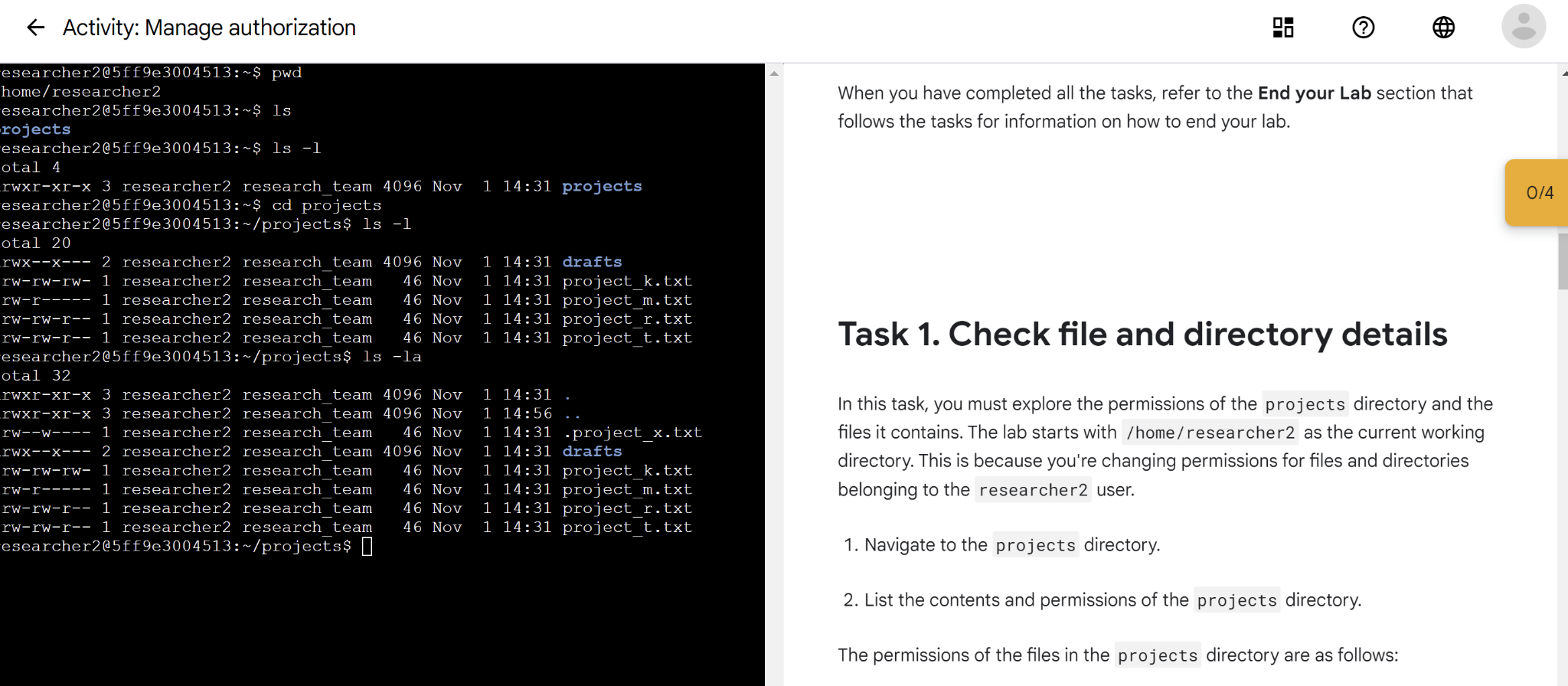
# Olajide Usman

# File permissions in Linux

## Project description

[To demonstrate the use of commands to modify file and directory permissions in Linux Os]

## Check file and directory details



## Describe the permissions string

Permission string is a10 character string assigning permissions to files and directories

d - directory

rwx - read, write and execute for user

rwx - read, write and execute for groups

rwx - read, write and execute for other users

## Change file permissions

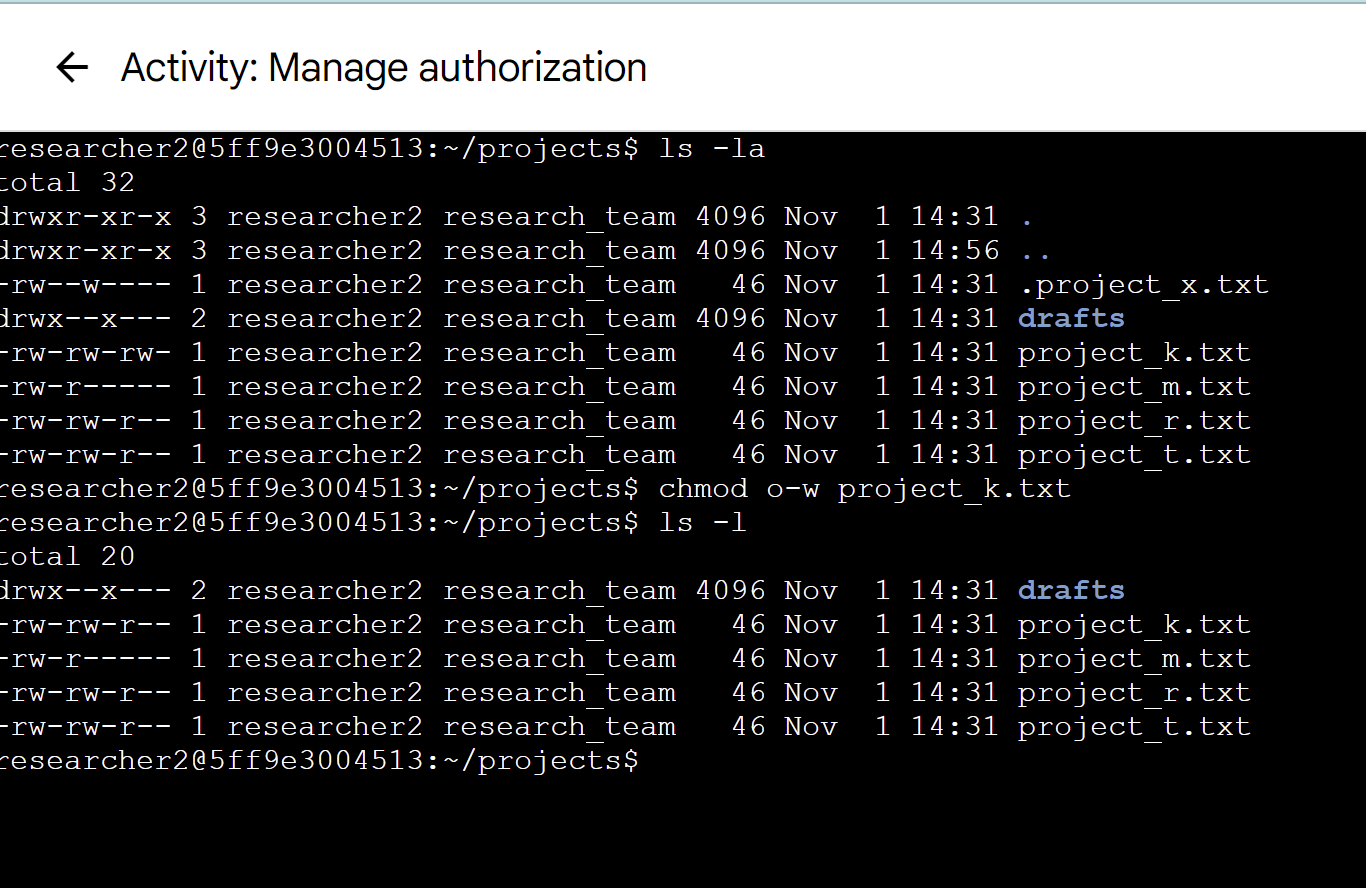
The chmod (change mode) command is used to change or modify file or directory permission. It is used alongside some parameters liek

u -user

g -group

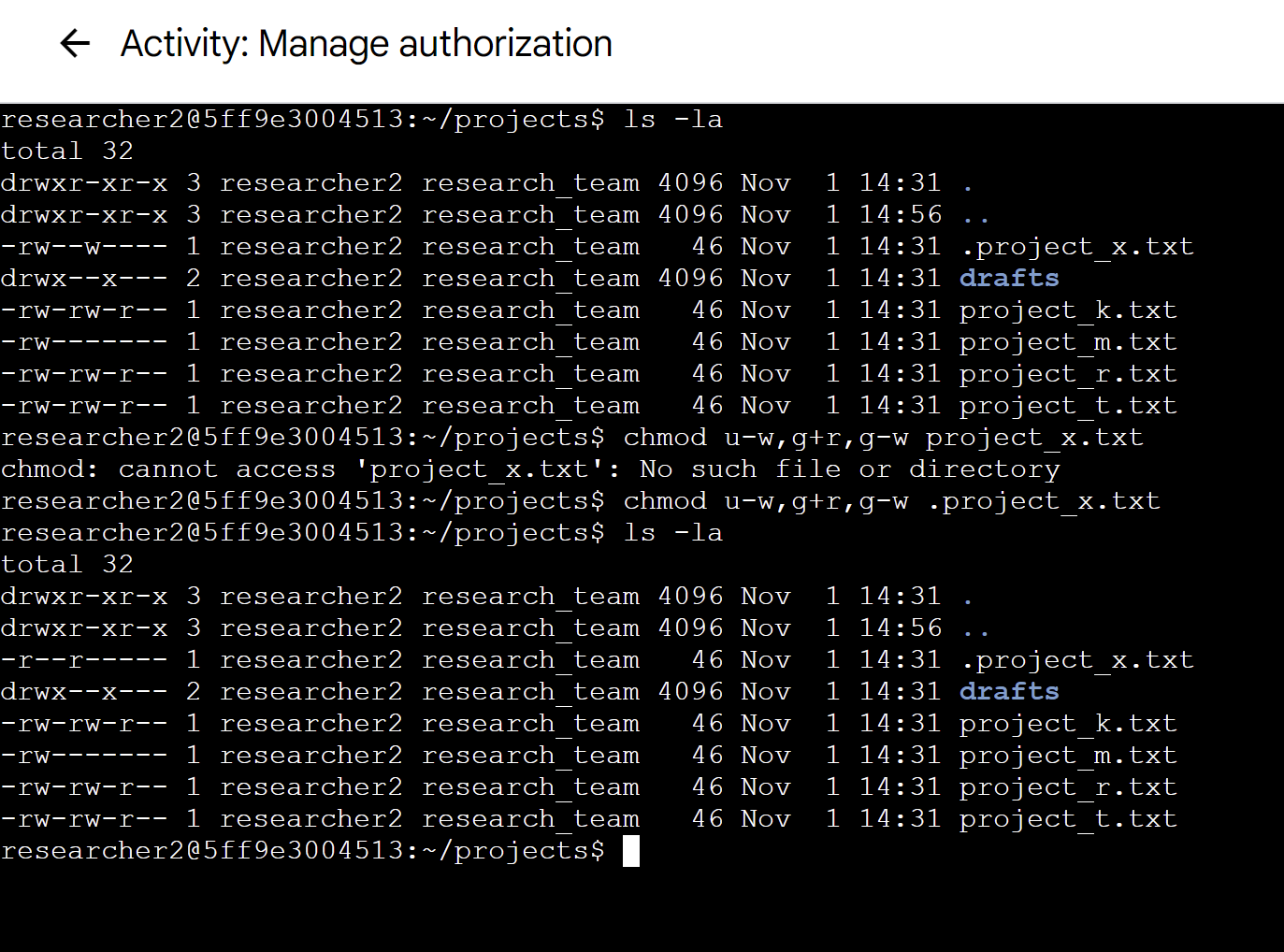
o -other users

* Means to add a permission while - means to remove a permission

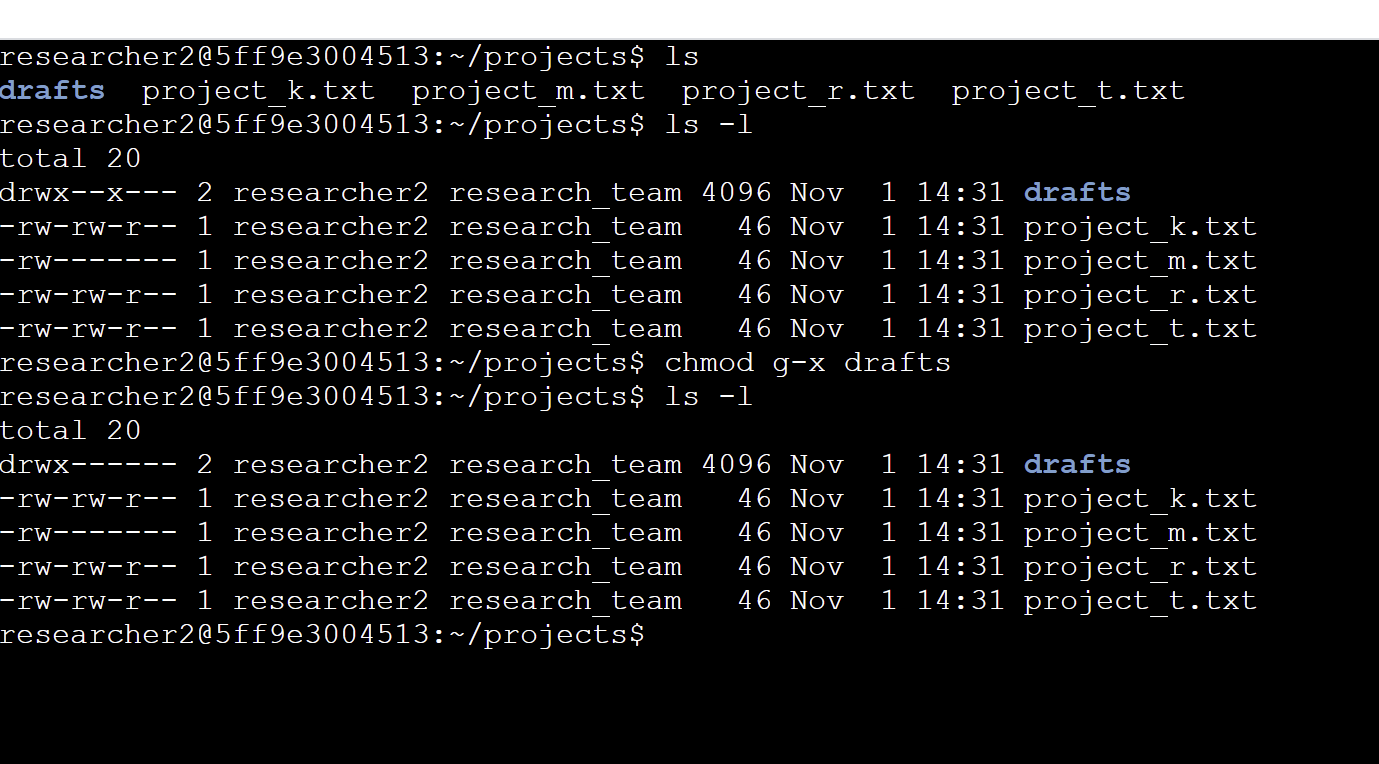


The above shows a chmod command used to remove write permission from other users of a file named project\_k.txt

## Change file permissions on a hidden file

TThe above removes write permission for users and groups on a hidden file named .project\_x.txt

## Change directory permissions



The chmod g-w was used to remove executable permission from the directory named drafts.

## Summary

Knowledge of file permission configuration is an essential tool for a cybersecurity analyst because it helps to achieve the confidentiality of files and data. For example, payroll information contains sensitive data which as a matter of privacy should not be accessible to other users who are not a member of the payroll department. Thus removing read, write and execute permissions for other users on a payroll file is important to the organization.