
[root@testsrv /]# rpm -ivh bind-libs-9.3.3-10.el5.i386.rpm
Preparing... ##### [100%]
1:bind-libs ##### [100%]
[root@testsrv /]# rpm -ivh bind-9.3.3-10.el5.i386.rpm
Preparing... ##### [100%]
1:bind ##### [100%]
[root@testsrv /]# rpm -ivh bind-utils-9.3.3-10.el5.i386.rpm
Preparing... ##### [100%]
1:bind-utils ##### [100%]
```

III/ Khai báo domain webtest.com:

- Tạo file /etc/named.conf như sau:

```
[root@testsrv /]# vi /etc/named.conf
```

```
options
{
    query-source      port 53;
    query-source-v6   port 53;
    directory         "/var/named"; // the default
    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";
    notify            yes;
};

zone "." in {
    type hint;
    file "named.root";
};

zone "webtest.com" {
    type master;
    file "webtest.com.db";
};

zone "36.168.192.in-addr.arpa" {
    type master;
    file "36.168.192.in-addr.arpa.db";
};
```

- Tạo file /var/named/named.root bằng cách download trên mạng như sau:

```
[root@testsrv /]# cd /var/named,
[root@testsrv named]# wget http://www.internic.net/zones/named.root
--08:29:53-- http://www.internic.net/zones/named.root
Resolving www.internic.net... 208.77.188.101
Connecting to www.internic.net|208.77.188.101|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2878 (2.8K) [text/plain]
Saving to: `named.root'

100%[=====>] 2,878      --.-K/s   in 0s

08:29:53 (38.6 MB/s) - `named.root' saved [2878/2878]
```

Chú ý: Server phải kết nối đến internet.

- Tạo file /var/named/webtest.com.db:

```
[root@testsrv /]# vi /var/named/webtest.com.db
$TTL 86400      ; 1 day
@               IN SOA  dns1.athena.edu.vn. root (
                                20080213      ; serial
                                10800          ; refresh (3 hours)
                                3600           ; retry (1 hour)
                                604800         ; expire (1 week)
                                86400          ; minimum (1 day)
                                )
web             IN      NS      dns1.athena.edu.vn .
web             IN      A       192.168.36.230
www             IN      CNAME   web
```

- Tạo file /var/named/36.168.192.in-addr.arpa.db:

```
[root@testsrv named]# vi /var/named/36.168.192.in-addr.arpa.db
```

```
$TTL 86400      ; 1 day
@               IN SOA  dns1.athena.edu.vn. root (
                                20080213      ; serial
                                10800          ; refresh (3 hours)
                                3600          ; retry (1 hour)
                                604800        ; expire (1 week)
                                86400         ; minimum (1 day)
                                )
                IN      NS      dns1.athena.edu.vn.
230            IN      PTR      athena.edu.vn.
```

- Start named daemon:

```
[root@testsrv named]# service named start
Starting named:
```

[OK]

- Stop firewall

```
[root@testsrv named]# service iptables stop
Flushing firewall rules:
Setting chains to policy ACCEPT: filter
Unloading iptables modules:
```

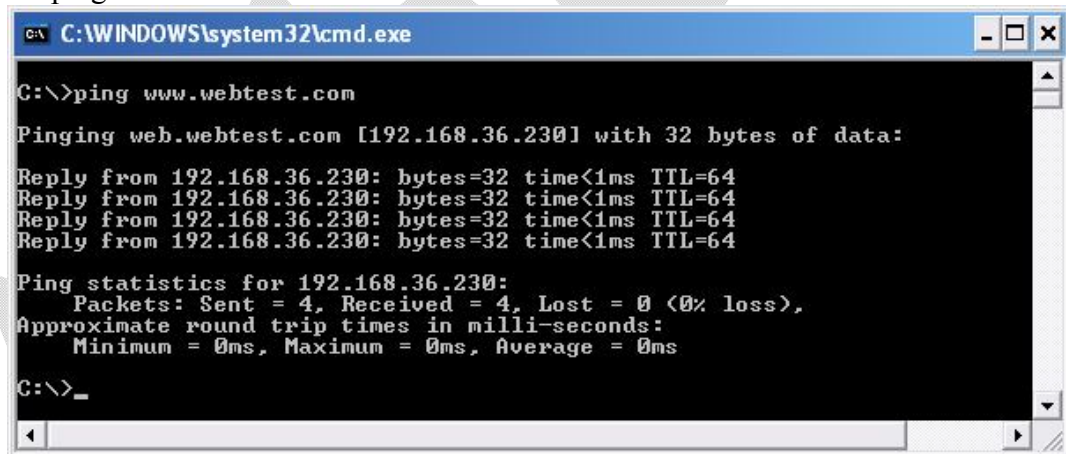
[OK]

[OK]

[OK]

IV/ Kiểm tra:

- Khai báo trên máy client chỉ đến DNS server là: 192.168.36.230
- Kiểm tra ping:



```
C:\WINDOWS\system32\cmd.exe

C:\>ping www.webtest.com

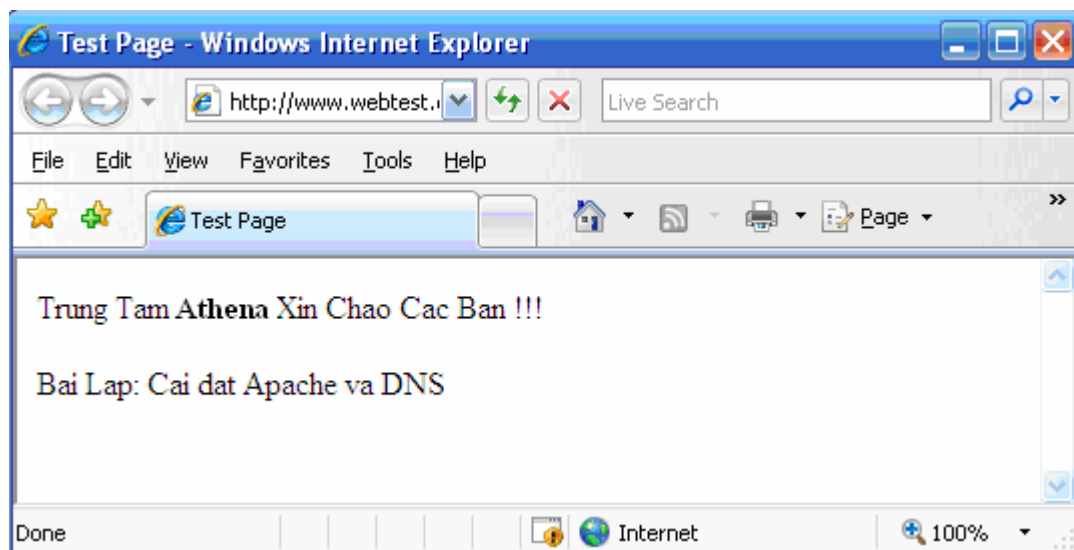
Pinging web.webtest.com [192.168.36.230] with 32 bytes of data:

Reply from 192.168.36.230: bytes=32 time<1ms TTL=64
Reply from 192.168.36.230: bytes=32 time<1ms TTL=64
Reply from 192.168.36.230: bytes=32 time<1ms TTL=64
Reply from 192.168.36.230: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.36.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>_
```

- Kiểm tra truy cập:



Bài Lab 5: Squid server

I/ Cài đặt Squid:

Squid là một chương trình Internet proxy-caching có vai trò tiếp nhận các yêu cầu từ các clients và chuyển cho Internet server thích hợp. Đồng thời, nó cũng lưu lại trên đĩa những dữ liệu được trả về từ Internet server gọi là caching.

Những giao thức hỗ trợ trên Squid: HTTP, FTP, SSL, ...

- Kiểm tra Squid đã được cài đặt hay chưa:

```
[root@testsrv /]# rpm -qa | grep squid
```

- Cài đặt (nếu chưa được cài đặt):

```
[root@testsrv /]# rpm -ivh squid-2.6.STABLE6-5.el5_1.2.i386.rpm
Preparing... ##### [100%]
1:squid ##### [100%]
```

- Kiểm tra Squid đã được cài đặt trên hệ thống:

```
[root@testsrv /]# rpm -qa | grep squid
squid-2.6.STABLE6-5.el5_1.2
```

II/ Cấu hình web server để test:

- Cài đặt apache

- Tạo thư mục gốc cho web site:

```
[root@testsrv html]# mkdir /var/www/html/myweb
```

- Tạo một trang html như sau:

```
[root@testsrv html]# vi /var/www/html/myweb/index.html
<html>
    <head><title>Test Page</title></head>
    <body>
        <p>Trung Tam Athena Xin Chao Cac Ban !!! </p>
    </body>
</html>
```

- Sửa file cấu hình httpd.conf như sau:

```
[root@testsrv /]# vi /etc/httpd/conf/httpd.conf
<Directory "/var/www/html/myweb">
    Options Indexes FollowSymLinks
    Order deny,allow
    Deny from all
    Allow from 192.168.36.0/255.255.255.0
</Directory>
```

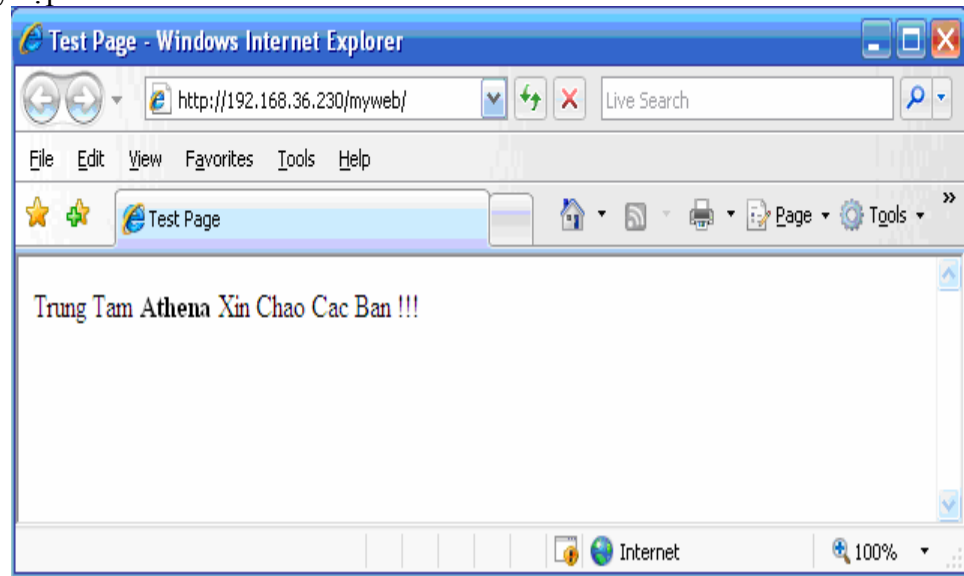
- Start httpd daemon:

```
[root@testsrv conf]# service httpd start
Starting httpd: _ [ OK ]
```

- Stop iptables:

```
[root@mail /]# service iptables stop
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
```


- Kiểm tra truy cập:



III/ Cấu hình Squid:

1/ Thông tin cấu hình chung: Thay đổi một số options sau:

```
[root@testsrv /]# vi /etc/squid/squid.conf
http_port      8080    #cổng http mà squid lắng nghe
cache_mem      10 MB   #cho phép cache 10MB
cache_dir      ufs      /var/spool/squid 100 16 255 #thư mục lưu trữ cache
```

Store type: ufs, aufs, diskd size thư mục (MB) Số thư mục con cấp 1 Số thư mục con cấp 2

```
access_log      /var/log/squid/access.log    # lưu active requests của clients
```

2/ Access Control: thêm vào cuối cùng của tag *acl* trong file *squid.conf*

a/ Cấu hình cho cho phép truy cập mạng nội bộ từ thứ 2 đến thứ 6 từ 8h đến 17h.

- Sửa file cấu hình

```
[root@testsrv /]# vi /etc/squid/squid.conf
.....
acl    my_network    src    192.168.36.0/24
acl    allow_hours    time    MTWHF 8:00-17:00    #thu bay:A    chu nhat:S

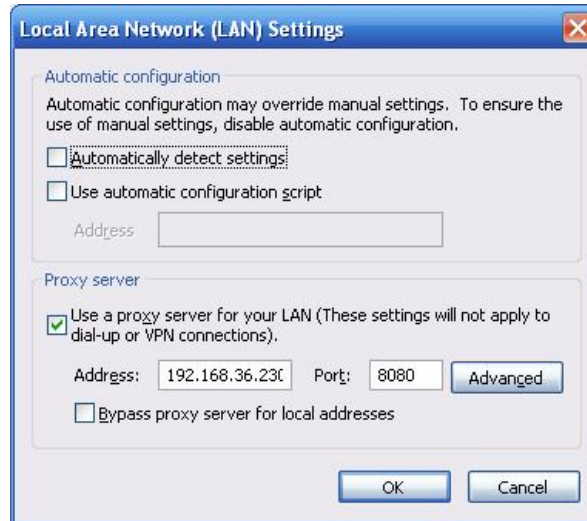
http_access      allow    my_network    allow_hours
http_access      deny     all

.....
```

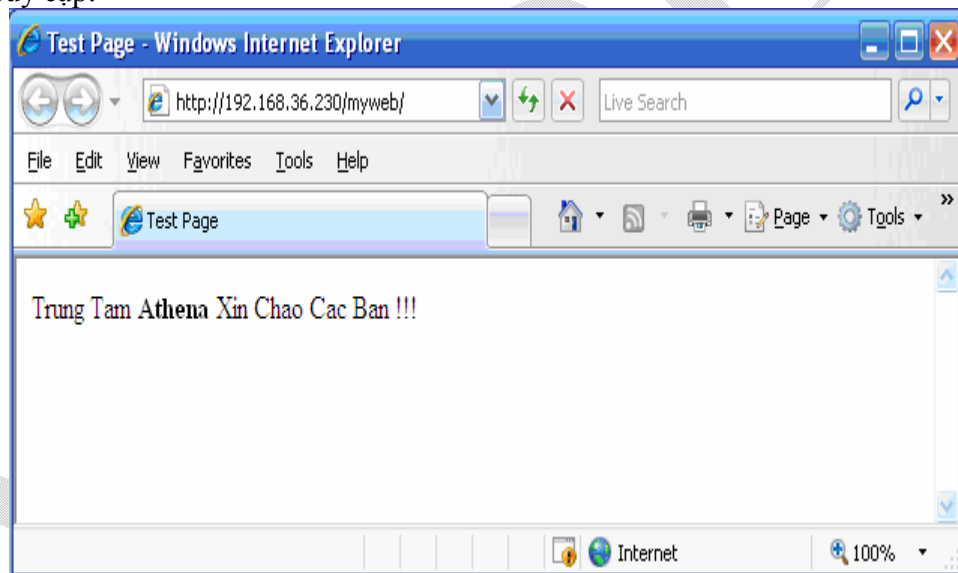
- Restart squid daemon:

```
[root@testsrv /]# service squid restart
Stopping squid: . [ OK ]
Starting squid: . [ OK ]
```

- Khai báo proxy trên clients:



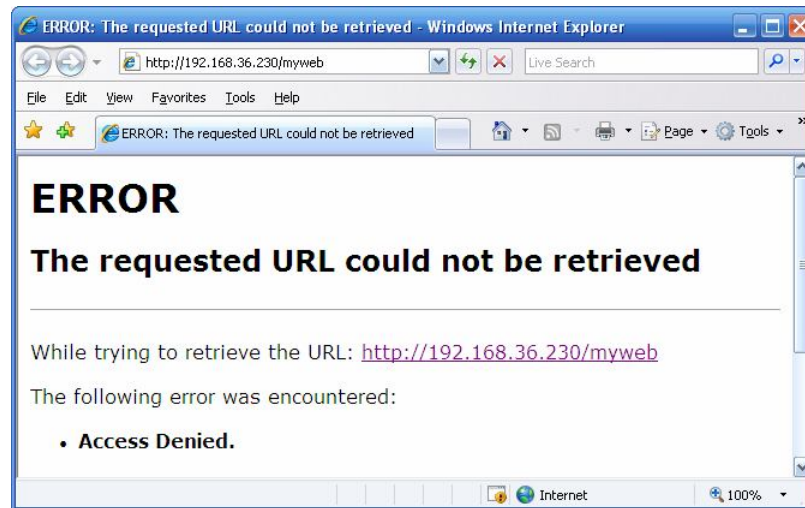
- Kiểm tra truy cập:



- Thay đổi giờ trên proxy server:

```
[root@testsrv /]# date -s 05:00  
Thu Feb 28 05:00:00 ICT 2008
```
- Kiểm tra ngày giờ trên hệ thống:

```
[root@testsrv /]# date  
Thu Feb 28 05:00:01 ICT 2008
```
- Kiểm tra truy cập:



b/ Cho phép truy cập/cấm truy cập đến một số websites.

- Tạo file chứa danh sách các sites được phép truy cập:

```
[root@testsrv /]# vi /etc/squid/allow_sites
```

```
www.yahoo.com
```

```
www.nhatnghe.com
```

- Tạo file chứa danh sách các sites cấm truy cập:

```
[root@testsrv /]# vi /etc/squid/deny_sites
```

```
www.vnexpress.net
```

```
www.tuoitre.com
```

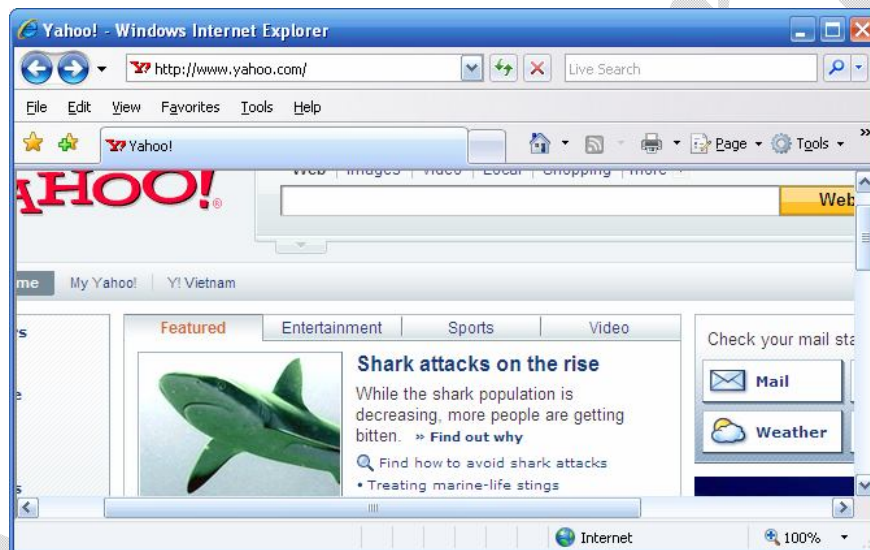
- Sửa file cấu hình:

```
[root@testsrv /]# vi /etc/squid/squid.conf
```

```
.....
acl    my_network      src      192.168.36.0/24
acl    allow_hours     time     MTWHF 8:00-17:00      #thu bay:A   chu nh:t:S
acl    good_sites      dstdomain  "/etc/squid/allow_sites"
acl    bad_sites       dstdomain  "/etc/squid/deny_sites"

http_access      deny    bad_sites
http_access      allow   my_network allow_hours good_sites
http_access      deny    all
.....
```

- Thực hiện kiểm tra truy cập:



Kiểm tra click vào Mail có được không ? tại sao ?

c/ Cho phép truy cập/cấm truy cập đến một số Domains.

- Tạo file chứa danh sách các domains được phép truy cập:

```
[root@testsrv /]# vi /etc/squid/allow_domains
yahoo.com
dantri.com.vn
```

- Tạo file chứa danh sách các domains cấm truy cập:

```
[root@testsrv /]# vi /etc/squid/deny_domains
vnexpress.net
tuoitre.com
```

- Sửa file cấu hình:

```
[root@testsrv /]# vi /etc/squid/squid.conf
.....
acl      my_network      src      192.168.36.0/24
acl      allow_hours     time     MTWTF 8:00-17:00      #thu bay:A  chu nhât:S
acl      good_domains    url_regex -i  "/etc/squid/allow_domains"
acl      bad_domains     url_regex -i  "/etc/squid/deny_domains"

http_access      deny      bad_domains
http_access      allow     my_network allow_hours good_domains
http_access      deny      all
.....
```

- Restart squid daemon:

- Thực hiện kiểm tra truy cập: *mail.yahoo.com*

d/ Dùng NCSA kiểm định password.

- Tạo user test:

```
[root@testsrv /]# useradd test
```

- Tạo file squid_passwd bằng công cụ htpasswd như sau:

```
[root@testsrv /]# htpasswd -c /etc/squid/squid_passwd test
New password:
Re-type new password:
Adding password for user test
```

- Sửa file cấu hình:

```
[root@testsrv /]# vi /etc/squid/squid.conf
.....
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/squid_passwd

acl      my_network      src      192.168.36.0/24
acl      ncsa_users      proxy_auth  REQUIRED

http_access      allow     my_network ncsa_users
http_access      deny      all
.....
```

- Restart squid daemon:

- Kiểm tra truy cập: trang www.dantri.com.vn

Nhập vào Username, password => chọn OK

e/ Giới hạn nội dung các file download.

- Tạo file chứa các phần mở rộng các files cần giới hạn download

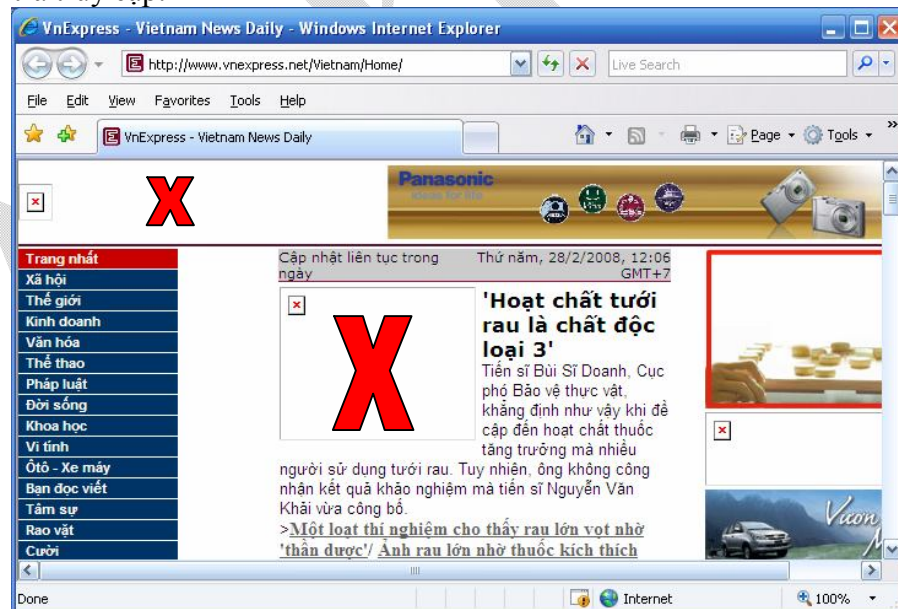
```
[root@testsrv /]# vi /etc/squid/lock_files.acl  
\.gif  
\.jpeg
```

- Sửa file cấu hình:

```
[root@testsrv /]# vi /etc/squid/squid.conf  
.....  
acl    my_network      src      192.168.36.0/24  
acl    lock_files      urlpath_regex  "/etc/squid/lock_files.acl"  
  
http_access      deny    lock_files  
http_access      allow   my_network  
http_access      deny    all  
.....
```

- Restart squid daemon:

- Kiểm tra truy cập:



f/ Một số thiết lập khác:

- Giới hạn truy cập theo IP


```
acl    my_network    src    192.168.36.0/24
acl    deny_host     dst    192.168.36.230
```

```
http_access    deny    deny_host
http_access    allow   my_network
http_access    deny    all
```

- Giới hạn truy cập theo cổng

```
acl    my_network    src    192.168.36.0/24
acl    deny_port     port    80 1000
```

```
#http_access    deny    deny_port
http_access    allow   my_network
http_access    deny    all
```

- Giới hạn truy cập theo giao thức

```
acl    my_network    src    192.168.36.0/24
acl    deny_protocols    proto    FTP HTTP
```

```
http_access    deny    deny_protocols
http_access    allow   my_network
http_access    deny    all
```

Bài Lab 6: Mail Server

I/ Cấu hình Hostname:

- Sửa file /etc/hosts:

```
[root@testsrv /]# vi /etc/hosts
127.0.0.1          mail.athena.edu.vn
192.168.36.230    mail.athena.edu.vn
```

- Sửa file /etc/sysconfig/network

```
[root@testsrv /]# vi /etc/sysconfig/network
NETWORKING=yes
NETWORKING_IPV6=YES
HOSTNAME mail.athena.edu.vn
```

- Restart hệ thống: init 6

- Kiểm tra hostname:

```
[root@mail /]# uname -n
mail.athena.edu.vn
```

II/ Cấu hình DNS:**1/ Cài đặt DNS:**

```
[root@testsrv /]# rpm -ivh bind-libs-9.3.3-10.el5.i386.rpm
Preparing... ##### [100%]
1:bind-libs ##### [100%]
[root@testsrv /]# rpm -ivh bind-9.3.3-10.el5.i386.rpm
Preparing... ##### [100%]
1:bind ##### [100%]
[root@testsrv /]# rpm -ivh bind-utils-9.3.3-10.el5.i386.rpm
Preparing... ##### [100%]
1:bind-utils ##### [100%]
```

2/ Cấu hình DNS:

- Tạo file /etc/named.conf như sau:

```
[root@testsrv /]# vi /etc/named.conf
```

```
options
{
    query-source      port 53;
    query-source-v6   port 53;
    directory         "/var/named"; // the default
    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";
    notify             yes;
};

zone "." in {
    type hint;
    file "named.root";
};

zone "athena.edu.vn" {
    type master;
    file "athena.edu.vn.db";
};

zone "36.168.192.in-addr.arpa" {
    type master;
    file "36.168.192.in-addr.arpa.db";
};
```

- Tạo file /var/named/named.root bằng cách download trên mạng như sau:

```
[root@testsrv /]# cd /var/named/
[root@testsrv named]# wget http://www.internic.net/zones/named.root
--08:29:53-- http://www.internic.net/zones/named.root
Resolving www.internic.net... 208.77.188.101
Connecting to www.internic.net|208.77.188.101|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2878 (2.8K) [text/plain]
Saving to: `named.root'

100%[=====>] 2,878      ---K/s   in 0s

08:29:53 (38.6 MB/s) - `named.root' saved [2878/2878]
```

Chú ý: Server phải kết nối đến internet.

- Tạo file /var/named/athena.edu.vn.db:

```
[root@testsrv named]# vi /var/named/athena.edu.vn.db
$TTL 86400      ; 1 day
@      IN SOA   dns1.athena.edu.vn. root (
                                20080213      ; serial
                                10800          ; refresh (3 hours)
                                3600           ; retry (1 hour)
                                604800         ; expire (1 week)
                                86400          ; minimum (1 day)
                                )
mail    IN      NS      dns1.athena.edu.vn .
mail    IN      A       192.168.36.230
```

- Tạo file /var/named/36.168.192.in-addr.arpa.db:

```
[root@testsrv named]# vi /var/named/36.168.192.in-addr.arpa.db
$TTL 86400      ; 1 day
@               IN SOA  dns1.athena.edu.vn. root (
                                20080213      ; serial
                                10800           ; refresh (3 hours)
                                3600           ; retry (1 hour)
                                604800        ; expire (1 week)
                                86400         ; minimum (1 day)
                                )
                IN      NS      dns1.athena.edu.vn.
230            IN      PTR      mail.athena.edu.vn.
```

- Start named daemon:

```
[root@testsrv named]# service named start
Starting named: [ OK ]
```

- Stop firewall

```
[root@testsrv named]# service iptables stop
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
```

III/ Cấu hình Mail Server:

1/ Cấu hình Postfix:

- Có thể cài đặt postfix bằng Add/Remove Program, bằng gói source, hoặc bằng rpm.
- Sửa file cấu hình /etc/postfix/main.cf, chú ý những phần sau:

Những option cấu hình chung:

```
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix
data_directory = /var/lib/postfix
mail_owner = postfix
mydomain = nhatnghe.com
myhostname = mail.nhatnghe.com
```

Server sẽ gửi mail ra ngoài bằng domain nào.

```
myorigin = $mydomain
```

#Server sẽ lắng nghe trên địa chỉ nào để nhận mail về.

```
inet_interfaces = all
mydestination = $mydomain
```

- Với những cấu hình cơ bản này, ta đã có thể start dịch vụ postfix, chkconfig để dịch vụ postfix có thể start mỗi khi khởi động:

```
[root@test root]# postfix start
postfix/postfix-script: starting the Postfix mail system
```

- Dùng lệnh `useradd` để thêm hai user `test1`, `test2` vào hệ thống.
- Kiểm tra việc gửi nhận qua postfix với 2 account này. Lúc này, postfix đang nhận account là account của hệ thống, mail được lưu trữ trong `/var/spool/mail`

Dùng các lệnh sau:

```
ehlo mail.athena.edu.vn
mail from: test1@athena.edu.vn
rcpt to: test2@athena.edu.vn
data
<nhập nội dung thư>
<kết thúc bằng dấu "." Và Enter >
```

- Kiểm tra mail trong `/var/spool/mail/test2`: `less /var/spool/mail/test2`

2/ Kiểm soát các policy của Postfix:

- Postfix hỗ trợ nhiều policy để kiểm soát quá trình gửi nhận mail rất linh hoạt.

Restriction list name	Status	Effect of REJECT or DEFER result
smtpd_client_restrictions	Optional	Reject all client commands
smtpd_helo_restrictions	Optional	Reject HELO/EHLO information
smtpd_sender_restrictions	Optional	Reject MAIL FROM information
smtpd_recipient_restrictions	Required	Reject RCPT TO information
smtpd_data_restrictions	Optional	Reject DATA command
smtpd_end_of_data_restrictions	Optional	Reject END-OF-DATA command
smtpd_etrn_restrictions	Optional	Reject ETRN command

- Có thể tìm kiếm thông tin chi tiết về các policy này ở www.postfix.org. Trong phạm vi của bài lab, chỉ nêu một số policy thông dụng.

- Đánh giá địa chỉ sender, để quyết định có chấp nhận mail hay không:

`smtpd_sender_restrictions` có thể nhận các giá trị sau:

```
check_sender_access
reject_authenticated_sender_login_mismatch
reject_non_fqdn_sender
reject_rhsbl_sender rbl_domain=d.d.d.d
reject_unauthenticated_sender_login_mismatch
reject_unverified_sender
```

.....

Vd: [smtpd_sender_restrictions = reject_unknown_sender_domain](#)
[smtpd_sender_restrictions = reject_unknown_sender_domain,](#)

- Đánh giá địa chỉ rcpt, để quyết định chuyển mail:

`smtpd_recipient_restrictions` có thể nhận các giá trị sau:

```
check_recipient_access
check_recipient_mx_access
```

permit_auth_destination
reject_non_fqdn_recipient
reject_unauth_destination
reject_rhsbl_recipient *rbl_domain=d.d.d.d*
.....

Vd: [smtpd_recipient_restrictions](#) = [permit_mynetworks](#), [reject_unauth_destination](#)

- Kiểm soát kích thước mailbox:

mailbox_size_limit
message_size_limit

- Kiểm soát số rept nhận mail đồng thời:

smtpd_recipient_limit

- Kiểm soát số kết nối đồng thời, số lượng kết nối đồng thời:

smtpd_client_connection_count_limit (default: 50)
smtpd_client_connection_rate_limit (default: no limit)
smtpd_client_message_rate_limit (default: no limit)
smtpd_client_recipient_rate_limit (default: no limit)
smtpd_client_new_tls_session_rate_limit (default: no limit)
smtpd_client_event_limit_exceptions (default: *\$mynetworks*)

3/ Cài đặt Cyrus-imapd:

- Cyrus-imapd là phần mềm dùng để lưu trữ mail. Mặc định, MTA sẽ lưu mail thành một file text cho từng user ở thư mục /var/spool/mail.
- Với sự hiện thực của phần mềm Cyrus-imapd, mail sẽ được lưu trữ thành cấu trúc phân cấp cây thư mục để tiện lợi cho việc quản lý, tìm kiếm.

- Kiểm tra cyrus-imapd đã được cài đặt hay chưa:

```
[root@mail packages]# rpm -qa | grep cyrus-imapd
```

- Cài đặt (nếu chưa được cài đặt):

```
[root@mail packages]# rpm -ivh cyrus-imapd-perl-2.3.7-1.1.el5.i386.rpm
Preparing... ##### [100%]
 1:cyrus-imapd-perl ##### [100%]
[root@mail packages]# rpm -ivh cyrus-imapd-utils-2.3.7-1.1.el5.i386.rpm
Preparing... ##### [100%]
 1:cyrus-imapd-utils ##### [100%]

[root@mail packages]# rpm -ivh db4-utils-4.3.29-9.fc6.i386.rpm
Preparing... ##### [100%]
 1:db4-utils ##### [100%]
[root@mail packages]# rpm -ivh lm_sensors-2.10.0-3.1.i386.rpm
Preparing... ##### [100%]
 1:lm_sensors ##### [100%]
[root@mail packages]# rpm -ivh cyrus-imapd-2.3.7-1.1.el5.i386.rpm
Preparing... ##### [100%]
 1:cyrus-imapd ##### [100%]
```

4/ Cấu hình cyrus-imapd:

- Cyrus-imapd có hai file cấu hình chính: /etc/cyrus.conf và /etc/imapd.conf
- File /etc/cyrus.conf điều khiển cấu hình:
 - o Hỗ trợ user check mail bằng POP, IMAP. Mở sẵn bao nhiêu tiến trình từ lúc đầu.
 - o Nhận mail deliver từ MTA bằng lmtp qua socket hay qua IP.

```
# standard standalone server implementation

START {
    # do not delete this entry!
    recover          cmd="ctl_cyrusdb -r"

    # this is only necessary if using idled for IMAP IDLE
    # idled           cmd="idled"
}

# UNIX sockets start with a slash and are put into /var/imap/socket
SERVICES {
    # add or remove based on preferences
    imap             cmd="imapd" listen="imap" prefork=0
    #imaps            cmd="imapd -s" listen="imaps" prefork=0
    pop3             cmd="pop3d" listen="pop3" prefork=0
    #pop3s            cmd="pop3d -s" listen="pop3s" prefork=0
    #sieve            cmd="timsieved" listen="sieve" prefork=0

    # these are only necessary if receiving/exporting usenet via NNTP
    # nntp            cmd="nntpd" listen="nntp" prefork=0
    # nntps           cmd="nntpd -s" listen="nntps" prefork=0

    # at least one LMTP is required for delivery
    # lmtp            cmd="lmtpd" listen="lmtp" prefork=0
    lmtpunix         cmd="lmtpd" listen="/var/imap/socket/lmtp" prefork=0

    # this is required if using notifications
    # notify          cmd="notifyd" listen="/var/imap/socket/notify" proto="udp" prefork=1
}

EVENTS {
    # this is required
    checkpoint       cmd="ctl_cyrusdb -c" period=30

    # this is only necessary if using duplicate delivery suppression,
    # Sieve or NNTP
    delprune         cmd="cyr_expire -E 3" at=0400

    # this is only necessary if caching TLS sessions
    tlsprune         cmd="tls_prune" at=0400
}
```

- File /etc/imapd.conf điều khiển cấu hình:
 - o Lưu trữ mailbox ở đâu.
 - o IMAP server sẽ hỗ trợ domain nào.
 - o Chứng thực user nhận mail bằng phương thức nào: user local, hoặc dùng qua cơ sở dữ liệu. Điều này tạo nên khả năng tùy biến cao trong việc quản lý user.

```
# vi /etc/imapd.conf
configdirectory: /var/lib/imap
partition-default: /var/spool/imap
admins: cyrus
sievedir: /var/lib/imap/sieve
sendmail: /usr/sbin/sendmail
hashimapspool: true
virtdomains: userid
defaultdomains: athena.edu.vn
sasl_pwcheck_method: saslauthd
sasl_mech_list: PLAIN
tls_cert_file: /etc/pki/cyrus-imapd/cyrus-imapd.pem
tls_key_file: /etc/pki/cyrus-imapd/cyrus-imapd.pem
tls_ca_file: /etc/pki/tls/certs/ca-bundle.crt
```


- Dùng những lệnh sau để tạo cấu trúc lưu trữ cho IMAP server:

```
[root@dnssrv1 /]# su cyrus
bash-3.1$ /usr/lib/cyrus-imapd/mkimap
reading configure file /etc/imapd.conf...
i will configure directory /var/lib/imap.
i saw partition /var/spool/imap.
done
configuring /var/lib/imap...
creating /var/spool/imap...
done
```

- Xem lại cấu trúc sau khi đã tạo:

```
[root@dnssrv1 /]# ls -lh /var/spool/imap/
total 32K
drwx----- 3 cyrus mail 4.0K Mar  3 14:43 domain
drwxr-x--- 2 cyrus mail 4.0K Mar  3 14:40 stage.
drwxr-x--- 2 cyrus mail 4.0K Mar  3 14:40 sync.
drwx----- 3 cyrus mail 4.0K Mar  3 14:43 t
[root@dnssrv1 /]# ls -lh /var/lib/imap/
total 160K
-rwxr-x--- 1 cyrus mail 144 Mar  3 15:16 annotations.db
drwxr-x--- 2 cyrus mail 4.0K Mar  3 14:42 backup
drwxr-x--- 2 cyrus mail 4.0K Mar  3 15:16 db
drwx----- 2 cyrus mail 4.0K Mar  3 15:16 db.backup1
drwx----- 2 cyrus mail 4.0K Mar  3 15:10 db.backup2
-rw----- 1 cyrus mail 8.0K Mar  3 15:16 deliver.db
drwxr-x--- 2 cyrus mail 4.0K Mar 14 2007 log
-rwxr-x--- 1 cyrus mail 1.9K Mar  3 15:16 mailboxes.db
drwxr-x--- 2 cyrus mail 4.0K Mar 14 2007 md5
drwxr-x--- 2 cyrus mail 4.0K Mar 14 2007 msg
drwxr-x--- 2 cyrus mail 4.0K Mar  3 15:17 proc
drwxr-x--- 2 cyrus mail 4.0K Mar 14 2007 ptclient
drwxr-x--- 2 cyrus mail 4.0K Mar 14 2007 quota
drwxr-x--- 2 cyrus mail 4.0K Mar  3 15:16 rpm
drwxr-x--- 2 cyrus mail 4.0K Mar 14 2007 sieve
drwxr-x--- 2 cyrus mail 4.0K Mar  3 15:16 socket
drwxr-x--- 2 cyrus mail 4.0K Mar 14 2007 sync
-rw----- 1 cyrus mail 8.0K Mar  3 15:16 tls_sessions.db
drwxr-x--- 2 cyrus mail 4.0K Mar 14 2007 user
```

5/ Test chứng thực với cyrus-imapd bằng saslauthd:

- Start service saslauthd để bắt đầu chứng thực:

```
[root@dnssrv1 /]# service saslauthd restart
Stopping saslauthd: [ OK ]
Starting saslauthd: [ OK ]
```

- Start cyrus-imapd bằng tiến trình cyrus-master. Tạo script để khởi động imap như một service, hoặc chạy trực tiếp bằng lệnh:

```
[root@dnssrv1 /]# service cyrus-imapd start
Importing cyrus-imapd databases: [ OK ]
Starting cyrus-imapd: [ OK ]
```

- Dùng lệnh imtest thử chứng thực với user cyrus (ở đây dùng cách chứng thực localuser cyrus là user của hệ thống).

Dùng lệnh: `imtest -a cyrus@athena.edu.vn -u cyrus@athena.edu.vn -m login localhost`

- Dùng lệnh `useradd` thêm hai user hệ thống test1, test2.

```
[root@dnssrv1 /]# useradd test1
[root@dnssrv1 /]# useradd test2
```

- Đăng nhập bằng user cyrus (user quản trị của domain nhatnghe.com), tạo mailbox cho hai user test1 và test2:

```
cyrusadm -u cyrus localhost
>cm user.test1@athena.edu.vn
>cm user.test1@athena.edu.vn.INBOX
>cm user.test1@athena.edu.vn.SENT
```

Tương tự cho việc tạo account mail test2.

- Xem lại cấu trúc sau khi đã tạo mailbox:

```
[root@dnssrv1 /]# ls -lh /var/spool/imap/domain/a/athena.edu.vn/t/user/
total 16K
drwx----- 2 cyrus mail 4.0K Mar  3 14:43 test1
drwx----- 2 cyrus mail 4.0K Mar  3 14:44 test2

[root@dnssrv1 /]# ls -lh /var/spool/imap/domain/a/athena.edu.vn/t/user/test1/
total 24K
-rw----- 1 cyrus mail  4 Mar  3 14:43 cyrus.cache
-rw----- 1 cyrus mail 166 Mar  3 14:43 cyrus.header
-rw----- 1 cyrus mail  96 Mar  3 14:43 cyrus.index
```

6/ Cấu hình postfix để chuyển mail cho cyrus-imapd:

- Để Postfix chuyển mail vào lưu trữ trong cấu trúc của cyrus-imapd thay vì lưu trữ local, sửa đổi dòng sau trong file `/etc/postfix/main.cf`
`local_transport = cyrus`
- Đồng thời uncomment, hoặc thêm dòng sau vào file `/etc/postfix/master.cf`
`cyrus unix - n n - - pipe flags=R user=cyrus argv=/cyrus/bin/deliver -e -r
${sender} -m ${extension} ${user}`
- Test lại quá trình gửi nhận mail bằng postfix, theo dõi xem mail được đưa vào đâu???

Bài Lab 7: Firewall

I/ Cài đặt IPTABLES:

Iptables cung cấp các tính năng sau:

- Tích hợp tốt hơn với kernel của hệ điều hành Linux.
- Có khả năng phân tích package hiệu quả.
- Lọc package dựa vào MAC và một số cờ hiệu trong TCP Header.
- Cung cấp chi tiết các tùy chọn để ghi nhận sự kiện hệ thống.
- Cung cấp kỹ thuật NAT.
- Có khả năng ngăn chặn được cơ chế tấn công theo kiểu DOS (Denial Of Service).

- Kiểm tra iptables đã được cài đặt hay chưa:

```
[root@testsrv /]# rpm -qa | grep iptables
```

- Cài đặt (nếu chưa được cài đặt):

```
[root@testsrv /]# rpm -ivh iptables-1.3.5-1.2.1.i386.rpm
Preparing... ##### [100%]
1:iptables ##### [100%]
```

- Kiểm tra iptables đã được cài đặt trên hệ thống:

```
[root@testsrv /]# rpm -qa | grep iptables
iptables-1.3.5-1.2.1
```

- Khởi động service iptables

```
[root@testsrv /]# service iptables start
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
Applying iptables firewall rules: [ OK ]
```

II/ Cấu hình iptables:

Có 2 cách cấu hình iptables là dùng lệnh và Sửa file /etc/sysconfig/iptables. Nếu cấu hình iptables bằng cách dùng lệnh sẽ không được lưu lại sau khi ta restart service iptables.

- Cấu hình iptables cho phép truy cập ssh:

```
[root@mail /]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Restart service iptables

```
[root@mail /]# service iptables restart
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
Applying iptables firewall rules: [ OK ]
Loading additional iptables modules: ip_conntrack_netbios_n[ OK ]
```

Kiểm tra: Sang máy khác gõ lệnh *ssh 192.168.36.230* hay:

```
[root@mail /]# telnet 192.168.36.230 22
Trying 192.168.36.230...
Connected to mail.athena.edu.vn (192.168.36.230).
Escape character is '^]'.
SSH-2.0-OpenSSH 4.3
```

Sau đó thực hiện # để bỏ dòng

```
#-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 22 -j ACCEPT
```

trong file */etc/sysconfig/iptables*, restart lại service iptables, và *telnet 192.168.36.230 22* để kiểm tra lại kết quả.

- Cấu hình iptables cấm ping:

Bỏ dòng

```
#-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
```

Trong */etc/sysconfig/iptables*

Restart service iptables

```
[root@mail /]# service iptables restart
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
Applying iptables firewall rules: [ OK ]
Loading additional iptables modules: ip_conntrack_netbios_n[ OK ]
```

Kiểm tra lại

```
C:\>ping 192.168.36.230

Pinging 192.168.36.230 with 32 bytes of data:

Reply from 192.168.36.230: Destination host unreachable.
Reply from 192.168.36.230: Destination host unreachable.
Reply from 192.168.36.230: Destination host unreachable.
Reply from 192.168.36.230: Destination host unreachable.

Ping statistics for 192.168.36.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Thực hiện mở lại dòng

```
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
```

Trong */etc/sysconfig/iptables* để cho phép ping

Restart service iptables

```
[root@mail /]# service iptables restart
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
Applying iptables firewall rules: [ OK ]
Loading additional iptables modules: ip_conntrack_netbios_n[ OK ]
```

- Cấu hình iptables giả mạo địa chỉ nguồn:

```
[root@mail /]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.

*nat
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -o eth0 -j SNAT --to-source 192.168.1.240

COMMIT

*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -s 0/0 -i eth0 -d 192.168.36.230 -p tcp -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Restart service iptables

```
[root@mail /]# service iptables restart
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
Applying iptables firewall rules: [ OK ]
Loading additional iptables modules: ip_conntrack_netbios_n[ OK ]
```

Kiểm tra iptables:

```
[root@mail /]# iptables -L -t nat
Chain PREROUTING (policy ACCEPT)
target    prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target    prot opt source                destination
SNAT      all  --  192.168.36.0/24        anywhere             to:192.168.1.240

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

Cho phép IP_FORWARD:

```
[root@mail /]# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Tiến hành ping đến một máy khác (192.168.36.233):

```
[root@mail /]# ping 192.168.36.233
PING 192.168.36.233 (192.168.36.233) 56(84) bytes of data.
```

Sang máy 192.168.36.233 để kiểm tra:

```
[root@testsrv /]# tcpdump -n icmp -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
15:51:44.959271 IP 192.168.1.240 > 192.168.36.233: ICMP echo request, id 8720, seq 59, length 64
15:51:44.960965 IP 192.168.36.233 > 192.168.1.240: ICMP echo reply, id 8720, seq 59, length 64
15:51:46.100230 IP 192.168.1.240 > 192.168.36.233: ICMP echo request, id 8720, seq 60, length 64
15:51:46.100331 IP 192.168.36.233 > 192.168.1.240: ICMP echo reply, id 8720, seq 60, length 64
15:51:47.214412 IP 192.168.1.240 > 192.168.36.233: ICMP echo request, id 8720, seq 61, length 64
15:51:47.214812 IP 192.168.36.233 > 192.168.1.240: ICMP echo reply, id 8720, seq 61, length 64
```

III/ Một số cấu hình iptables tham khảo:

- iptables chấp nhận các packet vào cổng 80 trên card mạng eth0

```
iptables -A INPUT -i eth0 --dport 80 -j ACCEPT
```

- iptables drop các packet đến cổng 23 dùng giao thức TCP trên card mạng eth0

```
iptables -A INPUT -i eth0 -p tcp --dport 23 -j DROP
```

- iptables được cấu hình cho phép firewall chấp nhận các gói tin TCP có địa chỉ nguồn là bất kỳ và địa chỉ đích là 192.168.1.1; và có hướng đi vào là cổng interface eth0:

```
iptables -A INPUT -s 0/0 -i eth0 -d 192.168.1.1 -p TCP -j ACCEPT
```

- Chấp nhận các gói tin TCP cho việc forward khi các gói tin có địa chỉ nguồn là bất kỳ đến từ interface ethernet 0, source port nằm trong dãy 1024-65535 và có địa chỉ đích là 192.168.1.58, ngõ ra là interface ethernet 1, với destination port là 80 (www)

```
iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.58 -o eth1 -p TCP --sport 1024:65535 --dport 80 -j ACCEPT
```

- Chấp nhận cho firewall send ICMP (echo-request) và nhận ICMP (echo-reply)

```
iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
```

```
iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

- Firewall chấp nhận các gói tin TCP sẽ được route khi chúng đi vào interface ethernet0 với địa chỉ nguồn là bất kỳ và có chiều đi ra là interface ethernet 1 với địa chỉ đích là 192.168.1.58. Source port là dãy 1024-65535 và destination port là 80 (www) và 443 (https).

```
iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.58 -o eth1 -p TCP --sport 1024:65535 -m multiport --dport 80,443 -j ACCEPT
```

Thay vì phải định ra source port và destination port, ta chỉ đơn giản sử dụng tùy chọn `-m state --state ESTABLISHED`

```
iptables -A FORWARD -d 0/0 -o eth0 -s 192.168.1.58 -i eth1 -p TCP \  
-m state --state ESTABLISHED -j ACCEPT
```


- iptables đổi IP nguồn cho các packet ra card mạng eth0 là 210.40.2.71. Khi nhận được packet vào từ Internet, Iptables sẽ tự động đổi IP đích 210.40.2.71 thành IP đích tương ứng của máy tính trong mạng LAN 192.168.0/24

iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source 210.40.2.71

Hoặc bạn có thể dùng MASQUERADE thay cho SNAT như sau:

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

(MASQUERADE thường được dùng khi kết nối đến Internet là pp0 và dùng địa chỉ IP động)

- Đổi địa chỉ đích của server thành 192.168.1.2 khi truy cập đến 172.28.24.199

iptables -t nat -A PREROUTING -d 172.28.24.199 -i eth0 -j DNAT to-destination 192.168.1.2

IV/ Cài đặt shorewall:

- Shorewall là một kiểu giao diện để dễ quản lý iptables hơn.
- Cài đặt shorewall bằng gói rpm như sau:

```
[root@centos-1 setup]# rpm -ivh shorewall-3.4.7-1.noarch.rpm
Preparing...                               ##### [100%]
      1:shorewall                           ##### [100%]
```

V/ Cấu hình shorewall:

- Cấu hình file /etc/shorewall/interfaces. Định nghĩa interface như sau:

#ZONE	INTERFACE	BROADCAST	OPTIONS
net	eth0	detect	

- Cấu hình file /etc/shorewall/zone:

#ZONE	TYPE	OPTIONS	IN OPTIONS	OUT OPTIONS
#				
fw	firewall			
net	ipv4			

- Cấu hình file /etc/shorewall/policy. File này định nghĩa các policy kết nối giữa những zone được định nghĩa trong file /etc/shorewall/zone:

#SOURCE	DEST	POLICY	LOG LEVEL	LIMIT: BURST
#				
net	all	DROP	info	
all	all	REJECT	info	
fw	all	ACCEPT		

- Cấu hình file /etc/shorewall/rules. Đây là file quan trọng nhất, kiểm soát những rule cho phép kết nối hay không. File /etc/shorewall/rules được hiểu như giao diện của iptables, thay vì định nghĩa bằng iptables phức tạp, thì ta tiến hành định nghĩa theo cấu trúc của shorewall, sau đó shorewall sẽ biên dịch lại thành những câu lệnh iptables.


```
#ACTION SOURCE          DEST          PROTO  DEST  SOURCE          ORIGINAL          RATE
      USER/    MARK
#
      GROUP
#SECTION ESTABLISHED
#SECTION RELATED
SECTION NEW
ACCEPT net      all      icmp echo-request
ACCEPT all      all      icmp echo-request
ACCEPT all      net      tcp 53
ACCEPT all      net      udp 53
```

- Cấu hình file /etc/shorewall/shorewall.conf. File định nghĩa các option hoạt động cho shorewall. Để file cấu hình như mặc định, sửa dòng sau:

```
STARTUP_ENABLED=Yes
```

- Check cấu hình shorewall:

```
[root@centos-1 setup]# vi /etc/shorewall/shorewall.conf
[root@centos-1 setup]# shorewall check
Checking...
Initializing...
Determining Zones...
  IPv4 Zones: net
  Firewall Zone: fw
Validating interfaces file...
Validating hosts file...
Pre-processing Actions...
  Pre-processing /usr/share/shorewall/action.Drop...
  Pre-processing /usr/share/shorewall/action.Reject...
Validating Policy file...
Determining Hosts in Zones...
  net Zone: eth0:0.0.0.0/0
Deleting user chains...
Checking /etc/shorewall/routestopped ...
Creating Interface Chains...
Checking Common Rules
Compiling IP Forwarding...
Checking /etc/shorewall/rules...
Checking Actions...
Checking /usr/share/shorewall/action.Drop for Chain Drop...
Checking /usr/share/shorewall/action.Reject for Chain Reject...
Checking /etc/shorewall/policy...
Checking Traffic Control Rules...
Checking Rule Activation...
Shorewall configuration verified
```

- Start shorewall, kiểm tra các luật iptables phát sinh từ shorewall:

```
[root@centos-1 ~]# service shorewall start
Starting shorewall: [ OK ]

[root@centos-1 ~]# service iptables status
Table: raw
Chain PREROUTING (policy ACCEPT)
num target      prot opt source          destination
.....
Chain fw2net (1 references)
num target      prot opt source          destination          state
1  ACCEPT        all  --  0.0.0.0/0        0.0.0.0/0            RELATED,ESTABLISHED
2  ACCEPT        icmp --  0.0.0.0/0        0.0.0.0/0            icmp type 8
3  ACCEPT        tcp  --  0.0.0.0/0        0.0.0.0/0            tcp dpt:53
4  ACCEPT        udp  --  0.0.0.0/0        0.0.0.0/0            udp dpt:53
5  all2all       all  --  0.0.0.0/0        0.0.0.0/0
```

Bài Lab 8: IDS

I/ Cài đặt Snort:

- Cài gói phụ thuộc:

```
[root@centos-1 Snort]# rpm -ivh pcre-devel-6.6-1.1.i386.rpm
Preparing... ##### [100%]
1:pcre-devel ##### [100%]
[root@centos-1 Snort]# rpm -ivh libpcap-devel-0.9.4-8.1.i386.rpm
Preparing... ##### [100%]
1:libpcap-devel ##### [100%]
```

- Cài snort từ gói source bằng những lệnh sau:

```
./configure
make
make install
```

- Giải nén tập luật của snort vào cùng thư mục source của snort:

```
[root@centos-1 Snort]# tar -xvzf snortrules.tar.gz -C /usr/snort-2.8.0.1/
rules
rules/Makefile.am
rules/sid-msg.map
rules/classification.config
rules/SnortIDAlertMIB.txt
rules/SnortCommonMIB.txt
rules/Makefile.in
rules/xll.rules
rules/web-misc.rules
rules/web-iis.rules
rules/web-frontpage.rules
rules/web-coldfusion.rules
rules/web-cgi.rules
rules/web-attacks.rules
rules/virus.rules
rules/tftp.rules
rules/telnet.rules
rules/sql.rules
rules/smtp.rules
rules/shellcode.rules
rules/scan.rules
rules/rservices.rules
```

- File cấu hình của snort là /usr/snort-2.8.0.1/etc/snort.conf, chỉnh sửa biến RULE_PATH, và một số tập luật rules (có những tập luật không chuẩn, không sử dụng được).

```
var RULE_PATH /usr/snort-2.8.0.1/rules
```

- Tạo user snort, tạo thư mục để ghi lại sự kiện log:

```
[root@centos-1 snort-2.8.0.1]# useradd snort
[root@centos-1 snort-2.8.0.1]# mkdir /var/log/snort
```

- Tạo một script để start/ stop snort như một service:

```
[root@centos-1 snort-2.8.0.1]# cp /var/setup/Snort/snortd /etc/init.d/
[root@centos-1 snort-2.8.0.1]# chkconfig --level 2345 snortd on
```

- Start snort ở dạng service:

```
[root@centos-1 snort-2.8.0.1]# service snortd start
Starting snort: -
```

[OK]

Start snort ở mode NIDS debug:

```
[root@centos-1 snort-2.8.0.1]# /usr/local/bin/snort -u snort -g snort -d -c /usr/snort-2.8.0.1/etc/snort.conf
Running in IDS mode

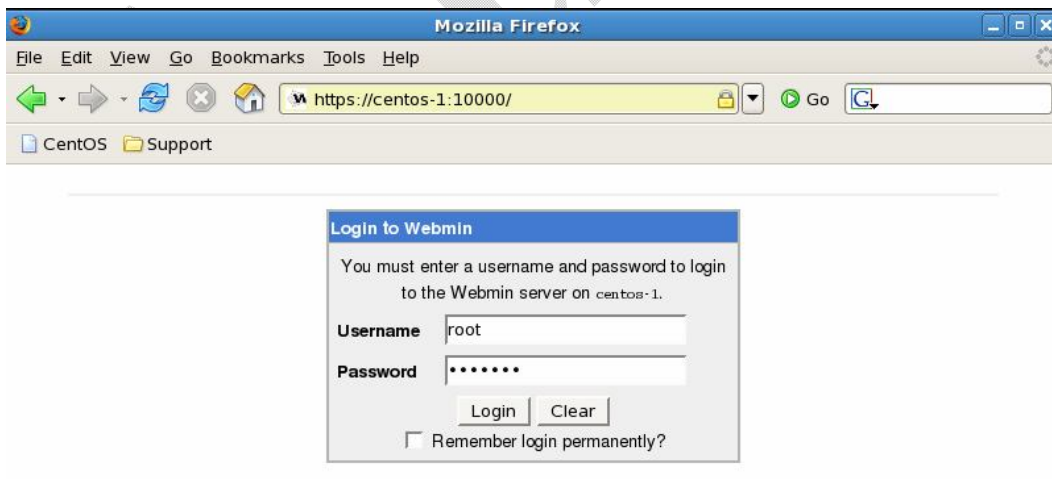
---= Initializing Snort =---
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file /usr/snort-2.8.0.1/etc/snort.conf
PortVar 'HTTP_PORTS' defined : [ 80]
PortVar 'SHELLCODE_PORTS' defined : [ 0:79 81:65535]
PortVar 'ORACLE_PORTS' defined : [ 1521]
Frag3 global config:
  Max frags: 65536
  Fragment memory cap: 4194304 bytes
Frag3 engine config:
  Target-based policy: FIRST
  Fragment timeout: 60 seconds
  Fragment min_ttl: 1
  Fragment ttl_limit: 5
  Fragment Problems: 1
Stream5 global config:
  Track TCP sessions: ACTIVE
  Max TCP sessions: 8192
  Memcap (for reassembly packet storage): 8388608
  Track UDP sessions: INACTIVE
  Track ICMP sessions: INACTIVE
```

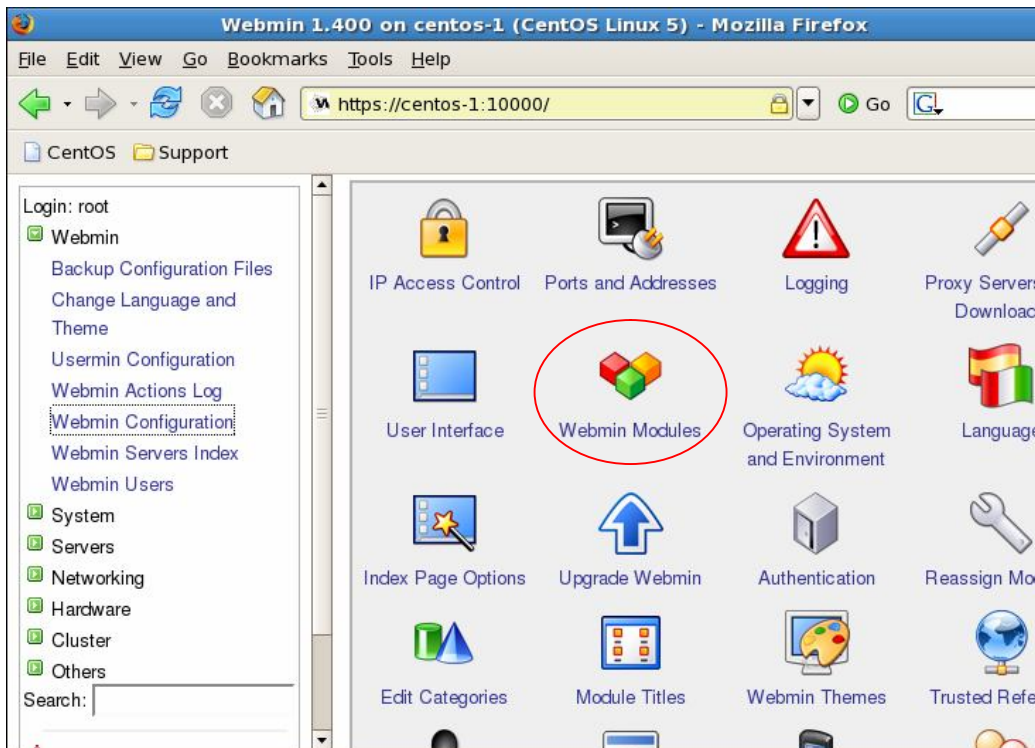
II/ Cấu hình, theo dõi Snort ở chế độ đồ họa:

- Cài đặt webmin:

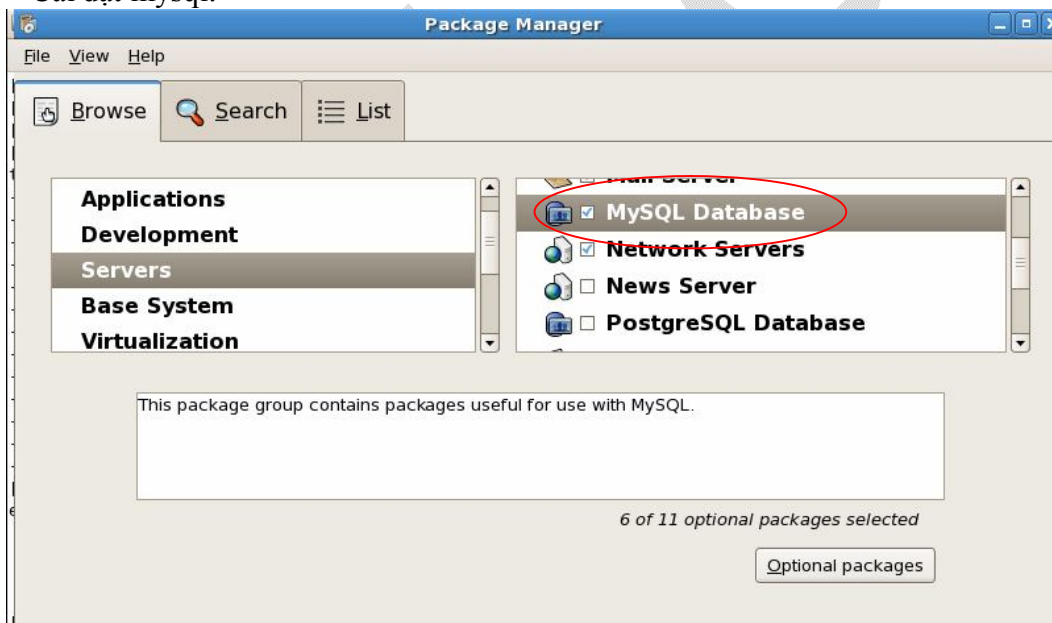
```
[root@centos-1 Snort]# rpm -ivh webmin-1.400-1.noarch.rpm
Preparing... ##### [100%]
Operating system is CentOS Linux
  1:webmin ##### [100%]
Webmin install complete. You can now login to https://centos-1:10000/
as root with your root password.
```

- Log vào Webmin, chọn chức năng Webmin Modules, import thêm Snort module vào Webmin:





- Cài đặt mysql:



- Tạo user, và cấp quyền cho user trong mysql:

```
# mysql -u root
```

```
mysql> set password for 'root'@'localhost'=password('123456');
```

```
mysql> create database snort;
```

```
mysql> exit;
```

```
# mysql -u root -p
```

```
mysql> connect snort;
```

File script tạo cấu trúc lưu trữ dữ liệu cho Snort

```
mysql> source create_mysql;
mysql> grant CREATE,INSERT,SELECT,DELETE,UPDATE on snort.* to
snort;
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to
snort@localhost;
mysql> grant CREATE,INSERT,SELECT,UPDATE on snort.* to acidviewer;
mysql> grant CREATE, INSERT, SELECT, UPDATE on snort.* to
acidviewer@localhost;
mysql> connect mysql;
mysql> set password for 'snort'@'localhost'=password('123456');
mysql> set password for 'snort'@'%'=password('123456');
mysql> set password for 'acidviewer'@'localhost'=password('123456');
mysql> set password for 'acidviewer'@'%'=password('123456');
mysql> flush privileges;
mysql> exit;
```

- Sửa file **snort.conf** ở những dòng sau:

```
# output database: log, mysql, user=root password=test dbname=db host=localhost
sửa thành
output database: log, mysql, user=snort password=123456 dbname=snort
host=000.000.000.000
```

- Tiếp theo chúng ta tiến hành cài đặt acid, adodb, gd, phplot

```
# tar -xzf acid-0.9.6b23.tar.gz -C /var/www/html
# tar -xzf adodb461.tar.gz -C /var/www/html
# tar -xzf gd-2.0.33.tar.gz -C /var/www/html
# tar -xzf phplot-4.4.6.tar.gz -C /var/www/html
```

- Đổi tên các thư mục gd-2.0.33 và phplot-4.4.6 thành gd và phplot. Copy thư mục acid thành một thư mục khác là acidviewer.
- Sửa file **/var/www/html/acid/acid_conf.php** và file **/var/www/html/acidviewer/acid_conf.php** ở các dòng sau:

```
$DBlib_path="./adodb";
$alert_dbname="snort";
$alert_user="snort"; (hoặc acidviewer)
$alert_password="123456";
$Chartlib_path="./phplot";
```

- Tiếp tục cấu hình các bước sau:

```
# mkdir /usr/lib/apache
# mkdir /usr/lib/apache/passwords
# htpasswd -c /usr/lib/apache/passwords/passwords snort
# htpasswd /usr/lib/apache/passwords/passwords acidviewer
```


- Thêm đoạn sau vào file /etc/httpd/conf/httpd.conf:

```
<Directory "/var/www/html/acid">  
    AuthType Basic  
    AuthName "snort solution"  
    AuthUserFile /usr/lib/apache/passwords/passwords  
    Require user snort  
    AllowOverride None  
</Directory>
```

```
<Directory "/var/www/html/acid">  
    AuthType Basic  
    AuthName "snort solution"  
    AuthUserFile /usr/lib/apache/passwords/passwords  
    Require user acidviewer  
    AllowOverride None  
</Directory>
```

- Bây giờ chúng ta truy cập vào trang acid thông qua địa chỉ: <http://localhost/acid/>, tiếp tục setup theo các bước trên web.
- Sau khi quá trình cài đặt hoàn tất, muốn xem snort log thì vào địa chỉ <http://localhost/acid> với quyền của snort hoặc <http://localhost/acidviewer> với quyền của acidviewer.
- Muốn thực hiện các thao tác quản trị snort thì vào <https://localhost:10000>:

