Portfolio Document: Managing File Permissions in Linux

Introduction

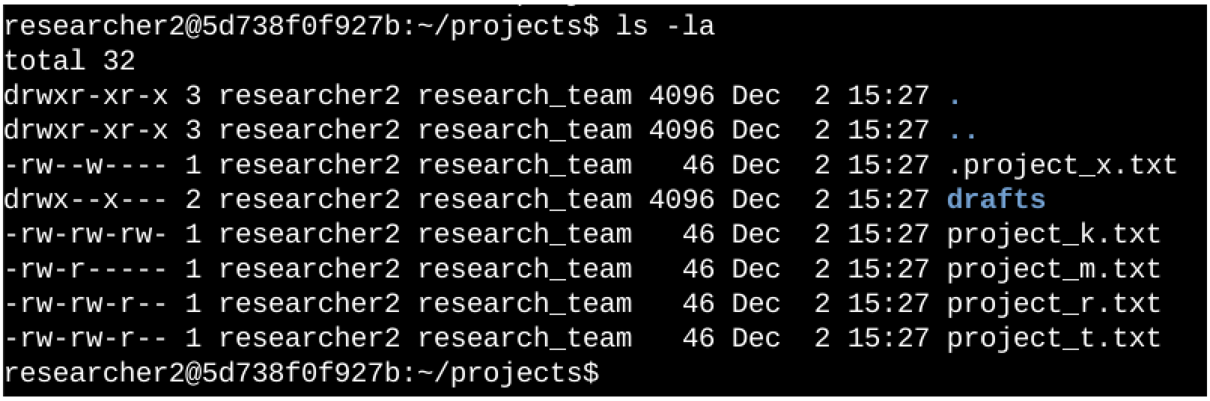
This portfolio document showcases my expertise in managing file permissions in Linux. As a cybersecurity professional, it is crucial to ensure that users have appropriate access permissions to maintain system security. This document provides a comprehensive overview of a scenario involving the examination and modification of file permissions, highlighting the commands used during this process.

Scenario

In this scenario, I work as a security professional in a large organization, primarily collaborating with the research team. My responsibility is to ensure that users within the team possess the correct authorization and access permissions. The goal is to align the existing permissions with the required authorizations, ensuring a secure system.

File and Directory Details

One of the key aspects of this scenario is the evaluation of existing permissions within the file system. To achieve this, I utilized Linux commands, providing a detailed listing of the contents, including hidden files, within the "projects" directory. The command used was ls -la as shown in the image below.



```
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$
```

This command revealed the contents, such as the "drafts" directory, the hidden file ".project_x.txt," and five other project files as shown in the image below The 10-character string in the first column signifies the permissions assigned to each file or directory.

Describe the Permissions String

The 10-character string can be deconstructed as follows:

1. The first character, either 'd' or '-', indicates the file type (directory or regular file).
2. The next three characters represent user permissions: read (r), write (w), and execute (x), or '-' if not granted.
3. The following three characters represent group permissions: read (r), write (w), and execute (x), or '-' if not granted.

4. The final three characters represent other user permissions: read (r), write (w), and execute (x), or '-' if not granted.

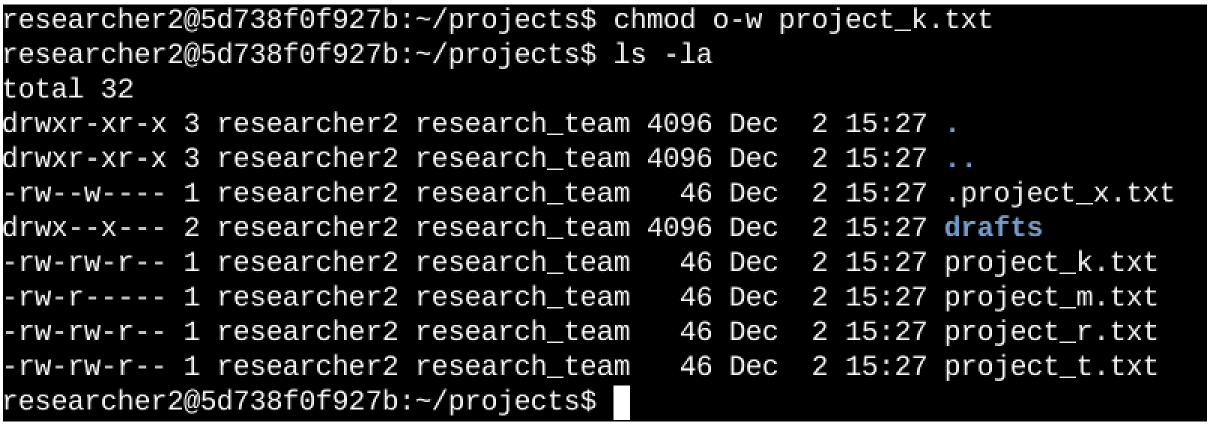
For example, the file permissions for "project_t.txt" are " -rw-rw-r--." This means that "project_t.txt" is a file, not a directory. The second, fifth, and eighth characters are 'r,' indicating read permissions for the user, group, and other. The third and sixth characters are 'w,' granting write permissions only to the user and the group. No one has execute permissions for "project_t.txt."

Change File Permissions

In response to the organization's requirement to restrict write access for "other" users, I reviewed the permissions. I identified "project_k.txt" as a file that required write access removal for "other." The following commands were executed:

```
chmod o-w project_k.txt
ls -la
```

The "chmod" command was used to remove write permissions from "other" for "project_k.txt." A subsequent listing with "ls -la" confirmed the successful permission change.



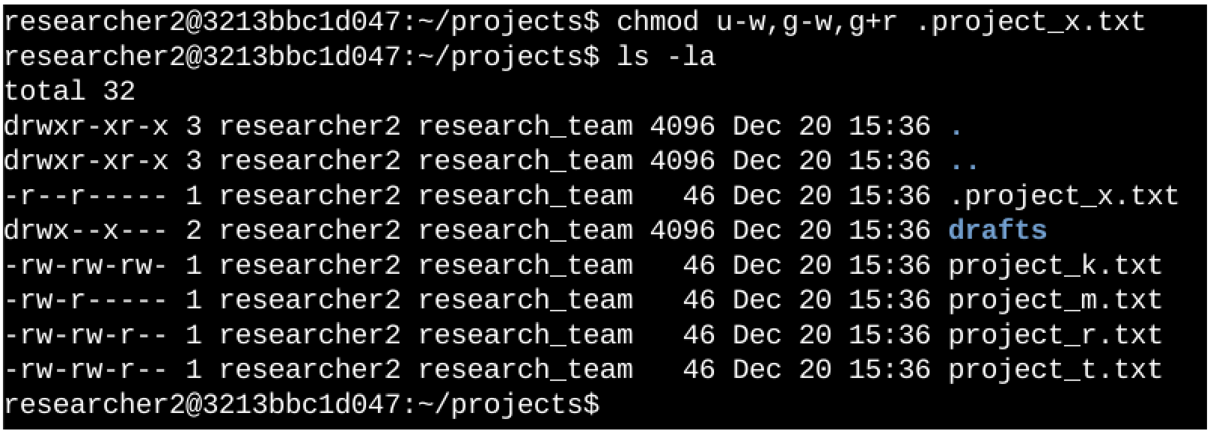
```
researcher2@5d738f0f927b:~/projects$ chmod o-w project_k.txt
researcher2@5d738f0f927b:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 15:27 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 15:27 ..
-rw--w---- 1 researcher2 research_team   46 Dec  2 15:27 .project_x.txt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

Change File Permissions on a Hidden File

The organization archived "project_x.txt" and necessitated that no one except the user and group should have read access to this file. I implemented the following commands:

```
chmod u-w,g-w g+r .project_x.txt
ls -la
```

These commands revoked write permissions from the user and group ("u-wg-w") while granting read permissions to the group ("g+r"). The changes were confirmed with "ls -la."



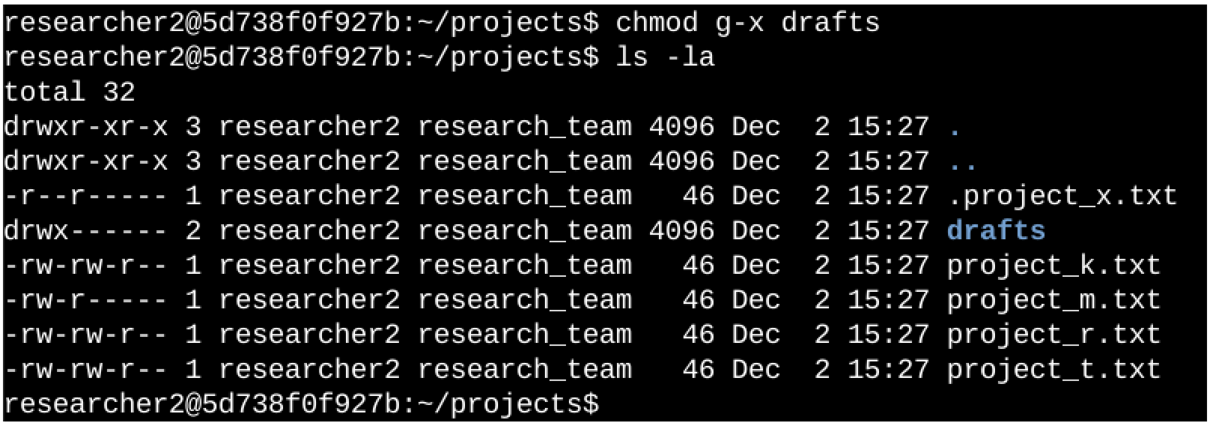
```
researcher2@3213bbc1d047:~/projects$ chmod u-w,g-w,g+r .project_x.txt
researcher2@3213bbc1d047:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Dec 20 15:36 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec 20 15:36 ..
-r--r----- 1 researcher2 research_team   46 Dec 20 15:36 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Dec 20 15:36 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Dec 20 15:36 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Dec 20 15:36 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec 20 15:36 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec 20 15:36 project_t.txt
researcher2@3213bbc1d047:~/projects$
```

Change Directory Permissions

The organization's requirement was to restrict access to the "drafts" directory and its contents to only the "researcher2" user, meaning that no one else should have execute permissions. I used the following commands:

```
chmod g-x drafts
ls -la
```

After identifying the group's execute permissions, I employed the "chmod" command to remove them, ensuring that only "researcher2" had execute permissions. A subsequent listing confirmed the permissions change.



```
researcher2@5d738f0f927b:~/projects$ chmod g-x drafts
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 ..
-r--r----- 1 researcher2 research_team   46 Dec  2 15:27 .project_x.txt
drwx------ 2 researcher2 research_team 4096 Dec  2 15:27 drafts
-rw-rw-r-- 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$
```

Summary

In this portfolio, I documented my process of modifying file and directory permissions to align with the organization's authorization requirements, ensuring system security. My initial step was to check the permissions using "ls -la," which served as a basis for subsequent actions. I effectively utilized the "chmod" command to make the necessary permissions adjustments.

By following these steps, I demonstrated my proficiency in managing Linux file permissions, a valuable skill in the field of cybersecurity.