**Lab Title:** User, Group and Permission

**Student Name:** Nebeuwa Ifeanyichukwu Raphael

**Student ID:** 202520850LE

**Course Name:** Linux System Administrative Adventure

**Instructor Name:** Zakariyya Dahuru Musa

**Date of Submission:** 20/10/2025

## Executive Summary

This lab exercise provides hands-on experience in **Linux system administration**, focusing on managing users, groups, file permissions, and software packages.
It simulates real-world administrative tasks in a company environment (TechVille Inc.), where system administrators are responsible for onboarding employees, controlling access to project files, and maintaining essential developer tools.

Throughout the lab, I perform key administrative functions such as creating and modifying user accounts**,** assigning group memberships**,** setting and verifying file permissions, and managing software packages using the apt package manager.
These operations strengthen my understanding of Linux command-line tools, security practices, and system maintenance.

By completing this lab, I demonstrate proficiency in executing administrative commands safely and efficiently

## Lab Objective

1. **User Management**

- Create, modify, lock/unlock, and delete user accounts.
- Assign and update user IDs (UID), group IDs (GID), usernames, and personal details.
- Test and verify user access and account functionality.

2. **Group Management**

- Create, rename, and delete groups representing organizational departments.
- Add or remove users from groups.
- Verify user group memberships and system group listings.

3. **File Permissions**

- Create and inspect file permissions.
- Modify permissions and ownership.
- Test permission restrictions.
- Accessing a restricted directory

4. **Package Management**

- Install, remove, update, and upgrade software packages using the apt tool.
- Search repositories for specific packages such as wget and curl.

Maintain system software integrity and currency

**Tools and Resources Used**

- **Kali Linux:** Primary environment for performing user, group, file, and package management tasks.
- **Bash Shell:** Command-line interface used to execute all administrative commands.
- **Operating System:** Kali Linux
- **Terminal Commands**: sudo, adduser, usermod, chmod, chown, apt, etc.
- **Package Manager:** apt
- **User Accounts:** root and standard users
- Documentation and online Linux resources

**Methodology**

User creation and verification

- I created interactive and non-interactive accounts to observe differences in workflow:
  i. sudo adduser alice - followed the prompts to set password and full name.
  ii. sudo useradd bob - created a non-interactive account and checked /etc/passwd to confirm the entry.
- To verify results I used getent passwd and id alice, confirming UID, GID and initial group membership

Modifying credentials and access

- When Bob resigned I removed his account and rechecked the user list:

    i. sudo deluser bob && getent passwd
    ii. Observed that Bob's entry was removed from /etc/passwd.

- I tested password and login workflows:

    i. sudo passwd alice - set a stronger password interactively.
    ii. su alice - switched to the account to validate login and shell environment.

Modifying account

- HR requested changes which I applied and verified:

    i. Change UID: sudo usermod -u 1501 alice then id alice to confirm the new UID.
    ii. Lock/unlock account during leave: sudo usermod -L alice and sudo usermod -U alice.
    iii. Rename user: sudo usermod -l Alicia alice followed by getent passwd
    iv. Update comment full name: sudo usermod -c "Alicia Johnson" Alicia.
    v. After each modification I used id, getent passwd, and checks of the home directory to ensure consistency

Group Management

- I created and managed departmental groups:

    i. sudo groupadd developers
    ii. sudo groupadd -g 5050 admins then realized the admins group was unnecessary and removed it with sudo groupdel admins.

- I added and removed users from groups:

    i. sudo usermod -aG developers alicia to add.
    ii. sudo gpasswd -d alicia developers to remove.
    iii. Verification used getent group and id alicia.

File Permission and ownership

- I created a file and examined default permissions:

    i. touch project.txt; ls -l project.txt

- I changed file modes and ownership stepwise and checked after each change:

    i. chmod 755 project.txt - owner full, group and others read+execute.
    ii. chmod u+x project.txt - ensured owner execute bit was set symbolically.

iii. sudo chgrp developers project.txt and sudo chown alicia:developers project.txt - verified with ls -l project.txt.

- I performed an access test as a regular user:

  i. cd /root - recorded “Permission denied” (expected) to demonstrate restricted access.

Package management

- I installed and removed packages and kept the system current:

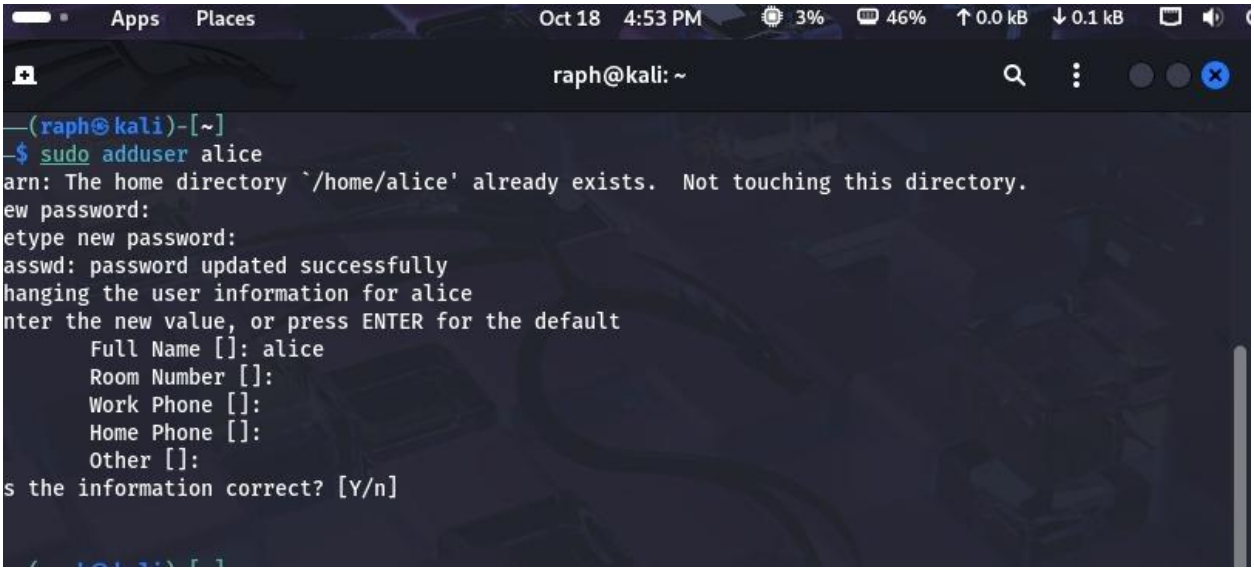
  i. sudo apt install wget -y and later sudo apt remove wget -y.
  ii. sudo apt update then sudo apt upgrade -y to refresh and upgrade packages.
  iii. Searched for packages with apt search curl.

- After installations I confirmed package presence via which wget or dpkg -l | grep wget.

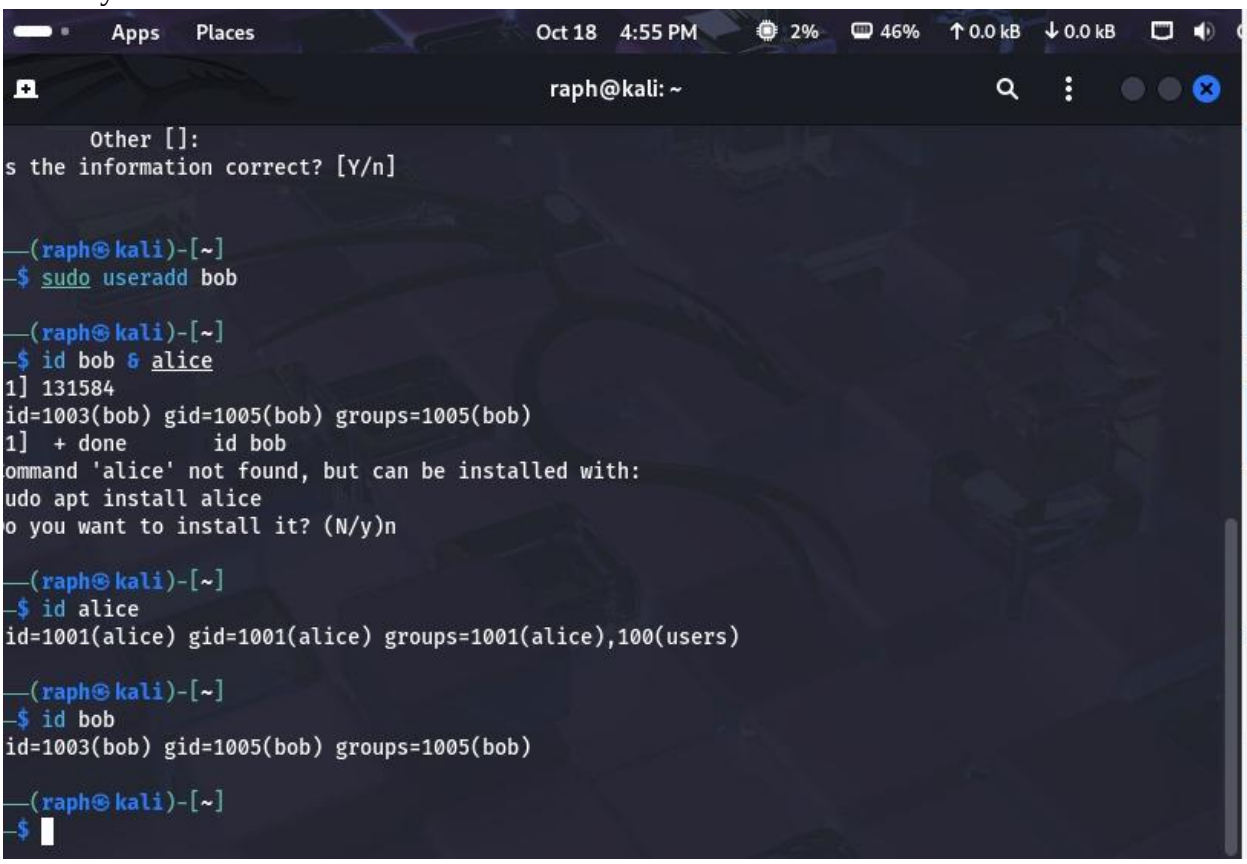
**Screenshot and Evidence**

User management

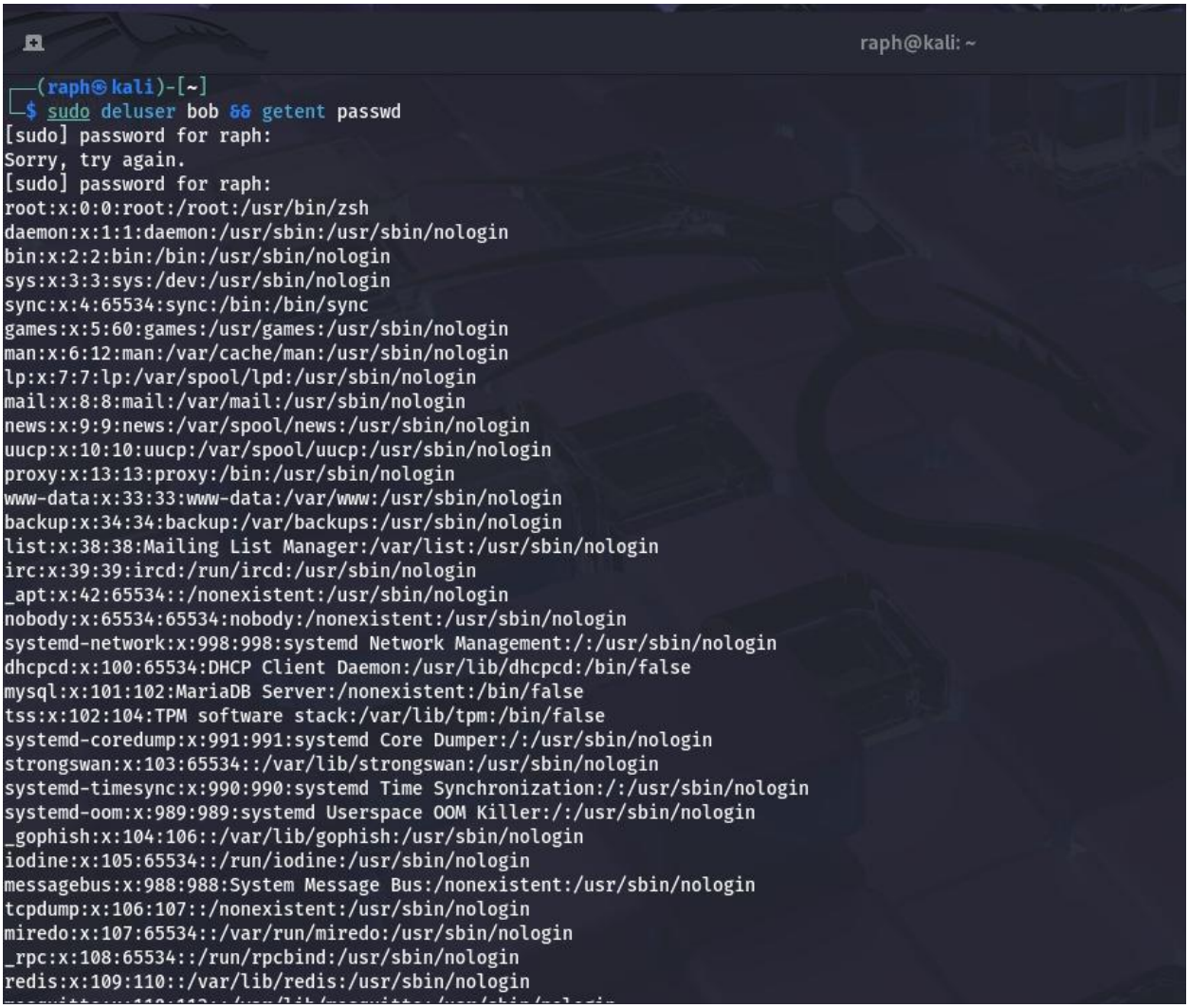
i. sudo adduser alice: followed the prompts to set password and full name.



ii. sudo useradd bob: create a non-interactive account and checked /etc/passwd to confirm the entry.




iii. sudo deluser bob && getent passwd. Observed that Bob's entry was removed from getent passwd

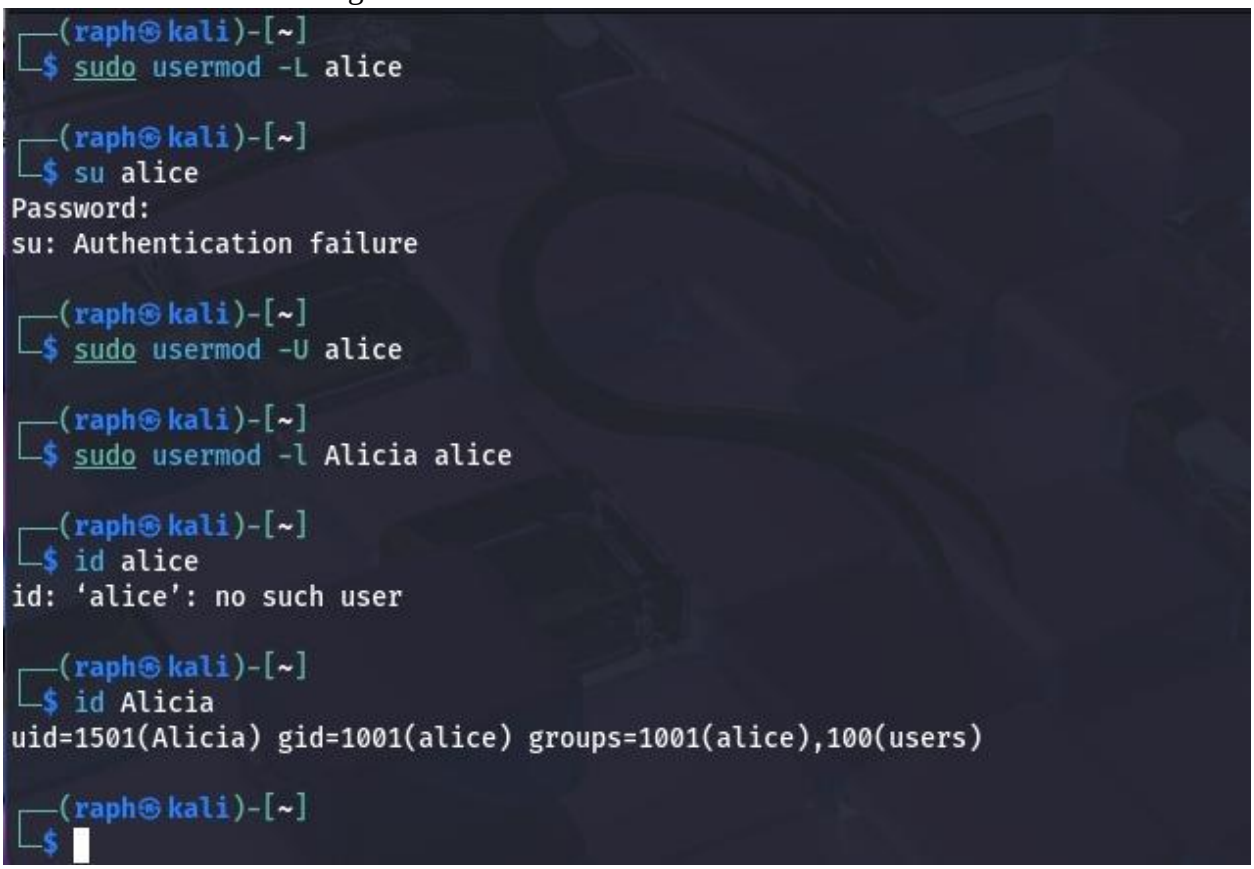



iv. sudo passwd alice: to set a stronger password interactively.

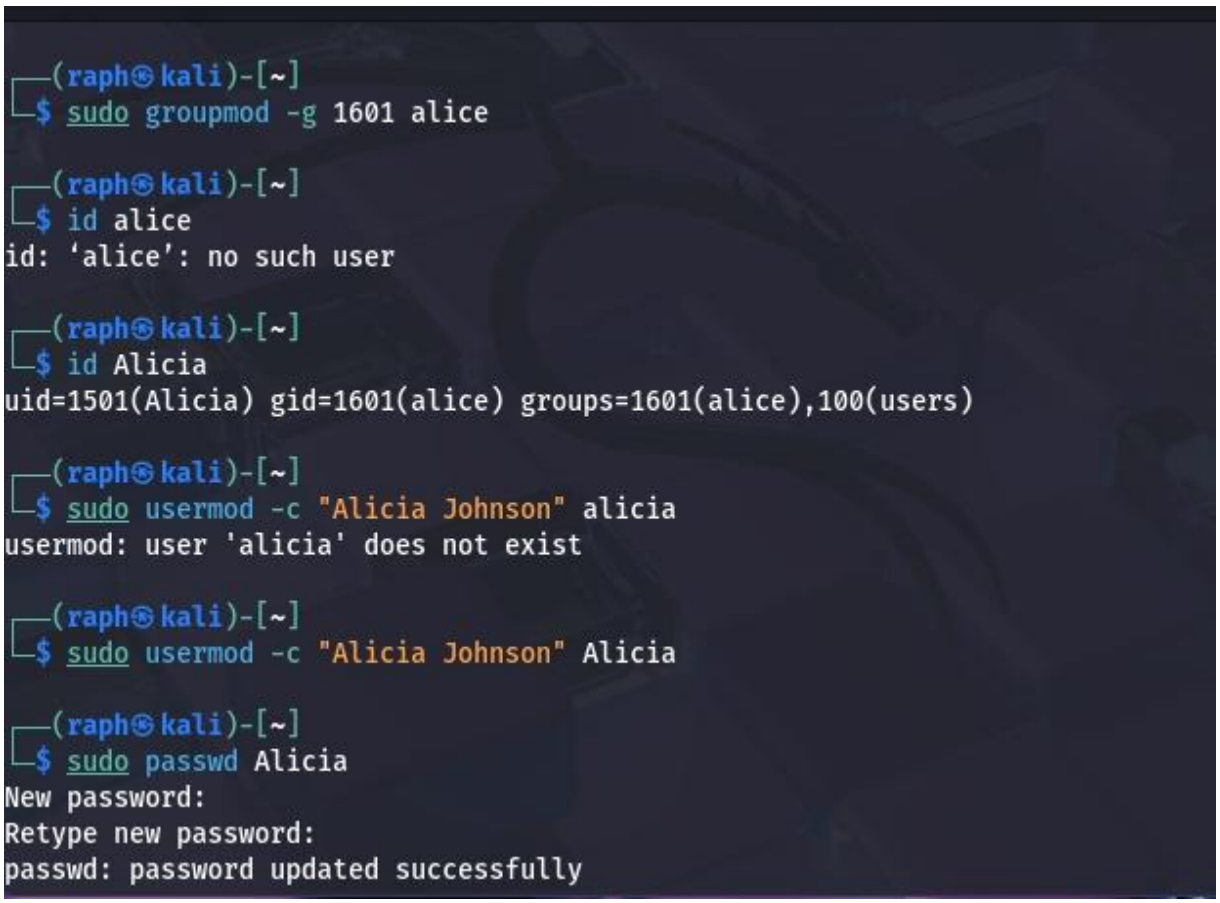

v. su alice: switched to the account to validate login and shell environment.

vi. Change UID: sudo usermod -u 1501 alice then id alice to confirm the new UID.


vii. Lock/unlock account during leave: sudo usermod -L alice and sudo usermod -U alice.

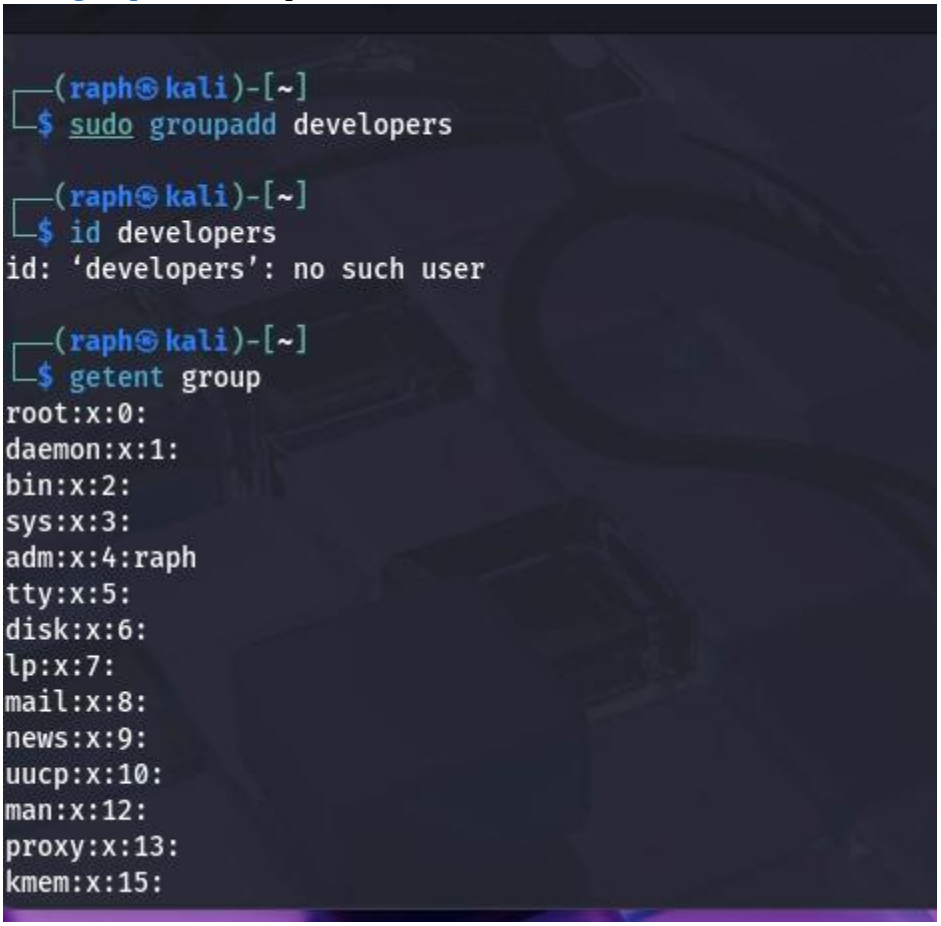



viii. Rename user: sudo usermod -l alicia alice followed by getent passwd | grep alicia. Update alice id: sudo groupmod -g 1601 alice. Update comment/full name: sudo usermod -c "Alicia Johnson" alicia.




Group management

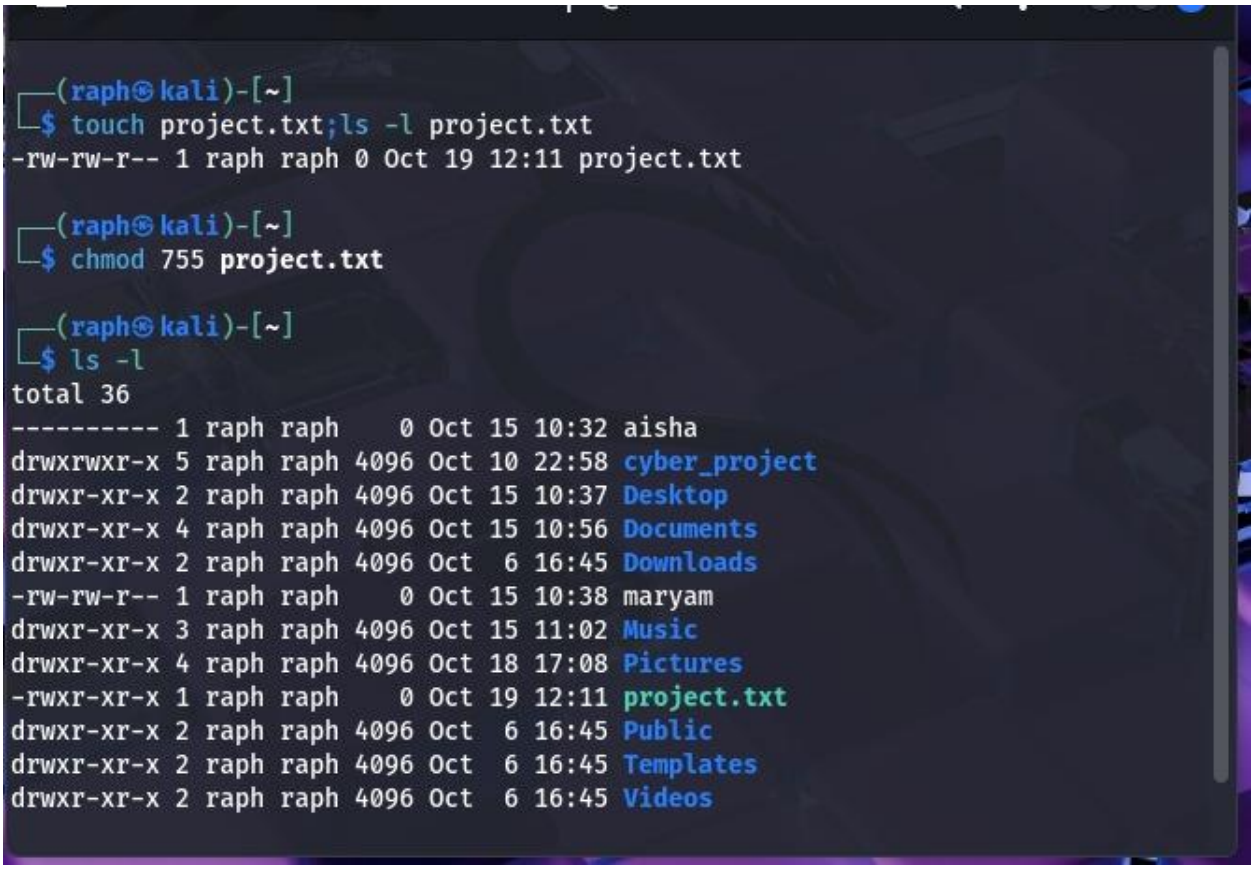
ix. sudo groupadd developers.




x. sudo groupadd -g 5050 admins then realized the admins group was unnecessary and removed it with sudo groupdel admins.

xi. sudo usermod -aG developers Alice: to add Alicia in developers group. sudo gpasswd -d alicia developers: to remove Alicia from developers group.


xii. touch project.txt; ls -l project.txt. chmod 755 project.txt - owner full, group and others read+execute.




xiii. chmod u+x project.txt - ensured owner execute bit was set symbolically. sudo chgrp developers project.txt and sudo chown alicia:developers project.txt - verified with ls -l project.txt.

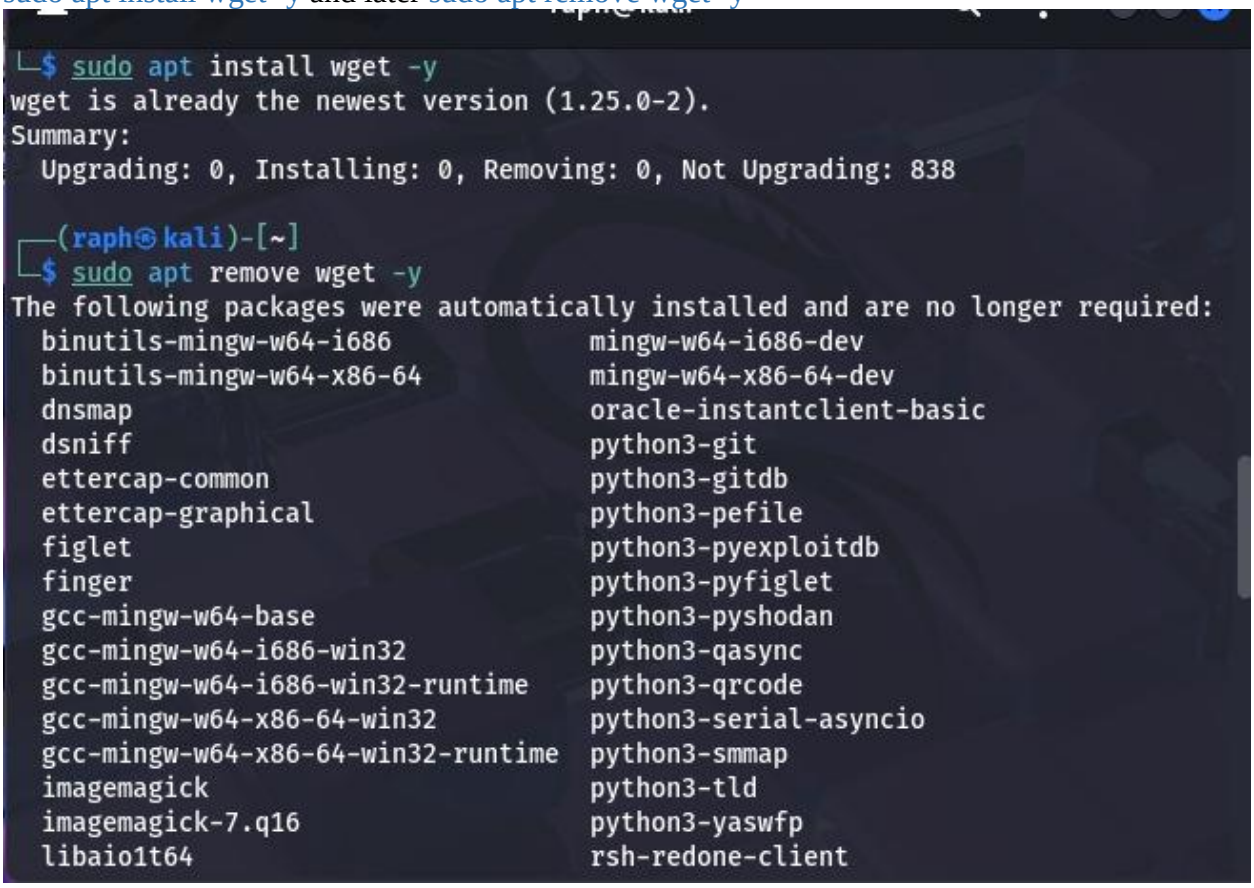
```
┌──(raph㉿kali)-[~]
└─$ chmod u+x project.txt

┌──(raph㉿kali)-[~]
└─$ ls -l
total 36
---------- 1 raph raph    0 Oct 15 10:32 aisha
drwxrwxr-x 5 raph raph 4096 Oct 10 22:58 cyber_project
drwxr-xr-x 2 raph raph 4096 Oct 15 10:37 Desktop
drwxr-xr-x 4 raph raph 4096 Oct 15 10:56 Documents
drwxr-xr-x 2 raph raph 4096 Oct  6 16:45 Downloads
-rw-rw-r-- 1 raph raph    0 Oct 15 10:38 maryam
drwxr-xr-x 3 raph raph 4096 Oct 15 11:02 Music
drwxr-xr-x 4 raph raph 4096 Oct 18 17:08 Pictures
-rwxr-xr-x 1 raph raph    0 Oct 19 12:11 project.txt
drwxr-xr-x 2 raph raph 4096 Oct  6 16:45 Public
drwxr-xr-x 2 raph raph 4096 Oct  6 16:45 Templates
drwxr-xr-x 2 raph raph 4096 Oct  6 16:45 Videos

┌──(raph㉿kali)-[~]
└─$ sudo chgrp developers project.txt

┌──(raph㉿kali)-[~]
└─$ sudo chown Alicia:developers project.txt
```

xiv. When I tried to access the /root directory using the command cd /root, the system displayed a “Permission denied” message. This happened because /root is the home directory of the root user and is restricted to administrative access only.

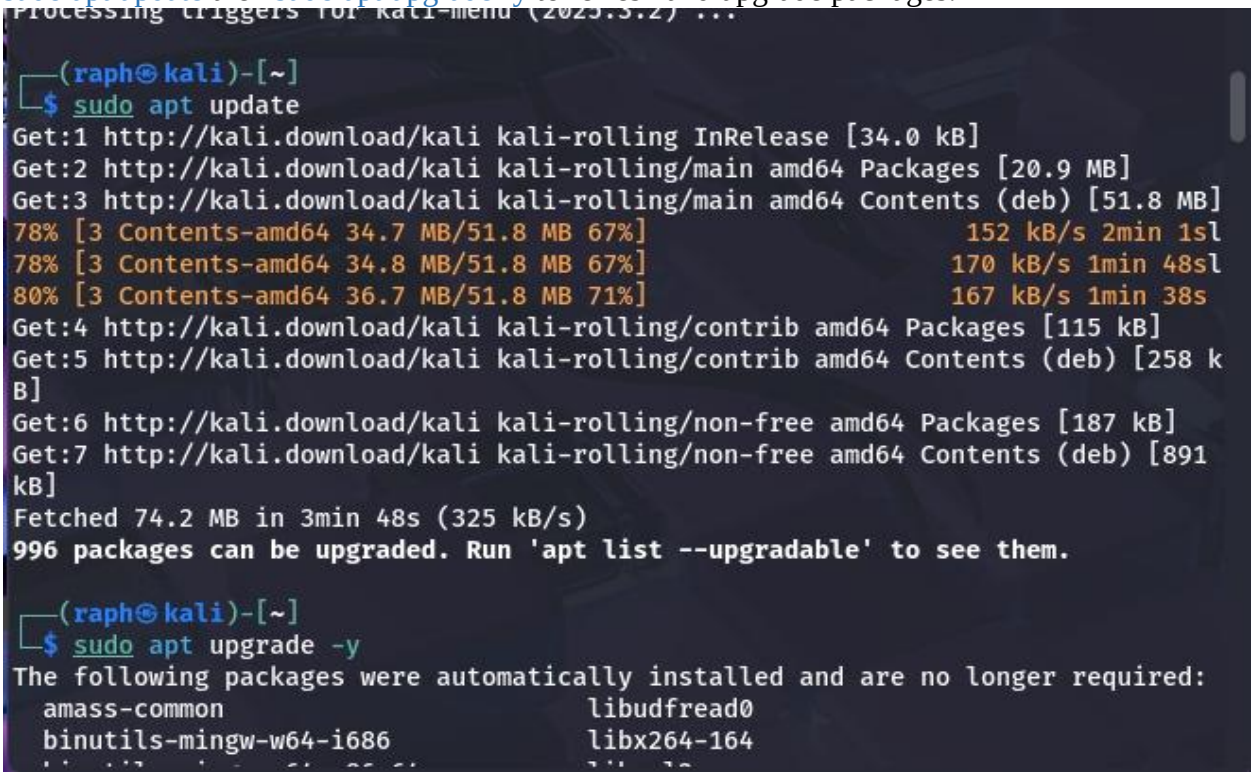
```
┌──(raph㉿kali)-[~]
└─$ ls -l project.txt
-rwxr-xr-x 1 Alicia developers 0 Oct 19 12:11 project.txt

┌──(raph㉿kali)-[~]
└─$ cd/root
zsh: no such file or directory: cd/root

┌──(raph㉿kali)-[~]
└─$ cd /root
cd: permission denied: /root

┌──(raph㉿kali)-[~]
└─$
```

Package management

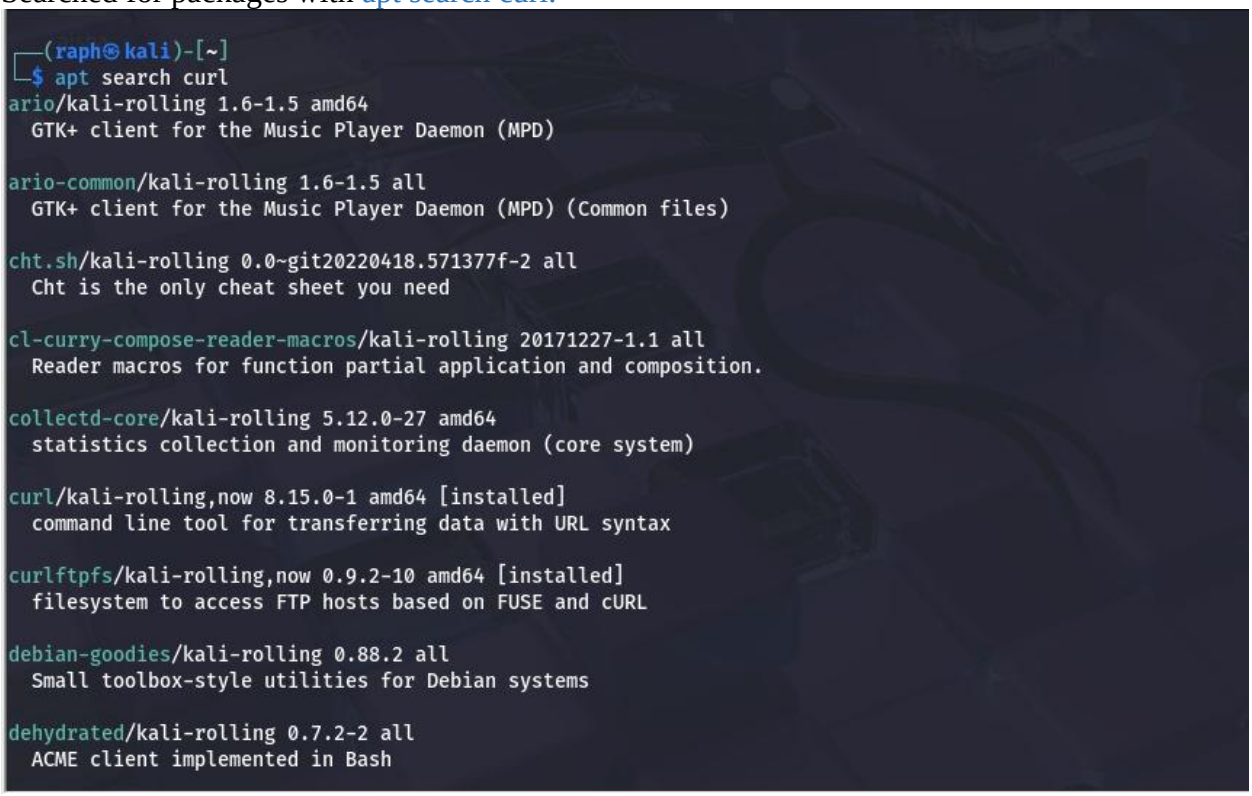
i. sudo apt install wget -y and later sudo apt remove wget -y




ii. sudo apt update then sudo apt upgrade -y to refresh and upgrade packages.



iii. Searched for packages with apt search curl.




**Analysis and findings**

- The analysis reveals the process of creating users, assigning user IDs (UIDs), group IDs (GIDs), usernames, and personal details, as well as modifying user accounts when necessary.
- The group management section shows how groups were created and modified - including renaming, deleting, and managing membership by adding, removing, and verifying users within groups.
- The file management part of the lab demonstrates how I created a file, inspected its permissions using the ls -l command, and modified both permissions and ownership using commands such as chmod, chown and chgrp.

**Challenges and solutions**

- During the lab, the sudo command initially failed to assign the UID 1501 to the user alice due to restricted access from the current login user. This issue was resolved by switching to the /root user for administrative privileges.
- However, when retrying the command as **/root**, the system reported that alice was currently in use by process **27599**, preventing the UID change. The issue was resolved by terminating the process using sudo kill -9 27599, after which the modification completed successfully.

## Conclusion

From this lab, I learned how important the /root user is when managing and assigning permissions to other users. It also showed me why it's necessary to think carefully before giving permissions to anyone who might not be trusted. I discovered that even the sudo command can sometimes be limited, depending on who is logged in. Overall, this lab helped me understand more about system security, user privacy, and how Linux keeps control over who can access what.

## Recommendation

To protect user privacy and system integrity, every user in an organization should have their own unique login credentials. It's also important to regularly update user accounts, review access permissions, and ensure that only authorized individuals can access sensitive data. Consistent monitoring and security updates help maintain a safer and more organized system environment.

## Reference


- Kali Linux Documentation. (2025). Official Kali Linux User Documentation. Retrieved from https://www.kali.org/docs/
- International Cybersecurity and Digital Forensics Academy.
- YouTube video. Networkchuks. Retrieved from https://youtu.be/jwnvKOjmtEA?si=bKgt7kH1MtKJ2ZzL