File permissions in Linux

Project description

Project description
In this project, I acted as a security professional managing file permissions for a research team at a large organization. Using Linux commands, I ensured that only authorized users (specifically researcher2) could access sensitive files and directories, removing unauthorized write permissions and restricting access to hidden or restricted files. This strengthened system security by aligning permissions with the principle of least privilege.

Check file and directory details
Command used: ls -la

Output snippet:

```
total 20
drwx--x--- 2 researcher2 research_team 4096 Oct 14 18:40 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Oct 14 18:40 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Oct 14 18:40 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Oct 14 18:40 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Oct 14 18:40 project_t.txt
```

Describe the permissions string

For instance, a directory with full permissions for all owner types would be drwxrwxrwx:
- The 1st character indicates the file type. The d indicates it's a directory. When this character is a hyphen (-), it's a regular file.
- The 2nd-4th characters indicate the read (r), write (w), and execute (x) permissions for the user. When one of these characters is a hyphen (-) instead, it indicates that this permission is not granted to the user.

- The 5th-7th characters indicate the read (r), write (w), and execute (x) permissions for the group. When one of these characters is a hyphen (-) instead, it indicates that this permission is not granted for the group.
- The 8th-10th characters indicate the read (r), write (w), and execute (x) permissions for the owner type of other. This owner type consists of all other users on the system apart from the user and the group. When one of these characters is a hyphen (-) instead, that indicates that this permission is not granted for other.

This document displays the file structure of the `/home/researcher2/projects` directory and the permissions of the files and subdirectory it contains.

In the `/home/researcher2/projects` directory, there are five files with the following names and permissions:
- `project_k.txt`
  - ○ User = read, write,
  - ○ Group = read, write
  - ○ Other = read, write
- `project_m.txt`
  - ○ User = read, write
  - ○ Group = read
  - ○ Other = none
- `project_r.txt`
  - ○ User= read, write
  - ○ Group = read, write
  - ○ Other = read
- `project_t.txt`
  - ○ User = read, write
  - ○ Group = read, write
  - ○ Other = read
- `.project_x.txt`
  - ○ User = read, write
  - ○ Group = write
  - ○ Other = none

There is also one subdirectory inside the `projects` directory named `drafts`. The permissions on `drafts` are:
- User = read, write, execute
- Group = execute
- Other = none

Change file permissions

Issue is that **project_k.txt** allowed others (O) to write.

Command used: <mark>chmod o-w project_k.txt</mark>

Result: Permissions changed from <mark>-rw-rw-rw-</mark> to <mark>-rw-rw-r--</mark>.

Change file permissions on a hidden file

Issue was: Hidden file **.project_x.txt** allowed user/group to write.

Command: <mark>chmod u-w, g-w, g+r .project_x.txt</mark>

Result: Permissions changed to -r-- r--- --- (read-only for user/group).

Change directory permissions

Issue was that **Group** had **execute** (x) access to draft\

Command: <mark>chmod g-x drafts</mark>

Summary

This project demonstrated critical Linux file permission management. I identified insecure permissions (e.g., world-writable files), removed unauthorized access, and restricted directories to the owner. These steps align with cybersecurity best practices to minimize attack surfaces. Skills like chmod, ls -la, and interpreting permission strings are essential for securing systems.

Complete configurations

researcher2@321e7665da73:~/projects$ <mark>ls -l</mark>
total 20
drwx--x--- 2 researcher2 research_team 4096 Apr 27 15:19 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Apr 27 15:19 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Apr 27 15:19 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Apr 27 15:19 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Apr 27 15:19 project_t.txt
researcher2@321e7665da73:~/projects$ <mark>ls -la</mark>
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Apr 27 15:19 .
drwxr-xr-x 3 researcher2 research_team 4096 Apr 27 15:26 ..
-rw--w---- 1 researcher2 research_team   46 Apr 27 15:19 .project_x.txt

drwx--x--- 2 researcher2 research_team 4096 Apr 27 15:19 drafts
-rw-rw-rw- 1 researcher2 research_team 46 Apr 27 15:19 project_k.txt
-rw-r----- 1 researcher2 research_team 46 Apr 27 15:19 project_m.txt
-rw-rw-r-- 1 researcher2 research_team 46 Apr 27 15:19 project_r.txt
-rw-rw-r-- 1 researcher2 research_team 46 Apr 27 15:19 project_t.txt
researcher2@321e7665da73:~/projects$ <mark>ls -l</mark>
total 20
drwx--x--- 2 researcher2 research_team 4096 Apr 27 15:19 drafts
-rw-rw-rw- 1 researcher2 research_team 46 Apr 27 15:19 project_k.txt
-rw-r----- 1 researcher2 research_team 46 Apr 27 15:19 project_m.txt
-rw-rw-r-- 1 researcher2 research_team 46 Apr 27 15:19 project_r.txt
-rw-rw-r-- 1 researcher2 research_team 46 Apr 27 15:19 project_t.txt
researcher2@321e7665da73:~/projects$ <mark>chmod o-w project_k.txt</mark>
researcher2@321e7665da73:~/projects$ <mark>ls -l</mark>
total 20
drwx--x--- 2 researcher2 research_team 4096 Apr 27 15:19 drafts
-rw-rw-r-- 1 researcher2 research_team 46 Apr 27 15:19 project_k.txt
-rw-r----- 1 researcher2 research_team 46 Apr 27 15:19 project_m.txt
-rw-rw-r-- 1 researcher2 research_team 46 Apr 27 15:19 project_r.txt
-rw-rw-r-- 1 researcher2 research_team 46 Apr 27 15:19 project_t.txt
researcher2@321e7665da73:~/projects$ <mark>chmod g-r project_m.txt</mark>
researcher2@321e7665da73:~/projects$ <mark>ls -l</mark>
total 20
drwx--x--- 2 researcher2 research_team 4096 Apr 27 15:19 drafts
-rw-rw-r-- 1 researcher2 research_team 46 Apr 27 15:19 project_k.txt
-rw------- 1 researcher2 research_team 46 Apr 27 15:19 project_m.txt
-rw-rw-r-- 1 researcher2 research_team 46 Apr 27 15:19 project_r.txt
-rw-rw-r-- 1 researcher2 research_team 46 Apr 27 15:19 project_t.txt
researcher2@321e7665da73:~/projects$ <mark>ls -la</mark>
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Apr 27 15:19 .
drwxr-xr-x 3 researcher2 research_team 4096 Apr 27 15:26 ..
-rw--w---- 1 researcher2 research_team 46 Apr 27 15:19 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Apr 27 15:19 drafts
-rw-rw-r-- 1 researcher2 research_team 46 Apr 27 15:19 project_k.txt
-rw------- 1 researcher2 research_team 46 Apr 27 15:19 project_m.txt
-rw-rw-r-- 1 researcher2 research_team 46 Apr 27 15:19 project_r.txt
-rw-rw-r-- 1 researcher2 research_team 46 Apr 27 15:19 project_t.txt
researcher2@321e7665da73:~/projects$ <mark>chmod u-w,g-w,g+r .project_x.txt</mark>
researcher2@321e7665da73:~/projects$ <mark>ls -la</mark>
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Apr 27 15:19 .
drwxr-xr-x 3 researcher2 research_team 4096 Apr 27 15:26 ..
-r--r----- 1 researcher2 research_team 46 Apr 27 15:19 .project_x.txt

```
drwx--x--- 2 researcher2 research_team 4096 Apr 27 15:19 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Apr 27 15:19 project_k.txt
-rw------- 1 researcher2 research_team   46 Apr 27 15:19 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Apr 27 15:19 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Apr 27 15:19 project_t.txt
researcher2@321e7665da73:~/projects$ ls -l
total 20
drwx--x--- 2 researcher2 research_team 4096 Apr 27 15:19 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Apr 27 15:19 project_k.txt
-rw------- 1 researcher2 research_team   46 Apr 27 15:19 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Apr 27 15:19 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Apr 27 15:19 project_t.txt
researcher2@321e7665da73:~/projects$ chmod g-x drafts
researcher2@321e7665da73:~/projects$
```