Bài 2: Lập trình ứng dụng Linux

1. Lý thuyết
   1. Khái niệm user, group; owner của file, folder; các cờ phân quyền đối với file, folder.
   2. User và group

User chính là người có thể truy cập đến hệ thống. Một User có username và password. Có hai loại User là Super User (hay thường gọi là Root) và Regular User. Mỗi User còn có một mã UID riêng. Mỗi loại User, mỗi User khác nhau có quyền trong hệ thống khác nhau phụ thuộc vào hệ thống đã thiết lập cho họ những quyền gì, Super User đã cấp cho họ những quyền gì.

Group là nhóm người dùng hệ thống. Mỗi nhóm có tên và mã GID riêng. Các User trong Group có thể có những quyền trong hệ thống khác nhau nhưng có một tập hợp quyền chung trong hệ thống đặc trưng cho Group đó.

* 1. Owner của file, folder

Mỗi tập tin (file) có một chủ sở hữu (owner), xác định người dùng (user) sở hữu của file. Mỗi file cũng có một nhóm (group), xác định nhóm người dùng của file. Bất kỳ người dùng hệ thống nào không phải là chủ sở hữu và không thuộc cùng một nhóm đều được xác định là thuộc lớp khác (others).

Mỗi người dùng thuộc 1 trong ba nhóm owner, group, other sẽ được chỉ định các quyền read (đọc – khả năng mở và xem nội dung của file), write (ghi – khả năng mở và sửa đổi nội dung của file) và execute (thực thi – khả năng chạy file như một chương trình thực thi khác nhau.

* 1. Các cờ phân quyền

Mỗi một file hay thư mục trong Linux đều có 3 quyền đọc, ghi, thực thi:

* + - Đọc(r): Nếu là một file thì quyền này cho phép mở file đó lên và đọc. Nếu là một thư mục thì nó cho phép liệt kê danh sách file hay thư mục trong thư mục đó.
    - Ghi(w): Quyền ghi cho phép sửa đổi nội dung của file. Nếu là thư mục thì nó cho phép có thể thêm, xóa và đổi tên các file trong thư mục đó.
    - Thực thi(x): Linux không thể chạy 1 file khi nó không được cấp quyền thực thi. Đối với thư mục thì không thể truy cập(cd) nếu không có quyền thực thi nó.
  1. Khái niệm real user id và effective user id của một process.
     + Real UID: à UserID của người dùng đã khởi động nó. Nó xác định các tệp mà process này có quyền truy cập.
     + Effective UID: Nó 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.
  2. Khái niệm cờ setuid và setgid của một file binary.

setuid (thiết đặt ID của người dùng thực thi) và setgid (thiết đặt ID của nhóm thực thi) là các cờ xác định quyền truy cập trên các hệ thống Linux cho phép người dùng chạy một tệp thực thi với quyền của chủ sở hữu hoặc nhóm sở hữu của tệp đó và để thay đổi các hành vi trong thư mục. Chúng 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. Mặc dù các đặc quyền user id hoặc group id được cung cấp không phải lúc nào cũng được nâng cao, chúng có thể được thiết đặt cụ thể ở mức tối thiểu.

setuid và setgid là cần thiết cho các tác vụ yêu cầu đặc quyền cao hơn so với các người dùng thông thường hiện có, chẳng hạn như thay đổi mật khẩu đăng nhập của họ. Tuy nhiên, một số tác vụ yêu cầu đặc quyền nâng cao có thể không rõ ràng - chẳng hạn như lệnh ping, lệnh này phải gửi và lắng nghe các gói điều khiển trên một giao diện mạng.

Các cờ setuid và setgid có ý nghĩa hoàn toàn khác nhau tùy thuộc vào việc chúng được đặt trên một tệp hay một thư mục.

Các quyền setuid/setguid được sử dụng để thông báo cho hệ thống chạy một tệp thực thi với tư cách là chủ sở hữu với quyền của chủ sở hữu.

Khi các cờ thuộc tính setuid hoặc setgid được thiết đặt trên một file thực thi, thì bất kỳ người dùng nào cũng có thể thực thi tập tin với các đặc quyền của chủ sở hữu (thường là root) hoặc nhóm của tập tin đó, tùy thuộc vào các cờ được đặt. Điều này cho phép nhà thiết kế hệ thống cho phép các chương trình đáng tin cậy được thực thi các tệp tin mà người dùng thông thường sẽ không được phép thực thi. Điều này không phải lúc nào cũng rõ ràng. Ví dụ, lệnh ping có thể cần quyền truy cập vào các đặc quyền mạng mà người dùng bình thường không thể truy cập; do đó nó có thể được gán cờ setuid để đảm bảo rằng người dùng cần ping một hệ thống khác có thể làm như vậy, ngay cả khi tài khoản của họ không có đặc quyền cần thiết để gửi gói.

1. Thực hành

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

chương trình (lưu ý không gọi các chương trình có sẵn như id, passwd,

cần xử lý các thông tin trong file /etc/passwd, /etc/shadow):

Tìm kiếm và hiển thị thông tin user theo id :

(kết quả tại github)

Chương trình cho phép user đổi mật khẩu mypasswd:

(kết quả tại github)

https://github.com/LuluL0g1n/VCSTraining/tree/main/PROG02