**Project Description**

**Project Overview:** In this project, I focused on managing file and directory permissions in a Linux environment to ensure proper authorization and security. The goal was to verify and update permissions to adhere to security policies, particularly for hidden files and directories, and to ensure that only authorized users had appropriate access.

**Step-by-Step Instructions**

**1. Check File Permissions**

**Command to Check Permissions:** To check the permissions of files and directories, including hidden ones, use the ls -la command.

**Example Command:**

ls -la

**Current Permissions:** Assuming you are checking permissions in the /home/analyst/projects directory, the output might look like this:

drwxr-xr-x 2 analyst users 4096 Sep 9 12:34 .

drwxr-xr-x 5 analyst users 4096 Sep 9 12:34 ..

-rw-rw-r-- 1 analyst users 1234 Sep 9 12:34 file1.txt

-rw-r--r-- 1 analyst users 5678 Sep 9 12:34 .project\_x.txt

**Description of the Permissions String:** For example, the string -rw-rw-r-- represents:

* -: Regular file
* rw-: User permissions (read and write)
* rw-: Group permissions (read and write)
* r--: Others permissions (read only)

**2. Change File Permissions**

**File Requiring Permission Modification:**

* **File:** file1.txt
* **Issue:** The file should not be writable by others.

**Command to Change Permissions:** To remove write permissions for others, use:

chmod o-w file1.txt

**Description of the Command:** The command chmod o-w file1.txt removes write permissions for others. After running the command, ls -l file1.txt would show:

-rw-rw-r-- 1 analyst users 1234 Sep 9 12:34 file1.txt

**3. Change File Permissions on a Hidden File**

**File Requiring Permission Modification:**

* **File:** .project\_x.txt
* **Requirement:** The file should not have write permissions for anyone, but should be readable by both the user and the group.

**Command to Change Permissions:** To ensure the file is readable but not writable, use:

chmod 644 .project\_x.txt

**Description of the Command:** The command chmod 644 .project\_x.txt sets permissions so:

* User: Read and write (rw-)
* Group: Read only (r--)
* Others: Read only (r--)

**Verification:** Check the permissions with:

ls -l .project\_x.txt

**Output:**

-rw-r--r-- 1 analyst users 5678 Sep 9 12:34 .project\_x.txt

**4. Change Directory Permissions**

**Directory Requiring Permission Modification:**

* **Directory:** /home/researcher2/projects/drafts
* **Requirement:** Only researcher2 should have access, with no permissions for the group or others.

**Command to Change Permissions:** To remove the execute permission for the group, use:

chmod g-x /home/researcher2/projects/drafts

**Description of the Command:** The command chmod g-x /home/researcher2/projects/drafts removes execute permissions for the group. Verify the change with:

ls -ld /home/researcher2/projects/drafts

**Output:**

drwx------ 2 researcher2 users 4096 Sep 9 12:34 /home/researcher2/projects/drafts

**Summary**

In this project, I examined and modified file and directory permissions to ensure that users and groups had the appropriate access levels according to security policies. I used commands like ls -la to check current permissions and chmod to update them. By following these steps, I helped secure the system by restricting unauthorized access and ensuring compliance with organizational security requirements.