Bài 8. Quản lý người dùng

1. Người dùng

Tạo tài khoản

Chương trình **/usr/sbin/useradd,** alias là **useradd**, sẽ thêm người dùng mới vào hệ thống.

Cú pháp:

```
useradd [options] login-name
```

Lựa chọn:

-c	ghi chú (Tên đầy đủ)
-d	đường dẫn tới thư mục gốc
-g	nhóm khởi tạo (GID). GID phải đang tồn tại
-G	dấu phẩy ngăn cách danh sách các nhóm bổ sung
-u	UID của người dùng
-s	shell mặc định của người dùng
-p	mật khẩu (mã hoá md5, sử dụng dấu !)
-e	ngày hết hạn của tài khoản
-k	thư mục skel
-n	tắt nhóm UPG

Ví dụ, thêm một người dùng với tên truy cập là **rufus**

```
useradd rufus
```

Các giá trị mặc định sẽ được sử dụng khi không có tham số lựa chọn nào xác định. Ta có thể liệt kê các giá trị này với **useradd –D**

```
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_EMAIL_SPOOL=no
```

Thông tin này nằm trong file **/etc/default/useradd**

Thay đổi mật khẩu

Để cho phép một người dùng truy cập vào tài khoản của mình, quản trị mạng phải thiết lập một mật khẩu cho người dùng bằng chương trình **passwd**

Cú pháp:

```
passwd login-name
```

Các bước trên dùng để tạo một người dùng mới. Nó cũng định nghĩa một môi trường người dùng như là thư mục home directory và một shell mặc định. Người dùng cũng có thể được gán cho một nhóm, và xác định nhóm mặc định của mình.

Xóa tài khoản

Tài khoản người dùng có thể được xoá bởi **userdel**. Để đảm bảo rằng thư mục gốc của người dùng cũng được xoá, ta sử dụng tham số lựa chọn **–r**. Ví dụ

```
userdel -r rufus
```

/etc/passwd

Tất cả người dùng trong hệ thống được lưu giữ trong tệp **/etc/passwd.** Mỗi người dùng trên một dòng có cấu trúc như sau:

1. Tên truy cập
2. Mật khẩu (hoặc x nếu sử dụng file shadow)
3. UID
4. GID
5. Đoạn text mô tả người dùng
6. Thư mục gốc của người dùng
7. shell của người dùng

Bảy trường trên được ngăn cách bởi dấu hai chấm như được minh hoạ trong ví dụ sau đây.

```
rufus:x:1000:1000:rufus,,,:/home/rufus:/bin/bash
```

/etc/shadow

Mật khẩu của gười dùng thông thường được lưu trong tệp **/etc/shadow** chỉ có thể đọc được bởi người dùng root. Bạn cần chuyển sang quyền root trước, hoặc thêm sudo vào trước lệnh trên và cung cấp mật khẩu root nếu được yêu cầu để xem /etc/shadow. Ví dụ

```
sudo  cat /etc/shadow
```

Nhìn giá trị băm sau tài khoản. Nó là xâu ký tự bao gồm nhiều xâu con được phân cách nhau bởi dấu $. Xâu con đầu tiên là **6**, đoạn 6 ở đầu, cho biết hàm băm được sử dụng là SHA-512 (type 6). Xâu con tiếp theo là SALT. Ở ví dụ trên, giá trị salt là Wx9uYeuo. Xâu con tiếp theo, đến trước dấu hai chấm (:) là giá trị băm của mật khẩu. Ví dụ

```
rufus:$6$Wx9uYeuo$2TWKGjbCgkype57Ku4xK4hgI.8nDuz/7BH0vSkITgDjwnenZ1eSQcks0dLcJBwRIqngMdBhhzyyfyHpQQCsTB.:16409:0:99999:7:::
```

Thuật toán băm được định nghĩa trong tệp /etc/login.defs. Để kiểm tra thuật toán băm được sử dụng thực sự là SHA-512, hãy chạy lệnh sau trong từ Terminal:

```
grep -A 18 ENCRYPT_METHOD /etc/login.defs
```

Nếu muốn sử dụng tệp shadow, sử dụng câu lệnh sau đây:

```
/usr/sbin/pwconv
```

Câu lệnh này sẽ bỏ '**x**' trong trường thứ hai của file **/etc/passwd** và tạo file **/etc/shadow**.

Nếu không muốn sử dụng tệp shadow, chạy lệnh sau:

```
/usr/sbin/pwunconv
```

Chú ý: Khi sử dụng tệp mật khẩu bóng (shadow password) **/etc/passwd** thì có thể đọc được với quyền (644) và file **/etc/passwd** phải được cấm nhiều hơn (600 hoặc thậm chí 400). Tuy nhiên, khi sử dụng **pwunconv** thì phải bảo đảm thay đổi quyền trên file **/etc/password** (600 hoặc 400).

2. Nhóm

Tạo nhóm

Công cụ **groupadd** được sử dụng để quản trị các nhóm. Câu lệnh này sẽ thêm một thực thể vào file **/etc/group**

Lựa chọn:

-g	gán một GID

Ví dụ, tạo một nhóm **sales**

```
groupadd sales
```

Thêm/bỏ người dùng vào/khỏi nhóm

Sử dụng **gpasswd,** có thể thêm (**-a**) hoặc gỡ bỏ (**-d**) người dùng từ một nhóm và gán một người quản trị (**- A**) nhóm. Ví dụ, thêm người dùng **rufus** vào nhóm **sales**

```
gpasswd -a rufus sales
```

Thành viên nhóm

Một người dùng có thể thuộc về một hoặc nhiều nhóm. Tuy nhiên, tại một thời điểm (ví dụ khi tạo một tệp mới) thì chỉ duy nhất một nhóm là *nhóm hiệu lực*.

Chương trình groups cho biết các nhóm một người dùng là thành viên.

Cú pháp:

groups [login-name]

Ví dụ:

```
groups rufus
➔ ►     thanh : rufus adm cdrom sudo dip plugdev lpadmin sambashare vboxusers
```

Để biết cả định danh nhóm và định danh người dùng, sử dụng chương trình id.

Cú pháp:

id [login-name]

Ví dụ:

```
id rufus
➔ ►     uid=1000(rufus) gid=1000(rufus)
groups=1000(rufus),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),109(lpadmin),124(sambashare),125(vboxusers)
```

Trong ví dụ trên, rufus thuộc nhiều nhóm người dùng, trong đó nhóm rufus có định danh 1000 là nhóm hiệu lực.

Nhóm hiệu lực

Lệnh tham gia (chuyển) vào nhóm sẽ làm thay đổi nhóm hiệu lực của người dùng (user's effective group). Điều này có thể được thực hiện qua câu lệnh **newgrp**. Ví dụ, tham gia nhóm sales

```
newgrp sales
```

Nếu câu lệnh **groups** được sử dụng thì nhóm đầu tiên trong danh sách sẽ không còn là rufus mà là sales

/etc/group

Thông tin nhóm được lưu giữ trong file **/etc/group**. Mỗi nhóm được lưu trên một dòng có 4 trường được ngăn cách nhau bởi dấu hai chấm.

1. Tên nhóm
2. Mật khẩu nhóm (hoặc x nếu file gshadow tồn tại)
3. GID
4. Danh sách các thành viên phân cách bởi dấu phẩy

Ví dụ:

```
java:x:550:jade, eric, rufus
```

/etc/gshadow

Cũng như với người dùng, tệp **/etc/gshadow** được tạo khi sử dụng mật khẩu bóng nhóm (shadow group passwords). Các tiện ích này được sử dụng để chuyển đổi xuôi hoặc ngược các file shadow hoặc non-shadow như sau:

```
/usr/sbin/grpconv
/usr/sbin/grpunconv
```

/etc/login.defs

Tệp chứa các thông tin sau đây:

- Thư mục mail (the mail spool directory): MAIL_DIR
- Các điều khiển thời gian của mật khẩu:

  PASS_MAX_DAYS, **PASS_MIN_DAYS**, **PASS_MAX_LEN**, **PASS_WARN_AGE**
  - giá trị max/min của UID tự động lựa chọn trong useradd: **UID_MIN**, **UID_MAX**
  - giá trị max/min đối với lựa chọn tự động GID trong groupadd: **GID_MIN**, **GID_MAX**
  - tự động tạo một thư mục gốc với useradd: **CREATE_HOME**

/etc/skel/

Thư mục chứa các file mặc định và sẽ được copy tới thư mục gốc của người dùng mới được tạo: **.bashrc**, **.bash_profiles**, …

3. Thiết lập mặc định

Tất cả các lựa chọn trong khi tạo một người dùng hoặc nhóm có thể được thay đổi. Tiện ích **usermod** có một số tham số lựa chọn chính sau:

usermod (tham số lựa chọn)

-d	thư mục người dùng
-g	GID khởi tạo người dùng
-l	tên đăng nhập của người dùng
-u	UID của người dùng
-s	shell mặc định

Chú ý: tất cả các tham số lựa chọn trên cũng giống đối với **useradd**.

Tương tự như vậy, bạn cũng có thể thay đổi chi tiết về thông tin nhóm với tiện ích **groupmod**. Có một số tham số lựa chọn chính sau đây:

groupmod (tham số lựa chọn)

-g	GID
-n	tên nhóm

Khoá tài khoản:

- Một tài khoản người dùng có thể bị khoá bằng cách thêm vào một dấu chấm than vào mật khẩu người dùng. Có thể thực hiện điều này bằng các câu lệnh sau:

Khoá	**Mở khoá**
passwd –l	**passwd** –u
usermode –L	**usermod** –U

- Khi sử dụng shadow password, thay thế **x** bởi một dãy *
- Một tham số lựa chọn ít hữu ích là xoá toàn bộ mật khẩu với câu lệnh

  passwd –d
- Cuối cùng, có thể gán **/sbin/nologin** hoặc **/bin/false** cho shell mặc định của người dùng trong **/etc/passwd**

Mặc định ban đầu, mật khẩu người dùng có giá trị trong 99999 ngày, tương đương với 2739 năm (mặc định **PASS_MAX_DAYS**). Người dùng được thông báo trong vòng 7 ngày rằng mật khẩu của bạn sẽ bị hết hạn (mặc định **PASS_WARN_AGE**) với dòng thông báo sau mỗi khi người dùng đăng nhập vào hệ thống.

Có một tham số thời gian của mật khẩu khác được gọi là **PASS_MIN_DAY**. Đây là số ngày nhỏ nhất trước khi một người dùng có thể thay đổi mật khẩu, giá trị này được thiết lập mặc định ban đầu bằng 0.

Công cụ **chage** cho phép quản trị hệ thống thay đổi các tham số lựa chọn trên:

Cách dùng:

chage [-l] [-m min_days] [-M max_days] [-W warn] [-I inactive] [-E expire] [-d last_day] user

Tham số **-l** đầu tiên liệt kê giá trị của policy hiện thời của một người dùng. Chúng ta chỉ đề cập đến tham số lựa chọn **–E**. Tham số này sẽ khoá một tài khoản người dùng tại thời điểm xác định. Định dạng ngày có thể theo định dạng của UNIX hoặc theo **YYYY/MM/DD**

Chú ý, tất cả các giá trị trên đều được lưu giữ trong file **/etc/shadow** và có thể thay đổi trực tiếp.

II. Thực hành

1. Tạo người dùng

Sử dụng **useradd** để tạo người dùng có tên là tux với ID người dùng là 600 và GID nhóm là 550.

Sử dụng **usermod** để thay đổi thư mục gốc của người dùng

Có cần thiết phải tạo một thư mục mới không?

Nội dung của **/etc/skel** có được copy sang thư mục mới không?

Các nội dung trong thư mục gốc cũ vẫn có thể được truy cập bởi người dùng tux không?

Sử dụng **usermod** để thêm **tux** vào nhóm **wheel**.

2. Làm việc với nhóm

Tạo một nhóm có tên là **sales** với câu lệnh **groupadd**.

Thêm người dùng **tux** vào nhóm này bằng câu lệnh **gpasswd**.

Đăng nhập với **tux** và tham gia vào nhóm **sales** với **newgrp**.

3. File cấu hình

Thêm một người dùng vào hệ thống bằng cách soạn thảo **/etc/passwd** và **/etc/group**.

Tạo một nhóm có tên là **share** và thêm người dùng **tux** vào nhóm này bằng cách soạn thảo bằng tay **/etc/group**.

4. Thay đổi tài khoản

Thay đổi tham số ngày hết hạn của tài khoản người dùng **tux** bằng cách sử dụng câu lệnh **usermod**.

Khoá tài khoản người dùng (Sử dụng các công cụ hoặc soạn thảo file **/etc/shadow**, ...)

Bảo vệ người dùng từ đăng nhập bằng cách thay đổi shell mặc định của người dùng thành **/bin/false**.

Thay đổi tham số **PASS_MAX_DAYS** của người dùng **tux** thành 1 trong file /etc/shadow.

5. Thay đổi thiết lập mặc định

Sử dụng **useadd –D** để thay đổi các thiết lập mặc định của hệ thống và do đó tất cả người dùng mới sẽ được gán trong **/bin/sh** thay vì **/bin/bash** (chú ý: điều này sẽ làm thay đổi file trong **/etc/defaults/**)

Soạn thảo **/etc/login.defs** và thay đổi tham số mặc định **PASS_MAX_DAYS** và do đó người dùng mới sẽ phải thay đổi mật khẩu của mình theo định kỳ 5 ngày.