Đặc quyền với tệp là cái chính trong mô hình bảo mật của hệ thống Linux. Chúng xác định ai có thể truy cập tệp và thư mục trên hệ thống và như thế nào.

**Cách xem đặc quyền của tệp trên Linux**



Đây là các thành phần của file vimrc:

* File type: -
* Permission: rw-r--r--
* Extended attribute: dot( .)
* User own : root
* Group own: root

tuned có file type là d tương ứng với thư mục.

**Cách đọc đặc quyền của tệp**

Đặc quyền trong file vimrc là:

rw-r--r--

Chia thành 3 nhóm:

* rw-: User
* r-- : Group
* r-- : Other

Đặc quyền có 2 định dạng:

* Symbolic mode:

chmod WhoWhatWhich file | directory

chmod ug+rw test.txt

Who: u, g, o, a (user, group, others, all)

What: +, -, = (add, remove, set exact)

Which: r,w,x (read, write, execute)

* Numeric mode: read: 4; write: 2; execute: 1

chmod ### file | directory

chmod 744 example.txt

Owner: rwx=4+2+1=7

Group: r--=4

Others: r--=4

**Linux file permission do?**

Read: truy cập nội dung của tệp: cat,less,vim,cp

Write: >,>>

Execute: bash,python,…

**Directory permission do?**

Read: xem nội dung có trong thư mục: ls

Write: thay đổi nội dung của thư mục: mv,rm,touch,cp file in directory

**Special file permissions:**

Special permission đã tạo ra mức độ truy cập thứ tư ngoài user, group và others.

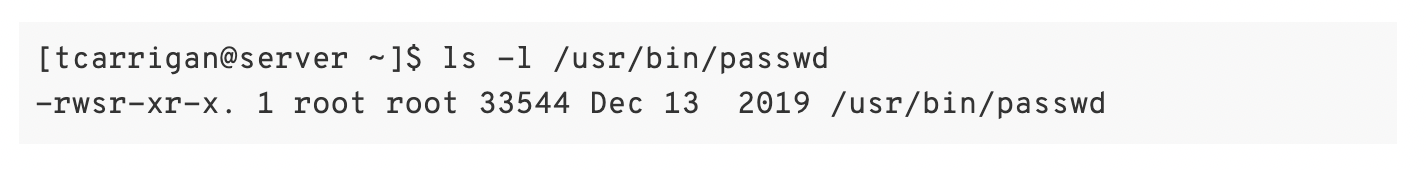
Với mỗi mức độ truy cập đã thảo luận trước đó, sẽ có thêm lựa chọn special permission.

Special permission cho chúng ta thêm nhiều đặc quyền hơn.

**user + s(pecial)**

Thường được nhắc đến là SUID, special permission của cấp độ user có duy nhất một chức năng: 1 tệp có SUID luôn thực thi với tư cách là chủ sở hữu tệp, bất kể người đó có gửi lệnh không. Nếu chủ sở hữu không có đặc quyền thực thi, hãy sử dụng “S” ở đây.

Ví dụ, hãy xem lệnh /usr/bin/passwd:

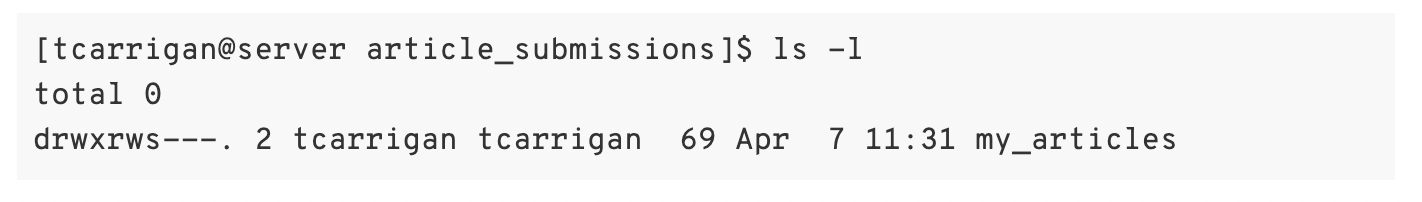


Lưu ý là s sẽ thay thế x.

**group + s(pecial)**

Thường được nhắc đến là SGID, special permission này có một vài chức năng:

* Nếu đặt trên 1 tệp, nó cho phép thực thi với tư cách là nhóm sở hữu tệp đó (tương tự như SUID)
* Nếu đặt trên 1 thư mục, bất cứ tệp nào được tạo ra trong thư mục sẽ có nhóm sở hữu là chủ của thư mục.



Dấu hiệu là chữ s sẽ thay thế x ở đặc quyền của nhóm. Điều này cũng rất hữu dụng với các thư mục thường được dùng trong các nỗ lực hợp tác giữa các thành viên trong 1 nhóm. Bất cứ thành viên nào trong nhóm cũng được truy cập tệp mới. Điều này cũng áp dụng cho các tệp thực thi luôn. SGID rất quyền lực khi được khởi tạo hợp lí.

other + t (sticky)

Special permission cuối cùng được gọi là sticky bit. Đặc quyền này không ảnh hưởng đến các tệp riêng lẻ. Tuy vậy, ở cấp độ thư mục, nó hạn chế xóa tệp. Chỉ có chủ sở hữu hay root mới có thể xóa tệp trong thư mục đó. Một ví dụ phổ biến là thư mục /tmp



Dấu hiệu của đặc quyền này là chữ t thay thế chữ x trong others.

**Setting special permissions**

Giả sử chúng ta muốn đặt SGID trên thư mục community\_content:

Symbolic mode:

chmod g+s community\_content/

Numeric mode:

* Start at 0
* SUID=4
* SGID=2
* Sticky=1

chmod X### file | directory

chmod 2770 community\_content/

