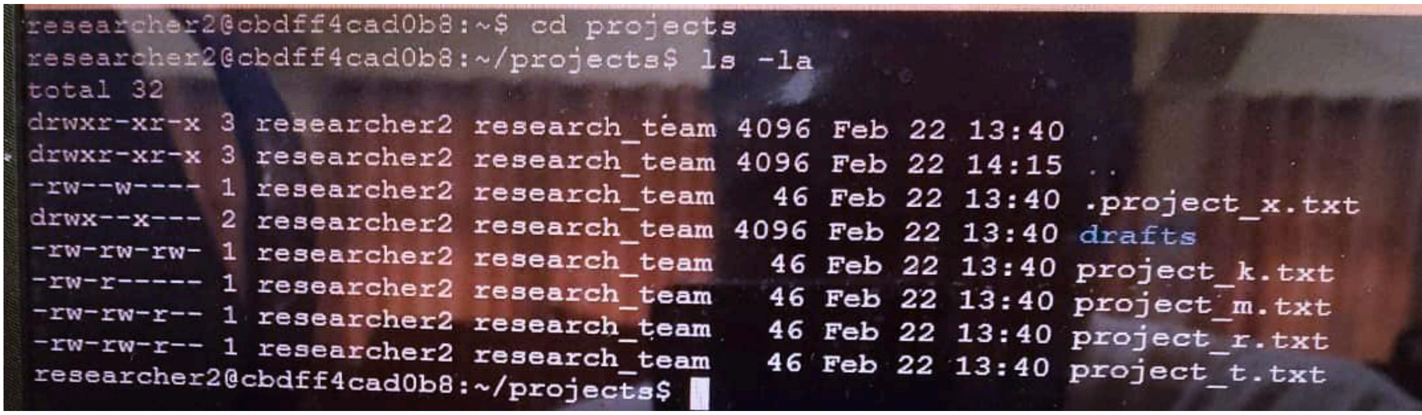
File permissions in Linux

Project description

As part of the Google Cybersecurity Professional Certificate, I completed a hands-on lab titled “Manage Authorization.” In this activity, I reviewed and updated file and directory permissions within the projects directory to ensure they reflected the appropriate level of access. Checking and updating these permissions helped reinforce proper access control and system security. To complete this task, I performed the following steps:

Check file and directory details

The following code demonstrates how I used Linux commands to determine the existing permissions set for a specific directory in the file system.



```
researcher2@cbdff4cad0b8:~$ cd projects
researcher2@cbdff4cad0b8:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Feb 22 13:40 .
drwxr-xr-x 3 researcher2 research_team 4096 Feb 22 14:15 ..
-rw--w---- 1 researcher2 research_team   46 Feb 22 13:40 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Feb 22 13:40 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Feb 22 13:40 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Feb 22 13:40 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb 22 13:40 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb 22 13:40 project_t.txt
researcher2@cbdff4cad0b8:~/projects$
```

The first line of the screenshot displays the command I entered, and the other lines display the output. The code lists all contents of the `projects` directory. I used the `ls` command with the `-la` option to display a detailed listing of the file contents that also returned hidden files. The output of my command indicates that there is one directory named `drafts`, one hidden file named `.project_x.txt`, and five other project files. The 10-character string in the first column represents the permissions set on each file or directory.

Describe the permissions string

The 10-character string identifies the file type and specifies access levels for the user, group, and other.
The characters and what they represent are as follows:

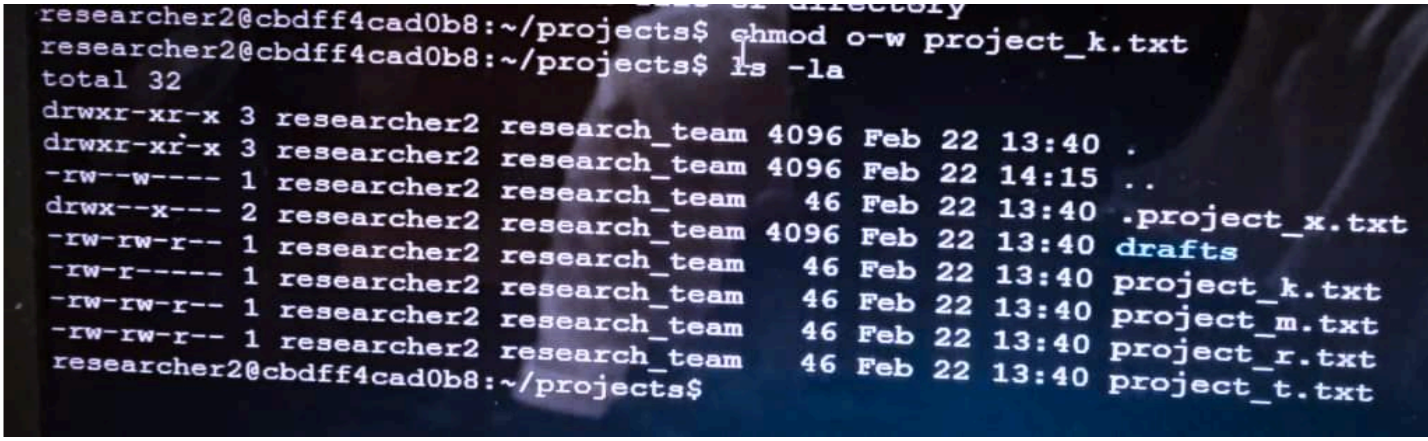
- **1st character**: This character is either a `d` or hyphen (`-`) and indicates the file type. If it's a `d`, it's a directory. If it's a hyphen (`-`), it's a regular file.
- **2nd-4th characters**: These characters indicate the read (`r`), write (`w`), and execute (`x`) permissions for the user. When one of these characters is a hyphen (`-`) instead, it indicates that this permission is not granted to the user.
- **5th-7th characters:** These characters indicate the read (`r`), write (`w`), and execute (`x`) permissions for the group. When one of these characters is a hyphen (`-`) instead, it indicates that this permission is not granted for the group.
- **8th-10th characters:** These characters indicate the read (`r`), write (`w`), and execute (`x`) permissions for other. This owner type consists of all other users on the system apart from the user and the group. When one of these characters is a hyphen (`-`) instead, that indicates that this permission is not granted for other.

For example, the file permissions for `project_t.txt` are `-rw-rw-r--`. Since the first character is a hyphen (`-`), this indicates that `project_t.txt` is a file, not a directory. The second, fifth, and eighth characters are all r, which indicates that user, group, and others all have read permissions. The third and sixth characters are `w`, which indicates that only the user and group have write permissions. No one has execute permissions for `project_t.txt`.

Change file permissions

In this Lab scenario, it was required that others should not have write access to any files. After reviewing the permissions, I determined that `project_k.txt` needed write access removed for other.

The following code demonstrates how I used Linux commands to do this:



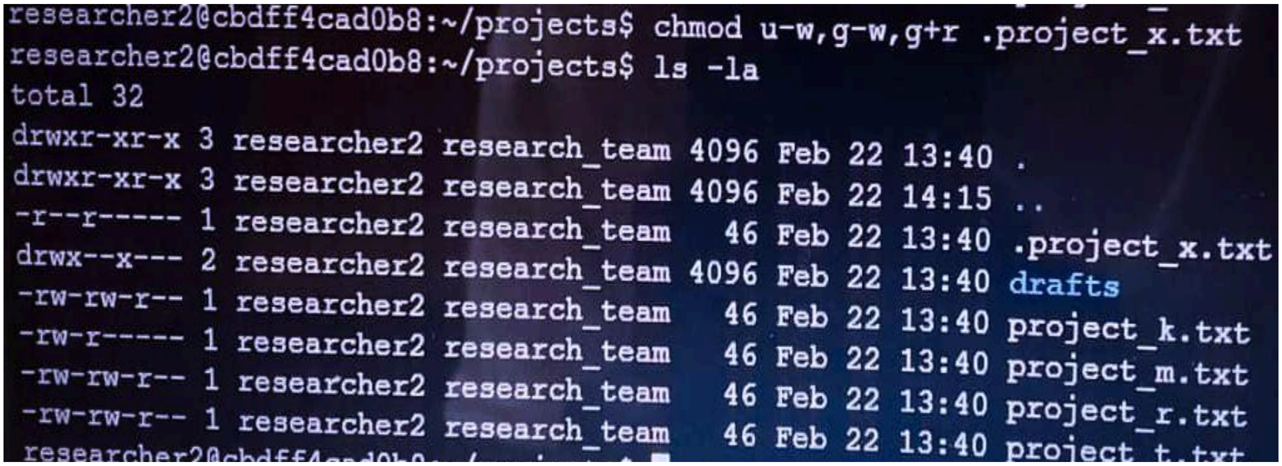
```
researcher2@cbdff4cad0b8:~/projects$ chmod o-w project_k.txt
researcher2@cbdff4cad0b8:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Feb 22 13:40 .
drwxr-xr-x 3 researcher2 research_team 4096 Feb 22 14:15 ..
-rw--w---- 1 researcher2 research_team   46 Feb 22 13:40 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Feb 22 13:40 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Feb 22 13:40 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Feb 22 13:40 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb 22 13:40 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb 22 13:40 project_t.txt
researcher2@cbdff4cad0b8:~/projects$
```

The first two lines of the screenshot display the commands I entered, and the other lines display the output of the second command. The `chmod` command changes the permissions on files and directories. The first argument indicates what permissions should be changed, and the second argument specifies the file or directory. In this example, I removed write permissions from other for the `project_k.txt` file. After this, I used `ls -la` to review the updates I made.

Change file permissions on a hidden file

In this Lab, .`project_x.txt` was archived and required restricted permissions. The task specified that no one should have write access, but the user and group should have read access.

The following code demonstrates how I used Linux commands to change the permissions:



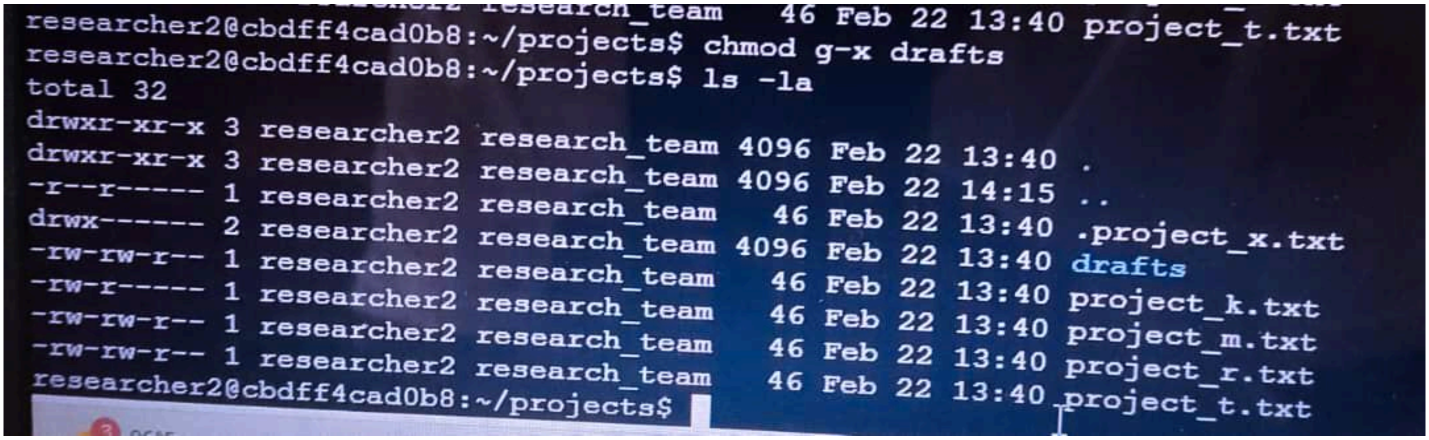
```
researcher2@cbdff4cad0b8:~/projects$ chmod u-w,g-w,g+r .project_x.txt
researcher2@cbdff4cad0b8:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Feb 22 13:40 .
drwxr-xr-x 3 researcher2 research_team 4096 Feb 22 14:15 ..
-r--r----- 1 researcher2 research_team   46 Feb 22 13:40 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Feb 22 13:40 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Feb 22 13:40 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Feb 22 13:40 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb 22 13:40 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb 22 13:40 project_t.txt
researcher2@cbdff4cad0b8:~/projects$
```

The first two lines of the screenshot display the commands I entered, and the other lines display the output of the second command. I know `.project_x.txt` is a hidden file because it starts with a period (`.`). In this example, I removed write permissions from the user and group, and added read permissions to the group. I removed write permissions from the user with `u-w`. Then, I removed write permissions from the group with `g-w`, and added read permissions to the group with `g+r`.

Change directory permissions

The Lab required that only the `researcher2` user should have access to the `drafts` directory and its contents. No other users or groups were permitted to execute files within that directory.

The following code demonstrates how I used Linux commands to change the permissions:



```
            researcher2 research_team   46 Feb 22 13:40 project_t.txt
researcher2@cbdff4cad0b8:~/projects$ chmod g-x drafts
researcher2@cbdff4cad0b8:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Feb 22 13:40 .
drwxr-xr-x 3 researcher2 research_team 4096 Feb 22 14:15 ..
-r--r----- 1 researcher2 research_team   46 Feb 22 13:40 .project_x.txt
drwx------ 2 researcher2 research_team 4096 Feb 22 13:40 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Feb 22 13:40 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Feb 22 13:40 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb 22 13:40 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb 22 13:40 project_t.txt
researcher2@cbdff4cad0b8:~/projects$
```

After reviewing the directory permissions, I used the `chmod` command to remove execute permissions from the group while ensuring that the required user retained access. I then confirmed the updated permissions using `ls -la`.

Summary

In this Lab activity, I reviewed and modified file and directory permissions to ensure proper authorization settings within a Linux environment. I used the `ls -la` command to examine existing permissions and the `chmod` command to make necessary changes.
This activity strengthened my understanding of Linux file permissions, access control, and secure system configuration as part of the Google Cybersecurity Professional Certificate program.