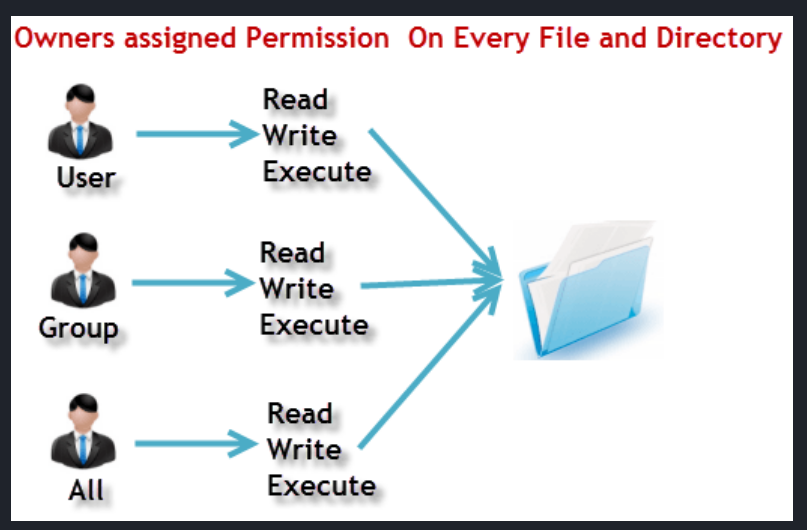
PRO02: Lập trình ứng dụng LINUX

**Lý thuyết:**

**1. Khái niệm user, group, owner của file, folder; các cờ phân quyền đối với file, folder**



**- Khái niệm:**

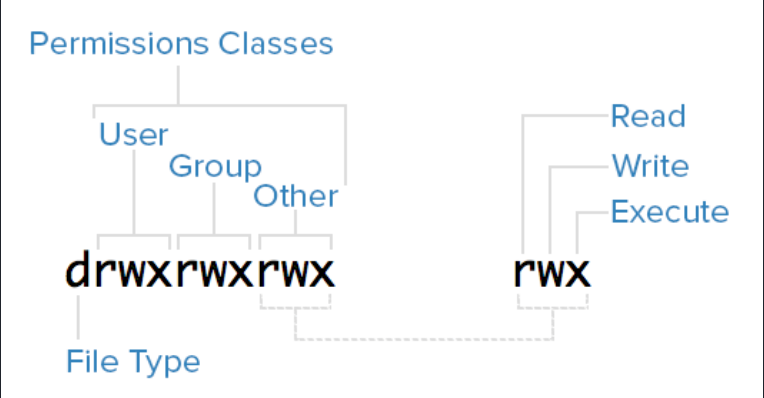
**+ User:** Linux là một hệ thống đa người dùng. Trong Linux, có hai loại người dùng: người dùng hệ thống và người dùng thông thường. Người dùng hệ thống được sử dụng để chạy các tiến trình không tương tác hoặc tiến trình nền trên một hệ thống, trong khi người dùng thông thường được sử dụng để đăng nhập và chạy các tiến trình có tương tác. Tệp /etc/passwd chứa thông tin về các người dùng trong hệ thống, mỗi dòng chứa một thông tin về người dùng.

Trong hệ thống Linux còn tồn tại một loại người dùng khác là siêu người dùng (superuser) hoặc người dùng root, có khả năng ghi đè lên bất kỳ quyền sở hữu và giới hạn quyền tệp nào. Superuser có quyền truy cập bất cứ thứ gì trên máy chủ. Người dùng này được sử dụng để thực hiện các thay đổi trên toàn hệ thống và phải được giữ an toàn.

**+ Group:** Là tập hợp không có hoặc có nhiều người dùng. Người dùng thuộc nhóm mặc định và cũng có thể là thành viên của bất kỳ nhóm nào khác trên máy chủ. Một tệp có thể được sở hữu bởi chính xác duy nhất một nhóm. Mỗi người dùng có thể là thành viên của nhiều nhóm và mỗi nhóm có thể chứa nhiều người dùng.

**+ Owner:** Theo như mặc định trên Linux thì người tạo ra file hay thư mục nào đó thì sẽ trở thành chủ sở hữu của chính nó. Mỗi tệp được sở hữu bởi chính xác một người dùng duy nhất.

**- Các cờ phân quyền đối với file, folder:**



Mỗi loại quyền (chủ sở hữa, nhóm sở hữu và người dùng khác) có thể được gán các quyền cho phép hoặc hạn chế khả năng đọc, ghi hoặc thực thi tệp của họ. Linux đại diện cho các loại quyền này bằng cách sử dụng hai ký hiệu riêng biệt: chữ cái và hệ bát phân.

**+ Read (r):** Quyền đọc đề cập đến khả năng của người dùng để đọc được nội dung của tệp. Đối với một tệp thông thường, quyền đọc cho phép người dùng xem nội dung của tệp còn đối với một thư mục, quyền đọc cho phép người dùng xem tên của tệp trong thư mục (không bao gồm quyền xem các nội dung hay tệp tin trong thư mục đó).

**+ Write (w):** Quyền ghi cho biết khả năng viết hoặc sửa đổi tệp hoặc thư mục của người dùng. Đối với một tệp thông thường, quyền ghi cho phép người dùng sửa đổi và xóa tệp. Đối với một thư mục, quyền ghi cho phép người dùng xóa thư mục, sửa đổi nội dung của nó (tạo, xóa và đổi tên tệp trong đó) và sửa đổi nội dung của tệp mà người dùng có thể đọc.

**+ Execute (x):** Quyền thực thi ảnh hưởng đến khả năng của người dùng trong việc thực thi một tệp hoặc xem nội dung của một thư mục. Đối với một tệp thông thường, quyền thực thi cho phép người dùng thực thi một tệp (người dùng cũng phải có quyền đọc). Như vậy, các quyền thực thi phải được đặt cho các chương trình thực thi và các kịch bản lệnh shell trước khi người dùng có thể chạy chúng. Đối với một thư mục, quyền thực thi cho phép người dùng truy cập hoặc duyệt qua (ví dụ: cd) và truy cập siêu dữ liệu (metadata) về các tệp trong thư mục (thông tin được liệt kê trong ls -l).

Dấu gạch ngang (-) thay cho một trong các ký tự (r, w, x) cho biết rằng quyền tương ứng không có sẵn cho lớp tương ứng. Ví dụ: nếu nhóm bộ ba quyền cho tệp có ký hiệu là r--, thì điều này có nghĩa là tệp là tệp "chỉ đọc" cho nhóm được liên kết tương ứng với tệp.

**2. Khái niệm real user id và effective user id của một process**

**- Real user id:** Đối với một process, Real UserId đơn giản là UserID của người dùng đã khởi động nó. Nó xác định các tệp mà quá trình này có quyền truy cập. Đó là người sở hữu hoạt động.

**- Effective user id:** Thường giống như Real UserID, nhưng đôi khi nó được thay đổi để cho phép người dùng không có đặc quyền truy cập vào các tệp mà chỉ người dùng có đặc quyền như root mới có thể truy cập được. Nó được sử dụng bởi hệ thống máy tính để xác định xem bạn có được làm một nhiệm vụ cụ thể hay không.

**3. Khái niệm cờ setuid và setgid của một file binary**

**- setuid (Set user ID upon execution - thiết đặt ID của người dùng thực thi):** Là một loại đặc quyền file (file permission) đặc biệt, có thể cho phép user tạm có quyền thực thi file bằng chính quyền của người sở hữu (owner) để thay đổi hành vi của file thực thi đó.

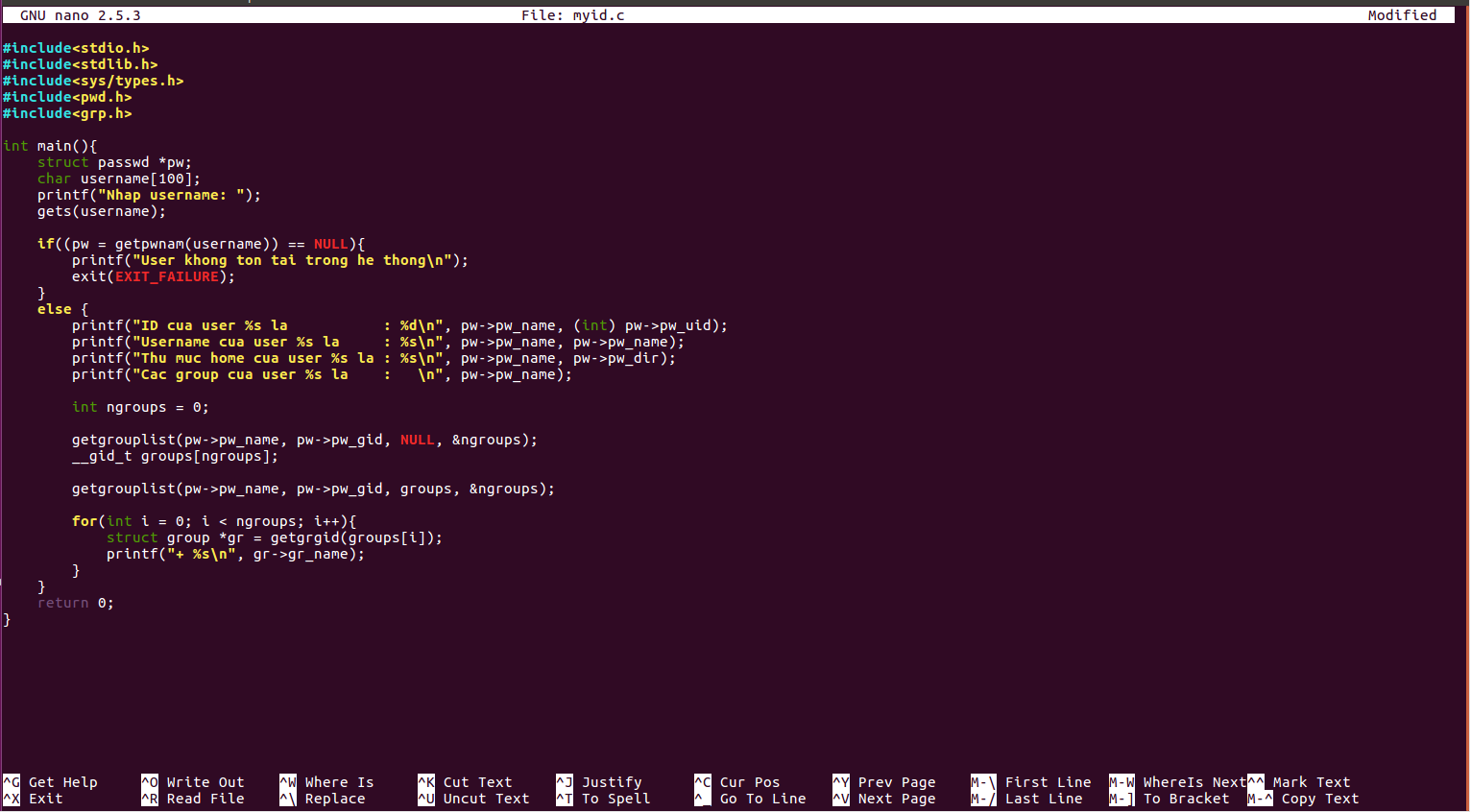
Nói một cách đơn giản hơn: Thông thường một file trong linux khi chạy thì sẽ được kế thừa quyền từ user đang login. SETUID sẽ cấp quyền tạm thời cho user chạy file quyền của user tạo ra file (owner user). Nói một cách khác, user chạy sẽ có UID và GID của người tạo ra file, khi chạy một file hay command.

=> Việc setuid cho file thực thi thì khi chạy file này, nó sẽ sử dụng các quyền của user tạo ra nó (ví dụ user root) thay vì sử dụng các quyền của user hiện tại đang thực thi chương trình (user được đặt quyền setuid).

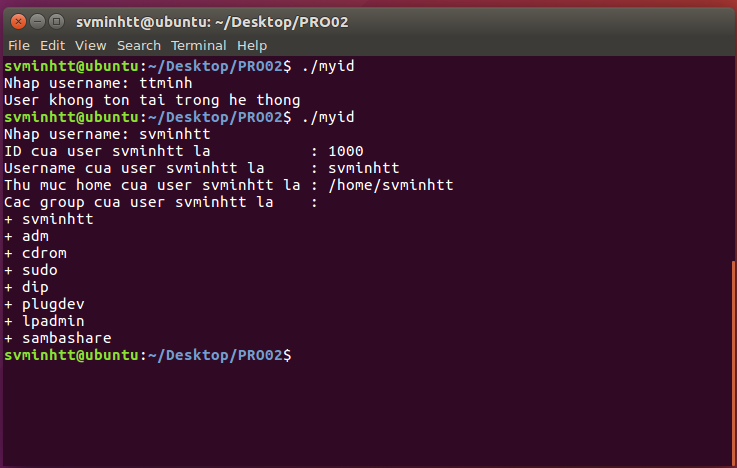
**- setgid (Set group ID upon execution – thiết đặt ID của nhóm thực thi):** Là cờ xác định quyền truy cập trên các hệ thống Linux cho phép người dùng chạy một tệp với quyền của nhóm sở hữu của tệp đó và để thay đổi các hành vi trong thư mục. Thường được sử dụng để cho phép người dùng trên một hệ thống máy tính chạy các chương trình với các đặc quyền tạm thời nâng cao để thực hiện một tác vụ cụ thể.

**Thực hành:**

1. Chương trình tìm kiếm và hiển thị thông tin user theo id:



Kết quả khi chạy chương trình:



2. Chương trình cho phép user đổi mật khẩu mypasswd





Kết quả chạy chương trình

