CSE301 - Linux và phần mềm mã nguồn mở

Bài 05: Người dùng và Nhóm

dungkt@tlu.edu.vn

COMPUTER SCIENCE AND ENGINEERING
THUYLOI UNIVERSITY

Nội dung

1) Tài khoản root và an ninh hệ thống
2) Quản lý người dùng
3) Quản lý nhóm

1. Tài khoản root và an ninh hệ thống

Các thuật ngữ root

- **File system**: Trong cấu trúc cây thư mục của Linux, thì root directory có ký hiệu là dấu / , là thư mục cấp cao nhất – nó không có thư mục cha.
- **Home directory**: Mỗi người dùng đều có thư mục chủ (home) để lưu trữ những dữ liệu, thiết lập cá nhân của họ. Thư mục home của người dùng root là /root , còn những người dùng bình thường (normal user) khác có thư mục home nằm tại /home/user_name
- **User account**: **root** là tên tài khoản có đặc quyền cao nhất trong các hệ thống

Tài khoản root và an ninh hệ thống

- **User ID** (UID) của root
  - Mỗi một user được tạo ra trên hệ thống đều phải có một số nhận dạng gọi là UID
  - Linux sẽ quản lý các tài khoản người dùng thông qua UID, còn Username chỉ là tên gọi thân thiện, giúp con người dễ dàng phân biệt các user.
  - Tài khoản root được Linux tự động tạo ra và mặc định, root luôn có UID=0
    - Có thể thay đổi UID của root nhưng điều này không hề được khuyến khích vì nó ảnh hưởng tới an ninh, ổn định của hệ thống
  - Linux cho phép nhiều user có cùng UID và các user này sẽ có quyền hạn ngang nhau
    - Xem UID của một user, sử dụng lệnh: id username

Tài khoản root và an ninh hệ thống

- **Quyền** của root
  - root có quyền lực lớn nhất và tuyệt đối, nó có quyền truy cập tới bất kỳ file nào và thực thi được mọi câu lệnh
    - Ngay cả việc chỉnh sửa các module của hệ điều hành và biên dịch lại Linux kernel – một điều không thể trên hệ thống Windows
  - root cũng có quyền cấp phát và thu hồi các quyền hạn truy cập file cho các user khác, bao gồm các file mặc định chỉ dành riêng cho root.

Tài khoản root và an ninh hệ thống

- **Hệ thống phân quyền**
  - Hệ thống phân quyền trong Linux mặc định cấm các normal user truy cập, thay đổi cấu hình các khu vực trọng yếu trên hệ thống và dữ liệu cá nhân thuộc về các user khác.
    - user chỉ có thể đọc file mà không có quyền ghi bất cứ gì vào root directory (/), ngoài ra user có tự do quyền hạn với home direcroty của mình.
  - Tránh lạm dụng đặc quyền root bởi thật dễ dàng để phá hủy hệ thống với quyền hạn root
    - rm -rf /: Ngay khi thực thi lệnh trên với quyền root và khởi động lại máy, toàn bộ dữ liệu trong phân vùng dành cho thư mục gốc (/) bị xóa bỏ... Bạn đã tự sát chính mình!
    - Tất cả các tiến trình (process) do root khởi động sẽ được cấp quyền hạn root

Tài khoản root và an ninh hệ thống

- **Mượn quyền root**
  - su -: nhấn Enter và nhập mật khẩu root
    - Không cần logout khỏi user hiện tại
    - Chuyển tạm sang "ngồi trên ghế" của root cho tới khi nhấn Ctrl+D hoặc gõ exit để nhảy khỏi "chiếc ghế quyền uy" này và trở lại là "công dân nghèo".
  - sudo command: nhập mật khẩu của user đang chạy lệnh sudo
    - File cấu hình của sudo là /etc/sudoers bạn có thể làm rất nhiều thứ như:
      - Cho phép user nào được quyền sudo.
      - Quy định các lệnh sudo nào mà user có thể chạy.
      - Ấn định lượng thời gian mà lệnh sudo còn hiệu lực.

Tài khoản root và an ninh hệ thống

- **Mượn quyền root**
  - **sudo** là con dao 2 lưỡi**:**
    - "Lưỡi cùn" (vô hại): normal user sẽ chỉ được quyền chạy 1 số lệnh quản trị do bạn ấn định trước trong file /etc/sudoers. Đồng thời, mật khẩu của root được giữ bí mật.
    - "Lưỡi sắc" (nguy cơ): nếu bạn kiểm soát vấn đề ủy quyền thông qua sudo không chặt chẽ thì normal user dễ dàng chiếm quyền điều khiển hệ thống với đặc quyền root.
  - sudo su –: thực hiện quyền root mà không cần đăng nhập root

2. Quản lý người dùng

Quản lý người dùng để làm gì?

- Khi được giao **quản lý máy chủ Linux**, người quản trị cần:
  - Biết cách thêm, chỉnh sửa, tạm dừng hoặc xóa tài khoản người dùng và cấp cho người dùng quyền cần thiết đối với tệp, thư mục và các tài nguyên hệ thống khác để thực hiện nhiệm vụ được giao.

Kiểm tra danh sách người dùng

- **Danh sách user** của Linux được lưu trong file **/etc/passwd**
  - Để xem danh sách user này sử dụng lệnh cat /etc/passwd
  - Thông tin của 1 user trong file /etc/passwd

```
[username]:[x]:[UID]:[GID]:[Comment]:[Home directory]:[Default shell]
```

  - Hiển thị thông tin 1 user bất kì bằng lệnh: id username

Tạo mới một người dùng

- Để thêm một user mới, chúng ta sử dụng lệnh **adduser** hoặc **useradd** trên Linux với quyền sudo
  - useradd là native command
  - adduser là perl script, sử dụng useradd như một back-end
- Cú pháp: sudo adduser username
- Tạo nhiều user (sử dụng bash script, chi tiết ở phần sau)

```
1.  #!/bin/bash
2.  for i in $( cat users.txt ); do
3.  useradd $i
4.  echo "user $i added successfully!"
5.  echo $i:$i"123" | chpasswd
6.  echo "Password for user $i changed successfully"
7.  done
```

Thêm/Xóa người dùng vào/khỏi group

- Một người dùng được thêm mới, mặc định thuộc vào group trùng tên username
- Để add 1 user vào group sử dụng command usermod:
  - sudo usermod -a -G root username
- Thêm user vào nhiều group:
  - sudo usermod -a -G group1,group2 username
- Thêm nhiều user vào 1 group:
  - sudo gpasswd -M user1,user2,user3 groupname
- Xóa user khỏi 1 group:
  - sudo gpasswd -d username groupname

Một số tùy chọn thay đổi thông tin người dùng

- Thay đổi mật khẩu: sudo passwd username
  - Nếu không có tham số username, sẽ thay đổi mật khẩu của user hiện tại
- Thay đổi thư mục người dùng: sudo usermod --home /home/user10/ username
- Khóa một user: sudo usermod --lock username
- Mở khóa một user: sudo usermod --unlock username
- Xóa một user: sudo userdel username

3. Quản lý nhóm

Kiểm tra danh sách nhóm

- Thông tin của 1 group trong file /etc/group
  - Để hiển thị danh sách group chúng ta sử dụng command cat /etc/group
- Thông tin 1 group trong file /etc/group như sau:

```
[Group name]:[Group password]:[GID]:[Group members]
```

Tạo mới một nhóm

- Tạo một nhóm:
  - sudo groupadd groupname
- Tạo nhiều nhóm:
  - sudo groupadd group1, group2, group3

Một số tùy chọn với nhóm

- Liệt kê danh sách người dùng trong một nhóm:
  - sudo groups
  - sudo groups username
- Xóa một nhóm:
  - sudo groupdel groupname