THỰC HÀNH HỆ ĐIỀU HÀNH MÃ NGUỒN MỞ

TUẦN 4

QUẢN LÝ NGƯỜI DÙNG

Hãy thực hiện các yêu cầu sau trên hệ điều hành mã nguồn mở

1. Xem nội dung tập tin **/etc/passwd** và cho biết có bao nhiêu người dùng do hệ thống tạo ra? (đếm số dòng dùng lệnh wc /etc/passwd hoặc sử dụng **vi**). Người dùng nào có **UID = 100**. (dùng lệnh grep để tìm kiếm hoặc sử dụng **vi**)
2. Cho biết có bao nhiêu người dùng có **UID=0, GID=0**. Ghi nhận danh sách những người dùng này vào tập tin **/baitap/dsuser**. (Sử dụng **grep** để tìm kiếm và sử dụng **vi** để ghi nhận) #grep "0:0" /etc/passwd
3. Xem nội dung tập tin **/etc/group** và cho biết có bao nhiêu nhóm do hệ thống tạo ra. (sử dụng **vi** rồi hiển thị số dòng)
4. Tạo các nhóm sau: **hocvien, admin, user**.

   #useradd –c"Nguyen van a" -d /home/nva -m -g hocvien nva

   a. Trong nhóm **hocvien** tạo các người dùng:

      i. **hv1** có mật khẩu 123456

      ii. **hv2** có mật khẩu 123456

      iii. **hv3** có mật khẩu 123456

   b. Trong nhóm **admin** tạo các người dùng:

      i. **admin1** có mật khẩu 123456

      ii. **admin2** có mật khẩu 123456

      iii. **admin3** có mật khẩu 123456

   c. Trong nhóm **user** tạo các người dung:

      i. **user1** có mật khẩu 123456

      ii. **user2** có mật khẩu 123456

5. Xem UID, GID của các người dùng vừa tạo ra

6. Cấp cho người dùng **admin1** và **admin2** có quyền quản trị hệ thống như người dùng **root** (Đặt UID=0 trong tập tin **/etc/passwd**)
7. Hủy người dùng **hv3** trong nhóm **hocvien (**kiểm tra lại trong **/etc/passwd)**
8. Chỉnh sửa thông tin trong phần mô tả của người dùng **admin1** và **admin2** là "**Nguoi dung quan tri hệ thong**" để phân biệt với những người dùng khác trong hệ thống (usermod -c)
9. Chuyển người dùng **user1** trong nhóm user sang nhóm **hocvien**
10. Khóa hai user **user1** và **user2**, sau đó kiểm tra bằng cách logout
11. Mở khóa cho **user1**
12. Xóa **user2** khỏi hệ thống
13. Chép file /etc/passwd sang file /data/dsuser (cp /etc/passwd /data/dsuser)
14. Cấp quyền hạn cho tập tin /data/dsuser như sau: chủ sở hữu có quyền đọc(4), ghi(2); nhóm sở hữu có quyền đọc; những người khác không có quyền truy cập(0).

    #chmod u+rw g+r o-rw dsuser

    #chmod 640 /data/dsuser
15. Cấp quyền hạn cho thư mục /baitap như sau: người sở hữu có quyền đọc, ghi, thực thi (7); nhóm sở hữu có quyền đọc(4); những người khác không có quyền truy cập.

    #chmod 740 /baitap
16. Tạo quyền hạn mặc định cho tập tin sao cho: người sở hữu có quyền đọc, ghi (6); nhóm sở hữu có quyền đọc (4); những người khác không có quyền (0) (**umask 026**). Thử tạo tập tin, thư mục và so sánh quyền hạn mặc định với những tập tin và thư mục trước khi đặt lại quyền hạn mặc định.
17. Thay đổi chủ sở hữu và nhóm sở hữu của tập tin **/data/dsuser** thành người dùng **hv1** và nhóm **hocvien**

    #chown hv1:hocvien /data/dsuser

Hãy thực hiện các yêu cầu dưới đây, và cố gắng giải thích theo yêu cầu:

Quản trị tài khoản

B1. Thực hiện, giải thích câu lệnh và kết quả của từng lệnh dưới đây. Sau khi thực hiện mỗi lệnh, kiểm tra nội dung của các tập tin /etc/passwd, /etc/shadow, /etc/group và thư mục /home xem có những thay đổi gì?

useradd UserA

useradd 12usera

useradd usera$

useradd -u 0 -o useradmin

useradd -G groupa,groupb,groupc userb

useradd -G root,apache userc

useradd -g groupc userd

B2. Thực hiện và giải thích ý nghĩa câu lệnh dưới đây, sau đó khảo sát tập tin /etc/group xem có những thay đổi gì?

groupadd *groupa* && groupadd *groupb* && groupadd -g 0 -o *groupc*

B3. Thực hiện lại bài B1. Sau đó xem lại thông tin tài khoản bằng lệnh **id** *tentaikhoan*.

B4. Giải thích kết quả khi thực hiện thủ tục: chuyển sang tty3 và đăng nhập với quyền tài khoản userc.

B5. Sử dụng lệnh passwd để gán mật mã truy nhập cho các tài khoản useradmin, userb, userc. Khảo sát tập tin /etc/passwd và /etc/shadow xem có những thay đổi gì?

B6. Thực hiện các thủ tục sau, tìm sự khác nhau của kết quả và giải thích:

- Đăng nhập với quyền tài khoản useradmin (tại tty4)
- Đăng nhập với quyền tài khoản userb (tại tty5)
- Đăng nhập với quyền tài khoản userc (tại tty6)

B7. Tạo tài khoản có tên **usera$**. Đánh giá kết quả.
Tạo tài khoản **usera**, mở tập tin /etc/passwd và /etc/shadow sửa tên **usera** thành **user$**. Sau đó gán mật mã cho **usera$**. Đánh giá kết quả.

B8. Thực hiện lần lượt:

- Khóa tài khoản userb. Tìm sự thay đổi trong /etc/shadow
- Mở khóa tài khoản userb. Tìm sự thay đổi trong /etc/shadow
- Xóa mật mã tài khoản userb. Tìm sự thay đổi trong /etc/shadow

B9. Thực hiện sửa nội dung trong /etc/shadow, (và đăng nhập lại để kiểm chứng) để

- Khóa tài khoản userc.
- Mở khóa tài khoản userc.
- Xóa mật mã tài khoản userc.

B10. Thực hiện thay đổi các thông tin (UID, GID, home dir, shell) tài khoản userd bằng lệnh usermod. Mở các tập tin /etc/passwd, /etc/shadow, /etc/group, và đăng nhập lại với quyền userd (nếu cần) để kiểm chứng.

B11. Thực hiện thay đổi nội dung tập tin /etc/login.defs và /etc/default/useradd, sau đó tạo tài khoản có tên userx. So sánh thông tin tài khoản userx với tài khoản usera$.

Quyền tập tin

B1. Tạo thư mục /baitap và tập tin /baitap/abc.txt (nội dung bất kỳ). Xác định nhóm, chủ nhân và quyền của thư mục, tập tin vừa tạo?

B2. Xem quyền mặc định khi tạo tập tin bằng lệnh umask -S. Thực hiện thay đổi quyền mặc định khi tạo tập tin, sau đó tạo tập tin abc1.txt và thư mục tm1 (trong /baitap) để kiểm chứng.
Cho nhận xét về quyền của tập tin mới tạo khi quyền mặc định có quyền x.

B3. Dùng lệnh chmod để thay đổi lại quyền cho các tập tin trong /baitap, sử dụng cả phương pháp tượng trưng và tuyệt đối (dùng lệnh ls -l để kiểm chứng kết quả)

B4. Thực hiện tuần tự và giải thích

- **chmod *700 /baitap/abc.txt***. Đăng nhập với quyền userb, và mở xem tập tin /baitap/abc.txt. Cho biết kết quả?
- Đổi chủ nhân tập tin abc.txt thành userb. Đăng nhập với quyền userb, và truy xuất tập tin /baitap/abc.txt. Cho biết kết quả?
- Đăng nhập với quyền userd, và truy xuất tập tin /baitap/abc.txt. Cho biết kết quả?
- Thực hiện lệnh **chmod *755 /baitap/abc.txt* && chown :*groupc /baitap/abc.txt***. Đăng nhập với quyền userd, và truy xuất tập tin /baitap/abc.txt. Cho biết kết quả?

B5. Thực hiện và giải thích

- Lệnh **mkdir /baitap2 ; chmod 777 /baitap2**
- Đăng nhập với quyền userb, tạo một tập tin có tên “tap tin cua b.txt” trong /baitap2.
- Đăng nhập với quyền userc, thực hiện sửa, xóa tập tin do userb tạo. Cho biết kết quả.
- Thực hiện lệnh **chmod 1777 /baitap2 ; ls -l /baitap2**. Kết quả?

- Đăng nhập với quyền userb, tạo một tập tin có tên “tap tin 2 cua b.txt” trong /baitap2.
- Đăng nhập với quyền userc, thực hiện sửa, xóa tập tin do userb tạo. Cho biết kết quả.

B6. Tạo một symbolic link cho một tập tin bất kỳ. Tiến hành thay đổi quyền của symbolic link mới tạo này. Cho biết kết quả.

Hãy thực hiện các yêu cầu dưới đây:

Một công ty gồm các phòng ban sau: kinh doanh (sale), nhân sự(HR) và web và những user AAA và BBB thuộc phòng kinh doanh, CCC và DDD thuộc phòng nhân sự, EEE và FFF thuộc bộ phận web. Ngoài ra công ty còn một nhóm quản lý chung(manager) các việc trong công ty do user GGG chịu trách nhiệm.

1. Đảm bảo rằng tất cả các user được tạo ra trong công ty đều có thể tạo ra files có quyền ghi trên group.
2. Hãy tạo 7 user trên và đặt password tương ứng cho từng user.
3. Tạo các group trên với GID tương ứng:
    a. sale: GID=200
    b. HR: GID=201
    c. web: GID=202
4. Tại sao ta phải thiết lập GID cho các group trên mà không dùng GID mặc định của hệ thống.
5. Đặt user AAA và BBB vào group sale, CCC và DDD vào group HR, EEE và FFF vào group web và GGG vào group manager và tất cả các group còn lại.
6. Thêm CCC vào group web (nghĩa là CCC sẽ thuộc 2 group HR và web).
7. Kiểm tra xem thông tin về GID của các user trên có chính xác hay chưa?
8. Tạo thư mục depts ở thư mục gốc của bạn, đồng thời tạo 3 thư mục con trong depts là: sale, hr và web
9. Kiểm tra quyền trên các thư mục vừa tạo và thay đổi quyền tương ứng với các group vừa tạo.
10. Thiết lập quyền trên thư mục depts sao cho mọi người trong công ty có thể đọc thông tin trên đó nhưng không thể chỉnh sửa.
11. Thiết lập quyền trên các thư mục con sale, hr và web sao cho những user trong các group đó có toàn quyền (rwx) nhưng tất cả những user khác đều không có bất cứ quyền gì trên thư mục đó.
12. Hãy đảm bảo rằng tất cả các file được tạo ra trong các thư mục con đều thuộc quyền sở hữu của group tương ứng.