File permissions in Linux

Project description

As a security professional, I reviewed and updated the file and directory permissions for the research team's project directory to ensure compliance with organizational security policies. This project involved inspecting current authorizations and applying the principle of least privilege to modify access rights for specific files and directories.Check file and directory details

ls -la projects

Describe the permissions string

he 10-character string (e.g., drwxr-xr-x) represents the file type and access permissions for the owner, group, and others:

- **First Character:** Indicates the file type (d for directory, - for file).
- **Next Nine Characters:** Divided into three sets, representing permissions:
  - **User (Owner, Characters 2–4: rwx)** – read, write, execute
  - **Group (Characters 5–7: r-x)** – read, execute; write denied
  - **Others (Characters 8–10: r-x)** – read, execute; write denied

Change file permissions

The file **project_b.txt** currently has -rw-rw-r--, granting write permission to the group. To adhere to a secure policy interpretation that disallows unnecessary write access, I will remove write access for the group.

Command to change permissions: chmod g-w projects/project_b.txt

The chmod command with the symbolic notation g-w was used to remove (-) the write (w) permission for the group (g) on the file.

Change file permissions on a hidden file

The hidden file **project_x.txt** should not have write permissions for anyone, but the user and group should be able to read the file. This is achieved using the octal notation 440.

Command to change permissions: chmod 440 projects/.project_x.txt

Explanation: Octal notation 440 sets read-only access for user and group, and no access for others.

Change directory permissions

Only researcher2 (the owner) should be allowed to access the drafts directory and its contents. This requires setting permissions to 700.

Command to change permissions: chmod 700 projects/drafts

Explanation: Octal notation 700 gives full access (rwx) to the owner and removes all permissions for group and others.

Summary

I have successfully reviewed file and directory permissions using ls -la and enforced security policies using chmod. Specifically:

- Removed group write access from a regular file
- Set read-only permissions for the user and group on a hidden file
- Restricted directory access to the owner only

These changes ensured that only authorized users have appropriate access, strengthening the security of the project directory.