File Permissions in Linux

Project Overview

As part of a security review, I was responsible for adjusting file and folder permissions in the `projects` directory to ensure proper access control based on internal policy. Maintaining accurate permissions is critical for system integrity and data confidentiality. Here's how I approached the task:

1. Viewing Current Permissions

To begin, I listed all files (including hidden ones) and their current permissions using the `ls -la` command. This allowed me to identify the presence of a hidden file named `.project_x.txt`, a subdirectory called `drafts`, and multiple project-related files.

2. Understanding Permission Strings

Each file and directory had a 10-character string representing its permissions.

- The first character indicates the type (`d` for directory, `-` for a file).
- The next three characters define permissions for the **user**, followed by three for the **group**, and three for **others**.

For example, the string `-rw-rw-r--` means:

- User and group can **read and write**
- Others can **only read**

3. Updating File Permissions

To comply with our security standards, I verified that no file allowed write access to “others.” For example, I removed this permission from `project_k.txt` using:

```
chmod o-w project_k.txt
```

I then confirmed the update using `ls -la`.

4. Securing a Hidden File

The file `.project_x.txt` had been archived and should remain unmodifiable. I tightened its permissions by removing write access for both the user and group:

```
chmod u-w .project_x.txt
chmod g-w .project_x.txt
```

To ensure readability for the group, I explicitly granted read access:

```
chmod g+r .project_x.txt
```

5. Restricting Directory Access

The `drafts` directory was intended to be accessible only by the `researcher2` user. I ensured that only this user had execute permissions by removing execute rights from the group:

```
chmod g-x drafts
```

Summary

By analyzing and adjusting permissions using `ls -la` and `chmod`, I aligned file and directory access with organizational security policies. These changes help prevent unauthorized modifications and enhance overall system security.