CSCI 274 - Intro to Linux OS

Week 12 - Identity, Ownership, and Permissions Part 1

Max Gawason (maxgawason@mines.edu) [A]
Rocco Marchitto (rmarchitto@mines.edu) [B/C/D]

Permissions

On Linux and other Unix-like operating systems, there is a set of rules for each file and directory that define who can access it, and what they can do with it. These rules are called **permissions** or modes. Permissions specify what a particular person may or may not do with a file or directory.

Linux permissions dictate **3** things you may do with a **file/directory**, **read, write and execute**. They are referred to in Linux by a single letter each.

Permissions

With files:

- r (aka read) - you may view the contents of the file
- w (aka write) - you may change the contents of the file
- x (aka execute) - you may execute or run the file.

With directories:

- r - you have the ability to read the contents of the directory (i.e. do an ls)
- w - you have the ability to write into the directory (i.e. create files and directories)
- x - you have the ability to enter that directory (i.e. cd)

Permissions

For every file (or directory) we define **3** sets of people for whom we may specify permissions.

- owner - a single person who owns the file. (typically the person who created the file but ownership may be granted to someone else by certain users)
- group - every file belongs to a single group of people
- others - everyone else who is not in the group or the owner

Example

-rwxr-xr--

1. The first character identifies the file type. If it is a dash (-) then it is a normal file. If it is a ‘d’ then it is a directory
2. The next 3 characters represent the permissions for the owner. A letter represents the presence of a permission and a dash (-) represents the absence of a permission
3. The following 3 characters represent the permissions for the group
4. The last 3 characters represent the permissions for others (or everyone else)

Common Commands

chmod (aka change mode) - used to change the permissions of files or directories

Only the file's owner or root can change permissions for a file.

Reference	Class	Description
u	owner	file's owner
g	group	users who are members of the file's group
o	others	users who are neither the file's owner nor members of the file's group
a	all	All three of the above, same as ugo

Operator	Description
+	Adds the specified modes to the specified classes
-	Removes the specified modes from the specified classes
=	The modes specified are to be made the exact modes for the specified classes

Common Commands

You can represent permissions with their alphanumeric characters, or with octal numbers (the digits 0 through 7). The octal numbers correspond to r,w,x as follows. Use one octal digit for each of the owner (user), group, and other.

Octal	Binary
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Example:

chmod u=rwx,g=rx,o=r myfile

chmod 754 myfile

Common Pipeline Utilities

chown - changes the owner and group

Only a privileged process or user, such as root, may change the owner of a file

```
root@kali:~# ls -l file1.txt
-rw-r--r-- 1 root root 12 Feb  4 12:04 file1.txt
root@kali:~# chown master file1.txt
root@kali:~# ls -l file1.txt
-rw-r--r-- 1 master root 12 Feb  4 12:04 file1.txt
root@kali:~#
```

```
root@kali:~# ls -l file1.txt
-rw-r--r-- 1 master root 12 Feb  4 12:04 file1.txt
root@kali:~# chown -v :group1 file1.txt
changed ownership of 'file1.txt' from master:root to :group1
root@kali:~#
```

Common Pipeline Utilities

id - prints user and group information for the specified USERNAME, or, when USERNAME omitted, for the current user.

This command is useful to find out the following information as listed below:

- User name and real user id.
- Find out the specific Users UID.
- Show the UID and all groups associated with a user.
- List out all the groups a user belongs to.

Syntax:

```
id [OPTION]… [USER]
```

Common Pipeline Utilities

users - prints the names of all users **currently logged** in to the host.

Syntax:

```
users [OPTION]... [FILE]
```

If the FILE is not specified, use /var/run/utmp. /var/log/wtmp as FILE is common.

Common Pipeline Utilities

who - prints information about all users who are currently logged in. Information shown with no options:

- Login name of the users
- Terminal line numbers
- Login time of the users in to system
- Remote host name of the user

whoami - To display system's username

w - To display list of users and their activities