File permissions in Linux

Project description

In this project, I analyzed and managed file permissions on a Linux system for a research team. My objective was to verify existing permissions, identify incorrect authorization, and apply the correct permissions to protect sensitive files and directories. By using Linux commands such as `ls -la` and `chmod`, I ensured that only authorized users had access, while unauthorized access was removed.

Check file and directory details

Typed Command Used:

```
ls -la /home/researcher2/projects
```

Explanation:
This command lists all files in the directory, including hidden files, and shows their full 10-character permission strings. Because screenshots weren't possible, the permissions were taken directly from the "Current file permissions" document.

Permission strings for each item:

```
-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 chosen:

`-rw-rw-rw-`

Explanation:

- `-` → regular file
- `rw-` → user can read and write
- `rw-` → group can read and write
- `rw-` → others can read and write

This indicates that *everyone* can write to this file, which violates the organization's policy.

Change file permissions

File requiring correction: `project_k.txt`

Reason: "Others" should not have write access.

Typed Command Used:

```
chmod o-w /home/researcher2/projects/project_k.txt
```

Explanation:

This command removes write permission from the "others" category.

After applying it, the correct permission string becomes:

`-rw-rw-r--`

Change file permissions on a hidden file

Hidden file: `.project_x.txt`

Goal:

- User = read, write
- Group = read
- Others = none

Typed Command Used:

```
chmod u=rw,g=r,o= /home/researcher2/projects/.project_x.txt
```

Explanation:

This command explicitly sets the correct permissions, ensuring the archived file cannot be modified by anyone except the owner.

Updated permission string:

```
-rw-r-----
```

Change directory permissions

Only the `researcher2` user should have full access to the `drafts` directory.

Typed Command Used:

```
chmod 700 /home/researcher2/projects/drafts
```

Explanation:

This sets the directory permissions to:

```
drwx------
```

Only the owner can read, write, and execute (enter) the directory.

Summary

In this activity, I reviewed and updated file permissions in a Linux environment using `ls -la` to inspect authorization and `chmod` to apply corrections. I removed write permissions for unauthorized users, updated the permissions on a hidden file for secure archiving, and restricted a directory to the appropriate user. These adjustments ensure that only authorized users can access or modify sensitive files, maintaining proper security across the research team's workspace.