File permissions in Linux

Scenario description

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.

Check file and directory details

```
researcher2@de4c59915b15:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 May 25 22:55 .
drwxr-xr-x 3 researcher2 research_team 4096 May 25 23:02 ..
-rw--w---- 1 researcher2 research_team   46 May 25 22:55 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 May 25 22:55 drafts
-rw-rw-rw- 1 researcher2 research_team   46 May 25 22:55 project_k.txt
-rw-r----- 1 researcher2 research_team   46 May 25 22:55 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 May 25 22:55 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 May 25 22:55 project_t.txt
researcher2@de4c59915b15:~/projects$
```

In this step, we used the command shown on the first line. Basically, we are telling the OS to show all the files within the current directory and also to show all the auth information of each file/directory (-l), even if they're hidden (-a).

Describe the permissions string

Let's take the "draft" directory as an example to explain the permissions string. The first char tells us that this element is a directory 'd', then the char from the 2th to the 4th position is about the permissions for the current user which tells us that is has all possible permissions like read, write and execute, the next 3 are for group permissions and the last 3 are for other permissions. As we can see, groups and others have only the execute permissions.

Change file permissions

```
researcher2@de4c59915b15:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 May 25 22:55 .
drwxr-xr-x 3 researcher2 research_team 4096 May 25 23:02 ..
-rw--w---- 1 researcher2 research_team   46 May 25 22:55 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 May 25 22:55 drafts
-rw-rw-rw- 1 researcher2 research_team   46 May 25 22:55 project_k.txt
-rw-r----- 1 researcher2 research_team   46 May 25 22:55 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 May 25 22:55 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 May 25 22:55 project_t.txt
researcher2@de4c59915b15:~/projects$ chmod o-w project_k.txt
researcher2@de4c59915b15:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 May 25 22:55 .
drwxr-xr-x 3 researcher2 research_team 4096 May 25 23:02 ..
-rw--w---- 1 researcher2 research_team   46 May 25 22:55 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 May 25 22:55 drafts
-rw-rw-r-- 1 researcher2 research_team   46 May 25 22:55 project_k.txt
-rw-r----- 1 researcher2 research_team   46 May 25 22:55 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 May 25 22:55 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 May 25 22:55 project_t.txt
researcher2@de4c59915b15:~/projects$
```

Removed the write permissions to the other, since the organization does not allow others to have write access to any files. The command used for this was the following:

- **chmod o-w project_k.txt**

Change file permissions on a hidden file

```
researcher2@de4c59915b15:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 May 25 22:55 .
drwxr-xr-x 3 researcher2 research_team 4096 May 25 23:02 ..
-rw--w---- 1 researcher2 research_team   46 May 25 22:55 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 May 25 22:55 drafts
-rw-rw-r-- 1 researcher2 research_team   46 May 25 22:55 project_k.txt
-rw-r----- 1 researcher2 research_team   46 May 25 22:55 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 May 25 22:55 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 May 25 22:55 project_t.txt
researcher2@de4c59915b15:~/projects$ chmod g+r, g-w, u-w .project_x.txt
chmod: invalid mode: 'g+r,'
Try 'chmod --help' for more information.
researcher2@de4c59915b15:~/projects$ chmod g+r,g-w,u-w .project_x.txt
researcher2@de4c59915b15:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 May 25 22:55 .
drwxr-xr-x 3 researcher2 research_team 4096 May 25 23:02 ..
-r--r----- 1 researcher2 research_team   46 May 25 22:55 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 May 25 22:55 drafts
-rw-rw-r-- 1 researcher2 research_team   46 May 25 22:55 project_k.txt
-rw-r----- 1 researcher2 research_team   46 May 25 22:55 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 May 25 22:55 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 May 25 22:55 project_t.txt
researcher2@de4c59915b15:~/projects$
```

We removed the write permissions to user and group and added only read to both since this file should not have write permissions for anyone, but the user and group should be able to read the file. The command used for this was the following:

- **chmod g+r,g-w,u-w .project_x.txt**

Change directory permissions

```
researcher2@de4c59915b15:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 May 25 22:55 .
drwxr-xr-x 3 researcher2 research_team 4096 May 25 23:02 ..
-r--r----- 1 researcher2 research_team   46 May 25 22:55 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 May 25 22:55 drafts
-rw-rw-r-- 1 researcher2 research_team   46 May 25 22:55 project_k.txt
-rw-r----- 1 researcher2 research_team   46 May 25 22:55 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 May 25 22:55 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 May 25 22:55 project_t.txt
researcher2@de4c59915b15:~/projects$ chmod g-x drafts
researcher2@de4c59915b15:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 May 25 22:55 .
drwxr-xr-x 3 researcher2 research_team 4096 May 25 23:02 ..
-r--r----- 1 researcher2 research_team   46 May 25 22:55 .project_x.txt
drwx------ 2 researcher2 research_team 4096 May 25 22:55 drafts
-rw-rw-r-- 1 researcher2 research_team   46 May 25 22:55 project_k.txt
-rw-r----- 1 researcher2 research_team   46 May 25 22:55 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 May 25 22:55 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 May 25 22:55 project_t.txt
researcher2@de4c59915b15:~/projects$
```

We removed the permission to any other than researcher 2, since drafts should only be accessible to researcher 2. The command used for this was the following:

- **chmod g-x drafts**

Project Description

- Secured file system access for a research team using Linux.
- Reviewed and modified file and directory permissions.
- Ensured only authorized users had appropriate access.

Tasks

- Checked Permissions
    - Used ls -la to list all files, including hidden, with full details.
    - Interpreted 10-character permission strings in draft as an example.
- Modified File Permissions
    - Removed write access for others:
      chmod o-w project_k.txt
    - Set read-only for user and group on hidden file:
      chmod g+r,g-w,u-w .project_x.txt
- Modified Directory Permissions
    - Removed group access to restrict directory:
      chmod g-x drafts

Summary

- Reviewed current permissions using ls -la.
- Used chmod to restrict unauthorized access.
- Protected sensitive data by enforcing least-privilege access.