File permissions in Linux

Project description

In this activity, I used Linux commands to manage file permissions for files and directories. By checking and modifying permissions, I ensured that access to sensitive files was restricted according to organizational policies. This activity shows my ability to interpret permissions strings, work with hidden files, and use commands such as ls -la and chmod to update authorizations.

Check file and directory details

Ls -la
The ls-la command lists all files and directories in long format (-l) and includes hidden files (-a).

Describe the permissions string

-rw-rw-r–
The 10 character string indicates file type and permissions.

- The first character (-) means it's a regular file.
- The next three (rw-) mean the owner or user has read and write access.
- The following three (rw-) mean the group has read and write access.
- The las three (r - -)mean others can only read the file.

Change file permissions

Policy requirement: No file should allow write access to "others"

Project_b.txt currently has -rw-rw-rw-, meaning others can write.

Chmod o-w project_b.txt

This removes write permissions from "others"

Change file permissions on a hidden file

.project_x.txt
Required Policy: Only user and group can read; no write permissions

```
researcher2@82a697df9c1e:~/projects$ chmod u-w,g-w,g+r .project_x.txt
researcher2@82a697df9c1e:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Sep 11 19:59 .
drwxr-xr-x 3 researcher2 research_team 4096 Sep 11 20:39 ..
-r--r----- 1 researcher2 research_team   46 Sep 11 19:59 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Sep 11 19:59 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Sep 11 19:59 project_k.txt
-rw------- 1 researcher2 research_team   46 Sep 11 19:59 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Sep 11 19:59 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Sep 11 19:59 project_t.txt
```

Change directory permissions

Directory: Drafts
Policy: Only “user” should have access to read, write and execute

```
researcher2@82a697df9c1e:~/projects$ chmod g-x drafts
```

```
researcher2@82a697df9c1e:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Sep 11 19:59 .
drwxr-xr-x 3 researcher2 research_team 4096 Sep 11 20:39 ..
-r--r----- 1 researcher2 research_team   46 Sep 11 19:59 .project_x.txt
drwx------ 2 researcher2 research_team 4096 Sep 11 19:59 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Sep 11 19:59 project_k.txt
-rw------- 1 researcher2 research_team   46 Sep 11 19:59 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Sep 11 19:59 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Sep 11 19:59 project_t.txt
```

Summary

Through this activity, I checked file permissions with ls -la, interpreted permission strings, and modified authorizations with chmod. I ensured that no file was writable by “others”, configured a hidden file with read-only permissions, and restricted a directory to user-only access. These actions demonstrate my ability to secure files in Linux systems using standard command-line tools- an essential skill for cybersecurity and system administration.