Scenario

You are a security professional at a large organization. You mainly work with their research team. Part of your job is to ensure users on this team are authorized with the appropriate permissions. This helps keep the system secure.

Your task is to examine existing permissions on the file system. You'll need to determine if the permissions match the authorization that should be given. If they do not match, you'll need to modify the permissions to authorize the appropriate users and remove any unauthorized access.

Current file permissions

This displays the file structure of the `/home/researcher2/projects` directory and the permissions of the files and subdirectory it contains.

In the `/home/researcher2/projects` directory, there are five files with the following names and permissions:

- `project_k.txt`
  - User = read, write,
  - Group = read, write
  - Other = read, write
- `project_m.txt`
  - User = read, write
  - Group = read
  - Other = none
- `project_r.txt`
  - User= read, write
  - Group = read, write
  - Other = read
- `project_t.txt`
  - User = read, write
  - Group = read, write
  - Other = read
- `.project_x.txt`
  - User = read, write
  - Group = write
  - Other = none

There is also one subdirectory inside the `projects` directory named `drafts`. The permissions on `drafts` are:

- User = read, write, execute
- Group = execute
- Other = none

File permissions in Linux

Project description

Examine existing permissions on the file system to make sure they match what they are supposed to be.

Check file and directory details

```
researcher2@5d738f0f927b:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 15:27 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 15:27 ..
-rw--w---- 1 researcher2 research_team   46 Dec  2 15:27 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Dec  2 15:27 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Dec  2 15:27 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Dec  2 15:27 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 15:27 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 15:27 project_t.txt
researcher2@5d738f0f927b:~/projects$
```

Here you can see all the files and their current permissions. These were displayed using the `ls -la` command to show all the files including hidden ones and their details.

Describe the permissions string

In Linux, permission strings are 10-character sequences that indicate the access rights of files or directories. The first character shows the file type (d for directory, - for regular file), while the remaining nine characters represent read (r), write (w), and execute (x) permissions for the user, group, and others in respective sets of three (e.g., -rwxr-xr--). Each set of three characters determines the specific permissions granted to the user, group, and others. The 2-4th characters for the user, 5-7th are for the group, and 8-10th characters are for other.

Change file permissions

After reviewing the current permissions and what they were supposed to be, it was determined that the write permission should be removed from `project_k.txt` which can be done with the following command: `chmod o-w project_k.txt`

Change file permissions on a hidden file

After reviewing the hidden files it was found that the `.project_x.txt` file needs to have write permissions removed from the user and group permissions as well as adding read permissions to the group, this can be done with the following command: `chmod u-w, g-w, g+r .project_x.txt`

Change directory permissions

After reviewing the directory permissions it was revealed that the group had execute permission that need to be removed as only the user should have access to that directory, this can be done with the following command: `chmod g-x drafts`

Summary

In this project, we examined and adjusted file and directory permissions to ensure they matched the required settings. We used the `ls -la` command to display current permissions, then modified them accordingly. Permissions for `project_k.txt` were adjusted by removing write access for others. For the hidden file `.project_x.txt`, write permissions were removed for both user and group, while read permission was added for the group. Lastly, we removed execute permissions for the group on the `drafts` directory to restrict access. These changes help maintain the security and integrity of the file system.