File permissions in Linux

Project description

In this task, my role is to review and adjust file and directory permissions on a Linux system to ensure that user access aligns with the organization's security standards. The main objective is to enhance file system security by correctly managing access rights and preventing unauthorized use or modification of sensitive data.

Check file and directory details

ls -la /home/researcher2/projects

Describe the permissions string

The permissions string is a 10-character code that shows the type of file and the access rights for different users.
The first character tells you the file type: a dash (-) means it's a regular file, d indicates a directory, and l stands for a symbolic link.
The next three characters, positions 2–4 show what the owner can do, read (r), write (w), or execute (x).
Characters 5 to 7 indicate the group's permissions.
The last three characters, 8–10 represent the permissions for all other users, also using r, w, and x.
For example, -rw-r--r-- indicates a regular file where the owner can read and write, while the group and others can only read it.

Change file permissions

chmod o-w /home/researcher2/projects/project_m.txt

Change file permissions on a hidden file

chmod o-w /home/researcher2/projects/.project_x.txt

Change directory permissions

chmod 700 /home/researcher2/projects/drafts

Summary

For this assignment, I analyzed and updated file and directory permissions in a Linux system. By using the `ls -la` command, I reviewed the existing permission settings to ensure they complied with the organization's access control policies. I then used the `chmod` command to modify permissions as required for different files including hidden ones and directories. These steps helped strengthen file system security and ensure that user access aligns with the organization's security guidelines.