File Permissions in Linux

# Project Description

As a security professional working with the research team in a large organization, it's my responsibility to ensure files and directories are only accessible to authorized users. This project demonstrates how to audit and modify file system permissions in Linux to enforce the organization's security policy, which prohibits unauthorized write access and restricts sensitive directories to specific users.

# Check File and Directory Details

To check file and directory permissions, we use the `ls -la` command. This command lists all files, including hidden ones, along with their permissions.

Command:

ls -la /home/researchteam/projects

Example Output:

-rw-r--rw- 1 researcher1 research 1234 Jun 1 11:15 project\_a.txt  
-rw-rw-r-- 1 researcher1 research 8752 Jun 2 08:03 .project\_x.txt  
drwxrwxrwx 2 researcher2 research 4096 Jun 2 10:22 drafts

# Describe the Permissions String

Let’s break down the permissions string from one example:

-rw-r--rw-

This 10-character string can be interpreted as follows:  
  
- `-` = regular file   
- `rw-` = the owner (researcher1) has read and write permissions   
- `r--` = the group (research) has read-only access   
- `rw-` = others have read and write permissions (This violates the organization's policy)

# Change File Permissions

The organization does not allow 'others' to have write access. The file project\_a.txt has rw- for others, which must be fixed.

Command:

chmod o-w /home/researchteam/projects/project\_a.txt

Output after rechecking with ls -la:

-rw-r--r-- 1 researcher1 research 1234 Jun 1 11:15 project\_a.txt

# Change File Permissions on a Hidden File

The file .project\_x.txt is a hidden file (starts with a dot). It should only be readable by the user and group — no write permissions for anyone.

Command:

chmod 440 /home/researchteam/projects/.project\_x.txt

Output:

-r--r----- 1 researcher1 research 8752 Jun 2 08:03 .project\_x.txt

# Change Directory Permissions

The drafts directory is currently accessible by all users (drwxrwxrwx). This violates policy. It should be restricted to researcher2 only.

Command:

chmod 700 /home/researchteam/projects/drafts

Output:

drwx------ 2 researcher2 research 4096 Jun 2 10:22 drafts

# Summary

This project demonstrated how to manage file permissions using Linux commands. We began by auditing file and directory permissions with ls -la, analyzed 10-character permission strings, and used chmod to revoke unauthorized write access. Special attention was given to hidden files and sensitive directories, ensuring they were properly secured in accordance with the organization’s policy. This hands-on activity reinforced how Linux access controls are crucial to enforcing least-privilege and preventing data exposure.