CU CHANDIGARH UNIVERSITY

CHANDIGARH UNIVERSITY

Discover. Learn. Empower.

CHANDIGARH UNIVERSITY

DEPARTMENT OF COMPUTER
APPLICATIONS

A PROJECT

REPORT ON

USER & GROUP MANAGEMENT WITH ACCESS CONTROL

Submitted by:

Kashish

Under the

Guidance of: Mr.

Rajat Patial

Assistant

Professor

Department of

UIC Chandigarh

University

CERTIFICATE

This is to certify that the project titled “User & Group Management with Access Control” has been successfully completed by Kashish under the supervision of Mr. Rajat Patial, Assistant Professor, Department of Computer Applications, Chandigarh University.

This work is submitted in partial fulfillment of the requirements for the course in Linux Administration and System Management.

We hereby declare that this report represents original work carried out by the students under the mentioned guidance and has not been submitted elsewhere for any other academic purpose.

(Signature)

Supervisor: Mr. Rajat
Patial Assistant Professor
Department of UIC
Chandigarh University

ACKNOWLEDGMENT

We take immense pleasure in expressing our sincere gratitude to our respected guide, Mr. Rajat Patial, Assistant Professor, Department of Computer Applications, Chandigarh University, for his constant support, valuable guidance, and encouragement throughout this project. His expertise and advice have been instrumental in the successful completion of our project.

We also wish to thank the Department of Computer Applications, Chandigarh University, for providing us with an excellent environment and facilities to carry out our project work. Finally, we extend our thanks to our friends and family members for their constant motivation and support during the entire project period.

INTRODUCTION

Linux operating systems have become the backbone of modern computing environments. It provides a secure, stable, and flexible foundation for servers, networks, and even personal devices. As organizations grow, managing user accounts, groups, and permissions becomes a critical task to ensure that only authorized personnel can access or modify system resources. This is not just about efficiency but also about protecting sensitive data. Through this project, we delve deeper into the system-level operations of Linux that control access rights, user privileges, and group management, highlighting the importance of following best practices in system administration and cybersecurity.

Linux is one of the most widely used operating systems in the world, known for its stability, flexibility, and open-source nature. One of the core responsibilities of a Linux system administrator is to manage users, groups, and permissions effectively. Proper management of users and access rights ensures that only authorized individuals can use system resources, preventing misuse and maintaining system integrity.

This project focuses on understanding and implementing the fundamental principles of Linux system administration — particularly, user and group management with access control. The tasks performed include creating and deleting users and groups, assigning permissions, and applying Access Control Lists (ACLs) for more granular permission management.

OBJECTIVE

This project aims to combine theoretical understanding with practical implementation of Linux user and group management. By completing this work, we intended not only to execute administrative commands but also to comprehend their underlying functionality.

Our objectives also include learning about system configuration files such as **/etc/passwd**, **/etc/shadow**, and **/etc/group**, which store vital user-related information. Another important objective was to explore how **Access Control Lists (ACLs)** extend traditional permission models, allowing administrators to set permissions at a more granular level—thereby improving flexibility and security across the system.

The main objective of this project is to gain a **practical understanding of managing users, groups, and file permissions** in Linux effectively. It aims to develop the ability to:

- Add, modify, and delete users and groups.
- Assign file and directory permissions based on organizational needs.
- Implement Access Control Lists (ACLs) for fine-grained access management.
- Ensure secure and efficient management of Linux systems.

Through this project, we intend to strengthen our knowledge of Linux commands related to system administration and security.

TASKS PERFORMED / PROCEDURE

In addition to the standard user and group operations, we experimented with permission scenarios to test system response. For example, we created users with restricted access to specific directories, tested file ownership transfers, and implemented group collaboration models. We also studied the differences between user ownership and group ownership of files, and how changing permissions can impact accessibility. Furthermore, we explored system logs to verify the actions performed, ensuring traceability and accountability in administrative tasks.

The following steps were performed to achieve the objectives of this project:

1.**User Creation:** Added new users using the `useradd` command and set passwords using
`passwd`.

2.**Group Creation:** Created groups with `groupadd` and assigned users to groups using
`usermod -aG`.

3.**User Modification:** Changed shell types, home directories, and passwords using
`usermod`.

4.**Permission Management:** Used `chmod` to assign read, write, and execute permissions for users, groups, and others.

5.**Ownership Changes:** Applied `chown` and `chgrp` commands to manage ownership of files and directories.

6.**Access Control Lists:** Implemented ACLs using `setfacl` and verified them with `getfacl`.

7.**Verification:** Checked the user and group configuration using `cat /etc/passwd` and `cat
/etc/group`.

Each of these steps was tested and verified in a Linux environment using the terminal.

COMMANDS USED

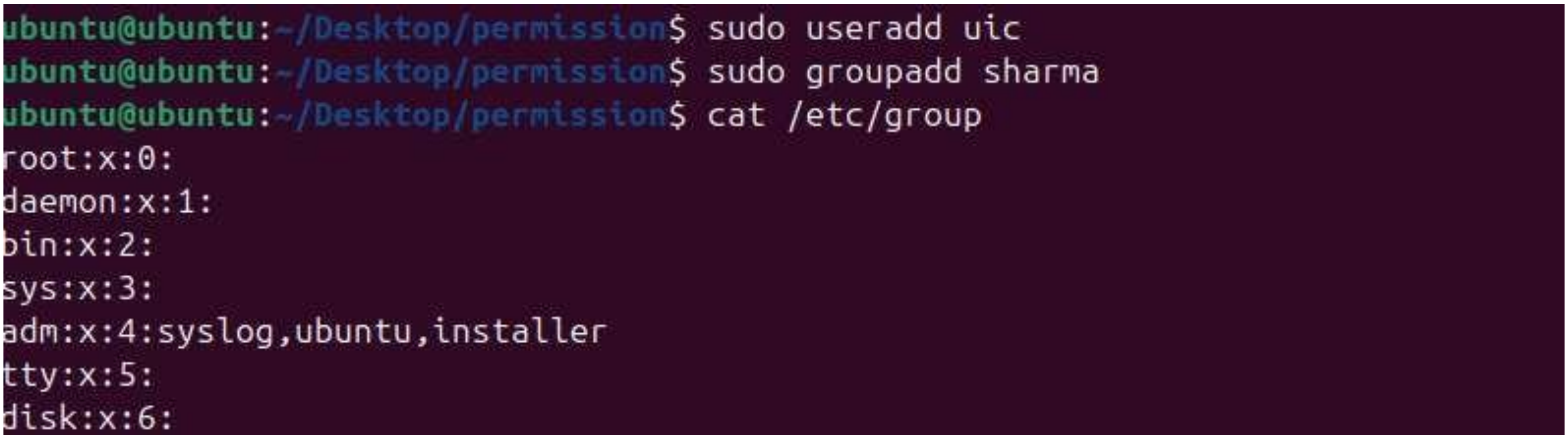
Alongside these commands, we also explored related utilities such as 'id' to display user identity, 'su' for switching users, and 'sudo' for executing administrative tasks securely. Understanding command syntax, flags, and real-world usage scenarios was an integral part of the learning process.

We also ensured proper documentation of each command’s purpose and tested variations to observe their behavior.

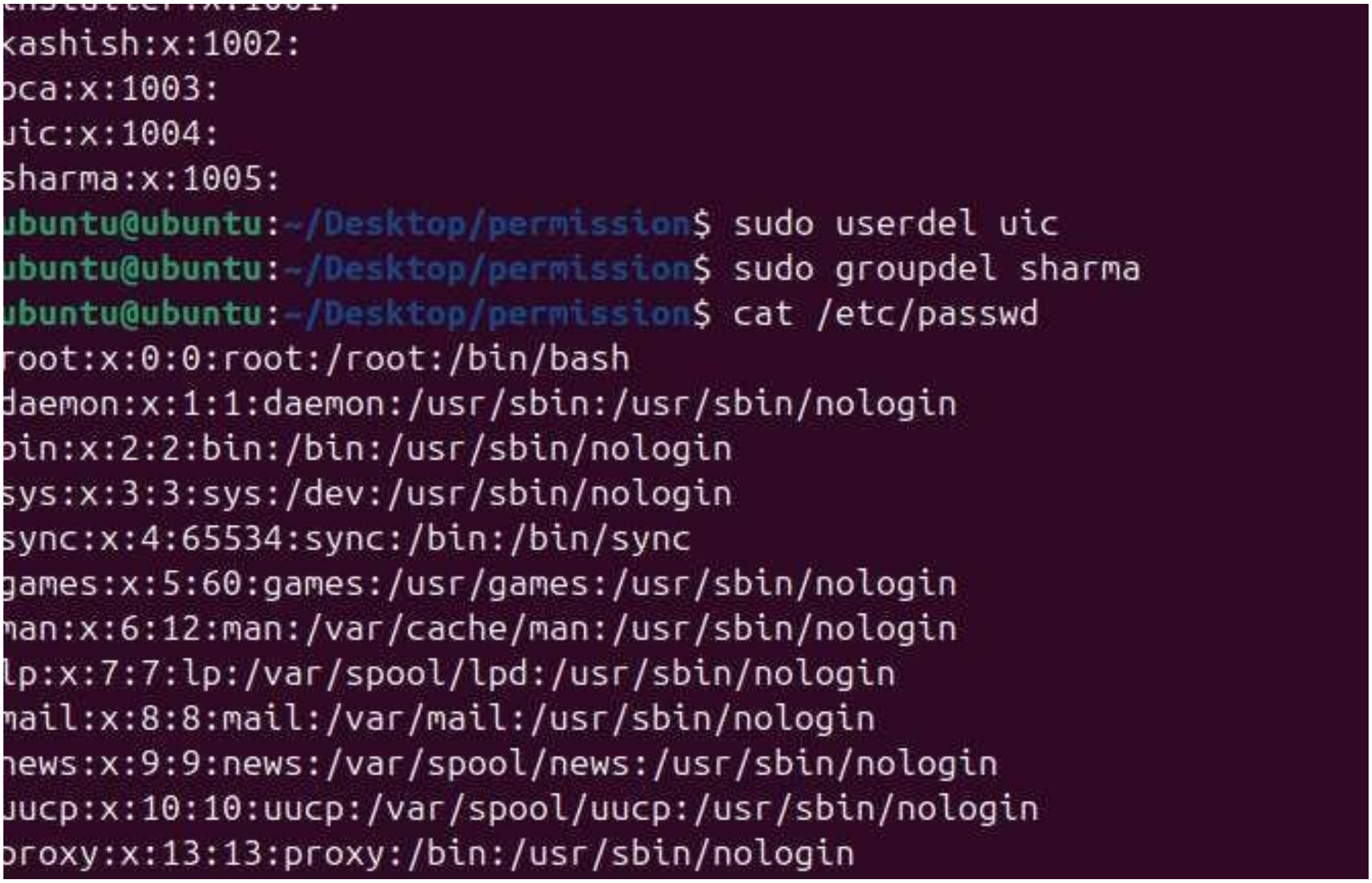
Below is the list of key commands used during the project:

- `useradd <username>` – Add a new user.
- `passwd <username>` – Set or change a user's password.
- `usermod -aG <group> <user>` – Add a user to a group.
- `userdel <username>` – Delete a user.
- `groupadd <groupname>` – Create a new group.
- `groupdel <groupname>` – Delete a group.
- `chmod <permissions> <file>` – Change file or directory permissions.
- `chown <owner> <file>` – Change file ownership.
- `chgrp <group> <file>` – Change group ownership.
- `setfacl -m u:<user>:rwx <file>` – Set ACL permissions.
- `getfacl <file>` – Display ACLs for a file or directory.
- `ls -l` – List files with detailed permissions and ownership.

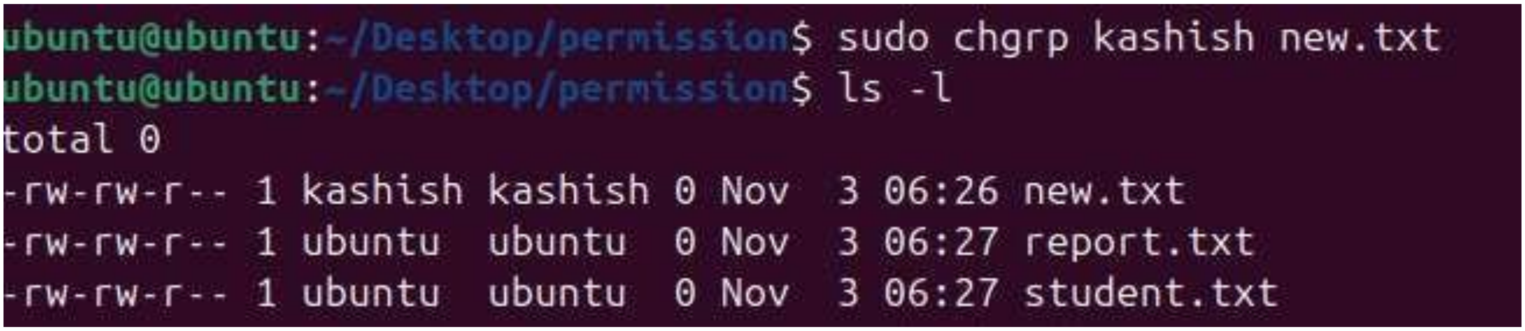
OUTPUT / SCREENSHOTS



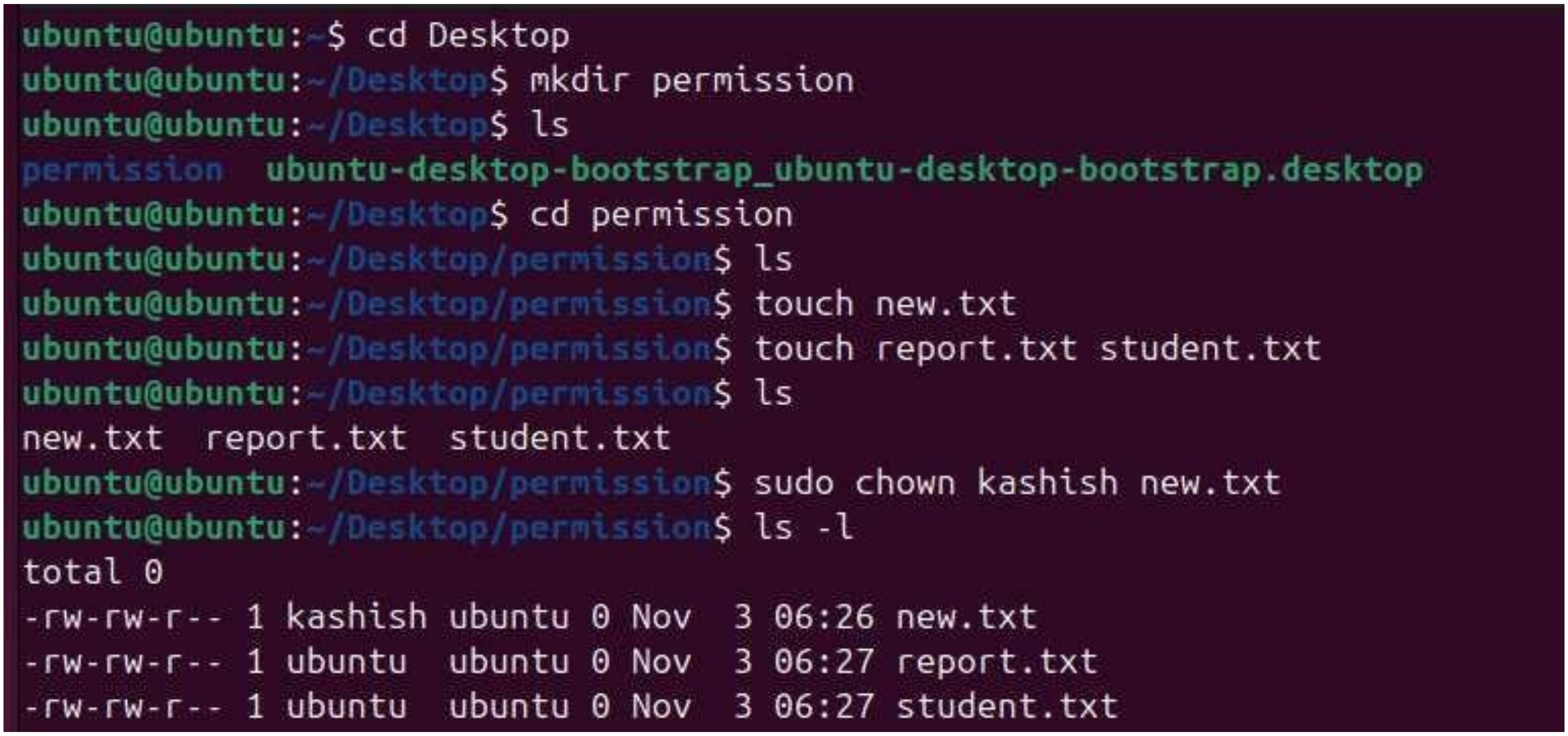
```
ubuntu@ubuntu:~/Desktop/permission$ sudo useradd uic
ubuntu@ubuntu:~/Desktop/permission$ sudo groupadd sharma
ubuntu@ubuntu:~/Desktop/permission$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,ubuntu,installer
tty:x:5:
disk:x:6:
```



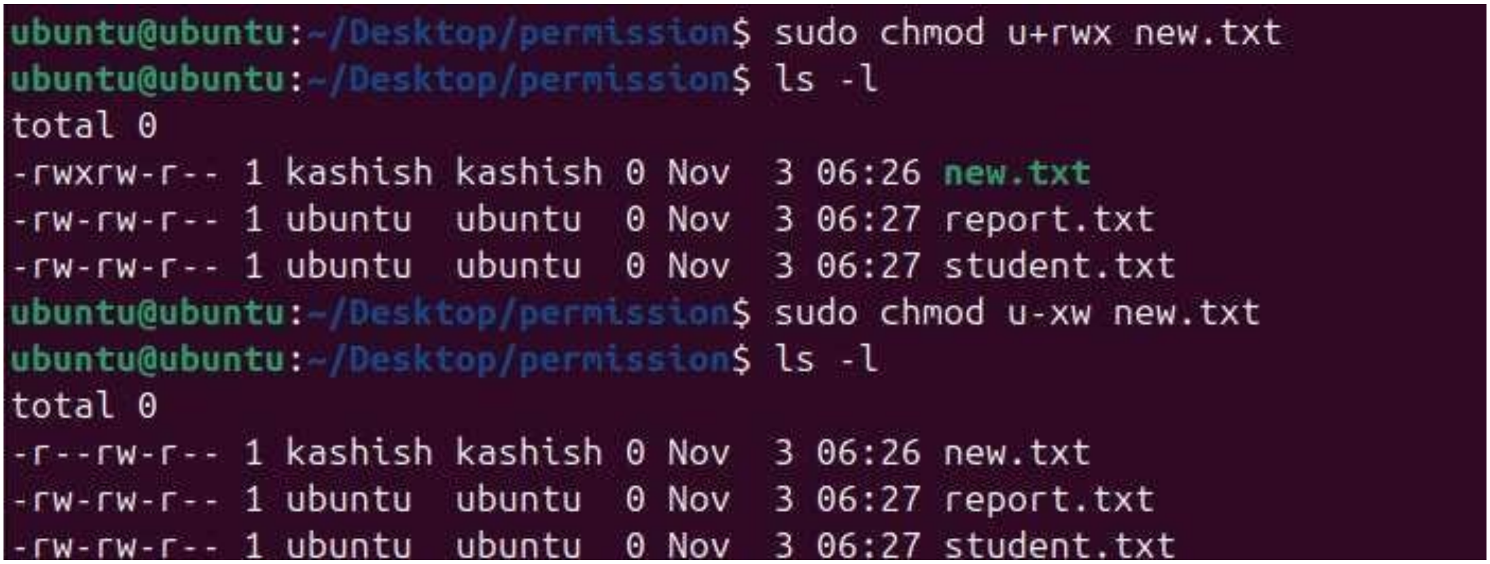
```
installer:x:1001:
kashish:x:1002:
bca:x:1003:
uic:x:1004:
sharma:x:1005:
ubuntu@ubuntu:~/Desktop/permission$ sudo userdel uic
ubuntu@ubuntu:~/Desktop/permission$ sudo groupdel sharma
ubuntu@ubuntu:~/Desktop/permission$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
```



```
ubuntu@ubuntu:~/Desktop/permission$ sudo chgrp kashish new.txt
ubuntu@ubuntu:~/Desktop/permission$ ls -l
total 0
-rw-rw-r-- 1 kashish kashish 0 Nov  3 06:26 new.txt
-rw-rw-r-- 1 ubuntu  ubuntu  0 Nov  3 06:27 report.txt
-rw-rw-r-- 1 ubuntu  ubuntu  0 Nov  3 06:27 student.txt
```



```
ubuntu@ubuntu:~$ cd Desktop
ubuntu@ubuntu:~/Desktop$ mkdir permission
ubuntu@ubuntu:~/Desktop$ ls
permission  ubuntu-desktop-bootstrap_ubuntu-desktop-bootstrap.desktop
ubuntu@ubuntu:~/Desktop$ cd permission
ubuntu@ubuntu:~/Desktop/permission$ ls
ubuntu@ubuntu:~/Desktop/permission$ touch new.txt
ubuntu@ubuntu:~/Desktop/permission$ touch report.txt student.txt
ubuntu@ubuntu:~/Desktop/permission$ ls
new.txt  report.txt  student.txt
ubuntu@ubuntu:~/Desktop/permission$ sudo chown kashish new.txt
ubuntu@ubuntu:~/Desktop/permission$ ls -l
total 0
-rw-rw-r-- 1 kashish ubuntu 0 Nov  3 06:26 new.txt
-rw-rw-r-- 1 ubuntu  ubuntu 0 Nov  3 06:27 report.txt
-rw-rw-r-- 1 ubuntu  ubuntu 0 Nov  3 06:27 student.txt
```



```
ubuntu@ubuntu:~/Desktop/permission$ sudo chmod u+rwx new.txt
ubuntu@ubuntu:~/Desktop/permission$ ls -l
total 0
-rwxrw-r-- 1 kashish kashish 0 Nov  3 06:26 new.txt
-rw-rw-r-- 1 ubuntu  ubuntu  0 Nov  3 06:27 report.txt
-rw-rw-r-- 1 ubuntu  ubuntu  0 Nov  3 06:27 student.txt
ubuntu@ubuntu:~/Desktop/permission$ sudo chmod u-xw new.txt
ubuntu@ubuntu:~/Desktop/permission$ ls -l
total 0
-r--rw-r-- 1 kashish kashish 0 Nov  3 06:26 new.txt
-rw-rw-r-- 1 ubuntu  ubuntu  0 Nov  3 06:27 report.txt
-rw-rw-r-- 1 ubuntu  ubuntu  0 Nov  3 06:27 student.txt
```

CONCLUSION

Through this project, we also developed problem-solving skills by encountering and resolving common system errors. It helped us understand user access hierarchies, privilege levels, and the concept of least privilege — a key principle in system security. The hands-on practice enhanced our confidence in handling Linux systems independently. We also recognized how these fundamental skills serve as the foundation for advanced topics such as server management, network security, and cloud system administration.

This project on 'User & Group Management with Access Control' provided us with practical experience in managing Linux users, groups, and file permissions. We learned how to ensure system security and integrity by setting appropriate access controls and applying ACLs for specific user-based permissions.

Through this project, we enhanced our understanding of the Linux command line interface and gained confidence in performing administrative tasks efficiently. The skills learned through this work are crucial for any future role involving system or network administration.

Linux is extensively used in enterprise servers, cloud deployments, and embedded systems. In this project, we not only practiced command usage but also examined real-world scenarios such as multi-user collaboration, permission inheritance, and mitigation of accidental data exposure. We discuss typical administrative workflows, including account lifecycle (creation, maintenance, and decommissioning), automated user provisioning considerations, and basic security practices such as enforcing strong passwords and limiting sudo privileges to trusted accounts.

During the lab sessions we simulated a departmental file share where different roles required different access levels. We created groups such as 'developers', 'testers', and 'admins' and mapped directory permissions accordingly. We also demonstrated how to revoke access cleanly, and how to use 'getfacl' output to audit who has access to sensitive files.

Finally, we scripted common repetitive administration tasks (user creation with default home directories, assigning groups, and applying ACL templates) to highlight how automation reduces human error.

Examples with Context

1. **Create a user with home directory and bash shell:**

bash

Copy code

```
useradd -m -s /bin/bash alice
```

2. **Add user to multiple groups:**

bash

Copy code

```
usermod -aG developers,sudo alice
```

3. **Set a default ACL allowing ‘developers’ group full control on** /srv/project**:**

bash

Copy code

```
setfacl -m g:developers:rwx /srv/project
```

4. **Remove a user and preserve their home directory for auditing:**

bash

Copy code

```
userdel -r alice
```

Explanation

These examples demonstrate practical command usage and explain common flags used in Linux user and permission management.

Sample Output Excerpts

- /etc/passwd **entry for ‘alice’:**

ruby

Copy code

```
alice:x:1001:1001:Alice:/home/alice:/bin/bash
```

- getfacl /srv/project **sample:**

makefile

Copy code

```
# file: /srv/project
user::rwx
group::r-x
user:alice:rwx
group:developers:rwx
mask::rwx
other::r--
```

These outputs confirm that ownership and ACL entries were successfully applied.

Recommendations

- Integrate **centralized authentication** (LDAP or Active Directory)
- Perform **regular permission audits**
- Implement **Role-Based Access Control (RBAC)** for scalability and security

---

Conclusion

Understanding these foundational commands prepares administrators to manage more complex infrastructures and adopt best practices that enhance both **security posture** and **operational efficiency**.

APPENDIX A: Troubleshooting Notes

1. 'Permission denied' while using sudo: ensure the user is in the 'sudo' group and that /etc/sudoers hasn't been modified incorrectly.

2. ACLs not taking effect: check the underlying filesystem supports POSIX ACLs (e.g., ext4 with acl enabled).

3. Home directory missing after userdel: use 'userdel -r' carefully; backups are recommended before removal.

.

APPENDIX B: Good Practices

- Enforce password policies with pam_pwquality.
- Use 'chage' to set password expiry policies.
- Keep an administrative log of user changes for auditability.

REFERENCES

1. Linux Documentation Project - Administrative Guides

2. man pages: useradd(8), usermod(8), userdel(8), chown(1), chmod(1), setfacl(1)

3. Official distribution admin guides (Debian, Ubuntu, CentOS) for filesystem and ACL specifics.