File permissions in Linux

Project description

In this project, I explored managing file and directory permissions in Linux, ensuring that users only have the appropriate authorizations. I used commands such as `ls -la` to inspect permissions and `chmod` to modify file and directory access, including hidden files. The goal was to protect sensitive research team data by removing unauthorized access and ensuring that only the correct users can read or modify files.

Check file and directory details

ls -la /home/researcher2/projects

Explanation:
This command lists all files and directories (including hidden files) with their permission string, owner, group, size, and modification date.

Current permissions:
-rw-rw-rw- project_k.txt
-rw-r----- project_m.txt
-rw-rw-r-- project_r.txt
-rw-rw-r-- project_t.txt
-rw--w---- .project_x.txt
drwx--x--- drafts/

Describe the permissions string

Example: project_k.txt ⟶ -rw-rw-rw-

- - ⟶ regular file
- rw- ⟶ owner permissions: read and write
- rw- ⟶ group permissions: read and write
- rw- ⟶ others permissions: read and write

This string clearly shows who can read, write, or execute the file.

Change file permissions

Command:
chmod o-w /home/researcher2/projects/project_k.txt
Explanation:
Removes the write permission for “others,” ensuring that only the owner and group can modify the file.

Change file permissions on a hidden file

Command:
chmod u=r,g=r,o= /home/researcher2/projects/.project_x.txt
Explanation:
Sets the hidden file .project_x.txt to read-only for the owner and group, removing write and execute permissions.

Change directory permissions

Command:
chmod go= /home/researcher2/projects/drafts
Explanation:
Removes all permissions for group and others on the drafts directory, ensuring only researcher2 can access its contents.

Summary

Throughout this project, I inspected file and directory permissions, interpreted the 10-character permission strings, and corrected unauthorized access using chmod. I protected sensitive files, including hidden files, and restricted access to critical directories to the owner only. This work demonstrates practical skills in Linux administration, data security, and user access control.