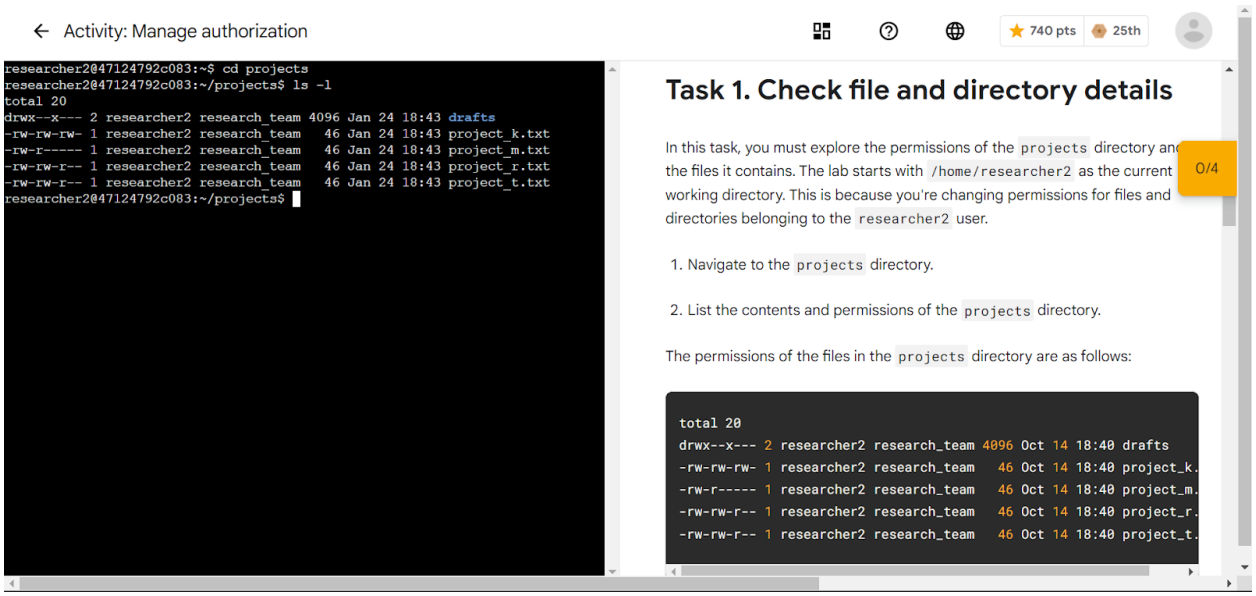
File permissions in Linux

Project description

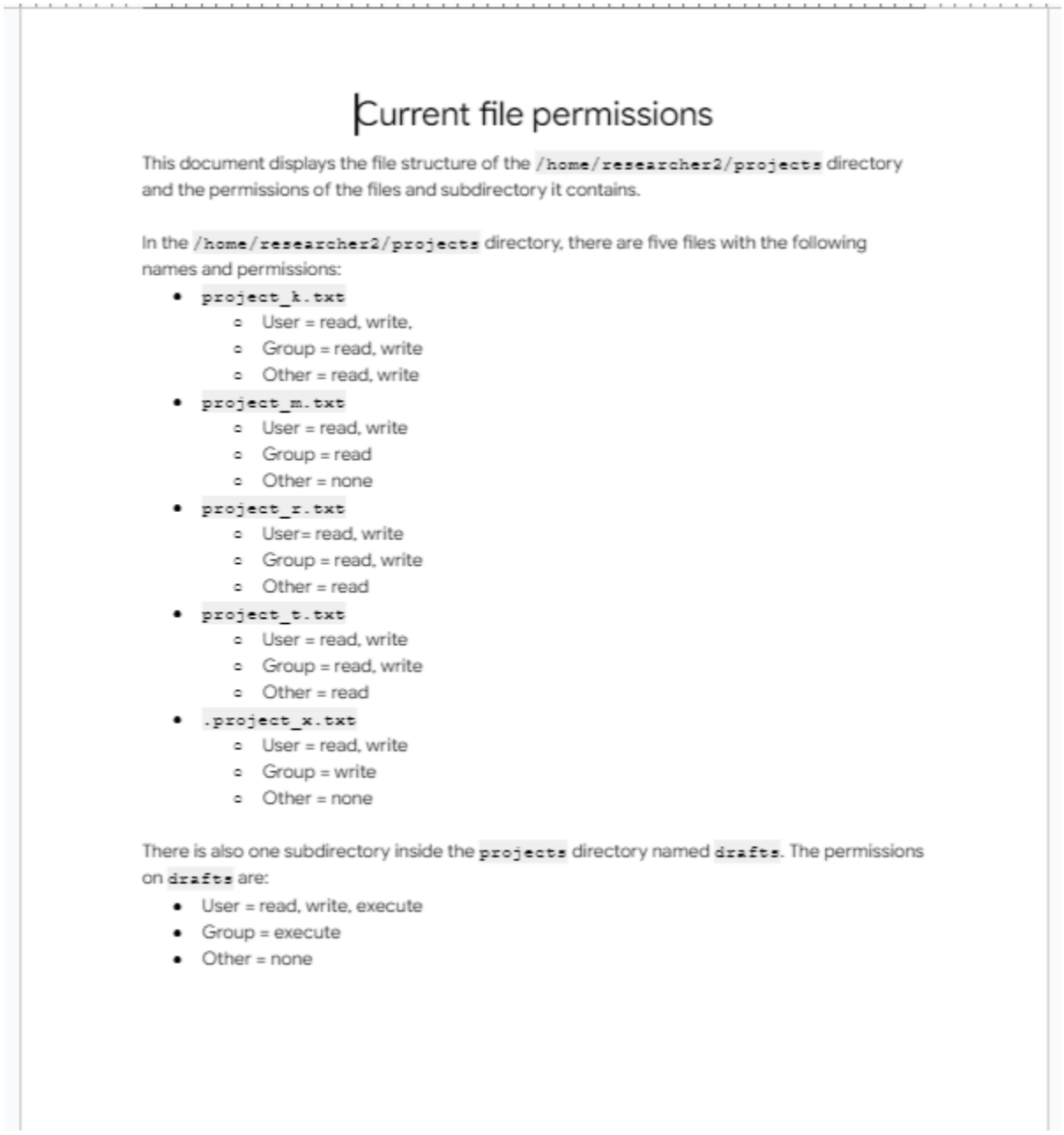
As a security analyst, I'm tasked with making sure the correct permissions are in place for all users, groups, and others.

Check file and directory details



First, a security analyst should check to see what permissions are in place for everyone. When using Linux, ls -l will allow the user to see everyones permissions in a directory.

Describe the permissions string



Current file permissions

This document displays the file structure of the `/home/researcher2/projects` directory and the permissions of the files and subdirectory it contains.

In the `/home/researcher2/projects` directory, there are five files with the following names and permissions:

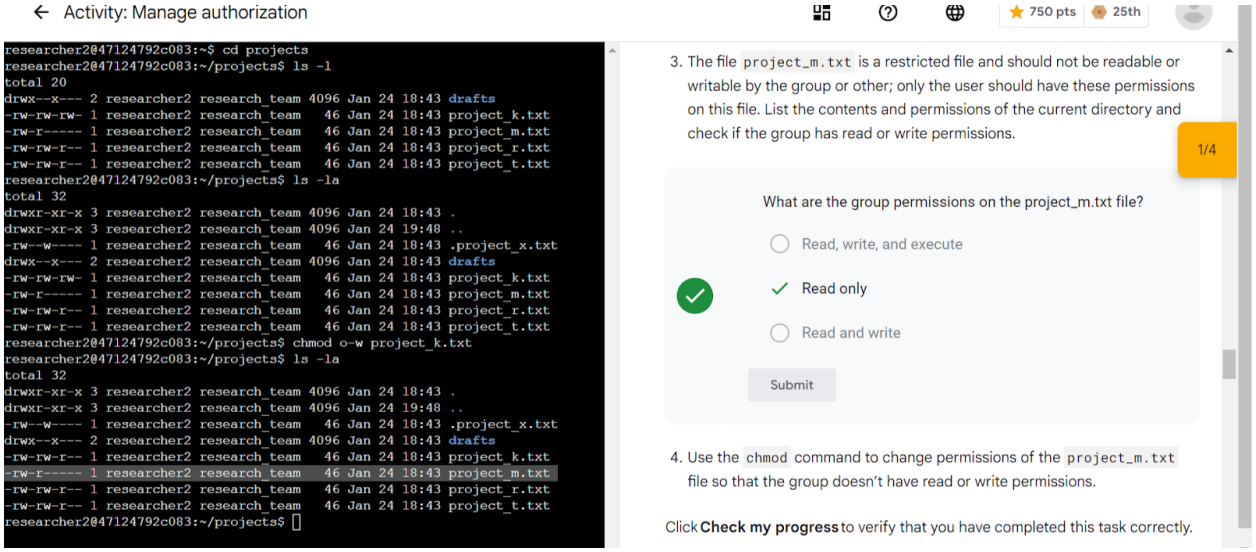
- `project_k.txt`
  - User = read, write,
  - Group = read, write
  - Other = read, write
- `project_m.txt`
  - User = read, write
  - Group = read
  - Other = none
- `project_r.txt`
  - User= read, write
  - Group = read, write
  - Other = read
- `project_t.txt`
  - User = read, write
  - Group = read, write
  - Other = read
- `.project_x.txt`
  - User = read, write
  - Group = write
  - Other = none

There is also one subdirectory inside the `projects` directory named `drafts`. The permissions on `drafts` are:

- User = read, write, execute
- Group = execute
- Other = none

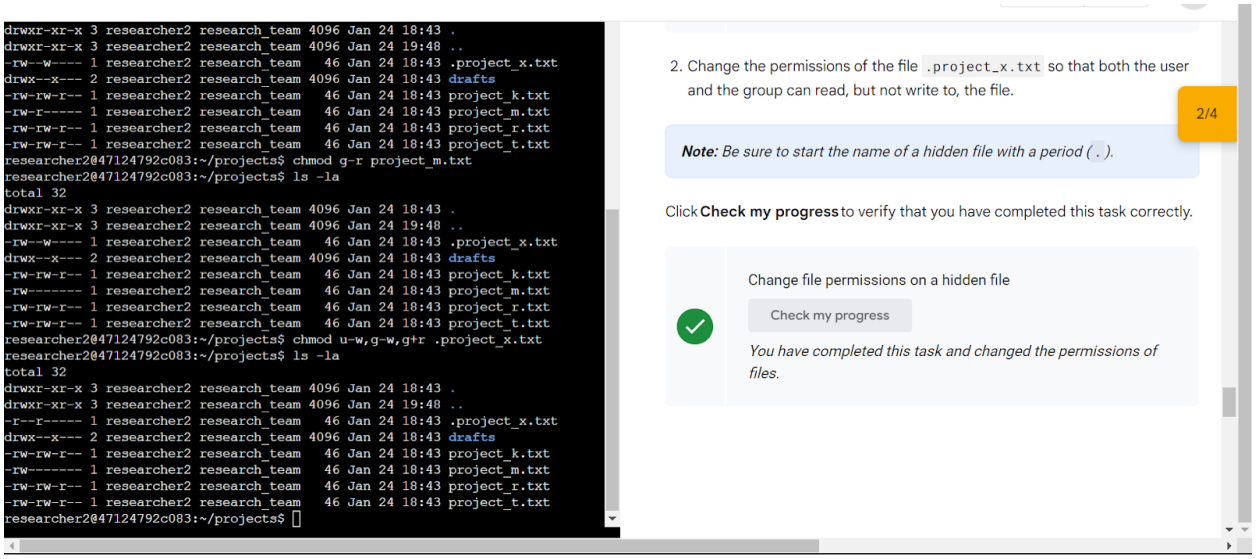
Permission strings are used to describe who can view and make changes to what material. When reading linux, the 10 strings of letter/dashes will represent what level of authority a user has. The first string will be the directory. The 2-4th strings will represent the users. 5th-7th is in charge of the groups. Lastly, the 8th-10th describe others' permissions.

Change file permissions



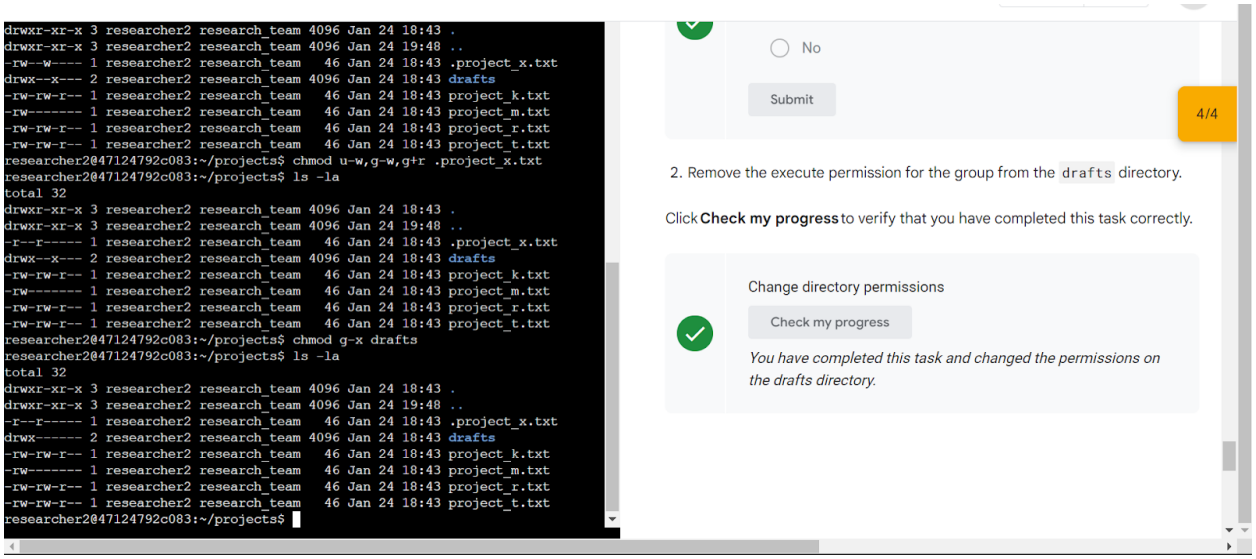
Changing the permissions for a file/directory requires the use of *chmod* in linux and then adding or subtracting the level of access the user requires.

Change file permissions on a hidden file



When a file is hidden, it can be found in Linux with the ls -la command. Using the prior commands to add or remove permissions is the same when working with hidden files. Only difference would be adding a period before the hidden file. For example, *chmod u-w .project_x.txt*.

Change directory permissions



Changing the directory permissions utilizes the same format except.

Summary

The company needed to make sure *researcher2* had the appropriate permissions for each file. Checking the work after each addition and removal of permissions is advised to make sure it's done correctly. Properly set up permissions leads to good least privileges principles in cybersecurity.