KHOA CÔNG NGHỆ THÔNG TIN

TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI

QUẢN TRỊ TÀI KHOẢN

Quản trị người dùng

- Cấp tài khoản để người dùng có thể truy cập vào Linux server
- Cấp quyền truy cập vào tài nguyên trên server
- Là một phần quan trọng trong vấn đề an toàn hệ thống
- Nhất thiết phải sử dụng một chính sách an toàn và hiệu quả

Nội dung

1. User.
2. Group.
3. Các cách quản lý user và group.
4. Tạo user với công cụ user manager.
5. Tạo user với công cụ linuxconf.
6. Tập lệnh quản lý user và group.
7. Những file lưu thông tin user và group.

1. User

- User là người có thể truy cập đến hệ thống.
- User có username và password.
- Mỗi user còn có một định danh riêng gọi là UID.
- Định danh của người dùng bình thường sử dụng giá trị bắt đầu từ 1000.

Các kiểu tài khoản

- **Tài khoản gốc (Root account –** superuser): sẽ có sự điều khiển tuyệt đối tới hệ thống.

Một superuser có thể chạy bất cứ lệnh nào mà không bị hạn chế. Người sử dụng này có thể được ví như người quản lý hệ thống.

- **Các tài khoản người dùng cá nhân**: Các tài khoản này cung cấp sự truy cập mang tính tương tác tới hệ thống với người dùng và nhóm sử dụng và thường bị giới hạn truy cập vào những file và thư mục có tính chất quan trọng.

Super User: root

- Không phải tài khoản superuser nào cũng gọi là root, mặc dù nó được tạo mặc định là root khi cài đặt Linux.
- Super user có thể có tên bất kỳ nhưng thường được dùng nhất dưới tên root.
- Tài khoản này được định nghĩa là tài khoản có UID = GID= 0, các UID được định nghĩa trong file /etc/passwd
- Nếu đang ở User thường thì dấu nhắc tại Shell là $
- Nếu đang ở Super User (root) thì dấu nhắc tại Shell là #

Sudo

- Là công cụ cho phép tài khoản được gán quyền nâng cấp lên quyền quản trị hệ thống một cách tạm thời
- Dựa trên mật khẩu của chính tài khoản người dùng được cấp quyền
- Không phải là mật khẩu của tài khoản root

2. Group.

- Group là tập hợp nhiều user lại.
- Mỗi user luôn là thành viên của một group.
- Khi tạo một user thì mặc định một group được tạo ra trùng tên với tên tài khoản.
- Mỗi group còn có một định danh riêng gọi là GID.
- Định danh của group thường sử dụng giá trị bắt đầu từ 1000.

Nhóm và các vấn đề liên quan

- Mọi người dùng trong các hệ unix hay Linux đều thuộc về một nhóm. Nhóm là một tập hợp các cá nhân đơn lẻ được gộp lại theo một lý do nào đó.
- Mỗi người có thể thuộc nhiều nhóm. Các nhóm được đặt quyền để các thành viên của nó có thể truy nhập đến các thiết bị, file, hệ thống file hoặc toàn bộ máy tính mà những người khác nhóm có thể bị hạn chế.
- Các thông tin về nhóm được lưu trong file /etc/groups

3. Quản lý user và group.

- Sử dụng lệnh.
- Chỉnh sửa trực tiếp vào file.

3.1. Lệnh tạo user

- `useradd [options] [login_name]`

- Công cụ sẽ tự động thêm các dòng tương ứng vào file /etc/passwd và /etc/shadow

Các bước thực hiện

- Tạo ra một tài khoản tên user-name
- Tạo ra một nhóm mới có cùng tên user-name với tài khoản
- Tạo thư mục cá nhân /home/user-name
- Sao chép profile mặc định từ /etc/skel
- Nhập các thông tin về người dùng
- Nhập mật khẩu cho tài khoản

- Các thông số thường dùng của lệnh useradd:

`-u` *UID*	user ID (default: next available number)
`-g` *GID*	default (primary) group (mặc định tạo group cùng tên với user)
`-G` *group*	Tên nhóm muốn user là thành viên
`-c` *comment*	Mô tả về user (default: blank)
`-d` *directory*	Đường dẫn home directory (default `/home/username`)
`-m`	Tự tạo home directory của user
`-M`	Không tạo home directory của user
`-k` *skel_dir*	Thư mục chứa template mẫu (default `/etc/skel`)
`-s` *shell*	login shell (default `/bin/bash`)

Ví dụ:

```
$ useradd -u 1003 -o -G sales,adv,team
                        alan
```

Bài tập

- Tạo user với tên Will và tên đầy đủ là Will Smiths:

```
useradd -c "Will Smiths" will
```

- Tạo user với tên justice và tên đầy đủ là Justice Smiths, user thuộc nhóm users và các nhóm wheel, sales:

```
useradd -g users -G wheel,sales -c
"Justice Smiths" justice
```

3.2. Thay đổi thuộc tính của user

- `usermod [options] [login_name]`
- Options :

  -c: comment: tạo bí danh (mô tả)

  -d: thay đổi thư mục home cho user

  -m: di chuyển nội dung từ thư mục home cũ sang thư mục home mới (chỉ dùng với -d)

  -g: chỉ định group chính

  -G: chỉ định group phụ (group mở rộng, nếu nhiều nhóm thì các nhóm cách nhau bởi dấu phẩy)

  -s: chỉ định shell cho user sử dụng

  -l: đổi tên tài khoản

  -L: khóa tài khoản

Ví dụ:

- Kết nạp tài khoản haui vào nhóm giaovien và đổi phần mô tả.

```
#usermod  -g  giaovien  haui
#usermod  -c "Quan tri he thong"  haui
```

- Một vài ví dụ khác:

```
# usermod -g users -c "Henry Blake" henry
# usermod -f 10 henry #disable tài khoản sau 10 ngày kể từ khi password hết hạn
# usermod -e 2023-12-31 majorh #expire_date
# usermod -L majorh #lock user
# usermod -U majorh #unlock user
```

Bài tập:

Đổi tên tài khoản will thành jaden (Jaden Smiths) với thư mục home của user là /home/jaden

```
usermod -l jaden -c "Jaden Smiths"
-m -d /home/jaden will
```

3.3. Xóa user :

- `userdel [option] <username>`
- Options :

  -r : xóa cả thư mục home của user
- Khi xóa tài khoản user bằng lệnh userdel, dòng mô tả tương ứng của user trong tập tin /etc/passwd và /etc/shadow cũng bị xóa .
- Ví dụ: `#userdel -r haui`

3.4. Khóa/Mở khóa tài khoản user

- Khóa

```
passwd -l <username>
usermod -L <username>
```

- Mở khóa

```
passwd -u <username>
usermod -U <username>
```

3.5. Thiết lập chính sách cho user

- `chage [options] [login_name]`
- Options:
  - `-l` : xem chính sách của 1 user
  - `-E` : thiết lập ngày hết hạn cho account
  - `-I` : thiết lập ngày bị khóa sau khi hết hạn mật khẩu (định dạng ngày tháng là YYYY-MM-DD)
  - `-m` : thiết lập số ngày tối thiểu được phép thay đổi password
  - `-M` : thiết lập số ngày tối đa được phép thay đổi password
  - `-W` : thiết lập số ngày cảnh báo trước khi hết hạn mật khẩu

Ví dụ

- `chage -E 2023-12-31 -m 5 -M 90 -I 30 -W 14 jaden`

- Mật khẩu hết hạn vào ngày 31/12/2023.
- Số ngày tối thiểu/tối đa giữa các lần thay đổi mật khẩu trong khoảng 5 và 90.
- Các tài khoản sẽ bị khóa sau 30 ngày sau khi hết hạn
- 1 tin nhắn cảnh báo sẽ được gửi ra 14 ngày trước khi hết hạn mật khẩu .

Ví dụ

```
chage -I -1 -m 0 -M 99999 -E -1 jaden
```

- Không bị hết hạn mật khẩu (thông số -1)
- Số ngày tối thiểu/tối đa giữa các lần đổi mật khẩu là vô hạn (0 -> 99999)
- Tài khoản không bao giờ bị hết hạn (thông số -1)

```
chage -d 0 jaden
```

Thiết lập bắt buộc user đổi mật khẩu trong lần đầu đăng nhập

3.6. Tạo/xóa nhóm

- **Tạo nhóm:**

  `groupadd <groupname>`

  Ví dụ: `#groupadd hocvien`

- **Xóa nhóm :**

  `groupdel <groupname>`

  Ví dụ: `#groupdel hocvien`

3.7. Xem thông tin về user và group

- `id <option> <username>`

  Ví dụ : Xem groupID của user haui

- `#id -g haui`
- `groups <username>`

  Ví dụ : Xem tên nhóm của user haui

- `#groups haui`

3.8. Những file lưu thông tin user và group.

- /etc/passwd

  Mỗi dòng trong tập tin gồm có 7 trường, được phân cách bởi dấu hai chấm.
- /etc/group

  Mỗi dòng trong tập tin gồm có 4 trường, được phân cách bởi dấu hai chấm.
- /etc/shadow

  Lưu mật khẩu đã được mã hóa và chỉ có user root mới được quyền đọc.

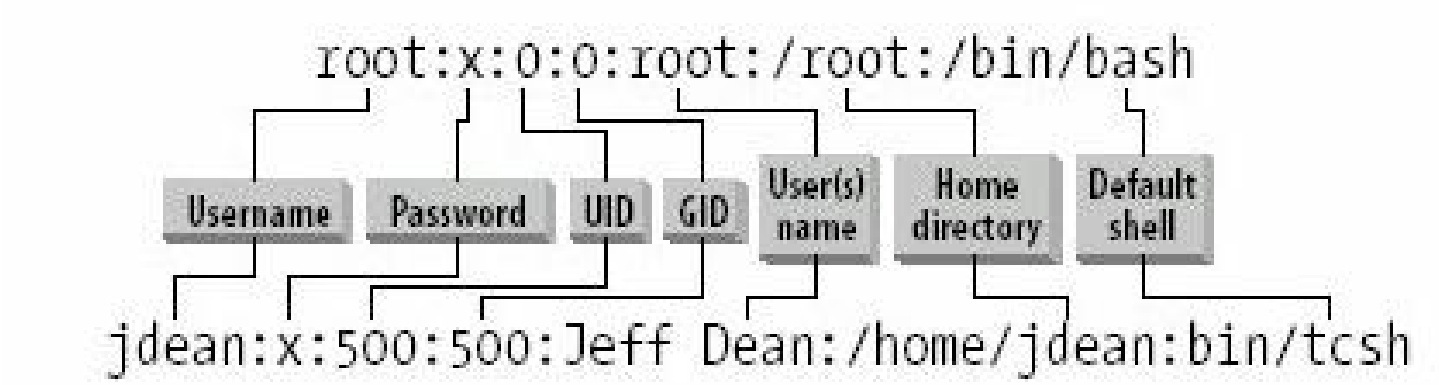
/etc/passwd

- Là file văn bản chứa thông tin về các tài khoản user trên máy .
- Mọi user đều có thể đọc tập tin này nhưng chỉ có user root mới có quyền thay đổi .
- Định dạng của dòng gồm nhiều cột, giá trị, dấu: được sử dụng để phân cách các cột.
- Để xem nội dung file ta dùng lệnh: ?

/etc/passwd

- Mỗi dòng trong file /etc/passwd ứng với một người dùng trong hệ thống.
- Cấu trúc mỗi dòng:

  name:password:UID:GID:User Name:home directory:shell



/etc/passwd

Mỗi user được lưu trong một dòng gồm 7 cột.

- Cột 1: tên người sử dụng
- Cột 2: mã liên quan đến passwd cho Unix chuẩn 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 3:4: user ID:group ID
- Cột 5: Tên đầy đủ của người sử dụng. Một số phần mềm phá password sử dụng dữ liệu của cột này để thử đoán password.
- Cột 6: thư mục cá nhân
- Cột 7: chương trình sẽ chạy đầu tiên sau khi login (thường là shell) cho user

/etc/shadow

- Là tập tin văn bản chứa thông tin về mật khẩu của các tài khoản user lưu trên máy.
- Chỉ có user root mới có quyền đọc tập tin này.
- User root có quyền reset mật khẩu của bất cứ user nào trên máy .
- Mỗi dòng trong tập tin chứa thông tin về mật khẩu của user.

KHOA CÔNG NGHỆ THÔNG TIN

TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI

Tuần sau chấm vở, lấy điểm TX1

/etc/shadow

```
name:password:lastchange:min:max:warn:inactive:expire:flag
```

- 1: Tên user, giống với trong /etc/passwd (login name)
- 2: Mật khẩu đã được mã hóa
  - Để trống (empty) – không có mật khẩu
  - * – tài khoản bị tạm ngưng (disable)
- 3: Số ngày kể từ lần cuối thay đổi mật khẩu (tính từ 1/1/1970)
- 4: Số ngày trước khi có thể thay đổi mật khẩu. Giá trị 0 là có thể thay đổi bất cứ lúc nào.
- 5: Số ngày mật khẩu có giá trị. 99999 có nghĩa mật khẩu có giá trị vô thời hạn.
- 6: Số ngày cảnh báo user trước khi mật khẩu hết hạn
- 7: Số ngày sau khi mật khẩu hết hạn tài khoản sẽ bị khóa. Thường có giá trị là 7 (1 tuần)
- 8: Số ngày kể từ khi tài khoản bị khóa (tính từ 1/1/1970)

/etc/shadow

- Các cách phá mật khẩu?

/etc/groups

- Là tập tin văn bản chứa thông tin về các group trên máy.
- Mọi user đều có quyền đọc tập tin này nhưng chỉ có user root mới có quyền thay đổi.

/etc/groups

```
group name:group password:group ID:users
```

- group name: Tên xác định nhóm, tối đa 8 ký tự
- group password: Trường mật khẩu đã được mã hoá, thường để trắng hoặc là x.
- group ID: Số duy nhất cho mỗi nhóm
- users: Chứa danh sách người dùng thuộc nhóm đó, phân cách bởi dấu “,”.

Có một số các nhóm mặc định thuộc HĐH (thường là bin, mail, uucp, sys…). Do vậy, không nên cho user thuộc vào nhóm này vì họ sẽ có quyền tương đương như root.

3.9. Bảo mật tài khoản

- Một số việc có thể làm để tăng độ an toàn:
  - Đặt ngày hết hạn cho những tài khoản tạm thời

    ```
    # usermod -e 2003-12-20 henry
    ```

  - Khóa những tài khoản lâu không dùng đến:

    ```
    # usermod -f 5 henry
    ```

  - Thay đổi thời hạn password với chage :

-I <inactive> Inactive lock, sau khi mật khẩu hết hạn bao lâu sẽ lock tài khoản.

3.10. Chuyển user:

```
su [- hoặc -l] username
```

-, -l: chạy đoạn mã login script của user mới

Để trở về user cũ, ta dùng lệnh exit

Tự nghiên cứu

Cách liệt kê các tài khoản trong Linux?