File permissions in Linux

Project description

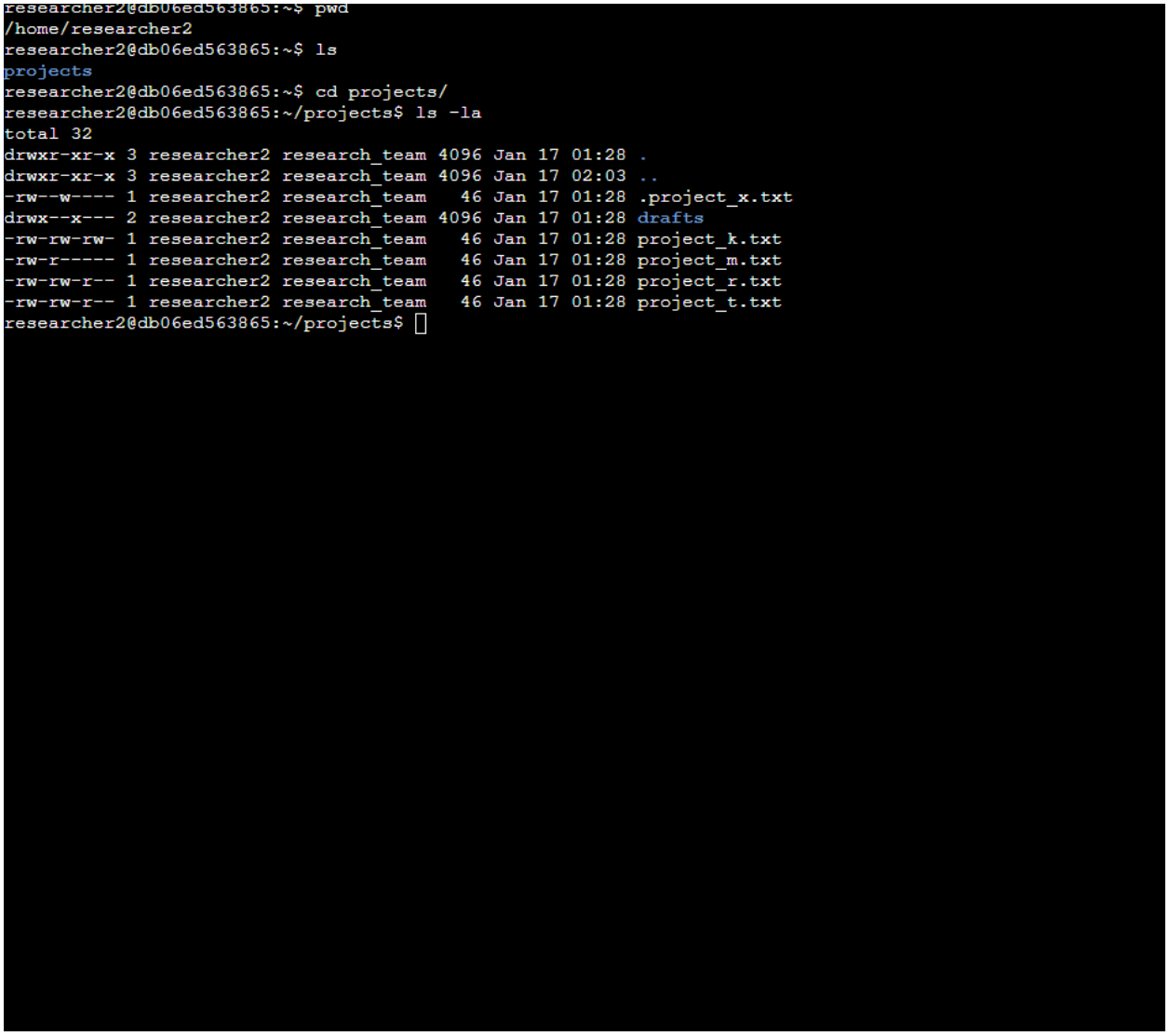
This scenario project will demonstrate my knowledge and case use of Linux commands, specifically user and file permissions in Linux.

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

To check for file and directory permissions, ls -la can be used. The command also lists permissions of hidden files and directories.



Describe the permissions string

If we look at the permissions for the drafts directory, there is a 10 character string that represents permissions. The first character signifies that it is a directory, represented by the letter “d”. Files do not have a letter, they are instead represented as “-”, this means it is a file or if it is found outside the first index of characters, it represents as an empty permission. These are the permissions for the drafts directory.

drwx - - x - - -

After the letter indicating the type of file/directory, the three letters represent read = r, write = w, executable = x.

- **read**: for files, this is the ability to read the file contents; for directories, this is the ability to read all contents in the directory including both files and subdirectories

- **write**: for files, this is the ability to make modifications on the file contents; for directories, this is the ability to create new files in the directory

- **execute**: for files, this is the ability to execute the file if it's a program; for directories, this is the ability to enter the directory and access its files

There are three groups that can be set/configured for permissions, the first group is the user, then the groups, lastly the last group is others.
We can see that the drafts directory has the user group with permissions r,w,x. Groups have executable permissions and others have none.

Change file permissions

Let's change the permissions of the drafts directory so that groups does not have executable permissions. To change permissions, make sure you have root user permissions by using sudo, chmod changes permissions on files or directories.

```
researcher2@db06ed563865:~/projects$ sudo chmod g-x drafts
researcher2@db06ed563865:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan 17 01:28 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan 17 02:03 ..
-rw--w---- 1 researcher2 research_team   46 Jan 17 01:28 .project_x.txt
drwx------ 2 researcher2 research_team 4096 Jan 17 01:28 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Jan 17 01:28 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Jan 17 01:28 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jan 17 01:28 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jan 17 01:28 project_t.txt
researcher2@db06ed563865:~/projects$
```

The first command in this screenshot shows the command to change the permissions for the directory "drafts". First we are using root permissions using sudo, the arguments show that groups, represented by "g" is losing executable permissions shown with the mathematical operator "-" and then "x".

Change file permissions on a hidden file

Files or directories with a period in front of their name, means the file or directory is hidden and will not show normally when entering the command ls. We can change the permissions the same way, we just add the period like it is shown.

```
researcher2@db06ed563865:~/projects$ sudo chmod g-w .project_x.txt
researcher2@db06ed563865:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan 17 01:28 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan 17 02:03 ..
-rw------- 1 researcher2 research_team   46 Jan 17 01:28 .project_x.txt
```

Summary

This project showcases an understanding of Linux file and directory permissions within a security-focused scenario. A security professional evaluates and adjusts file system permissions to ensure authorized access, using commands like `ls -la` to inspect permissions and `chmod` to modify them. Key concepts include interpreting the permission string and differentiating between user, group, and others' access levels.