**Assignment Report –** Creating a User with Limited Privileges

Course: Ethical Hacking

**Name: Diya Susan Binu**

**Roll Number:** 2463019

**Index:**

* **Introduction**
* **Objective**
* **Tools & Technologies Used**
* **Implementation Steps**
* **Problems Faced**
* **Output Examples**
* **Educational Benefits**
* **Conclusion**

# Introduction:

Modern systems follow the principle of least privilege to reduce the impact of mistakes and attacks by ensuring users only have the access they need to perform their tasks. This report documents the creation of a low-privilege user student01 on Kali Linux, verification that the user has no sudo rights, and a brief explanation of the security benefits of limited accounts.

# Objective:

* Create user student01 without administrative (sudo) permissions.
* Verify group membership and ensure sudo access is not present.
* Provide evidence via command outputs and /etc/passwd snippet.
* Explain why limiting privileges enhances system security.

# Tools & Technologies Used:

* Kali Linux (VM)
* Shell/Terminal
* Commands: adduser, usermod, userdel (optional), groups, id, cat, sudo -l, grep
* Files: /etc/passwd, /etc/group, /etc/sudoers (view only), /etc/sudoers.d/\* (view only

# Implementation Steps:

**Step 1: Add a New User Account (‘student01’)**

**Run the following command:**

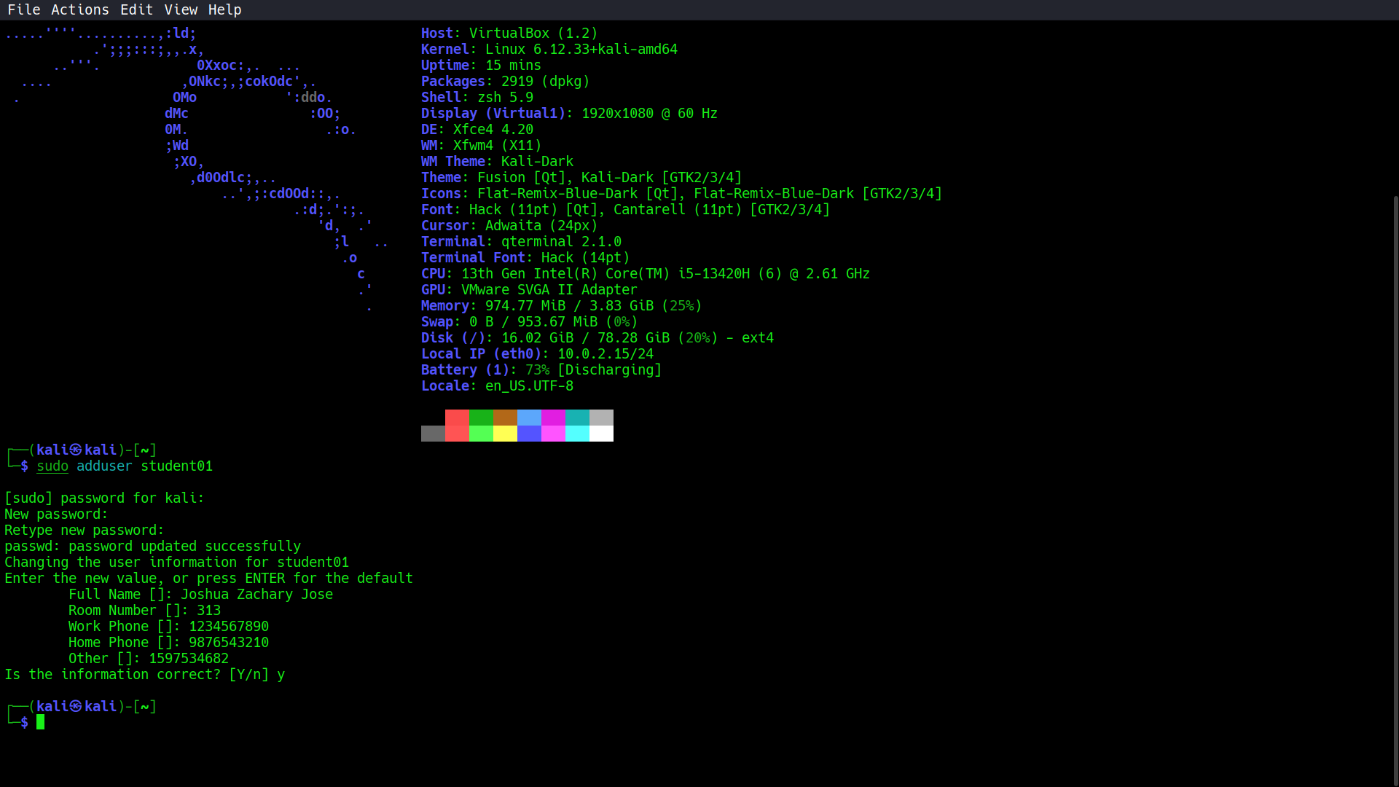
**sudo adduser student01**

**The system will prompt you for details such as full name and contact information (optional). Press Enter to skip or fill them in.**

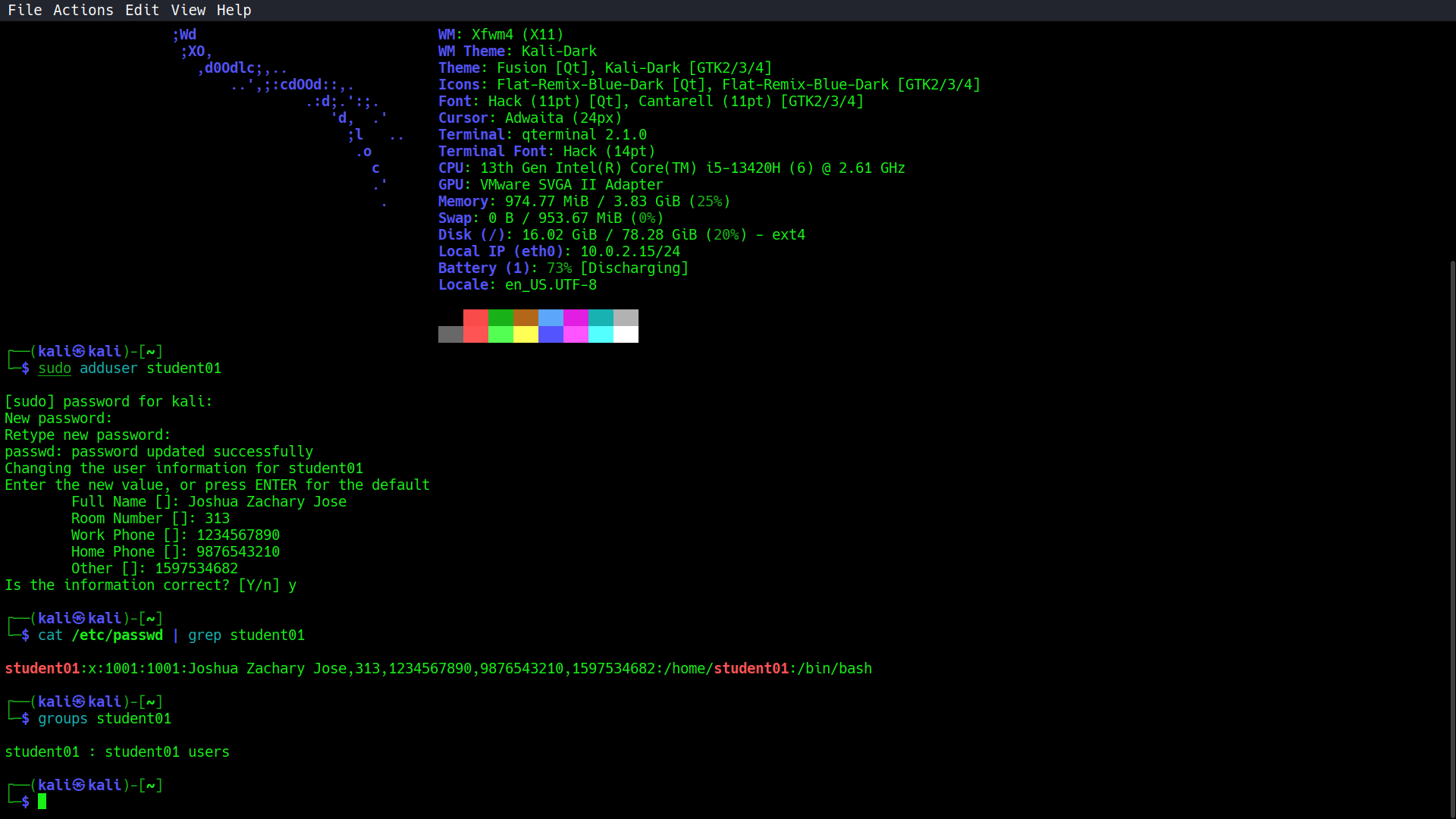
**To confirm successful creation, type:**

**groups student01**

**This will display the groups the user belongs to (see Fig.2).**



**Fig.1: Creation of User and Entering Data about User ‘student01’**



**Fig.2: Verification of Creation of User**

**Step 2: Remove Administrative Rights from ‘student01’**

**Execute:**

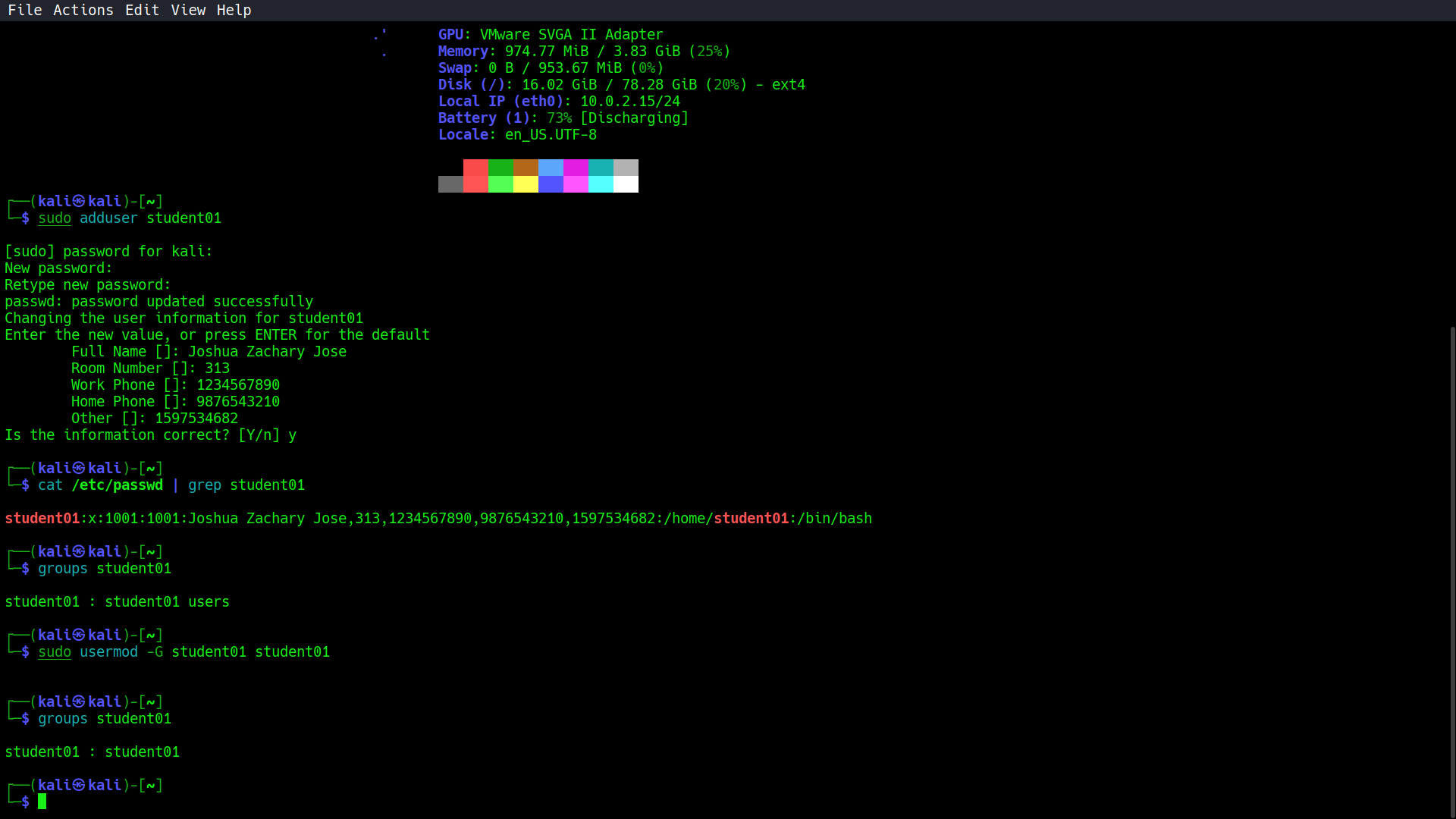
**sudo usermod -G student01 student01**

**This removes ‘student01’ from the sudo group, preventing execution of sudo commands.**

**Check the groups again using:**

**groups student01**

**You should no longer see the sudo group listed (see Fig.3).**



**Fig.3: Removing ‘sudo’ privileges from ‘student01’**

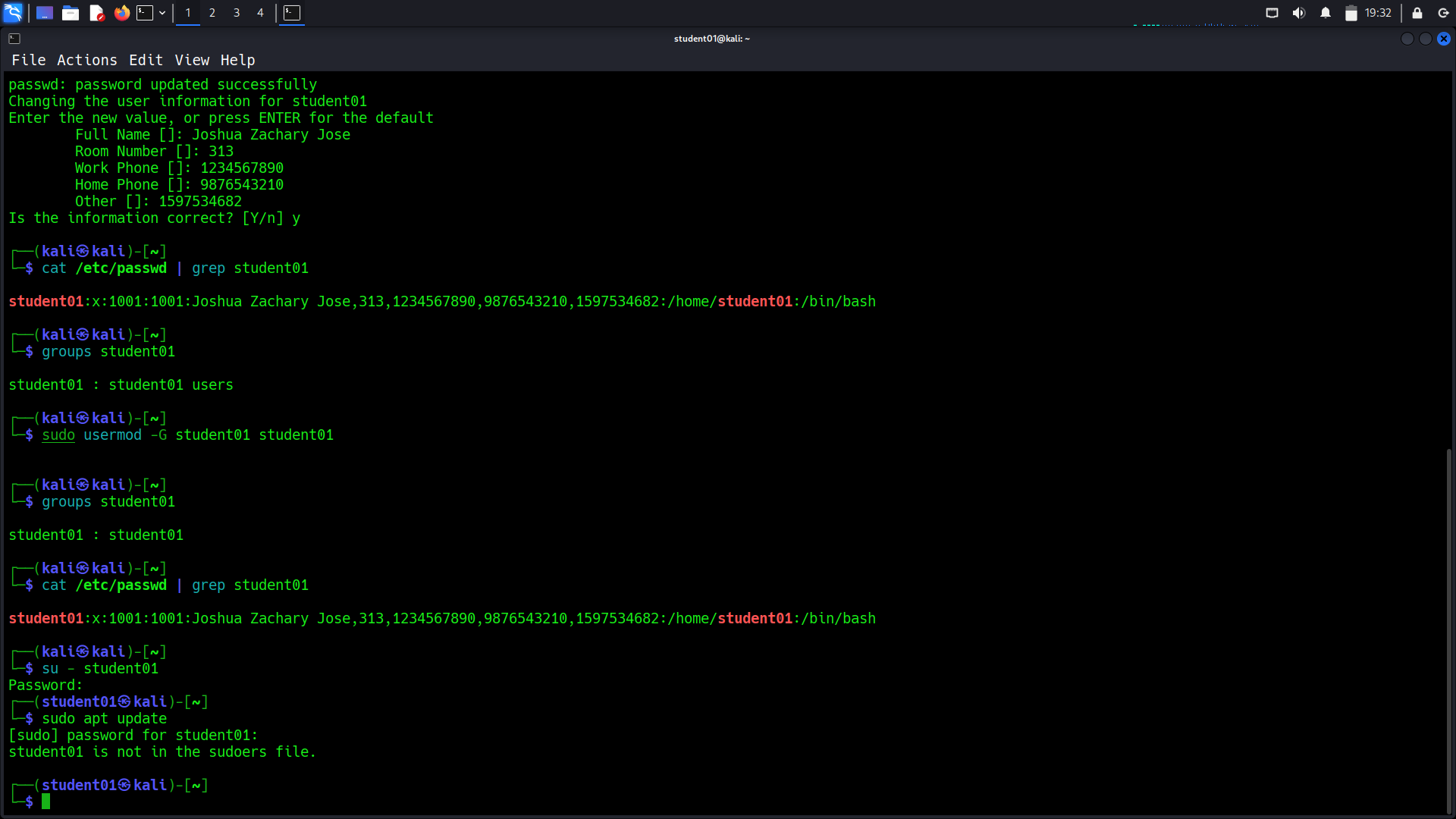
**Step 3: Confirm that ‘student01’ No Longer Has sudo Access**

**You can verify this in two different ways:**

**Method 1: Switch to the ‘student01’ account directly:**

**su - student01**

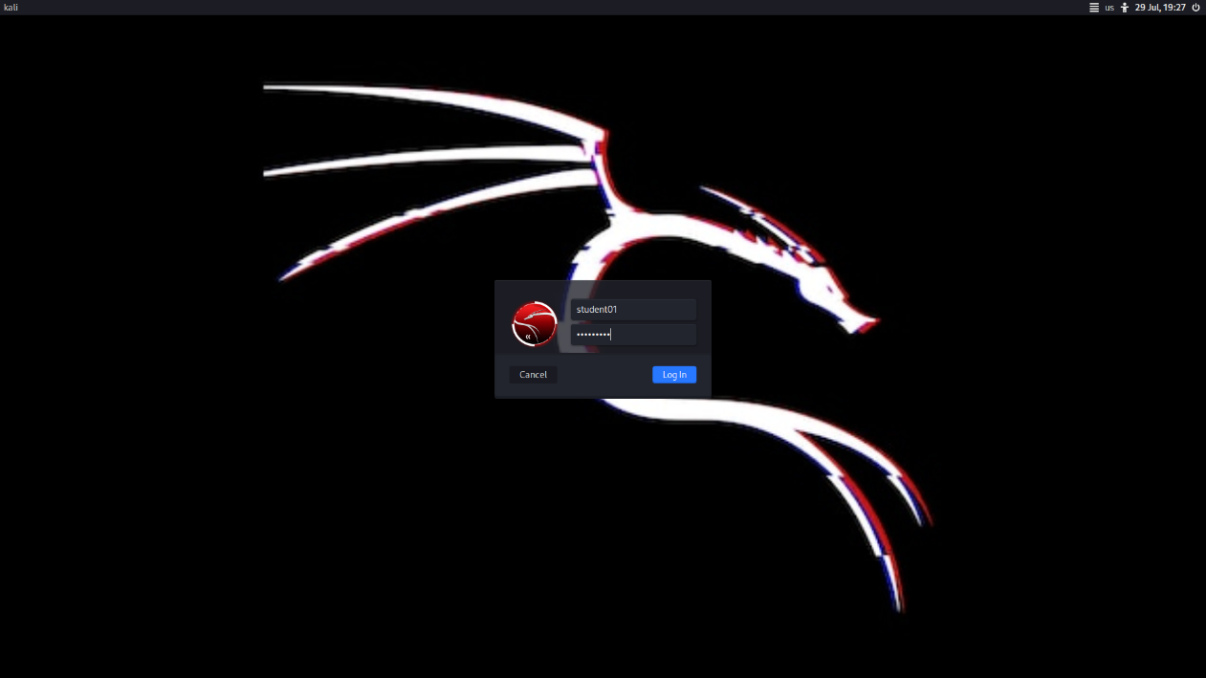
**Then attempt any sudo command — access should be denied (Fig.4).**



**Fig.4: Confirmation that ‘sudo’ privileges are denied, through terminal in main user**

**OR**

**Method 2: Log out from the current user (e.g., ‘kali’) and log in as ‘student01’ (see Fig.5).**



**Fig.5: Logging in to ‘student01’**

**Once logged in, open the terminal and run any sudo command. It should be denied (Fig.6).**

**Why Limiting User Privileges is Important**

**Ensures adherence to the Principle of Least Privilege**

**Minimizes potential harm if an account is compromised**

**Blocks any unauthorized changes to the system**

**Reduces system attack surface and enhances overall security**

# Problem Faced:

* **User accidentally added to sudo: Some setups add non-root users to sudo by default; removing with deluser student01 sudo fixed it.**
* **Cached terminal sessions: After group changes, the existing session may not reflect updates; logging out/in or running newgrp helps.**
* **Misinterpreting sudo -l: Running sudo -l as the admin user reports admin privileges; use sudo -l -U student01 or test from the student01 shell.**

# Output Examples:

* Create user
* $ sudo adduser student01
* Adding user 'student01' ...
* Setting up password ...
* ...
* Verify identity and groups
* $ id student01
* uid=1001(student01) gid=1001(student01) groups=1001(student01)
* $ groups student01
* student01
* Remove from sudo if present
* $ sudo deluser student01 sudo
* Removing user 'student01' from group 'sudo' ...
* Check sudo permissions
* $ sudo -l -U student01
* User student01 is not allowed to run sudo on this host.
* From student01 shell:
* $ su - student01
* $ sudo ls /root
* [sudo] password for student01:
* student01 is not in the sudoers file. This incident will be reported.
* /etc/passwd snippet
* $ grep "^student01:" /etc/passwd
* student01:x:1001:1001:,,,:/home/student01:/bin/bash
* Include screenshots for:
* adduser command and prompts.
* groups/id output showing no sudo.
* sudo denial message from student01 shell.
* /etc/passwd grep line.

# Educational Benefits:

* Reinforces least privilege: Minimizes blast radius of user errors and malware.
* Hardens system: Reduces risk of privilege escalation due to misconfigurations.
* Teaches Linux account and group management: Practical exposure to adduser, groups, sudoers.
* Auditable configuration: Clear, reproducible steps and evidence help in security reviews.

# Conclusion:

A non-privileged user student01 was created on Kali Linux and verified to have no sudo access. This configuration aligns with the principle of least privilege, lowering the risk of unauthorized system changes and improving overall security posture. Evidence via commands and /etc/passwd confirms the account is standard and not part of the sudo group.