Using Linux CLI to Manage File Permissions

A penguin with yellow feet

Description automatically generated

Material & instructions developed by: Google Cybersecurity Professional Certificate Course

Completed by: Alexander Herman on 01/26/24

**Table of Contents:**

Scenario (Provided): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2**

Step-By-Step Instructions (Provided): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2**

Instruction Output (My Work): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2-4**

Summary (My Work): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**4**

**Scenario**

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.

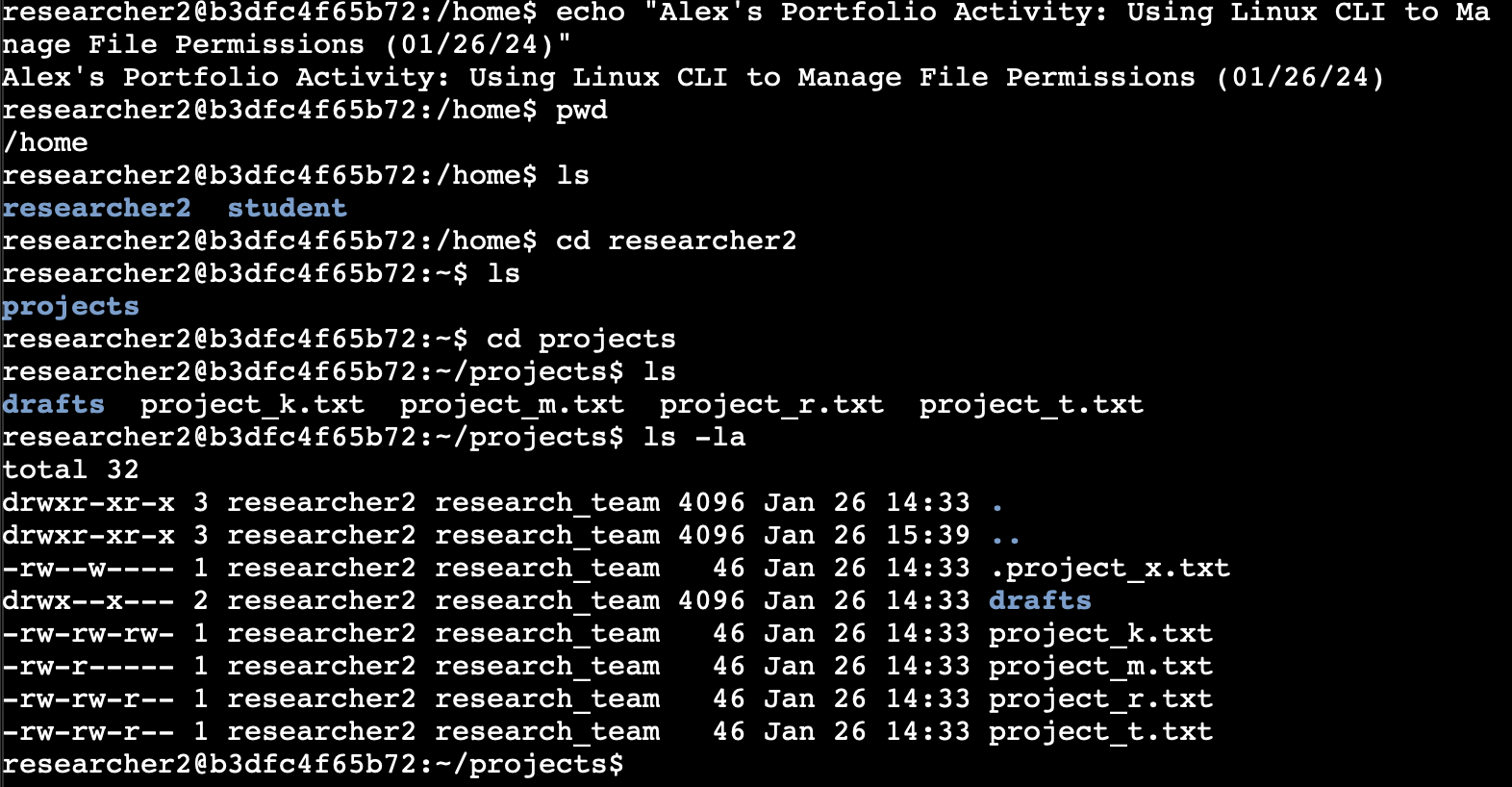
Your task is to examine existing permissions on the file system. You’ll need to determine if the permissions match the authorization that should be given. If they do not match, you’ll need to modify the permissions to authorize the appropriate users and remove any unauthorized access.

**Step-By-Step Instructions**

1. Check file and directory details
2. Describe one of the permission strings
3. Change file permissions
4. Change file permissions on a hidden file
5. Change directory permissions
6. Summary

**Instruction Output**

1. **Check file and directory details:** for projects in reseacher2



1. **Describe one of the permission strings**

Looking at the permissions for “drafts” it appears that it is another directory indicated by the “d” at the beginning of the string. Following the “d”, it has the letters “r, w, x” is straight succession indicating that the user has all three permissions to read, write, and execute. The only other letter that appears in the string is an “x” in the group area indicate that the group has execute permissions, which could be an error in need of correction.

1. **Change file permissions:** the organization does not allow other to have write access to any files

A screenshot of a computer program

Description automatically generated

1. **Change file permissions on a hidden file: “**.project\_x.txt” should not have write permissions for anyone, but the user and group should be able to read the file

A screenshot of a computer

Description automatically generated

1. **Change directory permissions:** only researcher2 should be allowed access to the “drafts” directory and its contents

**A screenshot of a computer

Description automatically generated**

**Summary**

In summation, I used the Linux CLI to review files and directories under the user researcher2 and change permissions to limit access. The major commands I used were “ls -la” to list the (viewable & hidden) files/directories with their permission strings, as well as “chmod” to change the permissions to restrict access within the three owner types.