Operating System Security

#05 - Securing Linux Filesystem

Herman Kabetta

Linux File Type

File Symbol	Meaning
-	Regular file
d	Directory
l	Link
c	Special file or device file
s	Socket
p	Named pipe
b	Block device

Sockets files are used for communication between processes. Generally, they are used by services such as X Windows, syslog, etc.
/dev/log

Similarly as Local sockets, named pipes allow communication between two local processes

Block devices are similar to character devices. They mostly govern hardware as harddrives, memory, etc.
/dev/sda

Character and block device files allow users and programs to communicate with hardware peripheral devices
/dev

Linux File Attributes

Total columns = 9

Type	# of Links	Owner	Group	Size	Month	Day	Time	Name
drwxr-xr-x.	21	root	root	4096	Feb	27	13:33	var
lrwxrwxrwx.	1	root	root	7	feb	27	13:15	bin
-rw-r--r--	1	root	root	0	Mar	2	11.15	test_file

The second column is the number of hard links to the file. For a directory, the number of hard links is the number of immediate subdirectories it has plus its parent directory and itself.

Linux File Ownership and Permissions

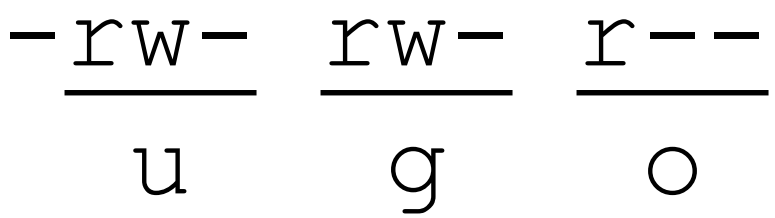
- There are 2 owners of a file or directory
  - User and Group
- Command to Change File Ownership
  - `chown` & `chgrp`
- Recursive ownership change option (Cascade)
  - `-R`

Linux File Ownership and Permissions

- Linux is a multi-user system. Every File and directory in your account can be protected from or made accessible to other users by changing its access permissions. Every user has responsibility for controlling access to their files
- Permissions for a file or directory may be restricted to by types
- There are 3 types of permissions
  - `r - read`
  - `w - write`
  - `x - execute = running a program`

Linux File Ownership and Permissions

- Each permission (rwx) can be controlled at three levels:
  - `u - user = yourself`
  - `g - group = can be people in same proj.`
  - `o - other = everyone on the system`
- File or Directory permission can be displayed by running `ls -l` command
- Command to change permission
  - `chmod`



Access Control List (ACL)

What is ACL ?

- Access control list (ACL) provides an additional, more flexible permission mechanism for file systems. It is designed to assist with UNIX file permissions. ACL allows you to givepermissions for any user or group to any disc resource.

Use of ACL :

- Think of a scenario in which a particular user is not a member of group created by you but still you want to give some read or write access, how can you do it without making user a member of group, here comes in picture Access Control Lists, ACL helps us to do this trick.
- Basically, ACLs are used to make a flexible permission mechanism in Linux.
- From Linux man pages, ACLs are used to define more fine-grained discretionary access rights for files and directories.
- Commands to assign and remove ACL permissions are
  - **`setfacl`** and **`getfacl`**

Access Control List (ACL)

List of commands for setting up ACL :

1) To add permission for user

```
setfacl -m "u:user:permissions" /path/to/file
```

2) To add permissions for a group

```
setfacl -m "g:group:permissions" /path/to/file
```

3) To allow all files or directories to inherit ACL entries from the directory it is within

```
setfacl -dm "entry" /path/to/dir
```

4) To remove a specific entry

```
setfacl -x "entry" /path/to/file
```

5) To remove all entries

```
setfacl -b path/to/file
```

For example:

```
setfacl -m u:akeo:rwx FILENAME
```

Note :

- As you assign the ACL permission to a file/directory it adds + sign at the end of the permission
- Setting w ermission with ACL does not allow to remove a file

Try it!

1. Create a file named "Red" as a regular user in your home directory
2. Change permissions to only allow yourself to read it
3. Change permission to allow other to read as well now
4. Become root and change the ownership of the file Red to root
5. Change the group ownership for Red file to root as well
6. Become yourself as a user now
7. Move the Red file from your home directory to /tmp directory
8. Are you able to move that file? If yes then what is the reason? You should have figured that out by now
9. Now cd into /tmp directory and delete the Red file. Are you able to delete it and if not why? Again you should know the answer
10. Become root and now using ACL assign yourself the read and write permission for Red file in /tmp directory
11. Verify the ACL permissions
12. Try to write to that file Red
13. Try to delete that file
14. Practice a few more times with different users and different files