File permissions in Linux

Project description

This project involves managing file permissions in a Linux environment to ensure appropriate access control for users in a research team. The goal is to examine the existing permissions, determine if they align with the organization's security policies, and modify them as needed to prevent unauthorized access.

Check file and directory details

To inspect the current file and directory permissions, use the following command:

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

This command lists all files and directories, including hidden ones, along with their permissions in the `/home/researcher2/projects` directory.

Current permissions:

```
-rw-rw-rw- 1 researcher2 researcher  project_k.txt
-rw-r--r-- 1 researcher2 researcher  project_m.txt
-rw-rw-r-- 1 researcher2 researcher  project_r.txt
-rw-rw-r-- 1 researcher2 researcher  project_t.txt
-rw--w---- 1 researcher2 researcher  .project_x.txt
drwx--x--- 1 researcher2 researcher  drafts
```

Describe the permissions string

`-rw-rw-rw-`

- The first character (`-`) indicates a regular file.
- The next three characters (`rw-`) mean the owner (user) has read and write permissions but no execute.
- The next three (`rw-`) mean the group has read and write permissions but no execute.

- The last three (`rw-`) mean others have read and write permissions.

This means `project_k.txt` is accessible and writable by all users, which violates security policies.

Change file permissions

Since the organization does not allow others to have write access, modify `project_k.txt` to remove write access for others:

chmod 664 /home/researcher2/projects/project_k.txt

This changes the file permissions to `-rw-rw-r--`, allowing only the owner and group to write, while others can only read.

Change file permissions on a hidden file

The file `.project_x.txt` should not have write permissions for anyone but should be readable by the owner and group. Modify its permissions:

chmod 440 /home/researcher2/projects/.project_x.txt

This results in permissions `-r--r-----`, which allows only the owner and group to read the file.

Change directory permissions

The `drafts` directory should be accessible only by `researcher2`. Modify its permissions:

chmod 700 /home/researcher2/projects/drafts

This changes the permissions to `drwx------`, restricting access to only the owner.

Summary

In this project, we examined file permissions using `ls -la`, interpreted permission strings, and updated them using `chmod`. We ensured files do not allow unauthorized write access and

restricted access to sensitive directories. These changes enhance security and align with organizational policies.