File permissions in Linux

Project description

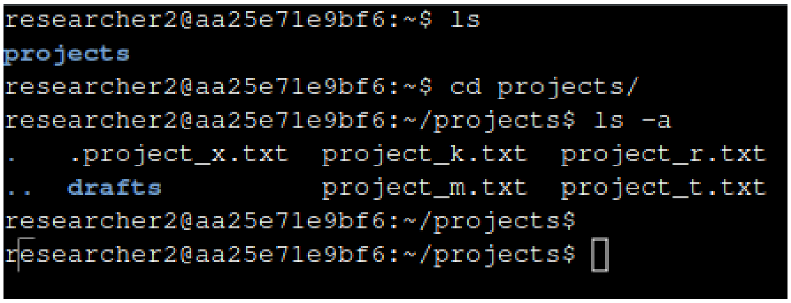
In this project the file permissions of a fictional research team were managed. Some files were archives that should not be written on, while others were limited access project files, that needed their permissions properly set for security reasons.

File and directory details

The researcher2 user is a part of the research_team group, and the directory structure for them is as follows:

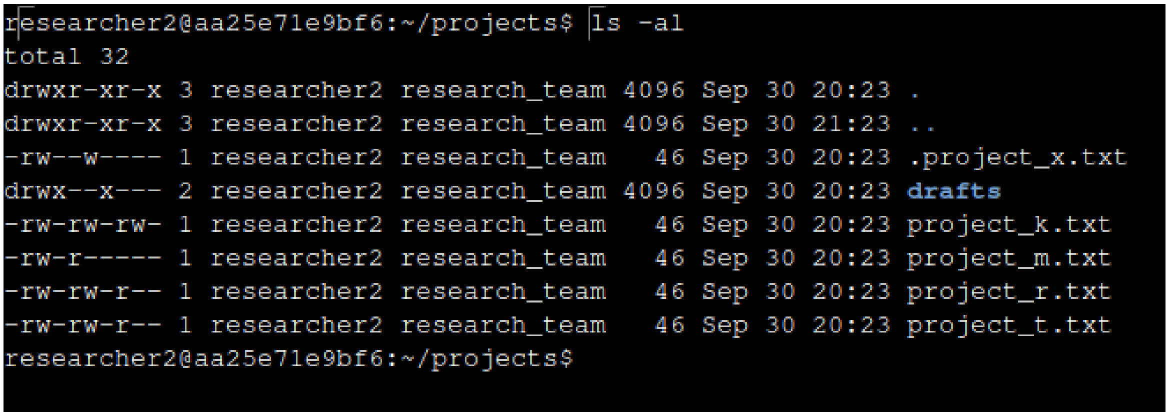
- ~/projects
  - /drafts/
  - .project_x.txt
  - project_k.txt
  - project_m.txt
  - project_r.txt
  - Project_t.txt

Structure of the directory:



```
researcher2@aa25e71e9bf6:~$ ls
projects
researcher2@aa25e71e9bf6:~$ cd projects/
researcher2@aa25e71e9bf6:~/projects$ ls -a
.   .project_x.txt  project_k.txt  project_r.txt
..  drafts          project_m.txt  project_t.txt
researcher2@aa25e71e9bf6:~/projects$
researcher2@aa25e71e9bf6:~/projects$
```

And the file permissions were set-up in the following manner:



```
researcher2@aa25e71e9bf6:~/projects$ ls -al
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Sep 30 20:23 .
drwxr-xr-x 3 researcher2 research_team 4096 Sep 30 21:23 ..
-rw--w---- 1 researcher2 research_team   46 Sep 30 20:23 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Sep 30 20:23 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Sep 30 20:23 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Sep 30 20:23 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Sep 30 20:23 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Sep 30 20:23 project_t.txt
researcher2@aa25e71e9bf6:~/projects$
```

The permissions string

In linux, file permissions are represented by a ten character string with a specific format, e.g.:

- drwrwxrwx
- -rw-r--r--
- d-wxr-xrwx

The first character can be either a “d” or a “-”, and it represents if the corresponding object is a directory (indicated by a “d”) or just a file (indicated by a “-”)

The following three characters (2-4) indicate respectively read, write and execute permissions for the current user.

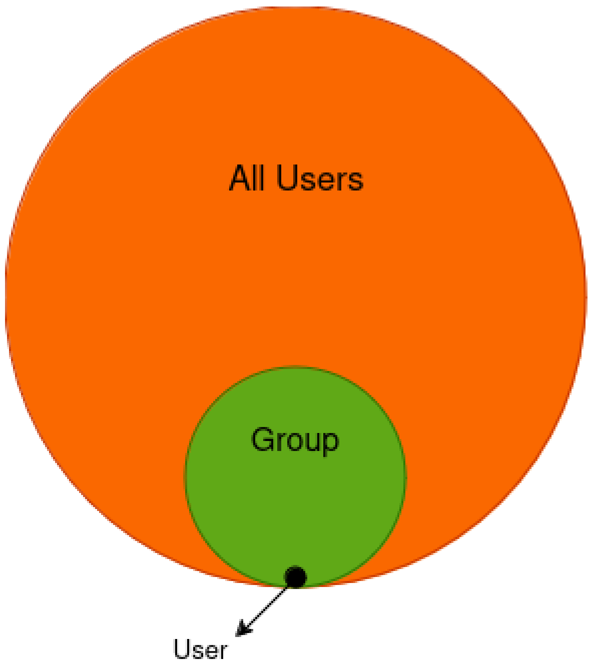
A read permission allows the user to access the contents of a file, but not change them in any way. Write permission allows a user to change the contents of a file. If the user’s permissions are read-only, usually it means that the file only accepts appends, but not changing the previous text.

An execute permission allows the user to execute the file, if the file is an executable binary.

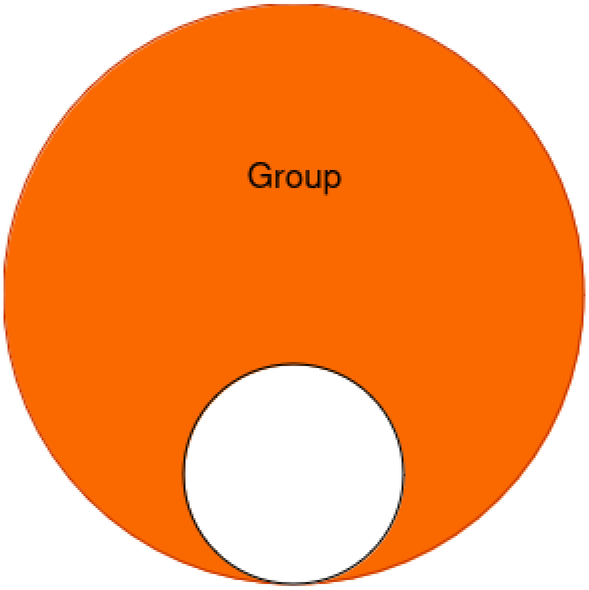
If the referred object is, instead, a directory, a read permission allows the user to access the name of he files on the directory, but not necessarily the actual contents of the files; a write permission allows the user to create new files n the directory, but not change or access the contents of the other files; and execute permissions allows the user to access the files of the directory.

The following three characters (5-7) indicate the permissions for the group, and the last three (8-10) indicate the permissions for the other category. The group category represents all of the users in the group that the current user is in, while the other category represents all users that are not in the same group as the current user.

Those permissions act exactly the same as the permissions for the user; but represent more significant cybersecurity risk, simply because there are more people in those categories, as shown in the diagram below:



(The “other” category is defined as the difference between all users and the group, or simply the orange area)

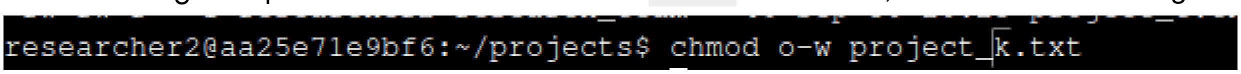


Change file and directory permissions

[Add content here.]

Change file permissions on a hidden file

You can change the permissions of a file with the `chmod` command, used like the following:



```
researcher2@aa25e71e9bf6:~/projects$ chmod o-w project_k.txt
```

Which will result in the permissions for the oject_k.txt file which started as:

`-rw-rw-rw-`

Being changed to:

`-rw-rw-r--`

It is possible to change directory permissions in the same way you would change file permissions, by using the chmod command.