**Lý thuyết**

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

r là quyền đọc (readable),

w là quyền ghi (writeable),

x là quyền thực thi (executable),

- là denied

Định dạng: (-)(---)(---)(---)

Với: 1 ký tự đầu là file type, '-' là file, 'd' là thư mục

3 ký tự tiếp theo là quyền truy cập file của người sở hữu (owner)

3 ký tự tiếp theo là quyền truy cập file của những người trong group của owner (group)

3 ký tự cuối là quyền truy cập file của những người còn lại không nằm trong group trên (other)

Ex: Quyền truy cập là -rwxrw-r--

* Đây là file với owner có quyền read write execute, group có quyền read write, other có quyền read
* **Khái niệm real user id và effective user id của một process**

Real User ID là UserID của người dùng start tiến trình. Nó xác định những file mà tiến trình của người dùng này có quyền truy cập. (Người dùng có quyền truy cập file nào thì tiến trình do người này tạo ra cũng chỉ truy cập được những file ấy)

Ví dụ: Khi 1 người dùng tạo ra process ‘cat’ (sử dụng câu lệnh cat) thì người dùng này chỉ có thể đọc được những file mà người dùng này có quyền truy cập.

Effective User ID là UserID người dùng được xác định bởi bit setuid trên một file thực thi (thường là owner của process). EUID xác định những file mà tiến trình hiện tại có thể truy cập dựa trên những quyền của UserID này. Nếu EUID = 0 (root) thì tiến trình này có toàn quyền truy cập các file. (EUID có quyền truy cập vào file nào thì tiến trình do người dùng khác tạo ra cũng có thể truy cập vào những file ấy)

Ví dụ: Nếu một file thực thi có cờ ‘s’ và có owner là root thì khi người dùng khác thực thi file (tạo ra tiến trình) thì tiến trình này sẽ truy cập được đến những file mà root có thể truy cập (thực thi file dưới quyền root).

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

SUID (Set User ID): được sử dụng trên các file thực thi (executable files) để cho phép việc thực thi được thực hiện dưới owner của file thay vì thực hiện như user đang login trong hệ thống

Cách thiết lập:

$chmod u+s <filename>: thêm SUID cho file, nếu user có quyền x thì sau khi thực hiện lệnh này sẽ hiện chữ s thường, nếu user không có quyền x thì sau khi thực hiện lệnh này sẽ hiện chữ S hoa

$chmod 4750 <filename>: tương tự như trên

SGID (Set Group ID): cũng tương tự như SUID, được sử dụng trên các file thực thi (excutable files) để cho phép việc thực thi được thực hiện dưới group owner của file thay vì thực hiện như group đang login trong hệ thống

Cách thiết lập:

$chmod g+s <filename>: thêm SGID cho file

$chmod 2750 <filename>: tương tự như trên

Sticky bit: Được dùng cho các thư mục chia sẻ, mục đích là ngăn chặn việc người dùng này xóa file của người dùng kia. Chỉ duy nhất owner file và root mới có quyền rename hay xóa các file, thư mục khi nó được set sticky bit

Cách thiết lập:

$chmod o+t <filename>: thêm sticky bit cho file

$chmod 1750 <filename>: tương tự như trên

**Thực hành**

Sử dụng ngôn ngữ lập trình C/C++ trên môi trường Ubuntu, xây dựng 2 chương trình:

* **Tìm kiếm và hiển thị thông tin user theo id**

*Mô tả: Chương trình tên là myid. Khi chạy ./myid, chương trình hỏi nhập username. Người dùng nhập username, chương trình sẽ tìm user có username tương ứng và hiển thị thông tin id, username, thư mục home, các group của user. Nếu không có user tương ứng thì báo không tìm thấy.*

Source code **myid.c**

* **Chương trình cho phép user đổi mật khẩu mypasswd**

*Mô tả: Khi một user A chạy chương trình ./mypassword. Chương trình sẽ yêu cầu nhập mật khẩu cũ, nếu mật khẩu cũ đúng thì sẽ hỏi mật khẩu mới. Sau đó chương trình sẽ đổi mật khẩu user sang mật khẩu mới.*

Source code **mypassword.c**