**CONCEPTS OF USERS AND GROUPS ON LINUX REPORT**

**GROUP 3**

**Macleana Mensah Oteng**

**Elizabeth Wallace Arthur**

**Nick Anderson**

**Eugene Essuman - Quansah**

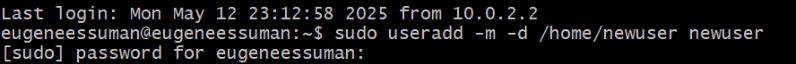
**Mohammed Razak Mikdar**

**INTRODUCTION**

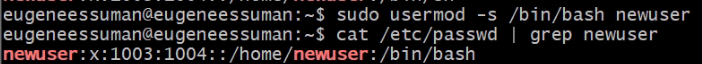
This report outlines the group’s practical experience with Linux system administration tasks using Oracle VirtualBox. The objective of this task was to explore and apply essential Linux commands and system management tools in a hands-on setting. Using Ubuntu as the base operating system within Virtualbox, we navigated various tasks such as creating, managing and modifying users and groups in Linux. Each tasks aimed to strengthen our understanding of Linux as a multi-user operating system and to build the skills necessary for effective system maintenance and troubleshooting. Through these tasks, we encountered and resolved real-world issues that system administrators commonly face, enhancing our technical knowledge, teamwork and collaboration as well as problem-solving abilities.

**Task 1: Create a New User**

1. Create a new user named newuser with a home directory in /home/newuser.

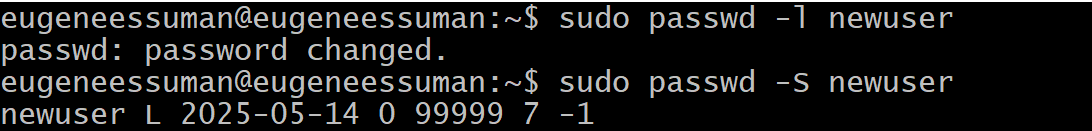


1. 
2. **Sudo** gives us the permission to create or edit users.
3. **Useradd** is to add users to the system.
4. **-m** creates a default home and **-d** manually set the home directory.
5. **Grep** is used to fetch the exact data we want to fetch.
6. Set a default shell for the user (e.g., bash).



**-s** is used to set the shell.

**Usermod** is to modify the user accounts

1. Disable the password for the user initially.
2. 
3. The **“L”** means the account is locked.

**Task 2: Add User to a Group**

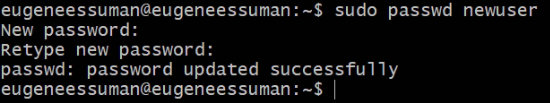
1. Add the newly created user to the sudo group, granting them administrative privileges.



**-a** is to make the user isn’t removed from the old group and **-G** gives the new group.

**Groups** command allows us to see the group a user belongs.

**Task 3: Set Password**

1. Use the passwd command to set a password for the new user.
2. 
3. **passwd** command is used to set a password for a user.

**Task 4: Verify User Creation**

1. Use the id command to verify the user's details, including username, UID, GID, and groups.
2. 
3. **id** command is used to view user id, group id and groups a user belong

**Task 5: Create a New Group**

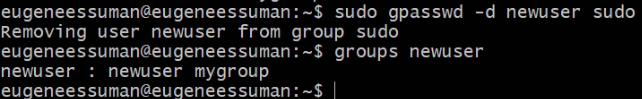
1. Create a new group named mygroup.
2. 

**Task 6: Add User to Group**

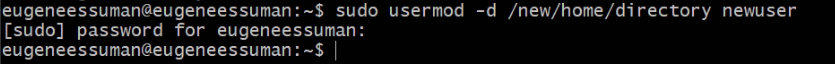
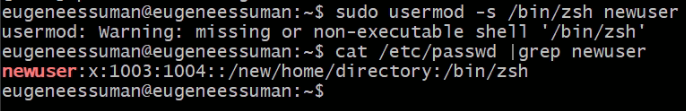
1. Add the newuser to the newly created mygroup.
2. 

**Task 7: Modify Group Membership**

1. Remove the newuser from the sudo group.
2. Add the newuser to the mygroup group



**Task 8: Change User Information**

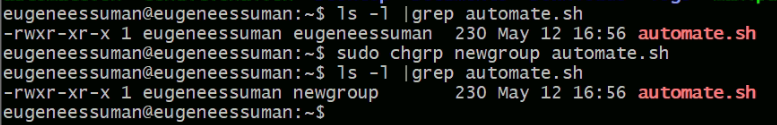
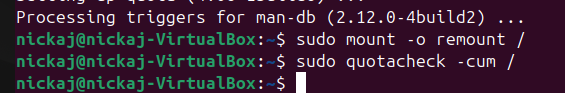
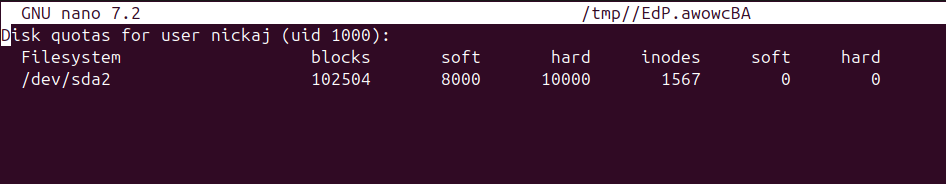
1. Modify the home directory of the newuser to a different location.
2. 
3. Change the user's shell to a different shell (e.g., zsh).
4. 

**Task 9: Delete User**

1. Delete the newuser account.
2. 

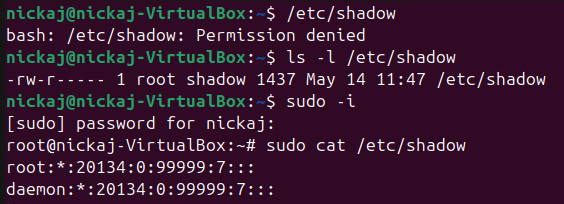
**Userdel** is used to delete/remove a user.

**Additional Tasks (Optional)**

1. **Create a Group with a GID:** Specify a specific GID (Group ID) when creating a group.
2. 
3. **Change Group Ownership:** Change the ownership of a file or directory to a specific group.
4. 
5. **Set User Quotas**: Limit the disk space and file usage for a user.
6. 
7. 
8. **Explore Shadow Password Storage:** Learn about how user passwords are securely stored in Linux (using the passwd command).

User passwords are not stored in plain text. They're encrypted (hashed) and stored in a secure file called /etc/shadow.

Only the **root account** has access to the /etc/shadow path.



**Conclusion**

This session helped clarify the roles of users, groups, and permissions in Linux and how critical proper privilege assignment is to system security. While lacking sudo access limited what could be done, it also reinforced a key concept in Linux security: access control is non-negotiable unless explicitly authorized.

We now have a solid foundation in, managing file and directory permissions, understanding sudo and group management and navigating permission errors and knowing when to escalate or adapt. We also learnt about the /etc/shadow file and how to view and access the hashed passwords using the root user.