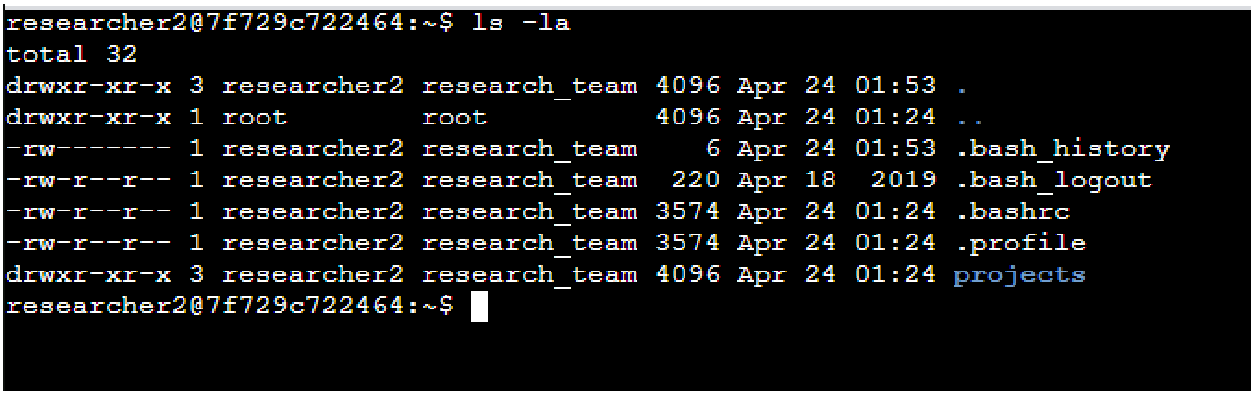
File permissions in Linux

Project description

As a security professional supporting the research department, I used Linux commands to review and modify file and directory permissions to ensure proper authorization. My responsibilities included removing unauthorized access and ensuring that sensitive files were only accessible to the appropriate users. This project demonstrates my ability to use ls -la to inspect permissions and chmod to correct them as needed.

Check file and directory details



```
researcher2@7f729c722464:~$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Apr 24 01:53 .
drwxr-xr-x 1 root        root          4096 Apr 24 01:24 ..
-rw------- 1 researcher2 research_team    6 Apr 24 01:53 .bash_history
-rw-r--r-- 1 researcher2 research_team  220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 researcher2 research_team 3574 Apr 24 01:24 .bashrc
-rw-r--r-- 1 researcher2 research_team 3574 Apr 24 01:24 .profile
drwxr-xr-x 3 researcher2 research_team 4096 Apr 24 01:24 projects
researcher2@7f729c722464:~$ 
```

This command displays file details, including ownership and permissions for user, group, and others. The output included files like project_k.txt, project_m.txt, project_r.txt, and a hidden file .project_x.txt. It also showed the drafts directory.

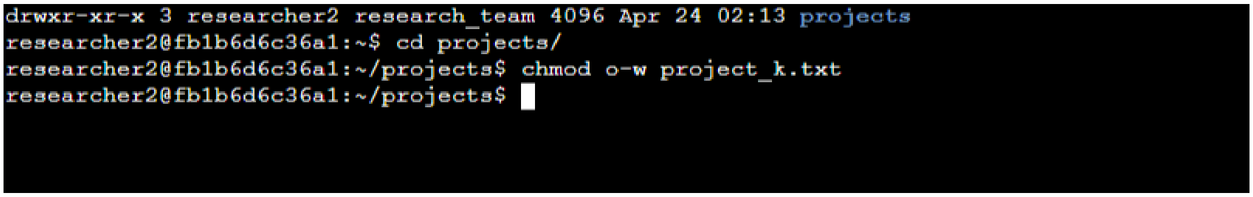
Describe the permissions string

This 10 character string is interpreted as:

- -: It's a regular file
- rw-: The user can read and write
- rw-: The group can read and write
- rw-: Others can read and write

This configuration is insecure because **"others" have write access**, allowing any user on the system to modify the file. It was one of the files that needed permission changes.

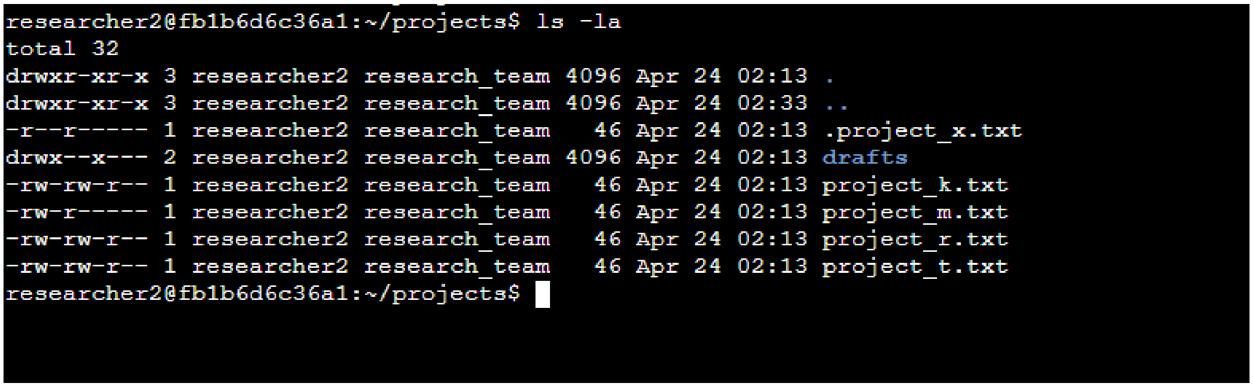
Change file permissions



```
drwxr-xr-x 3 researcher2 research_team 4096 Apr 24 02:13 projects
researcher2@fb1b6d6c36a1:~$ cd projects/
researcher2@fb1b6d6c36a1:~/projects$ chmod o-w project_k.txt
researcher2@fb1b6d6c36a1:~/projects$ 
```

To comply with the organization's policy of not allowing write access for "others", I modified the permissions on project_k.txt using: chmod o-w project_k.txt
This removed write access from "others" while maintaining it for the user and group.
I also updated project_m.txt, which was a restricted file. The group had read access (-rw-r-----), which violated policy. I removed group read access using: chmod g-r project_m.txt

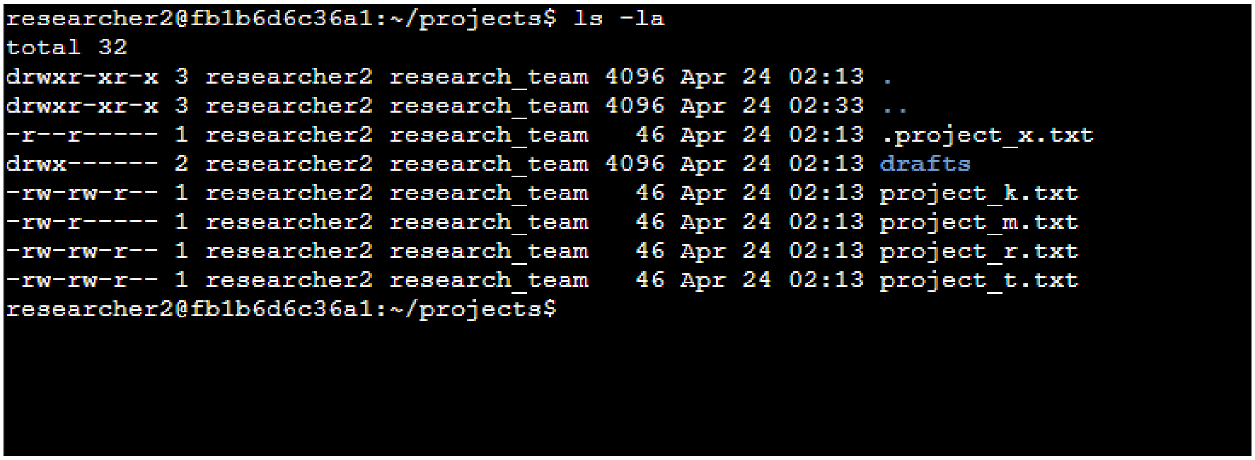
Change file permissions on a hidden file



```
researcher2@fb1b6d6c36a1:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Apr 24 02:13 .
drwxr-xr-x 3 researcher2 research_team 4096 Apr 24 02:33 ..
-r--r----- 1 researcher2 research_team   46 Apr 24 02:13 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Apr 24 02:13 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Apr 24 02:13 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Apr 24 02:13 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Apr 24 02:13 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Apr 24 02:13 project_t.txt
researcher2@fb1b6d6c36a1:~/projects$ 
```

The hidden file .project_x.txt was archived and should not be writable by anyone, although the user and group should still be able to read it. I used the following command: chmod 440 .project_x.txt
This set the permissions to: -r--r-----
Now, the file is read-only for both the user and the group, and inaccessible to others.

Change directory permissions



```
researcher2@fb1b6d6c36a1:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Apr 24 02:13 .
drwxr-xr-x 3 researcher2 research_team 4096 Apr 24 02:33 ..
-r--r----- 1 researcher2 research_team   46 Apr 24 02:13 .project_x.txt
drwx------ 2 researcher2 research_team 4096 Apr 24 02:13 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Apr 24 02:13 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Apr 24 02:13 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Apr 24 02:13 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Apr 24 02:13 project_t.txt
researcher2@fb1b6d6c36a1:~/projects$
```

The drafts subdirectory originally allowed group members to execute (enter) the directory, which violated the requirement that **only the user** should have access. Its permissions were: drwx--x---
To restrict access to only *researcher2*, I ran: chmod 700 drafts
This changed the permissions to: drwx------

Summary

Throughout this project, I used Linux commands to verify and adjust file permissions in line with the organization's security policy. I used ls -la to examine current permissions, interpreted permission strings, and used chmod to correct any unauthorized access. I ensured hidden files were not modifiable and restricted sensitive directories to the correct user. These actions helped protect confidential data and reinforced secure access practices on the system.