BÀI 5: QUẢN TRỊ NGƯỜI DÙNG VÀ NHÓM

Mã bài: MĐ 40-05

Mục tiêu:
- Hiểu cơ chế quản lý người dùng trong hệ điều hành Linux;
- Thực hiện việc tạo lập, quản lý người dùng.

Nội dung chính:

1. Thông tin của người dùng

Mục tiêu: Trình bày cơ chế quản lý người dùng trong hệ điều hành Linux, giúp người học biết được cách quản lý và lưu trữ các thống tin người dùng trên hệ thống.

1.1. Superuser

Trong Linux, tài khoản root có quyền cao nhất được sử dụng bởi người quản trị. Tài khoản này thường được sử dụng vào các mục đích cấu hình, bảo trì hệ thống. Khi quản trị hệ thống, cần tạo ra các tài khoản (account) cho người sử dụng thường sớm nhất có thể được. Với những server quan trọng và có nhiều dịch vụ khác nhau, có thể tạo ra các superuser thích hợp cho từng dịch vụ, tránh dùng root cho các công việc này. Ví dụ như superuser cho công việc backup chỉ cần chức năng đọc (read-only) mà không cần chức năng ghi.

Tài khoản root có quyền hạn rất lớn nên nó thường là mục tiêu chiếm đoạt; do vậy, người sử dụng tài khoản root phải cẩn thận, không sử dụng bừa bãi trên qua telnet hay kết nối từ xa mà không có công cụ kết nối an toàn.

Trong Linux, chúng ta có thể tạo tài khoản có tên khác nhưng có quyền của root, bằng cách tạo user có UserID bằng 0. Cần phân biệt tài khoản đang đăng nhập sử dụng là tài khoản root hay người sử dụng thường thông qua dấu nhắc của shell.

Để thay đổi tài khoản đăng nhập, sử dụng lệnh su [tên tài khoản]

Ví dụ:

```
login: nsd1
Password:******
[nsd1@DanaVTC nsd1]$ su -
Password: ******
[root@DanaVTC /root]#
```

Trong ví dụ trên, dòng thứ ba ([nsd1@DanaVTC nsd1]$) với dấu $ cho thấy người sử dụng thường (nsd1) đang kết nối; dòng cuối cùng với dấu # cho thấy đang thực hiện các lệnh với root.

1.2. User

Để đăng nhập và sử dụng hệ thống Linux cần phải có 1 tài khoản. Trừ tài khoản root, các tài khoản khác do người quản trị tạo ra.

Mỗi tài khoản người dùng cần có tên sử dụng (username) và mật khẩu (password) riêng. Các thông tin về tài khoản người dùng của hệ thống chứa trong tập tin /etc/passwd.

1.2.1. Tập tin /etc/passwd

Tập tin /etc/passwd được lưu dưới dạng văn bản, nó có vai trò rất quan trọng trong hệ thống Unix/Linux. Mọi người đều có thể đọc được tập tin này nhưng chỉ có root mới có quyền thay đổi nó.

Ví dụ sau cho thấy nội dung của một tập tin passwd:

root:x:0:0:root:/root:/bin/bash

bin:x:1:1:bin:/bin:

daemon:x:2:2:daemon:/sbin:

halt:x:7:0:halt:/sbin:/sbin/halt

mail:x:8:12:mail:/var/spool/mail:

news:x:9:13:news:/var/spool/news:

ftp:x:14:50:FTP User:/var/ftp:

nobody:x:99:99:Nobody:/:

nscd:x:28:28:NSCD Daemon:/:/bin/false

mailnull:x:47:47::/var/spool/mqueue:/dev/null

rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/bin/false

xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false

nthung:x:525:526:nguyen tien hung:/home/nthung:/bin/bash

natan:x:526:527::/home/natan:/bin/bash

Trong đó, các thông tin bao gồm:

- Dòng đầu tiên của tập tin /etc/passwd mô tả thông tin user root (tất cả những tài khoản có user_ID = 0 đều là root hoặc có quyền như root), tiếp theo là

các tài khoản khác của hệ thống (đây là các tài khoản không có thật và không thể login vào hệ thống), cuối cùng là các tài khoản người dùng thường.

- Cột 1: Tên người sử dụng;

- Cột 2: Mã liên quan đến mật khẩu của tài khoản và "x" đối với Linux. Linux lưu mã này trong một tập tin khác /etc/shadow mà chỉ có root mới có quyền đọc;

- Cột 3, cột 4: Mã định danh tài khoản (user ID) và mã định danh nhóm (group ID);

- Cột 5: Tên đầy đủ của người sử dụng;

- Cột 6: Thư mục cá nhân (Home Directory);

- Cột 7: Chương trình sẽ chạy đầu tiên sau khi người dùng đăng nhập vào hệ thống.

1.2.2. Username và UserID

Để quản lý người dùng, Linux sử dụng tên người dùng (user name) và định danh người dùng (user ID) để đăng nhập và truy xuất tài nguyên.

Trong đó, tên người dùng là chuỗi ký tự xác định duy nhất một người dùng; số định danh người dùng dùng để kiểm soát hoạt động của người dùng. Theo qui định, người dùng có định danh 0 là người dùng quản trị (root); số định danh từ 1-99 sử dụng cho các tài khoản hệ thống, số định danh của người dùng bình thường sử dụng giá trị bắt đầu từ 100-500.

1.2.3. Mật khẩu người dùng

Mỗi người dùng có mật khẩu tương ứng, mật khẩu có thể được thay đổi tùy theo người dùng; tuy nhiên, người quản trị có thể thay đổi mật khẩu của những người dùng khác.

Mật khẩu người dùng được lưu trong tập tin /etc/passwd.

1.2.4. Group ID

Group ID (GID) dùng để định danh nhóm của người dùng. Thông qua Group ID có thể xác định người dùng đó thuộc nhóm nào. Thông thường, trên Linux, GID được mặc định tạo ra khi tạo một user và có giá trị >= 500.

1.2.5. Home directory

Khi login vào hệ thống người dùng được đặt làm việc tại thư mục cá nhân của mình (home directory). Thông thường mỗi người dùng có một thư mục cá nhân riêng và người dùng có toàn quyền trên đó. Nó dùng để chứa dữ liệu cá nhân và các thông tin hệ thống cho hoạt động của người dùng như biến môi trường,

script khởi động, profile khi sử dụng X Window,… Home directory của người dùng thường là /home, của root là /root. Tuy nhiên, chúng ta cũng có thể đặt vào vị trí khác thông qua lệnh useradd hoặc usermod.

2. Quản lý người dùng

Mục tiêu: Trình bày các thao tác quản trị người dùng thông qua tài khoản người dùng.

2.1. Tạo tài khoản người dùng

Để tạo tài khoản, root có thể sử dụng lệnh useradd với cú pháp:

#useradd [-c mô_tả_người_dùng] [-d thư_mục_cá_nhân] [-m]

[-g nhóm_người_dùng] [tên_tài_khoản]

Trong đó:

- Tham số –m sử dụng để tạo thư mục cá nhân nếu nó chưa tồn tại.
- Chỉ có root được phép sử dụng lệnh này.

Ví dụ: # useradd –c “Nguyen van B“ nvb

Để đặt mật khẩu cho tài khoản, dùng lệnh passwd <username>.

Ví dụ: # passwd nvb

Changing password for user nvb
New password: ****
Retype new password: ****
passwd: all authentication tokens updated successfully

Lưu ý:

Khi đặt password nên:

- Đặt với độ dài tối thiểu 6 ký tự;
- Phối hợp giữa ký tự hoa, thường, ký số và ký tự đặc biệt.
- Không nên đặt password liên quan đến tên tuổi, ngày sinh,… của mình và người thân.

Khi nhiều người dùng có cùng một chức năng và cùng chia xẻ nhau dữ liệu, nên nhóm những người dùng này vào trong cùng nhóm. Mặc định, khi tạo một tài khoản, Linux sẽ tạo cho mỗi tài khoản một nhóm, tên nhóm trùng với tên tài khoản. Chẳng hạn, đọc tập tin /etc/passwd ta thấy:

nvb:x:1013:1013::/home/nvb:/bin/bash nghĩa là người dùng nvb có user_ID 1012 và thuộc nhóm 1013.

Xem tập tin /etc/group ta thấy:

```
# more /etc/group
root:x:0:root
……
users:x:100:
……
nvb:x:1013:
```

Lúc này, có thể kết nạp tài khoản nvb vào nhóm users bằng cách thay số 1013 bằng 100, là group_ID của nhóm users.

Có thể dùng lệnh useradd –d để xem các thông số mặc định khi ta tạo tài khoản người dùng (các thông tin này được lưu trong thư mục /etc/default/useradd):

```
# useradd -d
    GROUP=100
    HOME=/home
    INACTIVE=-1
    EXPIRE=
    SHELL=/bin/bash
    SKEL=/etc/skel
```

2.2. Thay đổi thông tin của tài khoản

Để thay đổi thông tin của tài khoản, có thể thay đổi từ tập tin /etc/passwd hoặc dùng lệnh usermod. Cú pháp lệnh usermod:

#usermod [-c thông_tin_người_dùng] [-d thư_mục_cá_nhân] [-m]

[-g nhóm_ người_dùng] [tên_tài_khoản]

Ví dụ: Cho tài khoản nvb vào nhóm admin

#usermod –g admin nvb

2.3. Tạm khóa tài khoản người dùng

Để tạm thời khóa tài khoản trong hệ thống ta có thể dùng nhiều cách:

Khóa (locking)	Mở khóa (unlock)
passwd –l <username>	passwd –u
usermod –L <username>	usermod –U

Có thể tạm khóa tài khoản bằng cách chỉnh sửa tập tin /etc/shadow và thay thế từ khóa x bằng từ khóa * hoặc có thể gán /bin/false vào shell mặc định của user trong file /etc/passwd.

2.4. Hủy tài khoản

Lệnh userdel dùng để xóa một tài khoản. Ngoài ra, cũng có thể xóa một tài khoản bằng cách xóa đi dòng dữ liệu tương ứng với tài khoản đó trong tập tin /etc/passwd. Cú pháp:

#userdel <option> [username]

Ví dụ: xóa tài khoản nvb (dùng tùy chọn –r để xóa toàn bộ thông tin liên quan tới user đó): #userdel –r nvb

3. Nhóm người dùng

Mục tiêu: Khi nhiều người dùng có cùng một chức năng, cùng chia xẻ nhau dữ liệu, có chung quyền trên tài nguyên, thường được nhóm thành một nhóm.

Trong Linux, mỗi nhóm được xác định bởi tên riêng và định danh nhóm; một nhóm có thể có nhiều người dùng và người dùng có thể là thành viên của nhiều nhóm khác nhau. Tuy nhiên tại một thời điểm, một người dùng chỉ có thể là thành viên của một nhóm duy nhất.

Thông tin về nhóm lưu tại tập tin /etc/group. Mỗi dòng định nghĩa một nhóm, các trường trên dòng cách nhau bởi dấu :

<tên-nhóm>:<password-của-nhóm>:<định-danh-nhóm:các-user-thuộc-nhóm>

3.1. Tạo nhóm

Để tạo một nhóm, có thể chỉnh sửa trực tiếp trong tập tin /etc/group hoặc dùng lệnh groupadd.

Cú pháp: #groupadd [tên-nhóm]

3.2. Thêm người dùng vào nhóm

Khi muốn thêm người dùng vào nhóm, có thể sửa từ tập tin /etc/group, các tên tài khoản người dùng cách nhau bằng dấu ";", hoặc có thể thêm người dùng vào nhóm bằng lệnh:

#usermod –g [tên-nhóm tên-tài-khoản]

3.3. Hủy nhóm

Để hủy nhóm, có thể xóa trực tiếp nhóm trong tập tin /etc/group, hoặc dùng lệnh: #groupdel [tên-nhóm]

3.4. Xem thông tin về user và group

Cú pháp: #id <option> <username>

Lệnh cho phép xem thông tin về tài khoản hay nhóm trong hệ thống.

Trong đó, tham số -g cho phép xem thông tin về nhóm.

Ví dụ: xem groupID của một user vanphong: #id –g vanphong

Để xem tên nhóm của một user nào đó, dùng lệnh: groups <username>

Ví dụ: [root@server root]# groups root

root: root bin daemon sys adm disk wheel

Câu hỏi

1. Trình bày các loại tài khoản trên Linux.

2. Cho biết ý nghĩa các thành phần trên tập tin /etc/passwd.

Bài tập thực hành

1. Quản lý người dùng Linux trên giao diện text
- Xem thông tin chi tiết liên quan đến người dùng trong tập tin /etc/passwd.
- Xem thông tin chi tiết liên quan đến nhóm người dùng trong tập tin /etc/group.
- Xem thông tin chi tiết về mật khẩu trong tập tin /etc/shadow.
- Tạo user và nhóm:

Tạo nhóm hocvien gồm các user hv1, hv2, hv3 và đặt mật khẩu cho các user vừa tạo

Tạo nhóm admin gồm các user admin1, admin2 đặt mật khẩu cho các user vừa tạo

Thay đổi UID của hai user admin1, admin2 là 0
- Thay đổi thông tin mô tả của người dùng

Thông tin mô tả hv1 là học viên thứ nhất, hv2 là học viên thứ 2, hv3 là học viên thứ 3

Thông tin mô tả admin1 là người quản trị 1, admin2 là người quản trị 2
- Thay đổi mật khẩu cho những người dùng trên
- Khóa tài khoản người dùng hv3
- Thử đăng nhập bằng tài khoản hv3
- Mở khóa tài khoản người dùng hv3
- Thử đăng nhập bằng tài khoản hv3
- Xóa tài khoản người dùng hv3

2. Quản lý người dùng trên giao diện đồ họa
- Tạo người dùng và nhóm:
  - hocvien (tung, thuy, thanh)
  - admin (adm1, adm2)
  - user (u1, u2)
- Thay đổi các thuộc tính liên quan đến người dùng
  - Thay đổi nhóm của người dùng
  - Giới hạn thời gian sử dụng tài khoản
  - Tạm khóa tài khoản người dùng
  - Giới hạn thời hạn sử dụng mật khẩu

BÀI 6: CẤU HÌNH MẠNG

Mã bài: MĐ 40-06

Mục tiêu:

- Nắm được cách khai báo và thay đổi cấu hình mạng cho máy tính;
- Truy cập và điều khiển máy tính từ xa;
- Thực hiện các thao tác an toàn với máy tính.

Nội dung chính:

1. Cấu hình địa chỉ IP cho card mạng

Mục tiêu: Trình bày các thao tác : Xem địa chỉ IP, cấu hình địa chỉ IP, kiểm tra trạng thái của tất cả các card mạng.

1.1. Xem địa chỉ IP

Lệnh ifconfig cho phép xem thông tin địa chỉ IP của PC.

Ví dụ: để xem thông tin cấu hình mạng, dùng lệnh ifconfig -a

```
# ifconfig –a
eth0    Link encap:Ethernet  HWaddr 00:0C:29:6D:F0:3D
        inet addr:172.29.14.150  Bcast:172.29.14.159
Mask:255.255.255.224
        inet6 addr: fe80::20c:29ff:fe6d:f03d/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500
Metric:1
        RX packets:6622 errors:0 dropped:0 overruns:0 frame:0
        TX packets:1425 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:793321 (774.7 Kb)  TX bytes:240320 (234.6 Kb)
        Interrupt:10 Base address:0x1080
lo Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:76 errors:0 dropped:0 overruns:0 frame:0
        TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:8974 (8.7 Kb)  TX bytes:8974 (8.7 Kb)
```

Trong đó, eth0 là tên của card mạng trong, lo là tên của loopback interface.

1.2. Thay đổi địa chỉ IP

Trong bài 4 – mục 4, trình tiện ích cho phép thiết lập cấu hình mạng; ngoài ra, có thể sử dụng các cách sau để thay đổi địa chỉ IP:

Sử dụng lệnh:

ifconfig <interfacename> <IPaddress> netmask <netmaskaddress> up

Ví dụ:

[root@bigboy tmp]# ifconfig eth0 10.0.0.1 netmask 255.255.255.0 up

Chú ý: Sau khi dùng lệnh này, hệ thống lưu trữ tạm thời thông tin cấu hình này trong bộ nhớ và sẽ bị mất khi hệ thống reboot lại; để thông tin này có thể được lưu giữ lại sau khi reboot hệ thống, phải thêm lệnh trên vào tập tin /etc/rc.local.

Hoặc: Thay đổi thông tin cấu hình mạng trực tiếp trong file /etc/sysconfig/network-scripts/ifcfg-eth0

Gán địa chỉ IP tĩnh (tham khảo file ifcfg-eth0)

```
#Advanced Micro Devices [AMD]|79c970 [PCnet32LANCE]
DEVICE=eth0
BOOTPROTO=static
BROADCAST=172.29.14.159
HWADDR=00:0C:29:6D:F0:3D
IPADDR=172.29.14.150
NETMASK=255.255.255.224
NETWORK=172.29.14.128
ONBOOT=yes
TYPE=Ethernet
```

Gán địa chỉ IP động (tham khảo file ifcfg-eth0)

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

Sau đó dùng lệnh:

```
# ifdown eth0
# ifup eth0
```

1.3. Tạo nhiều địa chỉ IP trên card mạng

Phương thức tạo nhiều địa chỉ IP trên card mạng được gọi là IP alias. Alias này phải có tên dạng: parent-interface-name:X, trong đó X là chỉ số của interface thứ cấp (subinterface number).

Sử dụng một trong các cách sau để tạo Alias IP:

Cách 1:

- Bước 1: Đảm bảo rằng tên interface thật phải tồn tại, và kiểm tra các IP Alias trong hệ thống có tồn tại hay không.

- Bước 2: Tạo Virtual interface dùng lệnh ifconfig:

ifconfig ifcfg-eth0:0 192.168.1.99 netmask 255.255.255.0 up

Hoặc tạo một tên file /etc/sysconfig/network-scripts/ifcfg-eth0:0 từ file /etc/sysconfig/network-scripts/ifcfg-eth0; sau đó, thay đổi thông tin địa chỉ trong file này.

- Bước 3: Bật và tắt alias interface thông qua lệnh ifconfig

ifup eth0:0

ifdown eth0:0

Hoặc dùng lệnh /etc/init.d/network restart

- Bước 4: Kiểm tra thông tin cấu hình alias interface dùng lệnh ifconfig:

ifconfig
eth0 Link encap:Ethernet HWaddr 00:0C:29:6D:F0:3D
inet addr:172.29.14.150 Bcast:172.29.14.159 Mask:255.255.255.224
inet6 addr: fe80::20c:29ff:fe6d:f03d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:7137 errors:0 dropped:0 overruns:0 frame:0
TX packets:1641 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:848367 (828.4 Kb) TX bytes:265688 (259.4 Kb)
Interrupt:10 Base address:0x1080
eth0:0 Link encap:Ethernet HWaddr 00:0C:29:6D:F0:3D
inet addr:172.29.15.150 Bcast:172.29.15.159 Mask:255.255.255.224
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:7137 errors:0 dropped:0 overruns:0 frame:0
TX packets:1641 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000

RX bytes:848367 (828.4 Kb) TX bytes:265688 (259.4 Kb)
Interrupt:10 Base address:0x1080

Cách 2:

- Tạo tập tin parent-interface-name:X bằng cách copy file /etc/sysconfig/network-scripts/ifcfg-eth0 thành file /etc/sysconfig/network-scripts/ifcfg-eth0:X (trong đó X là số thứ tự của subinterface).

- Thay đổi thông tin cấu hình mạng trong file ifcfg-eth0:X (các thông tin in đậm là thông tin bắt buộc phải thay đổi)

DEVICE=eth0:0
ONBOOT=yes
BOOTPROTO=static
IPADDR=172.29.14.151
NETMASK=255.255.255.224
GATEWAY=172.29.129

1.4. Lệnh netstat

Lệnh netstat cho phép kiểm tra trạng thái của tất cả các card mạng.

Cú pháp: #netstat –in

Ngoài ra, có thể dùng lệnh netstat –rn để xem bảng routing table của router.

2. Truy cập từ xa

Mục tiêu: Trình bày cơ chế hoạt động của dịch vụ truy cập từ xa.

Khi cấu hình hệ thống kết nối vào mạng, máy chủ sẽ cung cấp một số dịch vụ Internet. Thông thường mỗi dịch vụ Internet gắn liền với một daemon và thực hiện trong chế độ background. Những daemon này hoạt động bằng cách liên kết đến một cổng nào đó và sau đó đợi những yêu cầu kết nối được gởi đến từ chương trình client. Khi một kết nối xảy ra nó sẽ tạo ra một tiến trình con đảm nhiệm kết nối này và tiếp tục lắng nghe những yêu cầu kết nối khác. Nếu hệ thống có quá nhiều daemon sẽ làm tăng xử lý của CPU. Để khắc phục điều này, Linux tạo ra một super-server gọi là Xinetd.

2.1. xinetd

Mỗi dịch vụ Internet đều gắn liền với một cổng chẳng hạn như: smtp – 25, pop3 – 110, dns – 53... Việc phân bổ này do một tổ chức qui định.

Xinetd là một Internet server daemon. Xinetd quản lý tập trung tất cả các dịch vụ Internet. Xinetd quản lý mỗi dịch vụ tương ứng với một cổng (port).

Xinetd "lắng nghe" và khi nhận được một yêu cầu kết nối từ các chương trình client, nó sẽ đưa yêu cầu đến dịch vụ tương ứng xử lý; sau đó, Xinetd tiếp tục "lắng nghe" những yêu cầu kết nối khác. Khi hệ điều hành được khởi động, Xinetd được khởi tạo ngay lúc này bởi script /etc/rc.d/init.d/xinetd. Khi Xinetd được khởi tạo, nó sẽ đọc thông tin từ tập tin cấu hình /etc/xinetd.conf và sẽ dẫn đến thư mục /etc/xinetd – nơi lưu tất cả những dịch vụ mà Xinetd quản lý. Trong thư mục /etc/xinetd, thông tin cấu hình của mỗi dịch vụ được lưu trong một tập tin có tên trùng với tên dịch vụ đó. Nội dung tập tin của dịch vụ telnet như sau:

```
service telnet
{
        disable = yes
        flags = REUSE
        socket_type = stream
        wait = no
        user = root
        server = /usr/sbin/in.telnetd
        log_on_failure += USERID
}
```

Những thuộc tính trong tập tin bao gồm:

Tên	Ý nghĩa
Disable	Tạm đình chỉ dịch vụ này. Có 2 giá trị: yes, no
Socket_type	Loại socket. Trong trường hợp này là stream – một loại socket cho những kết nối connection-oriented (chẳng hạn như TCP)
Wait	Thường chỉ liên quan đến những kết nối có loại socket là datagram. Giá trị của nó có thể là: - ***nowait*** nghĩa là xinetd sẽ tiếp tục nhận và xử lý những yêu cầu khác trong lúc xử lý kết nối này - ***wait*** nghĩa là tại một thời điểm xinetd chỉ có thể xử lý một kết nối tại một cổng chỉ định
User	Chỉ ra user chạy dịch vụ này. Thông thường là root
Server	Chỉ ra đường dẫn đầy đủ đến nơi quản lý dịch vụ

2.2. Tập tin /etc/services

Khi xinetd được khởi tạo nó sẽ truy cập đến tập tin /etc/services để tìm cổng tương ứng với từng dịch vụ. Nội dung của tập tin này như sau:

```
echo 7/tcp
echo 7/udp
```

```
discard 9/tcp sink null
discard 9/udp sink null
systat 11/tcp users
systat 11/udp users
daytime 13/tcp
daytime 13/udp
qotd 17/tcp quote
qotd 17/tcp quote
msp 18/tcp# message send protocol
msp 18/udp# message send protocol
chargen 19/tcp ttytst source
chargen 19/udp ttytst source
ftp-data 20/tcp
ftp-data 20/udp

# 21 is registered to ftp, but also used by fsp
ftp 21/tcp
ftp 21/udp fsp fspd
ssh 22/tcp # SSH Remote Login Protocol
ssh 22/udp # SSH Remote Login Protocol
telnet 23/tcp
telnet 23/udp

# 24 - private mail system
smtp 25/tcp mail
smtp 25/udp mail
time 37/tcp timserver
time 37/udp timserver
rlp 39/tcp resource # resource location
rlp 39/udp resource # resource   location
nameserver  42/tcp  name # IEN 116
nameserver  42/udp  name # IEN 116
```

Mỗi dòng trong tập tin mô tả cho một dịch vụ, bao gồm những cột sau:

- Cột 1: tên của dịch vụ;
- Cột 2: số cổng và giao thức mà dịch vụ này hoạt động;
- Cột 3: danh sách những tên gọi khác của dịch vụ này.

2.3. Khởi động xinetd

Sau khi chỉnh sửa tập tin cấu hình của từng dịch vụ trong thư mục /etc/xinetd, ta thực hiện lệnh sau để đọc lại nội dung của tập tin cấu hình:

/etc/rc.d/init.d/xinetd restart

3. Dịch vụ Telnet

Mục tiêu: Trình bày cách cài đặt, cấu hình và các phương án bảo mật đối với dịch vụ truy cập từ xa Telnet.

3.1. Khái niệm telnet

Vì một lý do nào đó người dùng không thể ngồi trực tiếp trên máy Linux làm việc. Dịch vụ telnet hỗ trợ cho người dùng trong vấn đề làm việc từ xa; Nhưng để đảm bảo tính bảo mật cho hệ thống, một điều cảnh báo là chúng ta không nên làm việc từ xa bằng telnet mà nên làm việc trực tiếp tại máy Linux.

3.2. Cài đặt

Thông thường khi cài đặt Linux, dịch vụ telnet đã được cài sẵn. Nếu chưa cài, có thể cài telnet server từ packet bằng dòng lệnh sau:

rpm –i telnet-server-0.17-20.i386.rpm

3.3. Cấu hình

Có nhiều cách cấu hình telnet server, sau đây là hai cách cấu hình cơ bản nhất:

- Cách 1: Dựa vào tập tin cấu hình, Khi cài đặt xong trong thư mục /etc/xinetd.d sẽ xuất hiện tập tin telnet. Tập tin này lưu những thông tin cấu hình về dịch vụ telnet.

```
service telnet
{
        disable = yes
        flags = REUSE
        socket_type  = stream
        wait = no
        user = root
        server  =/usr/sbin/in.telnetd
        log_on_failure += USERID
}
```

Nếu disable là no thì TELNET server được khởi động, ngược lại nếu disable là yes thì TELNET server không được khởi động. Sau khi chỉnh sửa tập tin cấu hình trên ta start, stop bằng lệnh:

```
/etc/rc.d/init.d/xinetd restart
```

Hoặc dùng lệnh:

```
# service xinetd restart
```

- Cách 2: Cấu hình telnet Server bằng dòng lệnh: chkconfig telnet on

Kiểm tra telnet thông qua lệnh:

```
#netstat-a|grep telnet
tcp        0      0      *:telnet        *:*        LISTEN
```

Kiểm tra telnet có được đặt như dịch vụ hệ thống:

```
# chkconfig --list | grep telnet
telnet: on
```

Dừng telnet server:

```
# chkconfig telnet off
```

3.4. Bảo mật dịch vụ telnet

3.4. 1. Cho phép telnet server hoạt động trên tcp port khác

Vì telnet traffic không được mã hóa nên nếu cho telnet server hoạt động trên tcp port 23 thì không được an toàn. Do vậy, có thể đặt telnet server hoạt động trên tcp port khác 23. Để làm điều này ta thực hiện các bước sau:

- Bước 1: Mở tập tin /etc/services và thêm dòng

```
# Local services
stelnet        7777/tcp          # "secure" telnet
```

- Bước 2: Chép file telnet thành file stelnet

```
# cp /etc/xinetd.d/telnet /etc/xinetd.d/stelnet
```

- Bước 3: Thay đổi một số thông tin trong file file /etc/xinetd.d/stelnet

```
service stelnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
```

```
        server          = /usr/sbin/in.telnetd
        log_on_failure += USERID
        disable         = no
        port            = 7777
}
```

- Bước 4: Kích hoạt stelnet thông qua lệnh chkconfig

```
# chkconfig stelnet on
```

- Bước 5: Kiểm tra hoạt động stelnet thông qua lệnh netstat

```
# netstat -an | grep 777
tcp   0  0 0.0.0.0:7777       0.0.0.0:*          LISTEN
```

Ta có thể logon vào stelnet Server thông qua lệnh:

```
# telnet 192.168.1.100 7777
```

3.4.2. Cho phép một số địa chỉ truy xuất telnet

Ta hiệu chỉnh một số thông số sau::

```
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure += USERID
        disable         = no
        only_from       = 192.168.1.100 127.0.0.1 192.168.1.200
}
```

4. SSH

Mục tiêu: Trình bày cách cài đặt và sử dụng dịch vụ truy cập từ xa SSH với phương thức mã hóa dữ liệu.

Chương trình telnet trong Linux cho phép người dùng đăng nhập vào hệ thống Linux từ xa. Nhược điểm của chương trình này là tên người dùng và mật khẩu gởi qua mạng không được mã hóa. Do đó, dễ bị những người khác nắm giữ và sẽ là mối nguy hiểm cho hệ thống.

Phần mềm Secure Remote Access là một hỗ trợ mới của Linux nhằm khắc phục nhược điểm của telnet. Nó cho phép đăng nhập vào hệ thống Linux từ xa và mật khẩu sẽ được mã hóa. Vì thế, SSH an toàn hơn nhiều so với telnet.

4.1. Cài đặt SSH Server trên Server Linux

Dùng lệnh rpm để cài package openssh-server. *.rpm

rpm –ivh openssh-server.*.rpm

Tập tin cấu hình /etc/ssh/sshd_config và /etc/ssh/ssh_config. Để start hay stop server dùng lệnh sau:

/etc/init.d/sshd start/stop/restart

4.2. Sử dụng SSH Client trên Linux

Trên client (Linux hoặc Unix) dùng lệnh ssh để login vào server. Cú pháp của lệnh:

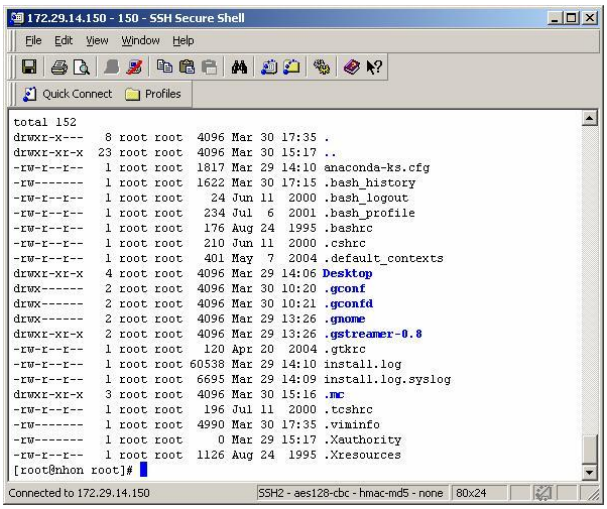
$ssh [tùy_chọn] [tên/IP_máy] [tùy_chọn] [lệnh]

Ví dụ: $ssh [–l] <tên_user> <ssh_address>

4.3. Quản trị hệ thống Linux thông qua SSH client for Windows

SSH client for Windows được thiết kế để cho phép người dùng có thể sử dụng/quản trị Unix/Linux từ hệ điều hành Windows. Có thể download phần mềm này từ site: http://www.ssh.com/support/downloads/.

Phần mềm này hỗ trợ cho người dùng có thể làm việc từ xa, cung cấp dịch vụ sftp.



Màn hình "SSH Client for Windows"

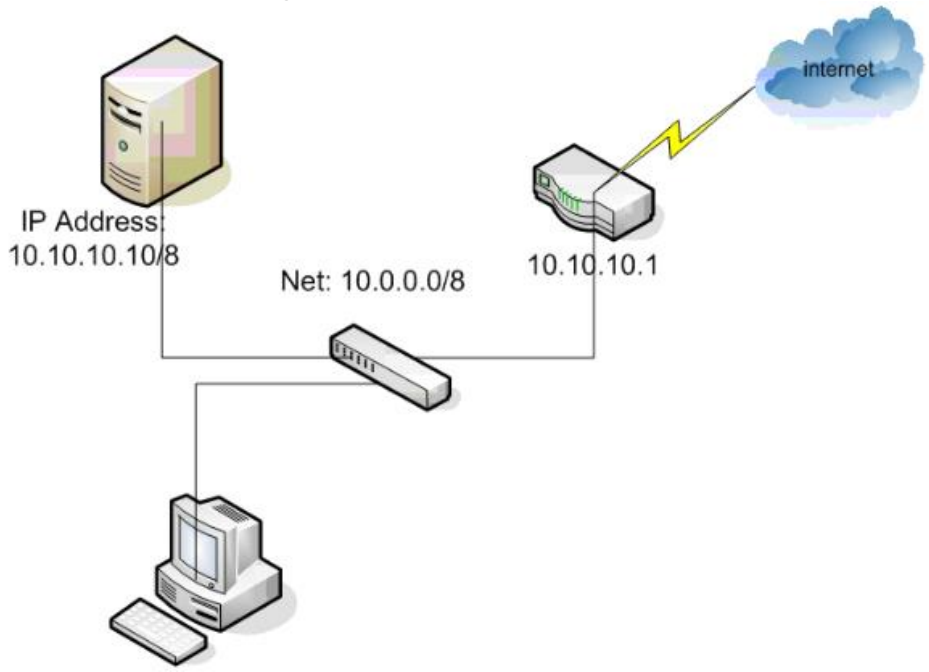
Câu hỏi

1. Trình bày các cách thay đổi địa chỉ IP (lệnh ifconfig, thay đổi từ file /etc/sysconfig/network-scripts/ifcfg-eth0).

2. Trình bày các cách tạo nhiều địa chỉ IP trên card mạng (IP alias).

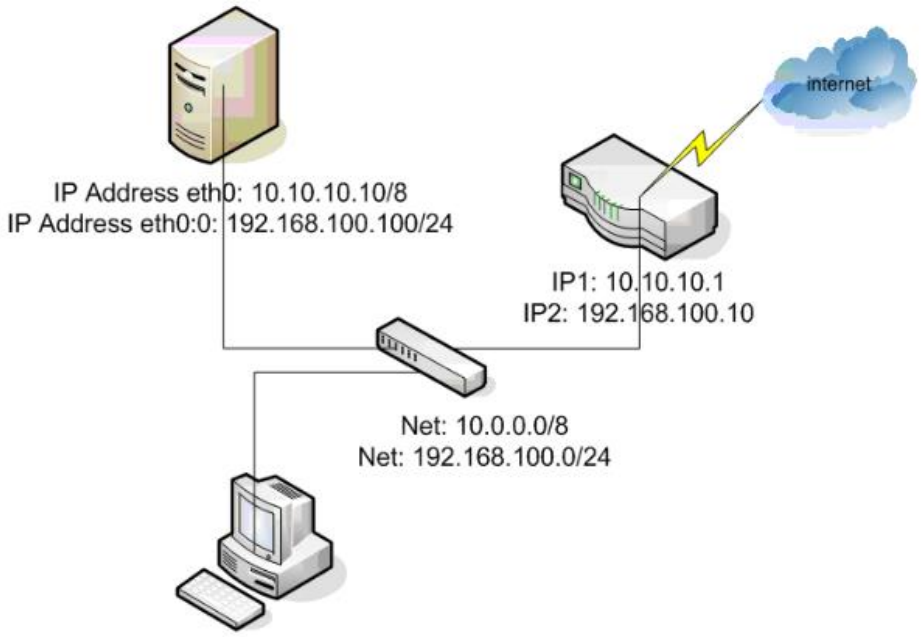
Bài tập thực hành

Bài 1: Cho hệ thống theo hình vẽ sau:



1. Thay đổi tên máy, sau đó khởi động lại bằng lệnh init 6
2. Xem địa chỉ mạng
3. Xem trạng thái kết nối vật lý của NIC
4. Đặt địa chỉ mạng và cập nhật
5. Dùng lệnh ping và ifconfig để kiểm tra cấu hình mạng
6. Kiểm tra cáp đã gắn vào card mạng hay chưa.

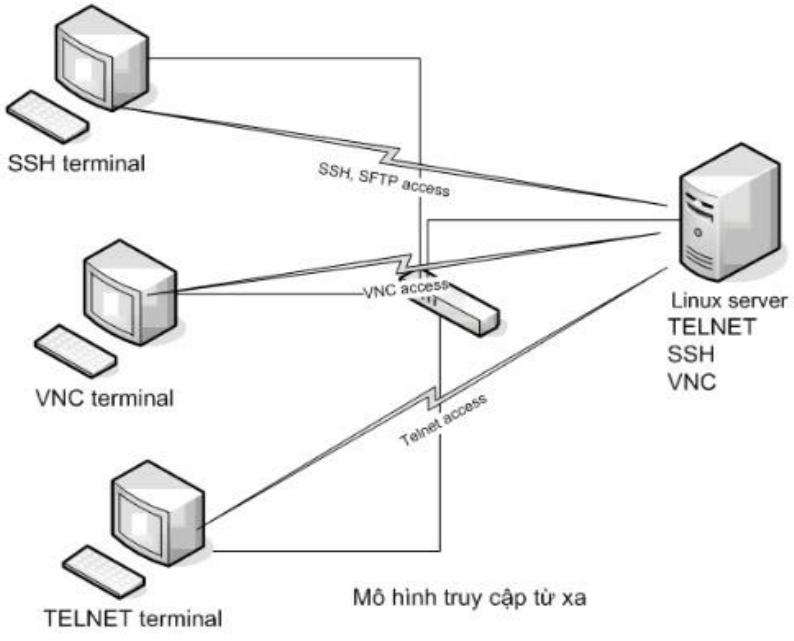
Bài 2: Cho hệ thống theo hình vẽ sau:



Thực hiện các yêu cầu sau:

1. Thêm địa chỉ IP cho card mạng eth0 với:
   - tên interface eth0:0
   - IP address: 192.168.100.100
   - netmask: 255.255.255.0
   - Gateway: 192.168.100.1
   - DNS: 192.168.100.1
2. Chỉ định default route cho hệ thống
3. Xem bảng định tuyến
4. Thống kê kết nối mạng

Bài 3: Cho hệ thống theo hình vẽ sau:



Cài đặt và cấu hình các dịch vụ hỗ trợ:

1. Cho phép mọi người kết nối từ xa vào máy chủ Linux qua telnet

2. Cho phép mọi người kết nối từ xa vào máy chủ Linux qua ssh
3. Cho phép mọi người kết nối từ xa vào máy chủ Linux qua VNC