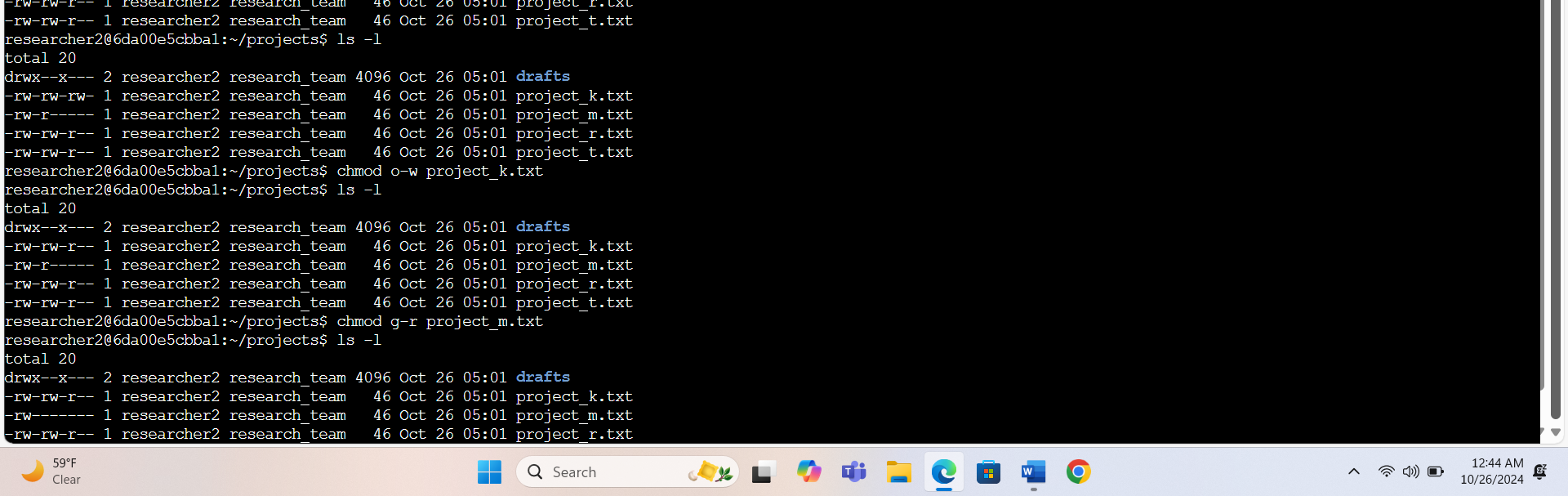
# File permissions in Linux (**Hands-on LAB)**

## Project description

In this **project (LAB),** I focused on understanding and managing file permissions within a Linux environment, a crucial skill in the field of cybersecurity. I completed a series of tasks aimed at enhancing my knowledge of access control mechanisms, which are vital for protecting sensitive data and ensuring system integrity. My key objectives are to Changing File Permissions: I learned how to modify file permissions using the *chmod* command. This involved setting appropriate read, write, and execute permissions for files to ensure that users have the necessary access while maintaining security protocols. Managing Hidden Files: I explored how file permissions apply to hidden files (those beginning with a dot). I practiced changing permissions on these files to understand the implications of their visibility and accessibility in a Linux system. Adjusting Directory Permissions: I also gained hands-on experience in changing permissions for directories. This included configuring permissions that control access to the directory contents, which is essential for maintaining secure file organization and user access rights.

## Check file and directory details

**The following code demonstrates how I used Linux commands to determine the existing permissions set for a specific directory in the file system.

## The first line of the screenshot displays the command I entered, and the other lines display the output. The code lists all contents of the projects directory. I used the ls command with the -la option to display a detailed listing of the file contents that also returned hidden files. The output of my command indicates that there is one directory named drafts, one hidden file named .project\_x.txt, and five other project files. The 10-character string in the first column represents the permissions set on each file or directory

The 10-character string can be deconstructed to determine who is authorized to access the file and their specific permissions. The characters and what they represent are as follows:

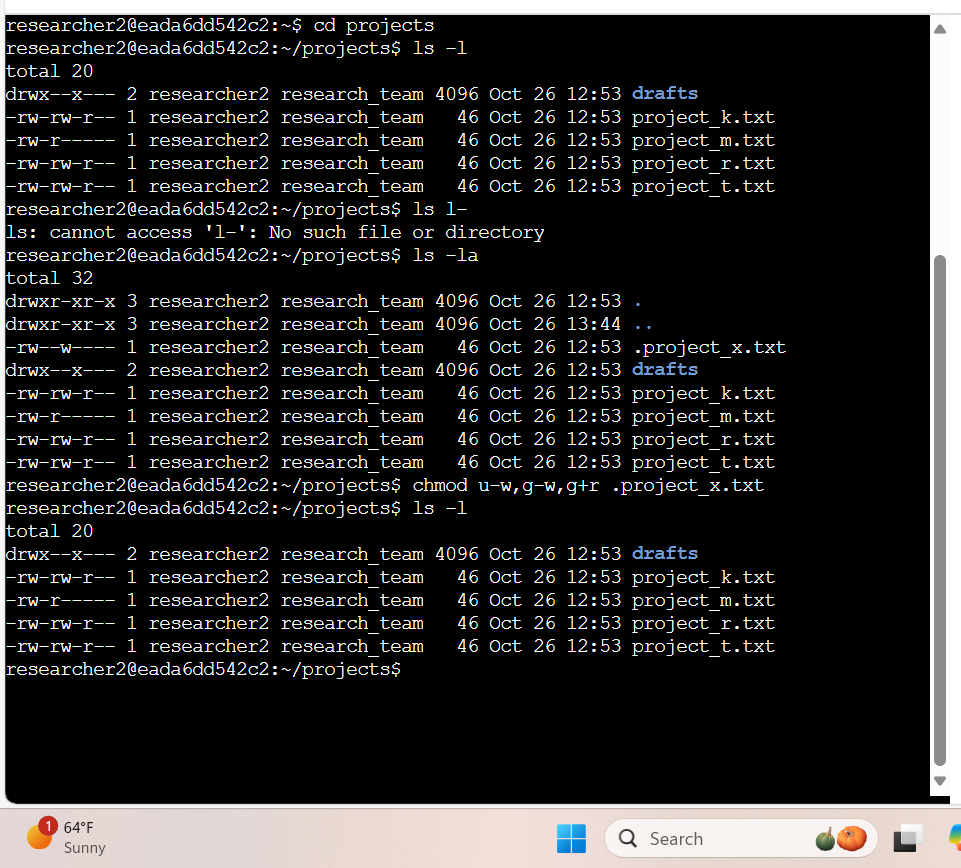
* **1st character**: This character is either a d or hyphen (-) and indicates the file type. If it’s a d, it’s a directory. If it’s a hyphen (-), it’s a regular file.
* **2nd-4th characters**: These characters indicate the read (r), write (w), and execute (x) permissions for the user. When one of these characters is a hyphen (-) instead, it indicates that this permission is not granted to the user.
* **5th-7th characters:** These characters indicate the read (r), write (w), and execute (x) permissions for the group. When one of these characters is a hyphen (-) instead, it indicates that this permission is not granted for the group.
* **8th-10th characters:** These characters indicate the read (r), write (w), and execute (x) permissions for other. This owner type consists of all other users on the system apart from the user and the group. When one of these characters is a hyphen (-) instead, that indicates that this permission is not granted for other.

For example, the file permissions for project\_t.txt are -rw-rw-r--. Since the first character is a hyphen (-), this indicates that project\_t.txt is a file, not a directory. The second, fifth, and eighth characters are all r, which indicates that user, group, and other all have read permissions. The third and sixth characters are w, which indicates that only the user and group have write permissions. No one has execute permissions for project\_t.txt.

## Change file permissions

The organization determined that other shouldn't have write access to any of their files. To comply with this, I referred to the file permissions that I previously returned. I determined project\_k.txt must have the write access removed for other.

The following code demonstrates how I used Linux commands to do this:

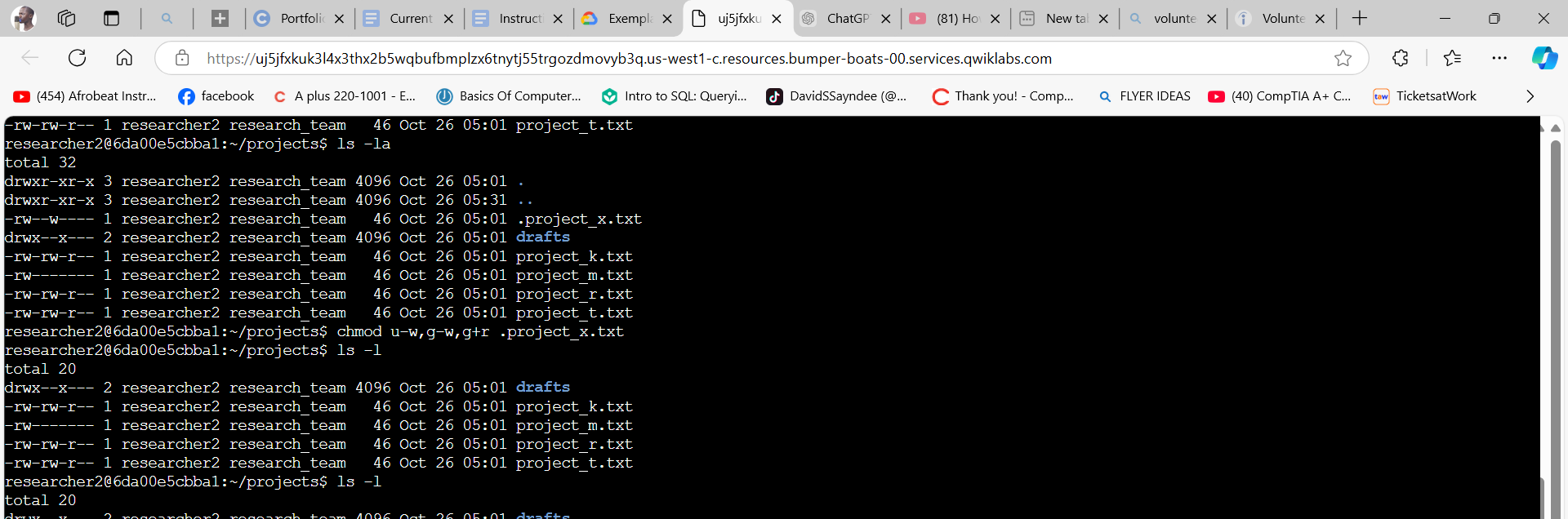


## 

The first two lines of the screenshot display the commands I entered, and the other lines display the output of the second command. The chmod command changes the permissions on files and directories. The first argument indicates what permissions should be changed, and the second argument specifies the file or directory. In this example, I removed write permissions from other for the project\_k.txt file. After this, I used ls -la to review the updates I made.

## Change file permissions on a hidden file

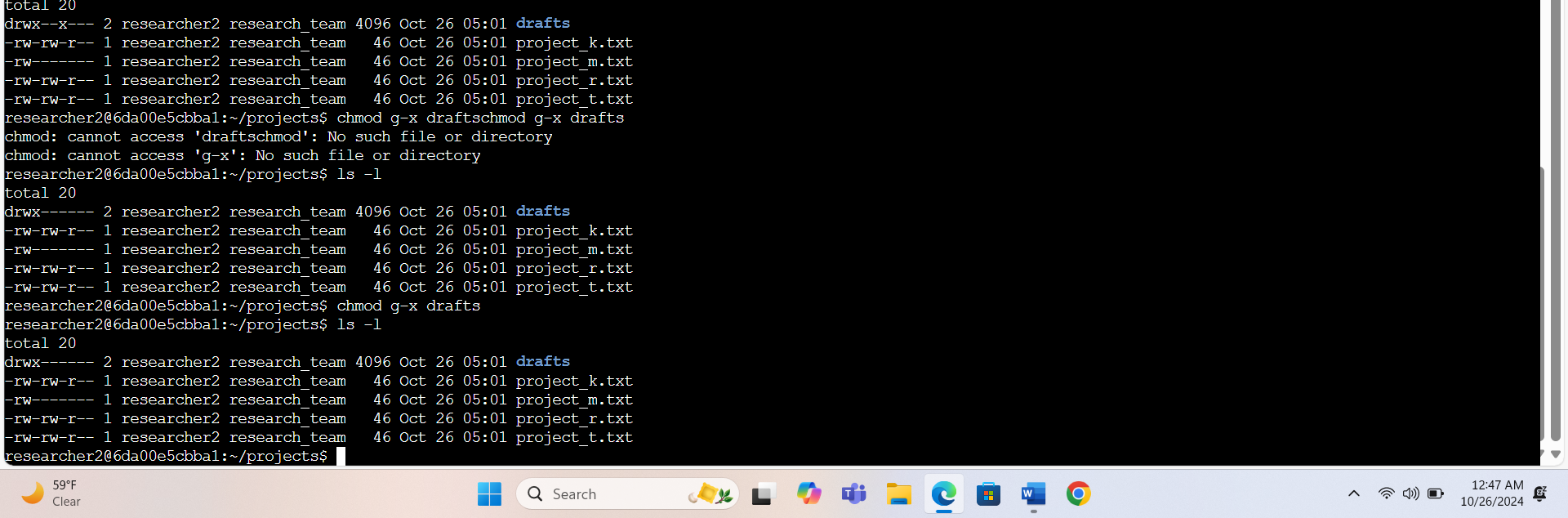
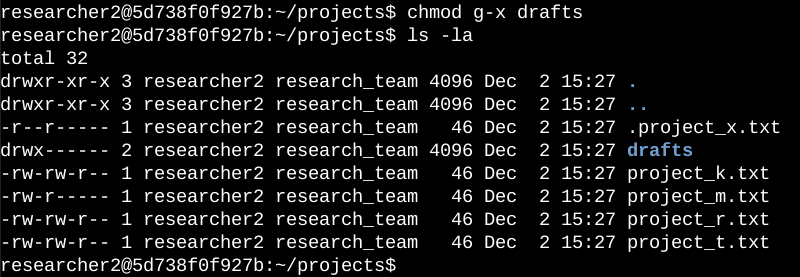
The research team at my organization recently archived project\_x.txt. They do not want anyone to have write access to this project, but the user and group should have read access.

**The following code demonstrates how I used Linux commands to change the permissions:

The first two lines of the screenshot display the commands I entered, and the other lines display the output of the second command. I know .project\_x.txt is a hidden file because it starts with a period (.). In this example, I removed write permissions from the user and group, and added read permissions to the group. I removed write permissions from the user with u-w. Then, I removed write permissions from the group with g-w, and added read permissions to the group with g+r.

## Change directory permissions

My organization only wants the researcher2 user to have access to the drafts directory and its contents. This means that no one other than researcher2 should have execute permissions. The following code demonstrates how I used Linux commands to change the permissions:



The first two lines of the screenshot display the commands I entered, and the other lines display the output of the second command. I previously determined that the group had execute permissions, so I used the chmod command to remove them. The researcher2 user already had execute permissions, so they did not need to be added.

## Summary

I changed multiple permissions to match the level of authorization my organization wanted for files and directories in the projects directory. The first step in this was using ls -la to check the permissions for the directory. This informed my decisions in the following steps. I then used the chmod command multiple times to change the permissions on files and directories.

This project has equipped me with practical skills in managing file permissions, reinforcing my understanding of cybersecurity principles, and preparing me for real-world scenarios in securing Linux environments. I gained insights into the three levels of access, owner, group, and others. The skills I developed include proficiency in using the Linux command line for file management.Understanding of Linux file permission structure, including user, group, and other classifications.Insight into the importance of file permissions in protecting sensitive information and securing systems against unauthorized access.