

BÀI THỰC HÀNH 4

SỬ DỤNG TERMINAL ĐỂ THỰC HIỆN CÁC THAO TÁC

1. Quản lý user, group

- File `/etc/passwd` chứa nội dung gì? Dùng lệnh `wc` để xem nội dung tập tin `/etc/passwd`. Cho biết số lượng user đang có trên hệ thống? User nào đang có `UID=100`?

Gợi ý: sử dụng lệnh `wc` để xem số dòng. Sử dụng `grep` để lọc dữ liệu

```
wc /etc/passwd
```

```
grep "root" /etc/passwd
```

```
grep "nologin" /etc/passwd | wc -l
```

```
cat /etc/passwd | grep root
```

- Tạo group có tên: **admin, nhanvien**
- Tạo user **nv01, nv02** thuộc group **nhanvien**. Password tùy ý.
- Tạo user **it01, it02** thuộc group **admin**. Password tùy ý.
- Xem lại thông tin của các user vừa tạo đã hoàn thành hay chưa: xem `UID, GID`. Kiểm tra `UID` và `GID` có giống nhau hay không?
- Cho biết có bao nhiêu user có thể login vào hệ thống?
- Xem nội dung tập tin `/etc/group`? Cho biết số lượng group đang có trên hệ thống?
- Sử dụng lệnh **id** để xem thông tin của user: `UID, GID, tên group` của user. Một vài tham số trong lệnh `id`: `-g, -u, -gn...`

- Cho biết có bao nhiêu người dùng có **UID=0** và **GID=0**? Lưu thông tin này vào file group.txt
Gợi ý: sử dụng `grep 0:0 /etc/passwd`
- Reset password của nv01 thành "Xacnhan246"
- Chuyển user it01 qua group nhanvien, và cho user này hoạt động đến ngày 30/11/2023
- Khóa user nv02, không cho user này hoạt động trên hệ thống.
- Xóa user nv02. Kiểm tra xem profile của user này còn trên hệ thống hay không?

2. Quản lý user với quyền admin (quyền sudo)

- **Super user:** là người dùng quản trị của hệ thống, là user root. User này được bởi hệ thống. UID có giá trị 0.
- **System user:** là người dùng được tạo ra khi ta cài đặt chương trình, dịch vụ hệ thống. UID trong khoảng 1-999
- **Regular user:** là user thường, những user này chỉ được quyền login vào hệ thống và sử dụng tài nguyên. UID có giá trị ≥ 1000 .

Để cấp quyền sudo cho user có thể sử dụng các lệnh sau:

- Sử dụng lệnh `sudo usermod -aG sudo "username"`
- Sử dụng lệnh `sudo gpasswd -a "username" sudo`
- Sử dụng lệnh `adduser "username" --group sudo`

Tạo một user có tên **quantrivien**, pass: **qtv7135@** và cấp cho user này có quyền sudo.

- Sử dụng lệnh `useradd....`
- Sử dụng lệnh `usermod -aG sudo quantrivien`

- Sử dụng lệnh `grep sudo /etc/group` để xem user nào thuộc group sudo.

Cấp quyền cho user **it02** có quyền tương tự như user **root**.

Gợi ý: Có thể sử dụng 2 cách: chuyển hẳn user it02 sang group root hoặc thêm it02 vào group root (user it02 có thể thuộc 2 group)

Dùng lệnh `usermod -aG "groupname" "username"`

3. Quản lý user root

- Trong hệ thống Linux, user root được enable hay disable?
- Enable user root

- Cách 1: dùng lệnh **`sudo passwd root`**
 - Sau đó nhập password cho user root
- Cách 2: mở file `/etc/passwd`
 - Đổi **`/sbin/nologin`** thành **`/bin/bash`**

- Disable user root (các user khác cũng thực hiện tương tự)

- Cách 1: dùng lệnh **`sudo passwd -dl root`**

Sau khi thực hiện cách 1, đăng nhập lại bằng user root xem có thành công hay không?

Mở file `/etc/passwd` xem dòng chứa user root có gì thay đổi không? **Cho nhận xét.**

- Cách 2: Sửa file `/etc/passwd`
 - Đổi **`/bin/bash`** thành **`/sbin/nologin`**

- Cách 3: Dùng lệnh **`usermod -L root`**

- Thực hiện enable/disable bằng các cách khác nhau như hướng dẫn bên trên.

4. Một vài lệnh liên quan đến quản lý user, group

- Sử dụng lệnh **group "username"** để xem user đang thuộc những group nào.
- Hiển thị tất cả tên user có trong hệ thống: `cat /etc/passwd | cut -d: -f1`
- Cho biết tên những user có thể login được trong hệ thống? Sau đó lưu danh sách này vào file `nguoidung.txt`
- Hiển thị tên của tất cả group có trong hệ thống? Sau đó lưu danh sách này vào file `group.txt`

5. Thực hiện script

- Viết script tạo user và pass cho user. Tên user và pass được nhập từ bàn phím.
- Viết script tạo user và pass. Tên user và pass được truyền vào từ các đối số. Kiểm tra nếu user này tồn tại thì báo lỗi.