Phần 8: Quản trị người dùng và nhóm người dùng.

Thiết lập quyền tệp trong Linux là nhiệm vụ cơ bản để quản lý quyền truy cập vào tệp và thư mục. Quyền tệp phù hợp đảm bảo rằng chỉ những người dùng được ủy quyền mới có thể đọc, ghi hoặc thực thi tệp, tăng cường bảo mật và chức năng của hệ thống.

I. Kiểm tra quyền của tập tin

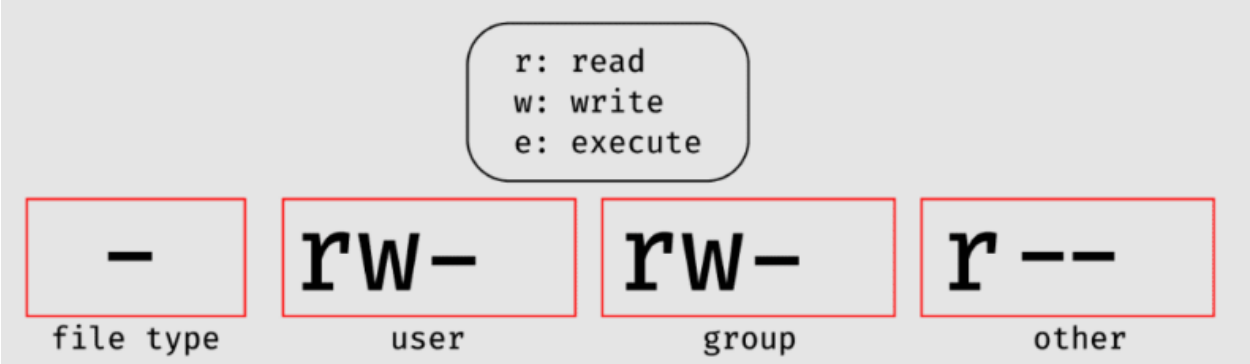
Dùng : **ls-l**

Có rất nhiều thông tin trong những dòng đó.

1. Ký tự đầu tiên = '-' , có nghĩa là đó là một tệp **'d'** , có nghĩa là đó là một thư mục.
2. Chín ký tự tiếp theo = (rw-r–r–) hiển thị bảo mật
3. Cột tiếp theo hiển thị chủ sở hữu của tệp. (Ở đây là `root`)
4. Cột tiếp theo hiển thị nhóm chủ sở hữu của tệp. (Ở đây là `root` có quyền truy cập đặc biệt vào các tệp này)
5. Cột tiếp theo hiển thị kích thước của tệp tính theo byte.
6. Cột tiếp theo hiển thị ngày và giờ tệp được sửa đổi lần cuối.
7. Cột cuối cùng = File_name hoặc Directory_name. (Ví dụ: prac, snap, test, example)

II. Có ba nhóm quyền nào trong Linux

1. **Chủ sở hữu:** Những quyền này chỉ áp dụng cho những cá nhân sở hữu tệp hoặc thư mục.
2. **Nhóm:** Quyền có thể được chỉ định cho một nhóm người dùng cụ thể, chỉ ảnh hưởng đến những người trong nhóm đó.
3. **Tất cả người dùng:** Các quyền này áp dụng chung cho tất cả người dùng trên hệ thống, mang lại rủi ro bảo mật cao nhất. Việc chỉ định quyền cho tất cả người dùng phải được thực hiện thận trọng để ngăn ngừa các lỗ hổng bảo mật tiềm ẩn.



- Nếu là -, đó là một file thường.
- Nếu là d, đó là một thư mục.
- Nếu là l, đó là symbolic link.
- Nếu là p, đó là đường ống (pipe).
- Nếu là c, đó là character device.
- Nếu là b, đó là block device.
- Nếu là s, đó là socket.

III. Có ba loại quyền truy cập tệp

Bức thư	Sự định nghĩa
r	quyền đọc file/folder. Dùng cho lệnh ls, cat,..
w	quyền ghi/sửa nội dung file/folder. Dùng cho các lệnh vi, nano,…

Bức thư	Sự định nghĩa
x	“quyền thực thi (truy cập) thư mục.. Dùng cho các lệnh cd.

Biểu tượng: Tùy chọn `+`, `-` và `=` trong Quyền tệp Linux

Người điều hành	Sự định nghĩa
+	Thêm quyền
-	Xóa quyền
=	Đặt quyền cho các giá trị đã chỉ định

Người dùng, nhóm và những người khác Tùy chọn trong Quyền tệp Linux

ref	class	Sự miêu tả
u	user	Quyền của người dùng chỉ áp dụng cho chủ sở hữu của tệp hoặc thư mục, chúng sẽ không ảnh hưởng đến hành động của những người dùng khác.
g	group	Quyền của nhóm chỉ áp dụng cho nhóm được chỉ định cho tệp hoặc thư mục, chúng sẽ không ảnh hưởng đến hành động của những người dùng khác.
o	others	Các quyền khác áp dụng cho tất cả người dùng khác trong hệ thống, đây là nhóm quyền mà bạn muốn theo dõi nhất.
a	all	Cả ba (chủ sở hữu, nhóm, những người khác)

Các lệnh cơ bản quản lý User và Group

Mô tả	Cú pháp
Thông tin user	**sudo less /etc/passwd** Mỗi dòng thường chứa những trường thông tin như dưới đây, ngăn cách bởi dấu hai chấm: Usename Mật khẩu được mã hóa (ký tự x cho biết mật khẩu được lưu trong file /etc/shadow) User ID (UID) Group ID của user (GID) Tên đầy đủ của user Home directory của user Login shell (mặc định là /bin/bash)

Tạo User	**adduser <username>**
	useradd [option] [option].. [option] <username> ***options:*** -c Thông tin user -d Thư mục cá nhân ở thư mục home. -m đồng thời tạo thư mục ở home -g nhóm người dùng
Chuyển đổi user	**sudo su [user-name]**
Tạo mật khẩu	**passwd <username>**
Thông tin người dùng và mật khẩu mã hóa.	**sudo cat /etc/shadow** Chuỗi hiện thị: [username]:[password]:[date of last password change]:[minimum password age]:[maximum password age]:[warning period]:[inactivity period]:[expiration date]:[unused] 2.1 Username (Tên người dùng) Mọi thứ theo sau trong chuỗi được liên kết với tên người dùng này. 2.2 Password (Mật khẩu) Trường mật khẩu bao gồm ba trường bổ sung, được phân định bằng ký hiệu đô la: idsalt$hash. id: Điều này xác định thuật toán mã hóa được sử dụng để mã hóa mật khẩu của bạn. Giá trị có thể là 1 (MD5), 2a (Blowfish), 2y (Eksblowfish), 5 (SHA-256) hoặc 6 (SHA-512). salt: Đây là salt được sử dụng để mã hóa và xác thực mật khẩu. hash: Đây là mật khẩu của người dùng khi nó xuất hiện sau khi băm. Tệp shadow lưu giữ phiên bản đã băm của mật khẩu để hệ thống có thể kiểm tra bất kỳ nỗ lực nào để nhập mật khẩu của bạn. *salt: dữ liệu ngẫu nhiên được sử dụng làm đầu vào bổ sung cho hàm một chiều có chức năng băm dữ liệu, mật khẩu hoặc cụm mật khẩu.Đôi khi trường mật khẩu chỉ chứa dấu hoa thị (*) hoặc dấu chấm than (!). Điều đó có nghĩa là hệ thống đã vô hiệu hóa tài khoản của người dùng hoặc người dùng phải xác thực thông qua các phương tiện khác ngoài mật khẩu. Điều này thường xảy ra đối với các quy trình hệ thống (còn được gọi là người dùng giả – pseudo-users) mà bạn cũng có thể tìm thấy trong tệp shadow. 2.3 Date of last password change (Ngày thay đổi mật khẩu cuối cùng) Tại đây, bạn sẽ tìm thấy lần cuối cùng người dùng này thay đổi mật khẩu của họ. Lưu ý rằng hệ thống hiển thị ngày ở định dạng thời gian Unix. 2.4 Minimum password age (Tuổi mật khẩu tối thiểu) Bạn sẽ tìm thấy ở đây số ngày mà người dùng phải đợi sau khi thay đổi mật khẩu của họ trước khi thay đổi lại. Nếu mức tối thiểu không được đặt, giá trị ở đây sẽ là 0. 2.5 Maximum password age (Tuổi mật khẩu tối đa) Điều này xác định thời gian người dùng có thể sử dụng mà không cần thay đổi mật khẩu của họ. Thường xuyên thay đổi mật khẩu của bạn có những lợi ích của nó , nhưng theo mặc định, giá trị sẽ được đặt ở mức 99,999 ngày – gần 275 năm. 2.6 Warning period (Thời gian cảnh báo) Trường này xác định số ngày trước khi mật khẩu đạt đến tuổi tối đa, trong đó người dùng sẽ nhận được lời nhắc thay đổi mật khẩu của họ. 2.7 Inactivity period (Thời gian không hoạt động) Đây là số ngày có thể trôi qua sau khi mật khẩu của người dùng đạt đến tuổi tối đa trước khi hệ thống vô hiệu hóa tài khoản. Hãy coi đây là “thời gian gia hạn” trong đó người dùng có cơ hội thứ hai để thay đổi mật khẩu của họ, ngay cả khi mật khẩu đó đã hết hạn về mặt kỹ thuật.

	2.8 Expiration date (Ngày hết hạn) Ngày này là ngày kết thúc thời gian không hoạt động khi hệ thống sẽ tự động vô hiệu hóa tài khoản của người dùng. Sau khi bị vô hiệu hóa, người dùng sẽ không thể đăng nhập cho đến khi quản trị viên bật lại. Trường này sẽ trống nếu không được đặt và nếu được đặt, ngày sẽ xuất hiện theo thời gian của kỷ nguyên. 2.9 Unuse (Không sử dụng) Trường này hiện không phục vụ mục đích nào và được dành để sử dụng trong tương lai.
Sửa thông tin User	**#usermod [option] <username>** ***options:*** -G: Thêm user vào group -c : thay đổi thông tin người dùng -e : thiết lập ngày hết hạn cho người dùng -L : Khóa tài khoản -U : mở khóa tài khoản -s : thay đổi shell script cho user usermod
Xóa người dùng	**#userdel [option] <username>** ***options:*** -m : dùng để xóa user -f Buộc xóa tài khoản người dùng, bao gồm thư mục gốc và thư mục email, ngay cả khi người dùng đã đăng nhập. -r Xóa thư mục gốc của người dùng cùng với tài khoản. Hữu ích cho việc dọn dẹp hoàn toàn. -h Hiển thị thông báo trợ giúp và thoát, cung cấp thông tin về cú pháp lệnh và các tùy chọn có sẵn. -R Áp dụng các thay đổi trong CHROOT_DIR đã chỉ định, hữu ích cho các hoạt động xóa người dùng trong môi trường chroot. -Z Xóa ánh xạ người dùng SELinux cho thông tin đăng nhập của người dùng, áp dụng trong các hệ thống hỗ trợ SELinux
Khóa người dùng	**#passwd -l <username>**
Mở khóa tài khoản	**#passwd -u <username>**
Thông tin nhóm	**sudo /etc/group** 1 - Tên group 2 - Mật khẩu group đã được mã hóa (vì có file /etc/gshadow) nên mặc định ở đây là x 3 - Mã nhóm (gid) 4 - Danh sách các user nằm trong nhóm
Tạo nhóm	**#groupadd <groupname>**
Tạo mật khẩu cho group	**# gpasswd <groupname>**
Sửa lại thông tin về group	**# groupmod [options] <groupname>** *options* g [gid] : sửa lại mã nhóm (gid) n [group_name] : sửa lại tên group
Xóa nhóm	**#groupdel <groupname>**

Để thay đổi chủ sở hữu file và nhóm sở hữu ta dùng lệnh "chown"

chown [OPTIONS] USER[:GROUP] FILE(s)

USER là tên người dùng hoặc UID của chủ sở hữu mới. GROUP là tên nhóm hoặc GID nhóm mới. FILE là tên của một hoặc nhiều file, thư mục hoặc symbolic link, nó chính là file đích cần xử lý.

- Nếu chỉ một người dùng được chỉ định (USER) thì người dùng được chỉ định đó sẽ trở thành chủ sở hữu (*ownership*), nhóm sở hữu sẽ không có gì thay đổi.
- Nếu nhập nhiều người dùng vào mục USER và được ngăn cách bởi dấu hai chấm :, và GROUP không được nhập thì người dùng trở thành chủ sở hữu, còn group đó thành nhóm sở hữu của file.
- Nếu cả USER và GROUP đều được chỉ định thì quyền sở hữu file sẽ thuộc về người dùng và nhóm sở hữu cũng chính là nhóm mà bạn đã chỉ định.
- Nếu bỏ qua USER và chỉ nhập GROUP thôi thì quyền sở hữu nhóm đổi thành group mà bạn chỉ định.
- Nếu chỉ có dấu hai chấm đưa ra, tức là không nhập USER và GROUP thì không có thay đổi nào được thực hiện.
- *options*
- -R : Để duyệt qua tất cả các file nằm trong một thư mục có nhiều cấp.
- Nếu thư mục có chứa symbolic links thì hãy sử dụng thêm tùy chọn -h.
- **Để thay đổi group mới của file ta có dùng lệnh "chgrp"**

chgrp **[OPTIONS]** [tên group mới] [tên file]

options

- -R : Để duyệt qua tất cả các file nằm trong một thư mục có nhiều cấp.
- Nếu thư mục có chứa symbolic links thì hãy sử dụng thêm tùy chọn -h.

Để có thể thay đổi các quyền của file ta có thể sử dụng lệnh "chmod"

Sử dụng phương pháp tượng trưng

chmod [OPTIONS] [ugoa…][-+=]perms…[,…] FILE...

options

- -R : Để duyệt qua tất cả các file nằm trong một thư mục có nhiều cấp.
- Nếu thư mục có chứa symbolic links thì hãy sử dụng thêm tùy chọn -h.
- Trong đó, nhóm flag [ugoa...] là flag dành cho user, dùng để chỉ định các lớp user nào sẽ thay đổi quyền truy cập file.
  - u: Chủ sở hữu file.
  - g: User thuộc group.
  - o: Mọi user khác.
  - a: Mọi user (tương đương với ugo).Nếu không truyền flag user vào thì mặc định sẽ là a.
  - Nhóm flag thứ hai là flag toán tử ([-+=]), định nghĩa xem lệnh cần xóa, thêm hay đặt quyền truy cập của file:
  - -: Xóa quyền được chỉ định.

- +: Thêm quyền truy cập cho file.
- =: Thay đổi sang một quyền truy cập cụ thể. Nếu không chỉ định quyền nào sau dấu = thì theo mặc định, mọi quyền từ user class sẽ bị xóa.

Phần quyền truy cập (perms...) có thể được thiết lập cụ thể bằng cách sử dụng các ký tự: r, w, x, X, s và t. Ngoài ra ta cũng có thể dùng một ký tự (trong nhóm u, g, o) để copy quyền truy cập từ một user class khác.

Khi thiết lập quyền truy cập cho một hay nhiều user class ([, ...]), hãy sử dụng dấu phẩy (không có khoảng trắng) để phân tách các mode tượng trưng.

Phương pháp số

chmod [OPTIONS] NUMBER FILE...

Biểu diễn số của các quyền đọc, ghi và thực thi file như sau:

- r (read) = 4
- w (write) = 2
- x (execute) = 1
- không có quyền (no permission) = 0

Giá trị số cho quyền của một user class được xác định bằng tổng của các giá trị quyền trong group đó. Để xác định được quyền truy cập một file ở dạng số thì ta có thể tính tổng giá trị của mọi user class.