HỆ ĐIỀU HÀNH LINUX CĂN BẢN

Lê Ngọc Sơn
lnson@fit.hcms.edu.vn

CuuDuongThanCong.com https://fb.com/tailieudientucntt

Định nghĩa Users

- Users được định nghĩa trong một hệ thống để xác định “ai? được quyền dùng cái gì?” trong hệ thống đó.
- Với Linux, mỗi user có một định danh duy nhất, gọi là UID (User ID).
  - 0 – 99: user có quyền quản trị.
  - > 99: user riêng. >= 500: user thường.
  - => UID có khả năng sử dụng lại???
- Mỗi user thuộc ít nhất một group. Mỗi group cũng có một định danh duy nhất là GID.

cuu duong than cong. com

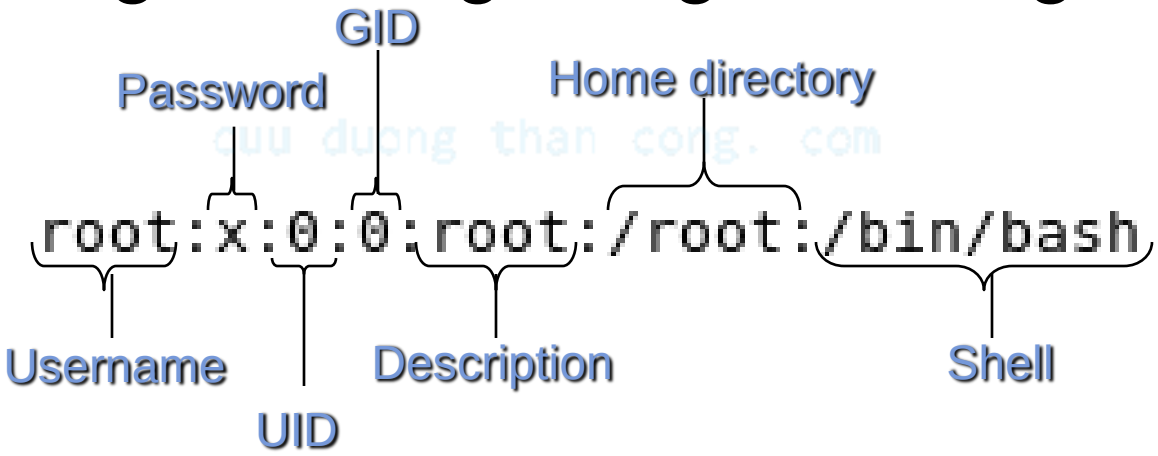
Định nghĩa Users (tt)

- Những file định nghĩa thông tin users:
  - /etc/passwd: chứa thông tin user login, password mã hóa, UID, GID, home directory, và login shell. Mỗi dòng là thông tin của một user.
  - /etc/shadow: chứa thông tin password mã hóa, thời gian sử dụng password, thời gian phải thay đổi password…
  - /etc/group: chứa thông tin group.
  - /etc/gshadow chứa password của group dưới dạng hash (ít khi dùng đến).

cuu duong than cong. com

Định nghĩa Users (tt)

- File /etc/passwd : Mỗi dòng trong file ứng với một người dùng trong hệ thống



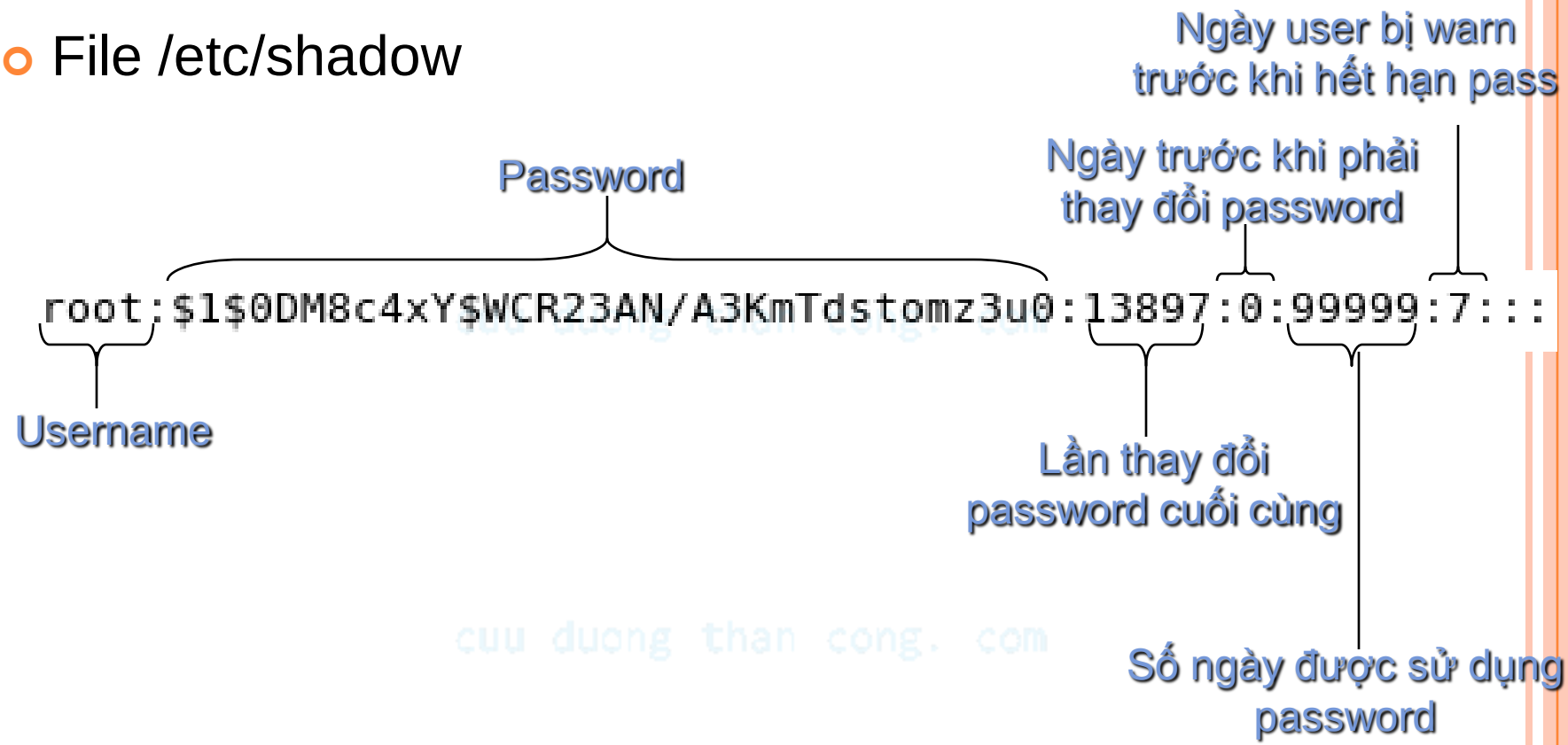
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin

Shell

cuu duong than cong. com

Định nghĩa Users (tt)

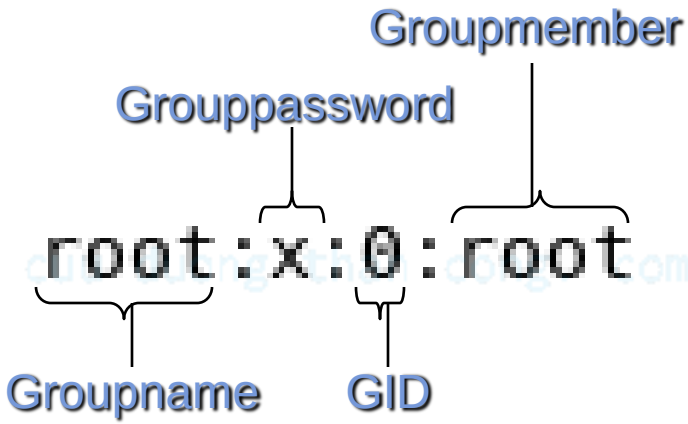
- File /etc/shadow



cuu duong than cong. com

Định nghĩa Users (tt)

- File /etc/group



cuu duong than cong. com

Công cụ quản lý Users

- Quản lý bằng command line
  - useradd: tạo user.
  - usermod: chỉnh sửa thông tin user.
  - userdel: xóa user (tham số -r xóa thư mục home của user).
  - groupadd: tạo group.
  - groupdel: xóa group.
  - groupmod: chỉnh sửa thông tin group
  - Groups: xem các users của group.
- Quản lý bằng giao diện đồ họa
- Quản lý trực tiếp trên file

cuu duong than cong. com

Cấu hình mặc định

- Khi dùng lệnh useradd không có option kèm theo để tạo user, các thuộc tính của user sẽ được tạo theo các cấu hình mặc định.
- Những file định nghĩa cấu hình mặc định:
  - /etc/default/useradd
  - /etc/skel/
  - /etc/login.defs
- Nếu muốn thay đổi cấu hình mặc định, thay đổi trực tiếp trong những file này.

cuu duong than cong. com

Cấu hình mặc định (tt)

- /etc/default/useradd: những giá trị mặc định cho việc tạo acount.
- /etc/skel: thư mục chứa nội dung mặc định sẽ tạo trong home directory của users.
- /etc/login.defs: những cấu hình mặc định cho shadow password.

cuu duong than cong. com

cuu duong than cong. com

Chuyển user

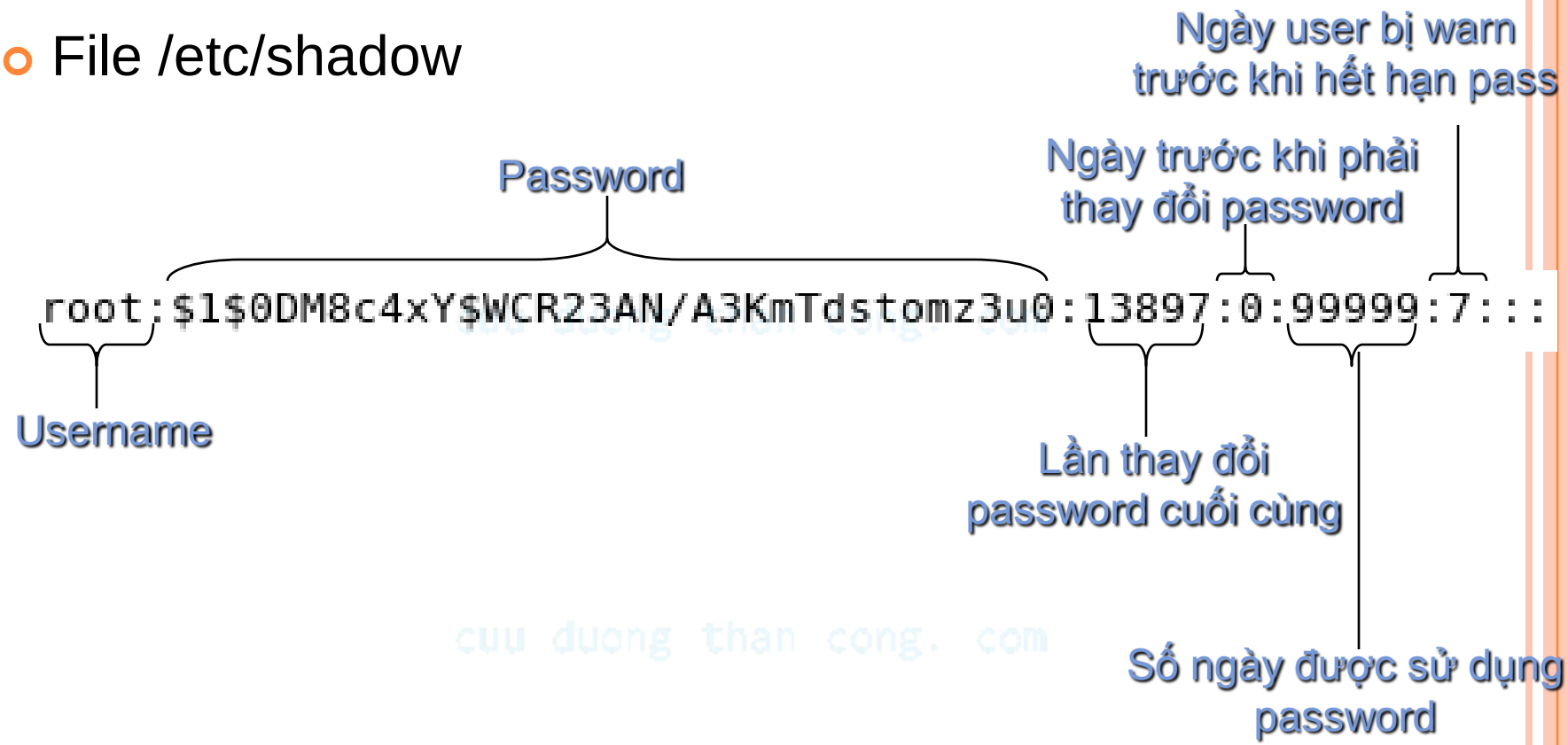
- Câu lệnh su được dùng để chuyển quyền điều khiển sang một người dùng khác.
- Cú pháp: su [- hoặc -l] username
  - -, -l: chạy đoạn mã login script của user mới
  - username thì mặc định là **root.**
- Để trở về user cũ ta dùng lệnh exit

cuu duong than cong. com

cuu duong than cong. com

Chính sách về mật khẩu

- File /etc/shadow



cuu duong than cong. com

/ETC/SHADOW

- Mật khẩu của user sẽ được băm (hash) và lưu trong file này.

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

`name`	**User login name, mapped to /etc/passwd**
`password`	**Encrypted password. If this field is blank, then there is no password ; "*","!!" : account is locked, …**
`lastchange`	**Number of days since the last password change, from 1/1/70**
`min`	**Minimum number of days between password changes**
`max`	**Maximum number of days password is valid**
`warn`	**Number of days before expiration that user will be warned**
`inactive`	**Number of inactivity days allowed for this user**
`expire`	**Absolute date, beyond which the account will be disabled**

CuuDuongThanCong.com https://fb.com/tailieudientucntt

THAY ĐỔI PASSWORD

- Để thay đổi password của user ta dùng câu lệnh passwd

```
# passwd henry
current password :
new password:
retype new password:
```

- Lời khuyên khi chọn password:
  - **Not use proper words or names**
  - **Use letters and digits**
  - **Include symbols: !, @, #, $, %, …**
- Không cho phép các tài khoản “guest” login vào hệ thống

cuu duong than cong. com
cuu duong than cong. com

THAY ĐỔI THỜI HẠN SỬ DỤNG

- **Thay đổi thời hạn password với `chage` :**

```
chage [options] <user>
```

- **Options:**

`-m <mindays>`	**Minimum days**
`-M <maxdays>`	**Maximum days**
`-d <lastdays>`	**Day last changed**
`-I <inactive>`	**Inactive lock, sau khi mật khẩu hết hạn bao lâu sẽ lock tài khoản.**
`-E <expiredate>`	**Expiration (YYYY-MM-DD or MM/DD/YY)**
`-W <warndays>`	**Warning days**

cuu duong than cong. com

BẢO MẬT TÀI KHOẢN

- **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

- **Để tìm và xóa tất cả các file/thư mục của user nằm ngoài home directory:**

  # find / -user henry –type f –exec rm –f {} \;

  # find / -user henry –type d –exec rmdir {} \;

cuu duong than cong. com

Chính sách mượn quyền

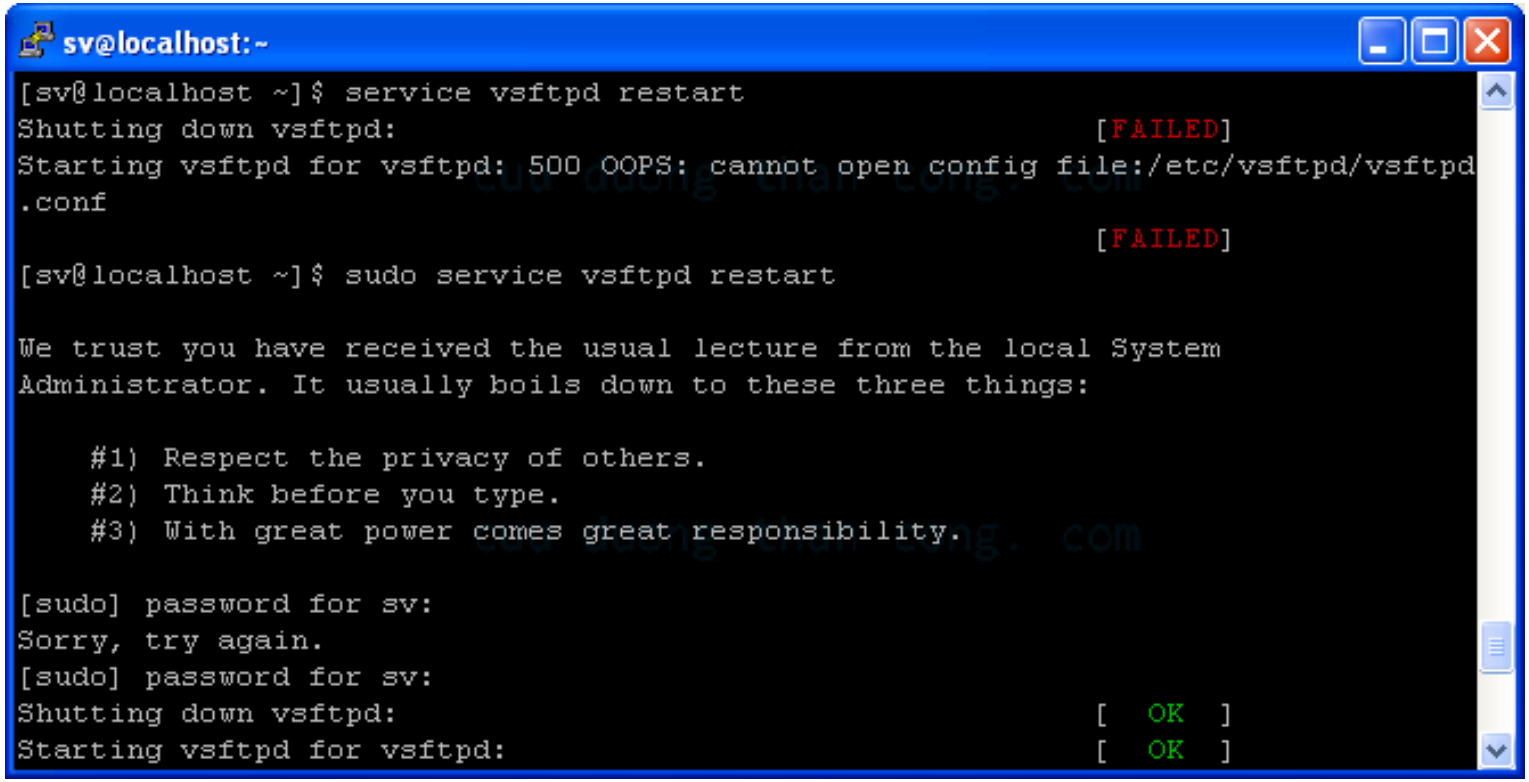
- Môi trường Linux là một môi trường có nhiều người dùng, nhiều người quản trị.
- Nếu người dùng nào cũng sử dụng tài khoản root, khi hệ thống có thay đổi sẽ rất khó để biết ai là người đã tạo nên thay đổi đó.
- Mỗi người sẽ dùng tài khoản riêng, khi cần tác động đến hệ thống sẽ mượn tạm quyền của user root thông qua công cụ “sudo”

cuu duong than cong. com

CuuDuongThanCong.com https://fb.com/tailieudientucntt

Sử dụng sudo

- Sử dụng sudo, user **sv** được yêu cầu nhập password của chính mình (không phải của **root**), khi nhập thành công sẽ thực thi được công việc



Những ai được sudo?

- Việc ai được phép sudo, và khi sudo sẽ được thực thi những quyền hạn nào được qui định trong tập tin /etc/sudoers
- Để chỉnh sửa tập tin này, dùng quyền root và thực thi câu lệnh visudo (tương tự lệnh vi, nhưng chuyên để sửa file sudoers vì vị trí file này có thể thay đổi trên các dòng linux khác nhau)

cuu duong than cong. com

cuu duong than cong. com

Cú pháp

- Cú pháp file sudoers

username/group servername = (usernames to run as) command

- Trong đó tham số “usernames to run as” không nhất thiết phải có, nếu tham số này không tồn tại người sudo sẽ chạy với quyền root
- Nếu nhiều username hoặc nhiều command, mỗi user/command cách nhau bằng dấu “,” (comma)

cuu duong than cong. com

Qui ước

- Ở cột đầu tiên, nếu là group sẽ có thêm dấu % trước trên group
- Có thể dùng từ khóa ALL để chỉ tất cả mọi user/server hoặc mọi command (sẽ có ví dụ)
- Nếu dữ liệu quá dài, không thể viết trên 1 dòng có thể dùng ký hiệu \ trước khi xuống dòng
- Nếu file sudoers chỉ dùng trên máy cục bộ, thường cột server sẽ là ALL

cuu duong than cong. com

cuu duong than cong. com

- Tham khảo thêm:
  - http://linuxhomenetworking.com

cuu duong than cong. com

cuu duong than cong. com