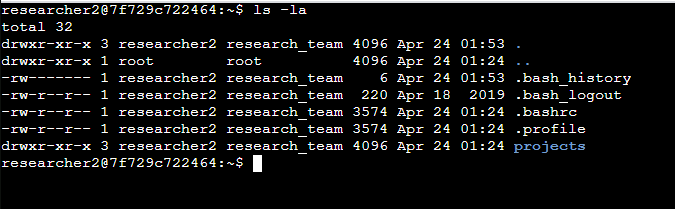
# File permissions in Linux

## 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



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.

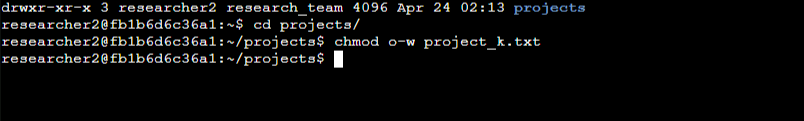
## Describe the permissions string

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

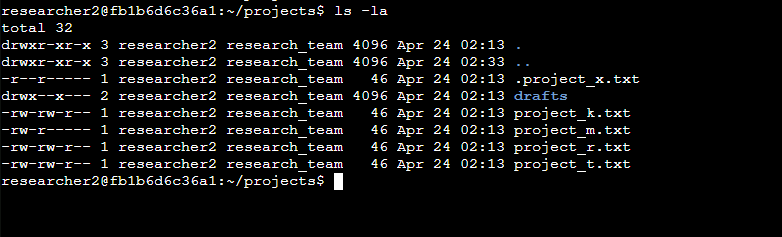


To comply with the organization's policy of not allowing write access for "others", I modified the permissions on project\_k.txt using: chmod o-w project\_k.txt

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

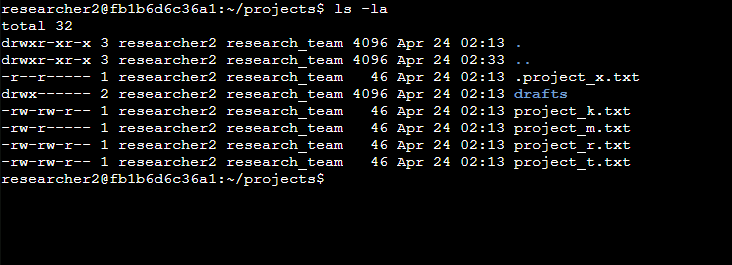


The hidden file .project\_x.txt was archived and should not be writable by anyone, although the user and group should still be able to read it. I used the following command: chmod 440 .project\_x.txt

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



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.