TRƯỜNG ĐẠI HỌC CẦN THƠ
KHOA CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG
BỘ MÔN MẠNG MÁY TÍNH & TRUYỀN THÔNG

Linux User Management

Trình bày: TS. NGÔ BÁ HÙNG
Email: nbhung@cit.ctu.edu.vn

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

root

- Là tài khoản quản trị hệ thống mặc định của Linux
- có uid=0
- Mật khẩu xác lập đầu tiên lúc cài đặt hệ thống
- Có toàn quyền trên hệ thống Linux
- Dưới Ubuntu
  - Mặc định vô hiệu hóa (không xóa)
  - Được thay thế bằng công cụ sudo
  - Có thể kích hoạt lại nếu cần thiết

Sudo

- Là công cụ cho phép tài khoản được gán quyền nâng cấp lên quyền quản trị hệ thông 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
- Dùng bởi người dùng thuộc nhóm quản trị **sudo** (từ 12.04 về sau) và **admin** (trước 12.04)
- **Lưu ý: Các lệnh phần sau đề phải có từ sudo đứng trước**

Thông tin về tài khoản

- Lệnh cho biết tên tài khoản hiện hành
  - $whoami
    nbhung
- Lệnh xem user id và các groups của một user
  - $id user-name
  - Nếu không có user-name thì sẽ lấy login name của người dùng hiện tại
- uid <1000: system users
- uid>=1000: normal users

Thêm người dùng mới

- sudo adduser *user-name*
  - 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

Cơ sở dữ liệu người dùng

- /etc/password:
  - Chứa thông tin cơ bản về người dùng
  - Mỗi dòng cho mỗi tài khoản gồm 7 trường ngăn cách bởi dấu hai chấm (:) như sau: username:password: uid:gid:comment:home:shell
  - Ví dụ:
    - root:x:0:0:root:/root:/bin/bash
    - nbhung:x:1000:1000:Ngo Ba Hung:/home/nbhung:/bin/bash
- /etc/shadow: Chứa mật khẩu đã mã hóa

Thực hành

- Tạo người dùng có
  - username: user1, password: userone
  - Nhập các thông tin cho người này theo ý bạn
- Khảo sát thông tin về user1 trong /etc/passwd
- Đánh lệnh logout để kết thúc phiên làm việc
- Login trở lại với tài khoản user1 vừa tạo
- Tạo một số thư mục với lệnh mkdir; Dùng lệnh ls, cd để khảo sát thư mục cá nhân của người dùng user1
- Login in trở lại với tài khoản nhà quản trị của bạn

Xóa/Khóa/Mở tài khoản

- sudo deluser user-name
  - Xóa tài khoản và nhóm có tên user-name
  - Không xóa thư mục cá nhân của tài khoản /home/user-name
- Khóa một tài khoản
  - sudo passwd -l user-name
- Mở khóa một tài khoản
  - sudo passwd -u user-name

Thực hành

- Xóa người dùng user1 (vẫn giữ lại home)
- Đánh lện ls /home để xem home của user1 còn tồn tại hay không
- Add lại người dùng user1
- Dùng lệnh su - user1 để đăng nhập như người dùng user1, tùy chọn - để đưa về home sau khi đăng nhập thành công
- Đánh lệnh cd ~ để chuyển về home của user1
- Đánh lệnh pwd để xem đường dẫn đến home user1

Thực hành

- Tạo tài khoản user2
- Khóa người dùng user2
- Thử đăng nhập vào server bằng tài khoản user2
  - Cho biết kết quả
- Đăng nhập bằng tài khoản nhà quản trị
- Mở khóa cho user2
- Thử đăng nhập vào server bằng tài khoản user2
  - Cho biết kết quả

Thực hành

- Đăng nhập bằng tài khoản nhà quản trị
- Xóa tài khoản user2 cùng với home của user bằng lệnh
  - deluser --remove-home user2
- Thử đăng nhập vào server bằng tài khoản user2
  - Cho biết kết quả
- Thư mục /home/user2 còn tồn tại không?

Thực hành

- Đăng nhập với vai trò nhà quản trị
- Tạo thư mục /backup
- Tạo lại người dùng user2
- Đăng nhập với tài khoản user2 và dùng vi để tạo tập tin với tên Readme.txt, nội dung tùy ý
- Đăng nhập lại với tài khoản quản trị
- Xóa người dùng user2, có backup home cho user2
  - deluser --remove-home --backup --backup-to /backup user2
- Kiểm tra nội dung thư mục /backup

Thực hành

- Chuyển vào /backup
- Giải nén tạp tin user2.tar.bz bằng lệnh sau
  - sudo tar xvjf user2.tar.bz
  - Lệnh trên sẽ tạo ra thư mục /backup/home/user2
- Copy /backup/home/user2 vào /home
  - sudo cp -r /backup/home/user2 /home
- Kiểm tra thư mục /home/user2
- Add lại người dùng user2
- Đăng nhập với user2

Thay đổi mật khẩu

- Nhà quản trị có quyền đặt lại (reset) mật khẩu cho các tài khoản khác
  - $sudo passwd user-name
    Nhập 2 lần mật khẩu mới
- Mỗi người dùng có thể tự đổi mật khẩu của mình
  - $passwd
    Nhập lại mật khẩu cũ
    Nhập 2 lần mật khẩu mới

Thực hành

- Đăng nhập vời tài khoản user1
- Đổi mật khẩu thành numberone
- Đăng nhập lại bằng tài khoản user1

- Đăng nhập với tài khoản quản trị
- Đặt lại mật khẩu người dùng user1 thành anhmot
- Đăng nhập lại bằng tài khoản user1

Đặt chiều dài tối thiểu mật khẩu

- File cấu hình /etc/pam.d/common-password
- Thay đổi dòng
  - Password …..... sha512 min=8

Thực hành

- Đặt chiều dài tối thiểu cho mật khẩu là 7
- Đăng nhập vào tài khoản user1
- Đổi mật khẩu thành 123456
  - Cho biết kết quả
- Đổi mật khẩu thành chuỗi lớn hơn hoặc bằng 7 ký tự
  - Cho biết kết quả

Xem trạng thái mật khẩu

- sudo chage -l user1
  - Last password change : Jul 23, 2010
  - Password expires : never
  - Password inactive : never
  - Account expires : never
  - Minimum number of days between password change: 0
  - Maximum number of days between password change: 99999
  - Number of days of warning before password expires : 7

Đặt thời hạn cho mật khẩu

- Account quá hạn (E) ngày 12/31/2013
- Tuổi thọ ít nhất (m) 5 ngày
- Tuổi thọ lâu nhất (-M) 90 ngày
- Không hoạt động (-I) 5 ngày sau khi mật khẩu quá hạn
- Cảnh báo trước (-W) 14 ngày trước khi mật khẩu quá hạn
  - sudo chage -E 12/31/2013 -m 5 -M 90 -I 5 -W 14 username
- Tham số đặt trong tập tin /etc/login.defs

Thay đổi thư mục cá nhân

- usermod -d /home/new-home username

Thực hành

- Đăng nhập với tài khoản người dùng user1
- Đánh lệnh pwd để xem thư mục home là gì?
- Đăng nhập với tài khoản quản trị
- Tạo thư mục /home/userone
- Đổi home directory của người dùng user1 sang /home/userone
- Đăng nhập với tài khoản người dùng user1
- Đánh lệnh pwd để xem thư mục home là gì?
- Đổi lại home của user1 về /home/user1

Nhóm người dùng

- Tập hợp nhiều tài khoản người dùng
- Được sử dụng để quản lý tài nguyên dễ dàng hơn
- Thành viên của một nhóm có quyền trên các tài nguyên đã gán cho nhóm
- Được định nghĩa trong tập tin /etc/group
- Một tài khoản thuộc một nhóm chính và có thể thuộc nhiều nhóm phụ
- Nhóm chính mặc định trùng tên với tên tài khoản

Cơ sở dữ liệu nhóm

- /etc/group
  - Chứa thông tin về các nhóm
  - Mỗi dòng một nhóm người dùng, gồm 4 mục từ ngăn cách nhau bởi dấu hai chấm (:) như sau: Groupname:password:gid:members
    - Các member ngăn cách bởi dấu ,
- /etc/gshadow
  - Chứa mật khẩu của người quản trị nhóm, gồm các trường: Groupname:Password:Admins:members

Quản trị nhóm người dùng

- Thêm nhóm
  - sudo addgroup my-group
- Thêm người dùng mới vào nhóm
  - sudo adduser user-name my-group
- Thêm người dùng đã có vào nhóm
  - sudo usermod -G group-name user-name
- Xóa nhóm
  - sudo delgroup my-group

Quản trị nhóm người dùng

- Thay đổi nhóm chính của một người dùng
  - usermod -g new-primary-group user-name
- Thay đổi nhóm chính tạm thời
  - newgrp new-temp-primary-group
- Trở lại nhóm chính ban đầu:
  - exit
- Xác định người quản trị nhóm
  - gpasswd -A user-admin group-name

Thực hành

- Tạo nhóm có tên là nhom1
- Add người dùng user1 vào nhom1
- Hiển thị danh sách các nhóm của user1 đang tham gia bằng lệnh: id user1
- Cho biết nhóm chính của người dùng user1 là gì
- Đăng nhập với người dùng user1, tạo thư mục dir1
- Đánh lệnh ls -ld dir1 để xem nhóm chủ sở hữu của dir1
- Đánh lệnh chuyển nhóm chính tạm thời về nhom1
- Tạo thư mục dir2, cho biết nhóm chủ sở hữu của dir2

Quyền trên hệ thống tập tin

- Tất cả thành phần trên hệ thống tập tin là tập tin
- Có 3 chủ thể có quyền trên một tập tin
  - Chủ sở hữu (owner)
  - Thành viên thuộc nhóm chủ sở hữu (group)
  - Những người còn lại (other)
- Có 3 loại quyền:
  - Đọc (Read), Ghi (Write), Thực thi (eXecute)
- Owner Group Others
  rwx rwx rwx

Quyền trên tập tin

- Quyền read (r): Được quyền đọc dữ liệu lưu trong tập tin
- Quyền write (w): Được quyền thay đổi nội dung tập tin
- Quyền thực thi (x): Được quyền thực thi tập tin như là một chương trình

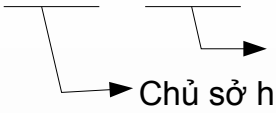
Quyền trên thư mục

- Quyền read (r): Được quyền liệt kê nội dung thư mục
- Quyền write (w): Được quyền tạo, xóa, đổi tên tập tin hay thư mục con chứa trong thư mục
- Quyền thực thi (x): Được quyền đi ngang qua thư mục

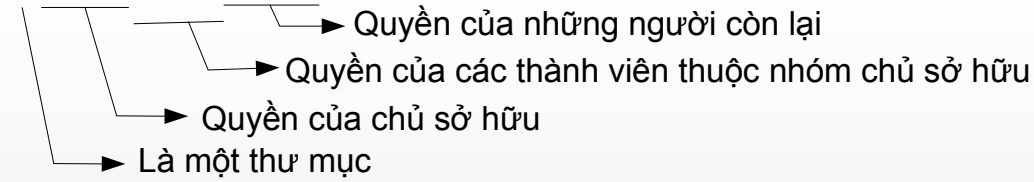
Liệt kê quyền

- ls -l /home/nbhung

```
drwxrwxr-x  2 nbhung nbhung   4096 2009-11-24 15:45 Ubuntu One
-rwxr-xr-x  1 nbhung nbhung   7094 2011-01-03 03:23 untitled
-rw-r--r--  1 nbhung nbhung    973 2011-01-03 03:23 untitled.c
drwxr-xr-x  2 nbhung nbhung   4096 2010-03-11 16:28 untitled folder
```



drwxrwxrwx



Qui tắc áp dụng quyền

- Nếu bạn là chủ sở hữu của tập tin
  - Các quyền trên chủ sở hữu sẽ được áp dụng
- Ngược lại, nếu bạn là thành viên của nhóm chủ sở hữu
  - Các quyền trên nhóm chủ sở hữu sẽ được áp dụng
- Nếu bạn không thuộc 2 trường hợp trên
  - Nhóm quyền cho tất cả mọi người sẽ được áp dụng

Thay đổi quyền trên tập tin

- Được thực hiện bởi chủ sở hữu hoặc admin/root
- Sử dụng lệnh chmod [ugoa][+=-][rwxX] a-file
  - u: áp dụng lên quyền chủ sở hữu
  - g: áp dụng lên quyền nhóm chủ sở hữu
  - o: áp dụng lên quyền những người còn lài
  - a: áp dụng lên cả 3 nhóm quyền u,g,o
  - +: gán quyền; =: gán chính xác; -:bỏ quyền
  - rwx: loại quyền đọc, viết, thực thi
  - X: gán quyền x cho thư mục và các tập tin đã có quyền x

Một số ví dụ chmod

- chmod a+x my-prog
  - Bổ sung (+) quyền thực thi (x) tập tin my-prog cho tất cả người dùng (a)
- chmod o-w my-data
  - Loại bỏ (-) quyền ghi (w) trên tập tin my-data đối với những không phải là chủ sở hữu hoặc không thuộc nhóm chủ sở hữu
- chmod go=rx my-prog
  - Gán quyền đọc (r) và thực thi (x) tập tin my-prog cho thành viên nhóm chủ sở hữu và những người khác

Thực hành

- Đăng nhập vào người dùng user1
- Tạo tập tin my-prog, có nội dung
  - echo "Hello World ! "
- Cho biết chủ sở hữu có quyền gì trên my-prog?
  -
- Thực thi my-prog
  - ./my-prog
- Thêm quyền thực thi cho chủ sở hữu trên my-prog
- Thực thi lại my-prog

Thực hành

- Xóa quyền write đối với chủ sở hữu tập tin my-prog
  - chmod u-w my-prog
- Thêm dòng sau vào my-prog
  - echo «I'm here»
  - Cho biết kết quả

Thực hành

- Hãy gán quyền trên my-prog như sau
  - Owner: read, write, execute
  - Group: read, execute
  - Others: read, execute
- Đánh lệnh ls -l my-prog để xem quyền hiện tại trên my-prog là gì
  - -rwx,r-x,r-x

Thay đổi quyền trên thư mục

- chmod -R g+rwX,o+rX my-dir
  - Đệ qui cho tất cả các thư mục hậu duệ
  - Thêm quyền rwx cho nhóm chủ sở hữu và quyền rx cho những người khác một cách đệ qui trên các thư mục con và trên các tập tin có thể thực thi
  - Đối với các tập tin không thực thi: Thêm quyền rw cho nhóm chủ sở hữu và quyền r cho những người khác

Quyền sticky trên thư mục

- Thường gán cho thư mục công cộng, ví dụ /tmp

```
ls -ld /tmp
drwxrwxrwt 18 root root 8712192 2011-01-07 16:11 /tmp
```

- Một tập tin nằm trong thư mục có quyền stick chỉ được xóa bởi chủ sở hữu hoặc admin/root
- chmod +t public-dir
  - Gán quyền sticky trên thư mục public-dir

Thực hành

- Tạo tài khoản user2
- Đăng nhập vào user2, tạo tập tin /tmp/file2.txt; gán tất cả người dùng có quyền rw trên file2.txt
- Đăng nhập vào user1,
  - Tạo tập tin /tmp/file1.txt, gán tất cả người dùng có quyền rw trên file1.txt
  - Đánh lệnh ls -l file*.txt để xem quyền trên file1 và file2
  - Thử xóa tập tin /tmp/file2.txt
- Đăng nhập vào user2
  - Thử xóa file1.txt
  - Thử xóa file2.txt

Thực hành

- Đăng nhập với tài khoản quản trị
  - Tạo thư mục /opt/publics
  - Gán tất cả mọi người có toàn quyền trên publics
  - Gán quyền sticky trên publics
- Đăng nhập vào user2, tạo thư mục /opt/publics/project2; gán tất cả người dùng có quyền rwx trên project2
- Đăng nhập vào user1, tạo tập tin /opt/publics/project2/file1.txt, gán tất cả người dùng có quyền rw trên file1.txt
  - Thử xóa project2
- ~~Đăng nhập vào user2: Thử xóa /opt/publics/project2/file1.txt~~
- ~~Đăng nhập vào [illegible]: Thử xóa~~

Quyền setuid và setgid (1)

- Vấn đề:
  - user-a sở hữu tập tin file-a và chương trình prog-a
  - Chỉ có user-a có quyền write trên file-a
  - user-a thực thi prog-a, prog-a thể write lên file-a
  - user-b thực thi prog-a, prog-a không thể write lên file-a
- Mong muốn
  - user-b thực thi prog-a với các quyền của user-a để có thể thao tác lên file-a

Quyền setuid và setgid (2)

- Quyền setuid:
  - Khi một chương trình được gán quyền này, nó sẽ thực thi (bởi bất kỳ người dùng nào) với tư cách như thể là chủ sở hữu của nó đã thực thi (với toàn quyền của chủ sở hữu chương trình)
- Quyền setgid: Tương tự như setuid
  - Khi một chương trình được gán quyền này, nó sẽ thực thi (bởi bất kỳ người dùng nào) với tư cách như thể là thành viên của nhóm chủ sở hữu của nó đã thực thi (với toàn quyền của nhóm chủ sở hữu chương trình)

Ví dụ về setuid

- $ls -l /etc/passwd
  -rw-r--r-- 1 root root 3022 Jan 9 21:34 /etc/passwd
- $ls -l /usr/bin/passwd
  -rw**s**r-xr-x 1 root root 41284 Sep 13 05:29 /usr/bin/passwd
- Khi người dùng bất kỳ thực thi chương trình passwd, nhờ đã có quyền suid, chương trình passwd được phép sửa đổi tập tin /etc/passwd như thể là người dùng root đang thực thi chương trình

Gán quyền setuid lên tập tin

- Quyền setuid dùng ký tự s nằm tại vị trí x của owner
  - s = x+suid
  - S=suid
- Gán quyền:
  - $chmod u+s prog-a
- Lấy lại quyền
  - $chmod u-s prog-a
- $ls -a prog-a
  - -rwsrwxr-x 1 nbhung nbhung 7159 Aug 31 09:10 prog-a

Quyền setgid trên thư mục (1)

- Gán cho thư mục chia sẻ bởi nhóm người dùng
- Dùng cho các thư mục của dự án
- Tập tin/thư mục tin tạo ra trong thư mục có quyền sgid sẽ có cùng nhóm chủ sở hữu với thư mục
- Thư mục con tạo ra trong thư mục có quyền setgid cũng được gán quyền setgid như thư mục cha
- Thể hiện bằng ký tự s tại vị trí x của nhóm chủ sở hữu
- Gán: $chmod g+s project
- Loại bỏ: $chmod g-s project

Quyền setgid trên thư mục (2)

- Ví dụ
  - mkdir proj-a
  - chmod g+ws proj-a
  - ls -ld proj-a
    drwxrwsr-x 3 nbhung develop 4096 Jan 15 16:29 proj-a
  - sudo usermod -a -G develop u1

Quyền setgid trên thư mục (3)

- Ví dụ
  - su – u1
  - $ touch ~nbhung/tam/proj-a/test1.txt
  - $ mkdir ~nbhung/tam/proj-a/mydir
  - exit
  - ls proj-a
    drwxr-sr-x 2 u1 develop 4096 Jan 15 16:29 mydir
    -rw-r--r-- 1 u1 develop 0 Jan 15 16:27 test1.txt

Thực hành

- Tạo nhóm develop
- Thêm người dùng quản trị (cms), user1, user2 vào nhóm develop
- Đăng nhập với tài khoản quản trị
  - Tạo thư mục /opt/project-a
  - sudo chgrp develop /opt/project-a
  - Thêm nhóm quyền ghi và setguid cho project-a
  - ls-a để xem quyền và nhóm chủ sở hữu của project-a
- Lần lược đăng nhập vào user1 và user2, tạo trong project-a các tập tin tương ứng file1.txt và file2.txt

Hiển thị các quyền đặc biệt

- Sử dụng lệnh ls -l
- Setuid và Setgid biểu thị bằng ký tự **s** tại vị trí quyền thực thi của chủ sở hữu và nhóm chủ sở hữu
- Quyền sticky sẽ được thể hiện bằng ký tự **t** tại vị trí thực thi của other
- Nếu là s hoặc t: Có cả quyền thực thi
- Nếu là **S** hoặc **T**: Không có quyền thực thi

Thể hiện quyền bằng số

user			group			Other		
r	w	x	r	w	x	r	w	x
0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1
0-7			0-7			0-7		

- rwxr-xr-x => 111101101 => 755
- chmod 755 my-prog.sh
- ls -l myprog.sh

  -rwxr-xr-x 1 nbhung nbhung 0 2011-01-10 11:07 my-prog.sh

Thiết lập quyền mặc định

- Cho các tập tin, thư mục mới tạo
- Sử dụng lệnh umask XYZ
  - XYZ
    - là 3 con số tương đương rwxrwxrwx
    - Các quyền KHÔNG gán cho tập tin/thư mục mới tạo được đặt lên 1; Quyền x không gán cho tập tin không thực thi
- Ví dụ umask 002 (000 000 010 = --- --- -w-)
  - Không muốn gán quyền ghi cho những người khác
- Thường được đặt trong tập tin khởi động lúc đăng nhập hoặc mở terminal mới

Thực hành

- Hãy thiết đặt để các tập tin/thư mục mới tạo ra có quyền sau: rwx r-x r-x
  - umask 000 010 010 (022)
- Tạo tập tin file-new.txt
- Kiểm tra quyền của file-new.txt có đúng là quyền rwx r-x r-x =>
- Tạo thư mục new-dir
- Kiểm tra quyền của new-dir có đúng là quyền rwx r-x r-x

An toàn cho hồ sơ người dùng

- Hồ sơ (profile) mặc định được sao chép từ /etc/skel
- Ubuntu đặt home directory ở chế độ read/execute
  - Thư mục các nhân có thể đọc bởi người khác
- Kiểm tra quyền trên thư mục cá nhân
  - ls -ld /home/user-name
- Không cho người khác đọc thư mục cá nhân
  - sudo chmod 0750 /home/username
- Sửa đổi/etc/adduser.conf
  - DIR_MODE=0750

Thay đổi chủ sở hữu và nhóm

- Thay đổi chủ sở hữu
  - chown new-owner file-name
  - chown new-owner [-R] dir-name
    - Tùy chọn -R để thay đổi một cách đệ qui trên thư mục
- Thay đổi nhóm chủ sở hữu
  - chgrp new-group file-name
  - chgrp new-group [-R] dir-name
    - Tùy chọn -R để thay đổi một cách đệ qui trên thư mục

Thực hành

- Đăng nhập vào tài khoản quản trị
  - Tạo thư mục /opt/user1
- Đăng nhập vào người dùng user1
  - Thử tạo tập tin và thư mục trong /opt/user1
- Đăng nhập vào tài khoản quản trị
  - Chuyển chủ sở hữu của thư mục /opt/user1 sang người dùng user1
- Đăng nhập vào người dùng user1
  - Thử tạo tập tin và thư mục trong /opt/user1