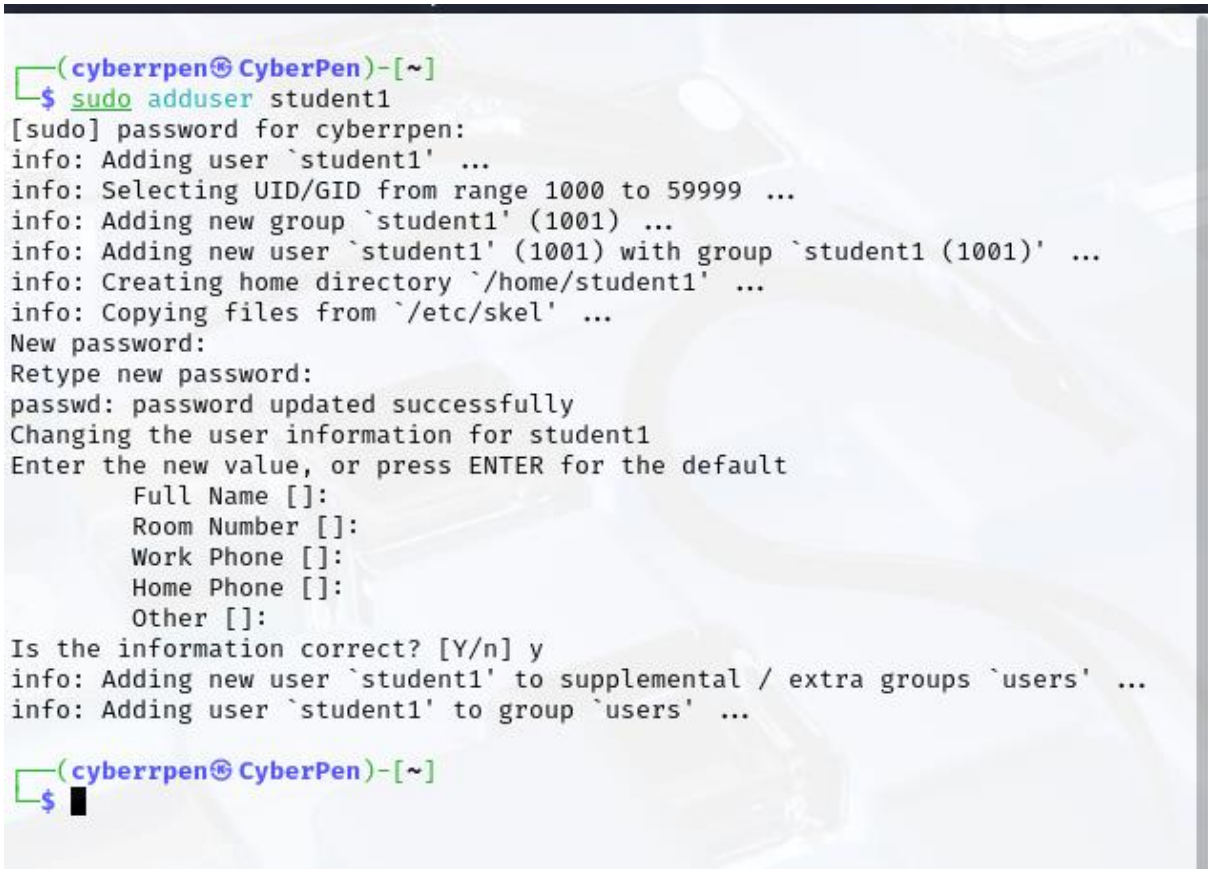
Lab 1: User Management

Objectives

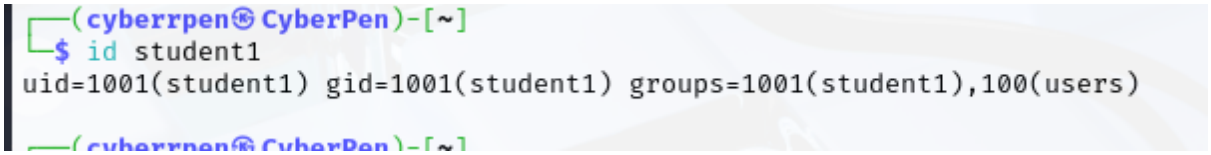
- Learn how to create, modify, and manage user accounts securely in Linux.
- Understand the importance of user account management for maintaining system security.
- Practice best practices in user administration, including user creation, modification, and deletion.

Creating User Accounts

- Create a new user named student1 using the following command: sudo adduser student1

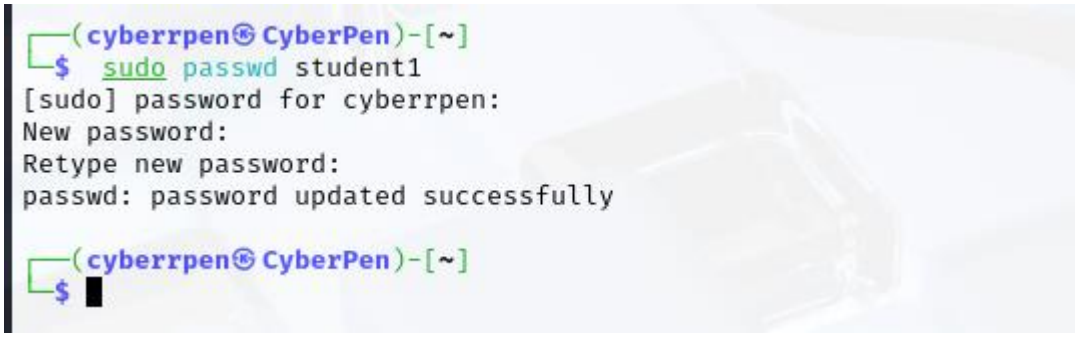


- Verify that the user account has been created successfully: id student1

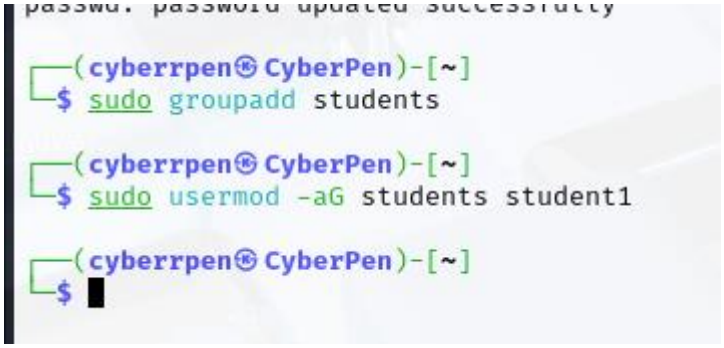


Modifying User Accounts

- Change the password for student1 to ensure secure access: sudo passwd student1

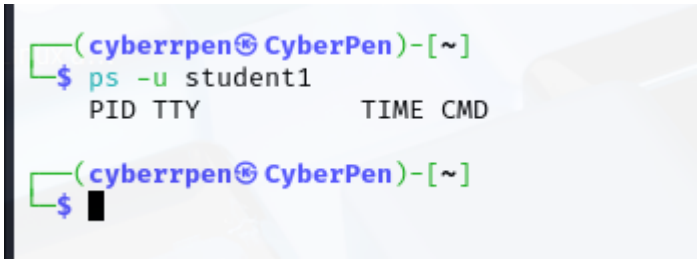


- Create a group named students and add student1 to this group to manage permissions effectively: sudo groupadd students
- Only if the group doesn't exist sudo usermod -aG students student1

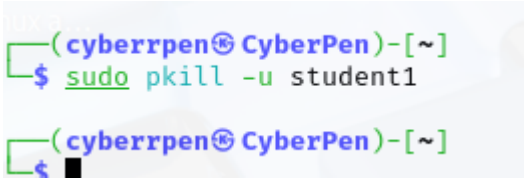


Locking and Unlocking User Accounts

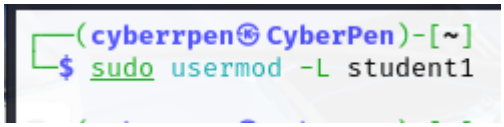
- Check for any active processes associated with student1: ps -u student1



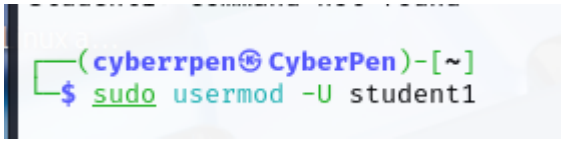
- Terminate any processes if necessary: sudo pkill -u student1



- Lock the user account: sudo usermod -L student1

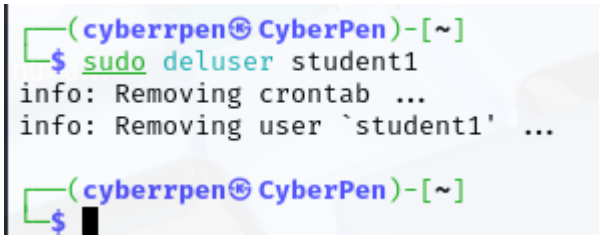


- Unlock the user account when needed: sudo usermod -U student1

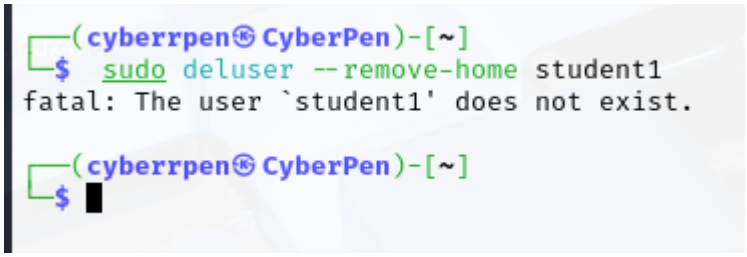


Deleting User Accounts

- Delete student1 while keeping their home directory: sudo deluser student1

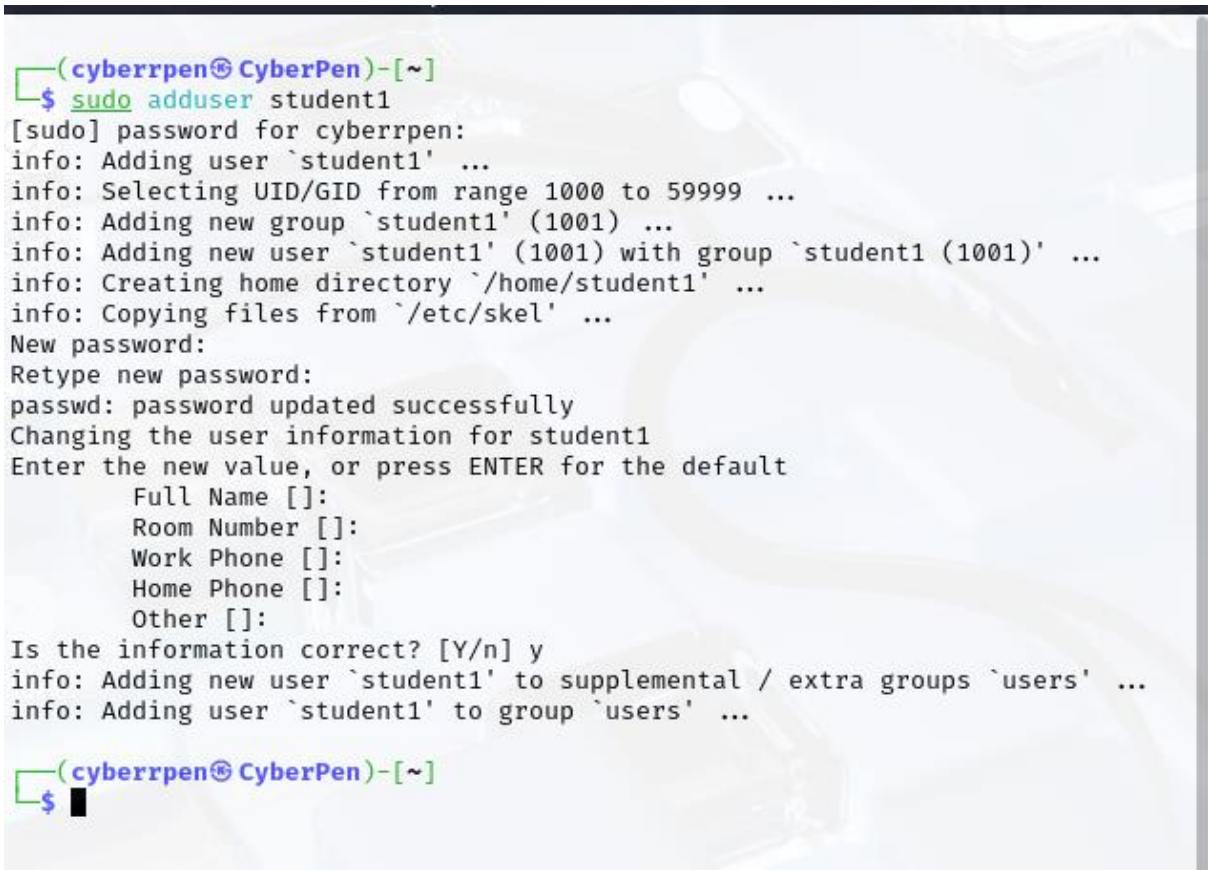


- Completely remove the user and their home directory: sudo deluser --remove-home student1

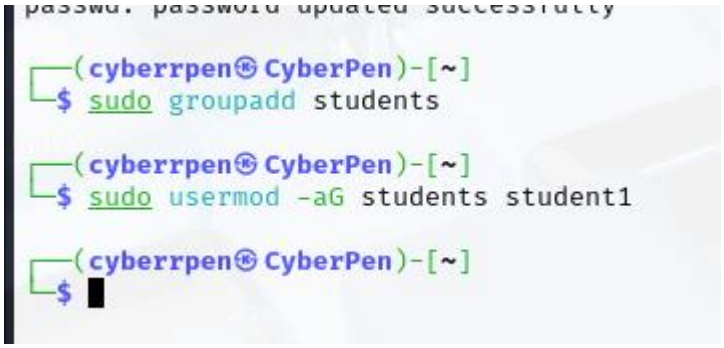


Exercise

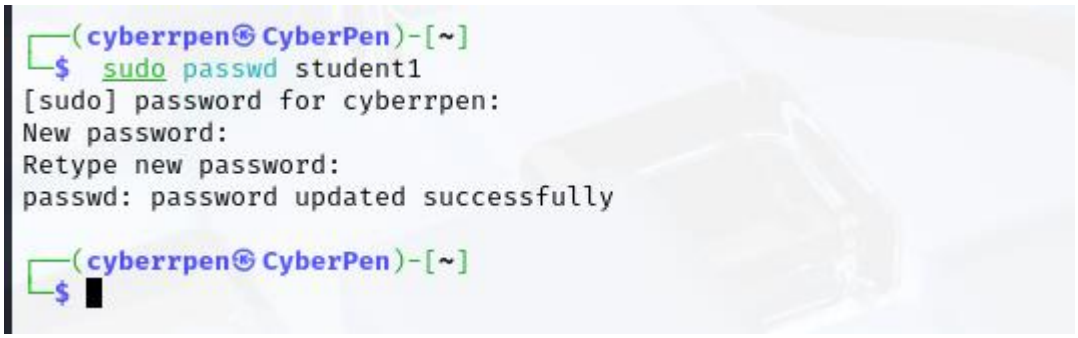
1. User Account Creation and Modification:
    - Create a user named student1
        - Command use: sudo adduser students1



    - Add student1 to the group students.
        - Command use: sudo groupadd students
            - Sudo usermod -aG student student1

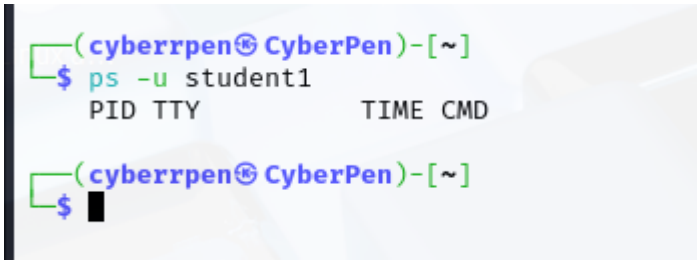


- Change the password for student1 to a secure value.
  - Command Use: sudo passwd student1

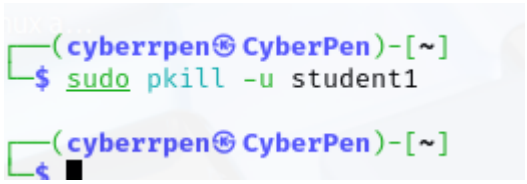


2. Account Locking and Unlocking:

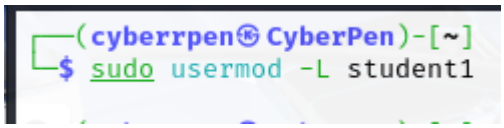
- Check for any active processes under student1 and terminate them if necessary.
  - Command Use to check for active processes: ps -u student1



  - Command Use to terminate processes: sudo pkill -u student1



- Lock the student1 account
  - Command use: sudo usermod -L student1



- Verify that the account is locked
    - Command use: sudo passwd -S student1

```
┌──(cyberrpen㉿CyberPen)-[~]
└─$ sudo usermod -L student1

┌──(cyberrpen㉿CyberPen)-[~]
└─$ sudo passwd -S student1

student1 L 2025-06-23 0 99999 7 -1

┌──(cyberrpen㉿CyberPen)-[~]
└─$
```

- Unlock the account and confirm it is accessible again.
    - Command Use: : sudo usermod -U student1

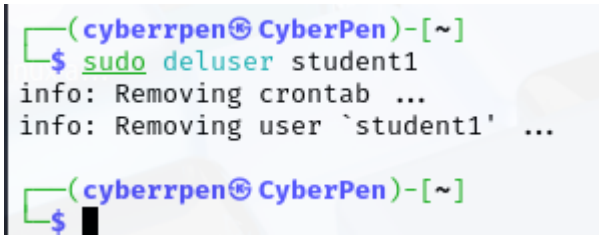
```
┌──(cyberrpen㉿CyberPen)-[~]
└─$ sudo usermod -U student1
```

- Confirm Student1 is accessible again

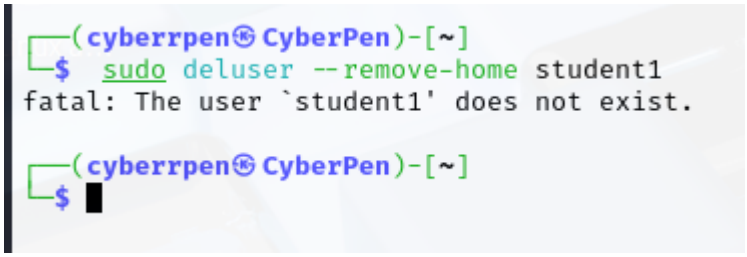
```
┌──(cyberrpen㉿CyberPen)-[~]
└─$ sudo usermod -U student1


┌──(cyberrpen㉿CyberPen)-[~]
└─$ sudo passwd -S student1

student1 P 2025-06-23 0 99999 7 -1

┌──(cyberrpen㉿CyberPen)-[~]
└─$
```

3. User Account Deletion:

- Delete the student1 user account while keeping the home directory.
    - Command use: sudo deluser student1



- Finally, remove student1 completely, including their home directory.
    - Command Use: sudo deluser --remove-home student1



Implications of User Management Practices in Maintaining System Security

User management is a critical component of system administration and plays a significant role in maintaining the security and integrity of an operating system. Each user account represents a potential entry point into the system, and improper management can lead to serious security vulnerabilities. Listed bellow are few of the implications:

1. **Control of Access:**

By carefully creating, modifying, and deleting user accounts, administrators control who can access the system and what resources they can interact with. Assigning users to appropriate groups (e.g., `students`) ensures that users only have the permissions necessary to perform their tasks, following the principle of least privilege.

2. **Mitigation of Insider Threats:**

Inactive or unused accounts can be exploited by malicious insiders or external attackers if not properly managed. Locking accounts that are temporarily unused and promptly deleting accounts that are no longer needed helps reduce the attack surface.

3. **Incident Response:**

Account locking allows for quick containment of potentially compromised accounts. For example, if suspicious activity is detected under a user's account, locking the account prevents further damage while investigations are ongoing.

4. **Password Security:**

Enforcing strong passwords during account creation ensures that accounts are not easily compromised through brute-force or credential-stuffing attacks. Regularly updating passwords also contributes to ongoing security.

5. **Auditing and Accountability:**

Proper user management ensures that activities on the system can be traced back to specific users. This accountability discourages misuse of the system and aids forensic investigations in the event of a breach.

6. **Compliance:**

Many regulations and security standards require strict user management controls (e.g., GDPR, HIPAA, ISO 27001). Maintaining good user management practices helps organizations remain compliant with such legal and industry requirements.

In conclusion, user account management is not merely an administrative task it is a foundational security control. Regular reviews, timely updates, and adherence to best practices in user management significantly enhance the security posture of any Linux system.

Group Discussion

- **Importance of secure user account management in operating systems:** Secure user account management is a fundamental aspect of operating system security. It ensures that only authorized individuals can access system resources, minimizing the risk of unauthorized access, data breaches, and system compromise. Key reasons why secure account management is vital include:

- **experiences and challenges faced during the hands-on activities.**

Experiences:

- Successfully created a user account student1 and assigned it to the students group.
- Learned the proper use of Linux user management commands such as useradd, usermod, passwd, userdel, and groupadd.
- Practiced locking and unlocking accounts to simulate account compromise scenarios.
- Understood how to check for active processes running under a specific user before deletion.

Challenges Faced:

- **Command Syntax Errors**: Accidentally breaking commands into multiple lines led to errors (e.g., when running usermod -U student1 incorrectly at first).
- **Process Management:** Identifying and terminating active processes for a user required careful attention to avoid affecting critical system processes.
- **Permissions**: Some commands required elevated privileges (sudo). Forgetting to use sudo initially led to permission denied errors.
- **Understanding Outputs:** Interpreting the output of commands such as passwd -S required reading documentation to understand the account status codes (e.g., L for locked, P for active).

Insights gained regarding user management practices.

Through this hands-on activity, I gained several practical and security-related insights into how user account management is handled in Linux systems listed below are few of the insight:

1. **The Importance of the Principle of Least Privilege:** Assigning users only the permissions they need helps reduce the risk of accidental damage or intentional misuse. Adding users to specific groups, rather than granting them wide access, reinforces controlled privilege delegation.

2. **User Accounts Are Entry Points into the System:** Every user account represents a potential attack vector. Managing them carefully especially by locking inactive or compromised accounts is crucial for minimizing the system's exposure to threats.

3. **Account Locking is a Quick Containment Tool:** Locking a user account is a powerful way to immediately halt suspicious activity without deleting the user. This is especially useful in scenarios involving compromised credentials or insider threats.

4. **User Deletion Requires Care:** Simply deleting a user does not always remove their home directory or running processes. I learned that it's important to check for active sessions and to understand the impact of preserving or removing user data.

5. **Strong Password Policies Are Foundational:** Setting strong, secure passwords for user accounts is a basic but vital control. Passwords are often the first line of defense, and ensuring they meet complexity requirements reduces the risk of brute-force attacks.

6. **Proper Documentation Matters:** Maintaining a record of user-related changes (creation, group assignment, password changes, account status) is essential for auditing and accountability. In enterprise environments, these practices support compliance and traceability.

7. **Commands Can Be Powerful and Dangerous:** Some user management commands, especially `userdel -r`, can delete all user data. It's important to double-check syntax and understand the effects of each command to avoid accidental data loss or system misconfiguration.

These insights reinforced the idea that user management is not just a technical task it is a strategic security practice. Regular reviews, proper access control, and good command-line hygiene are key to maintaining system integrity and operational security.