# Exemplar: Manage authorization

# Overview: Authorization is the concept of granting access to specific resources in a system. It's important because without authorization any user could access and modify all files belonging to other users or system files. This would certainly be a security risk.

# In Linux, file and directory permissions are used to specify who has access to specific files and directories. You’ll explore file and directory permissions and change the ownership of a file and a directory to limit who can access them. As a security analyst, setting appropriate access permissions is critical to protecting sensitive information and maintaining the overall security of a system.

# Scenario: The researcher2 user is part of the research\_team group. In this scenario, you must examine and manage the permissions on the files in the /home/researcher2/projects directory for the researcher2 user.

# Here’s how you’ll do this task: **First**, you’ll check the user and group permissions for all files in the projects directory. **Next**, you’ll check whether any files have incorrect permissions and change the permissions as needed. **Finally**, you’ll check the permissions of the /home/researcher2/projects/drafts directory and modify these permissions to remove any unauthorized access.

**Start your lab:** click on “start lab” to start the lab.

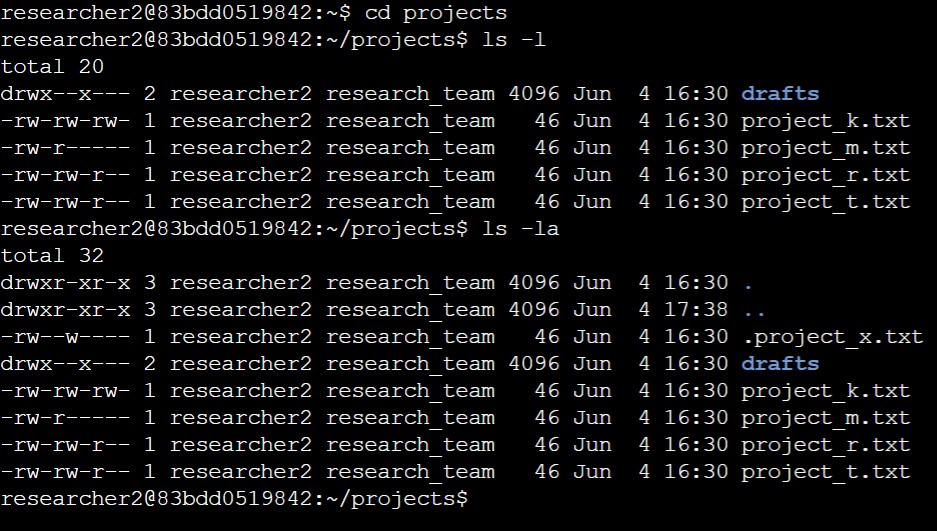
**Task 1. Check file and directory details**

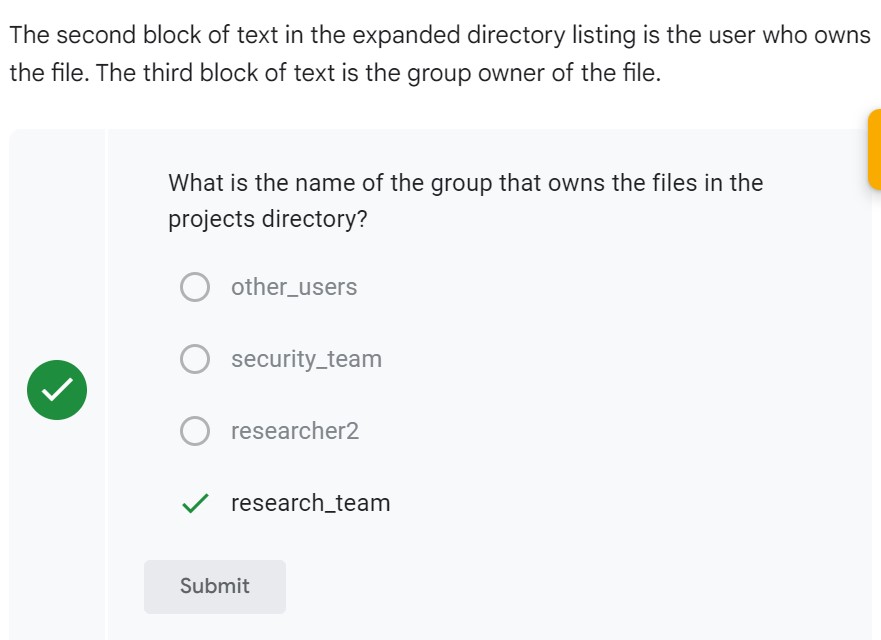
In this task, you must explore the permissions of the projects directory and the files it contains. The lab starts with /home/researcher2 as the current working directory. This is because you're changing permissions for files and directories belonging to the researcher2 user.

1. Navigate to the projects directory.

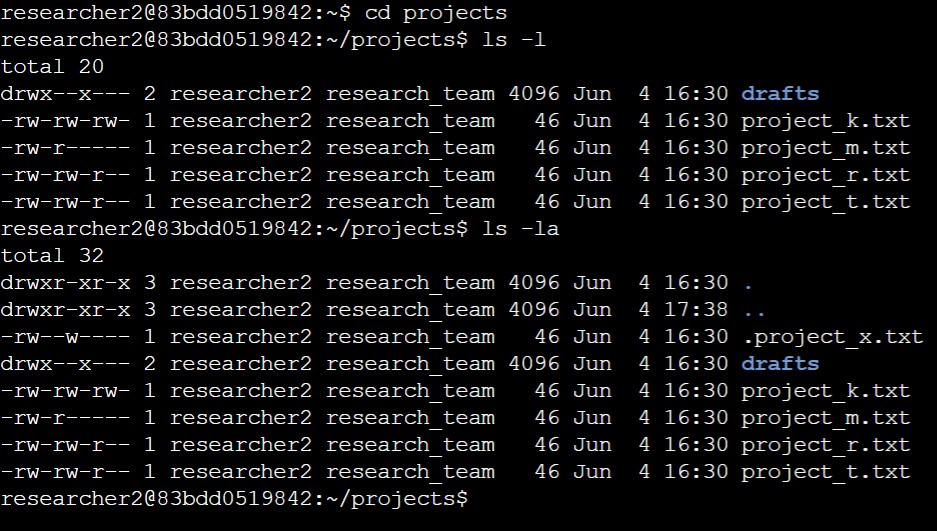
**$cd projects**

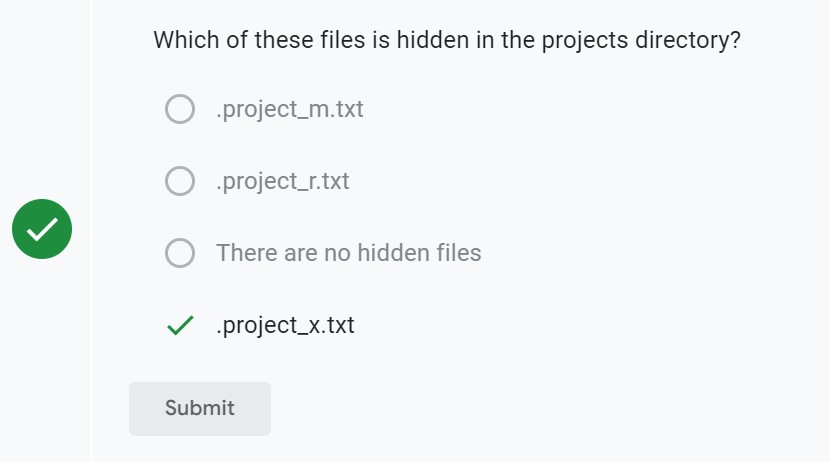
1. List the contents and permissions of the projects directory.

**$ls -l**



1. Check whether any hidden files exist in the projects directory.

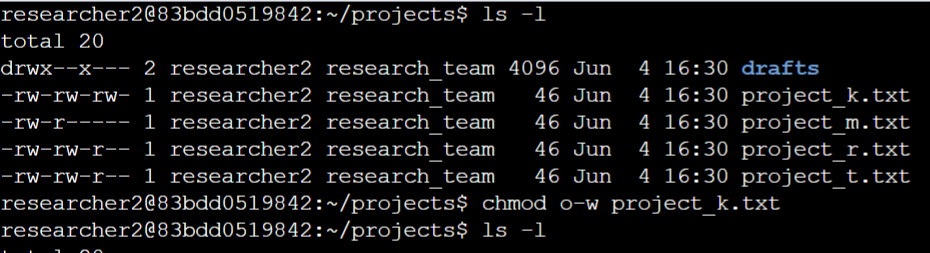
**$ls –la**



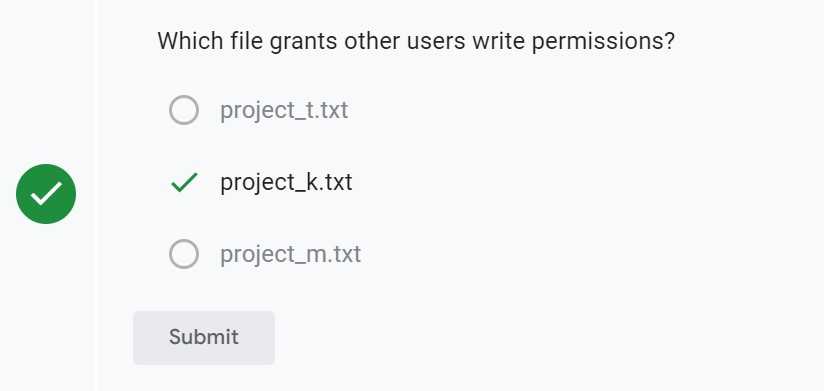
**Task 2. Change file permissions**

In this task, you must determine whether any files have incorrect permissions and then change the permissions as needed. This action will remove unauthorized access and strengthen security on the system.

1. Check whether any files in the projects directory have write permissions for the owner type of other.

**$ls -l**

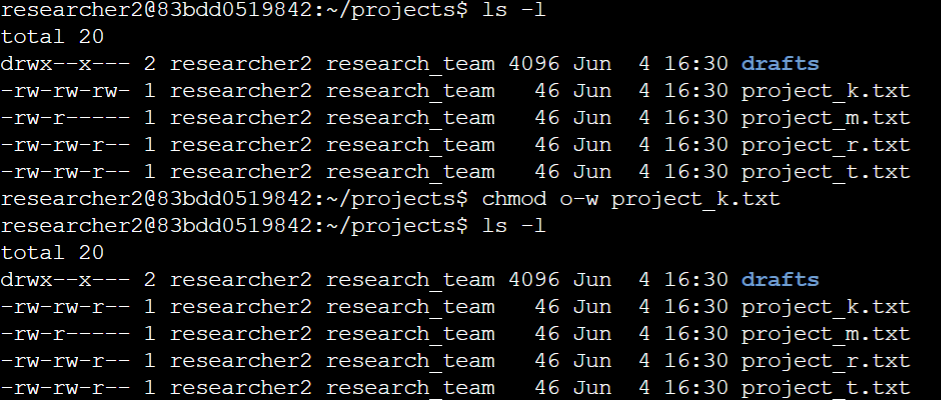
Here we can observe that project\_k.txt has write permission to others.

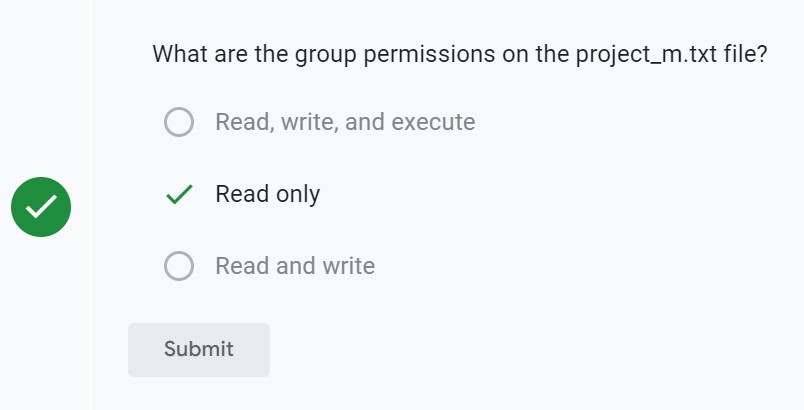


1. Change the permissions of the file identified in the previous step so that the owner type of other doesn’t have write permissions.

**$chmod o-w project\_k.txt**

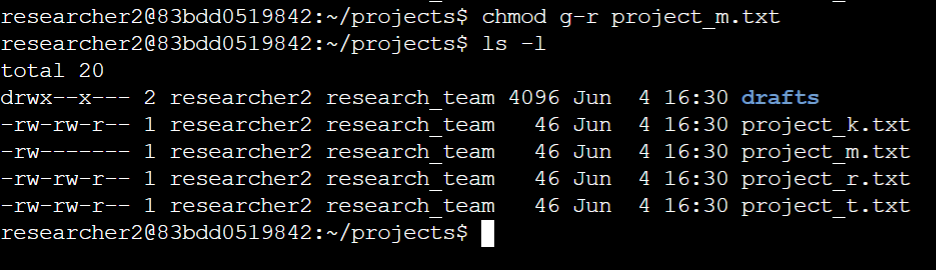
1. List the contents and permissions of the current directory and check if the group has read or write permissions.

**$ls –l**



1. Use the chmod command to change permissions of the project\_m.txt file so that the group doesn’t have read or write permissions.

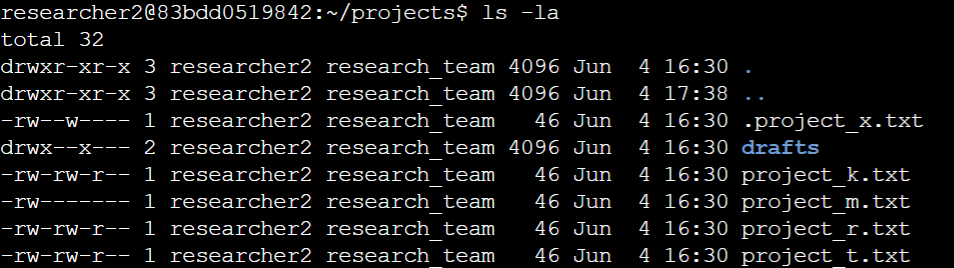
**$chmod g-r project\_m.txt**

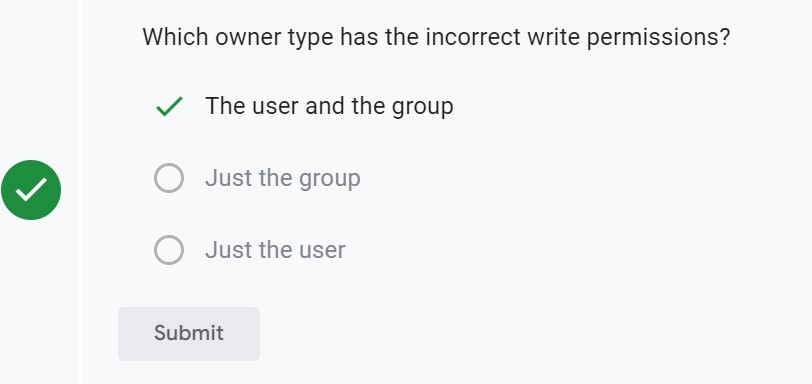
**$ls –l**

**Task 3. Change file permissions on a hidden file**

In this task, you must determine if a hidden file has incorrect permissions and then change the permissions as needed. This action will further remove unauthorized access and strengthen security on the system. The file .project\_x.txt is a hidden file that has been archived and should not be written to by anyone. (The user and group should still be able to read this file.)

1. Check the permissions of the hidden file .project\_x.txt and answer the question that follows.

**$ls -la**



1. Change the permissions of the file .project\_x.txt so that both the user and the group can read, but not write to, the file.

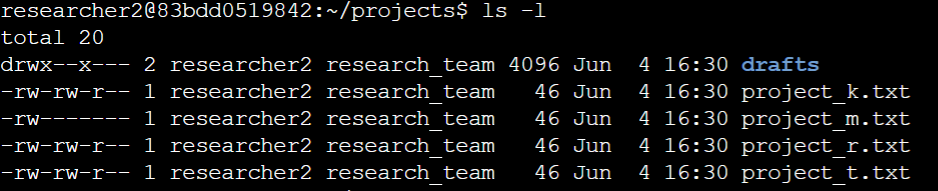
**$chmod u-w,g-w,g+r .project\_x.txt**

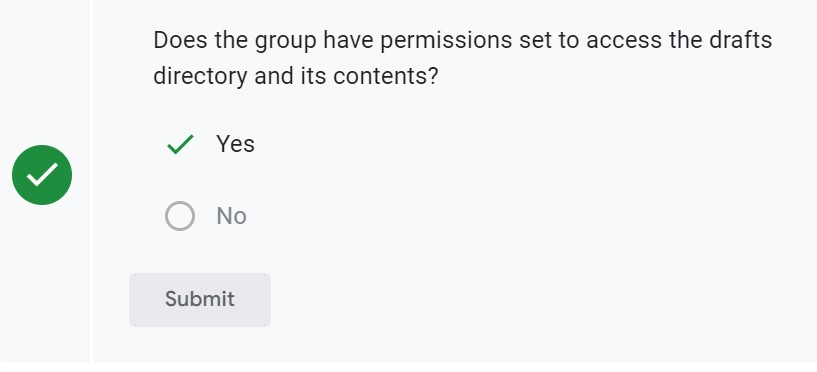
**$ls –la**

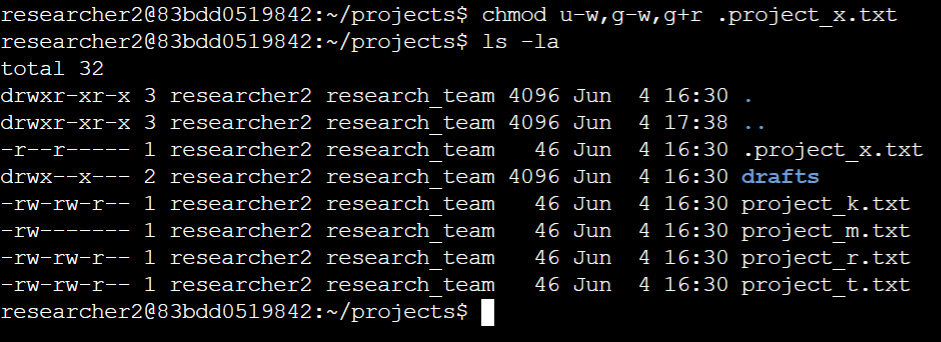
**Task 4. Change directory permissions**

In this task, you must change the permissions of a directory. First, you’ll check the group permissions of the /home/researcher2/projects/drafts directory and then modify the permissions as required. (You should be in the projects directory while managing the permissions of its subdirectory drafts.). Only the researcher2 user should be allowed to access the drafts directory and its contents. (This means that only researcher2 should have execute privileges.)

1. Check the permissions of the drafts directory and answer the following question.

**$ls -l**

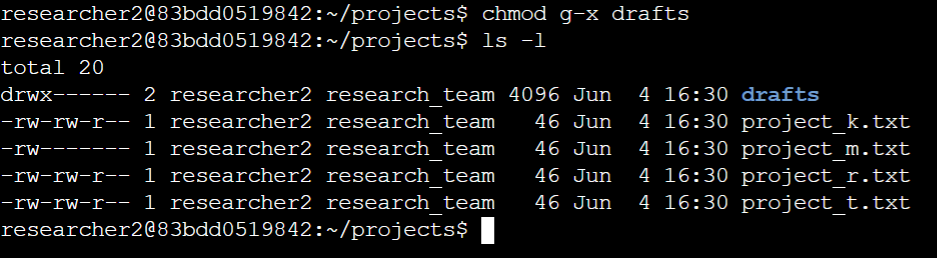




1. Remove the execute permission for the group from the drafts directory.

**$chmod g-x drafts**

**$ls –l**



**Conclusion:**

You now have practical experience in using basic Linux Bash shell commands to

* examine file and directory permissions,
* change permissions on files, and
* change permissions on directories.