Linux IAM & System Hardening

Name: Vikash Kumar
ERP: 6604703
Course: B.Tech CSE (Cybersecurity)
Semester: 5th | Section: CY5A

1. INTRODUCTION

This project focuses on implementing Identity and Access Management (IAM) and Linux system hardening. IAM ensures correct access control based on user roles while hardening minimizes security risks by removing vulnerabilities. This project simulates Admin, Developer, and Auditor roles.

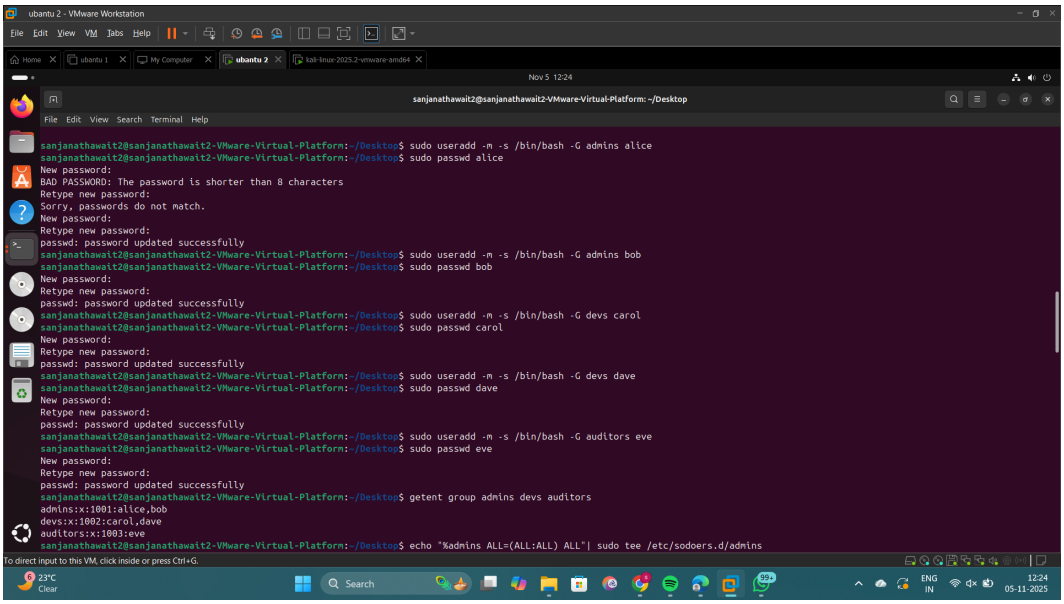
2. PROJECT OBJECTIVE

• To configure secure role-based access control in Linux. • To implement least privilege access using sudo and ACL. • To simulate real-world attack scenario using Kali Linux. • To identify security weaknesses and apply system hardening. • To document results with proof of execution.

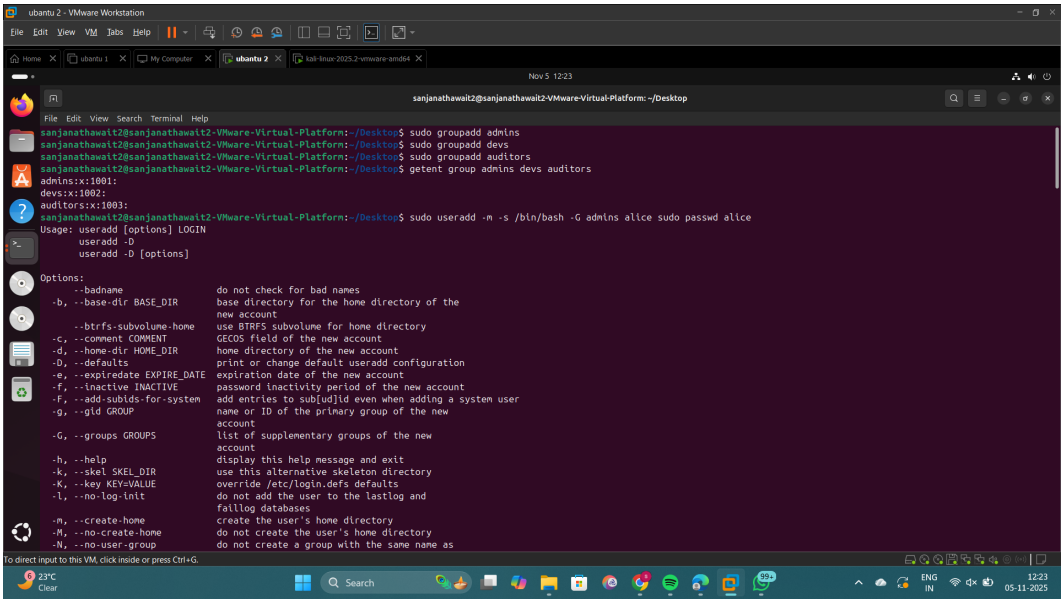
3. TOOLS USED

• Ubuntu Linux (Target System) • Kali Linux (Attacker System) • User and Group Management Utilities • sudo and ACL Permissions • auditd Monitoring Service • SSH, nmap and basic networking utilities

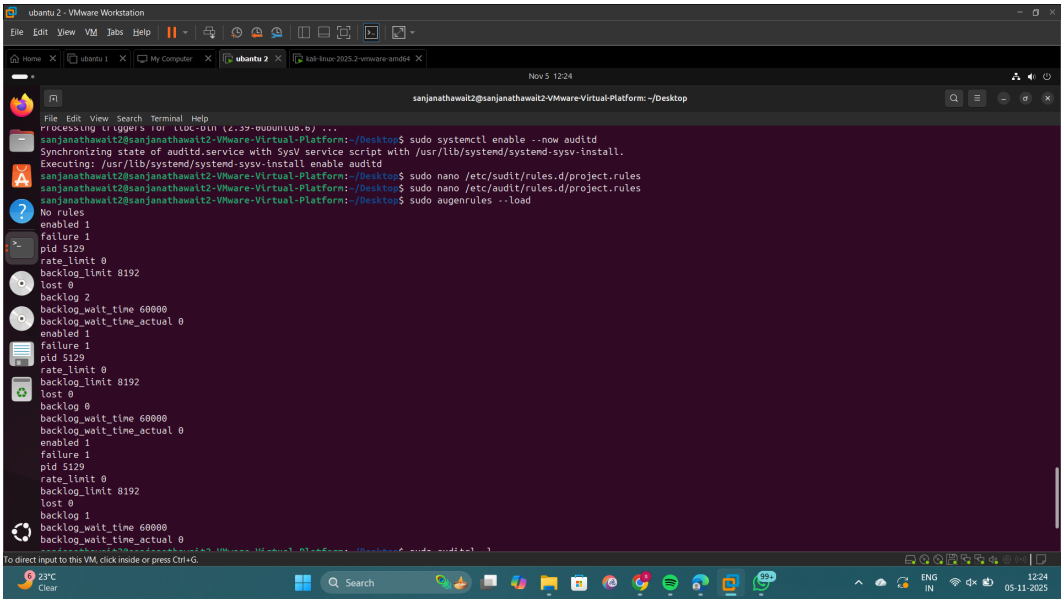
4. PRACTICAL EXECUTION EVIDENCE



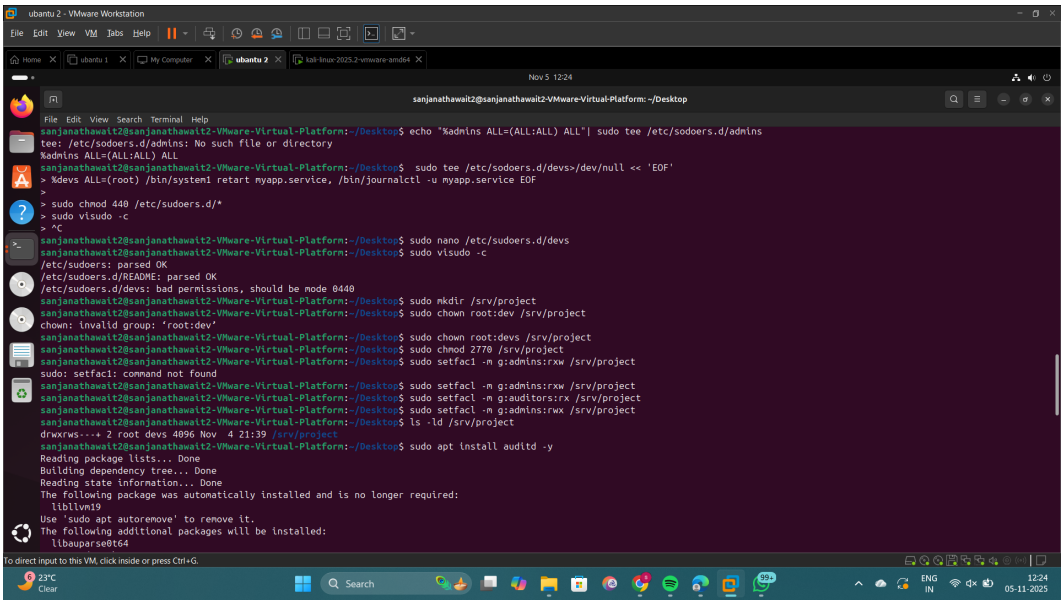
Proof of Execution



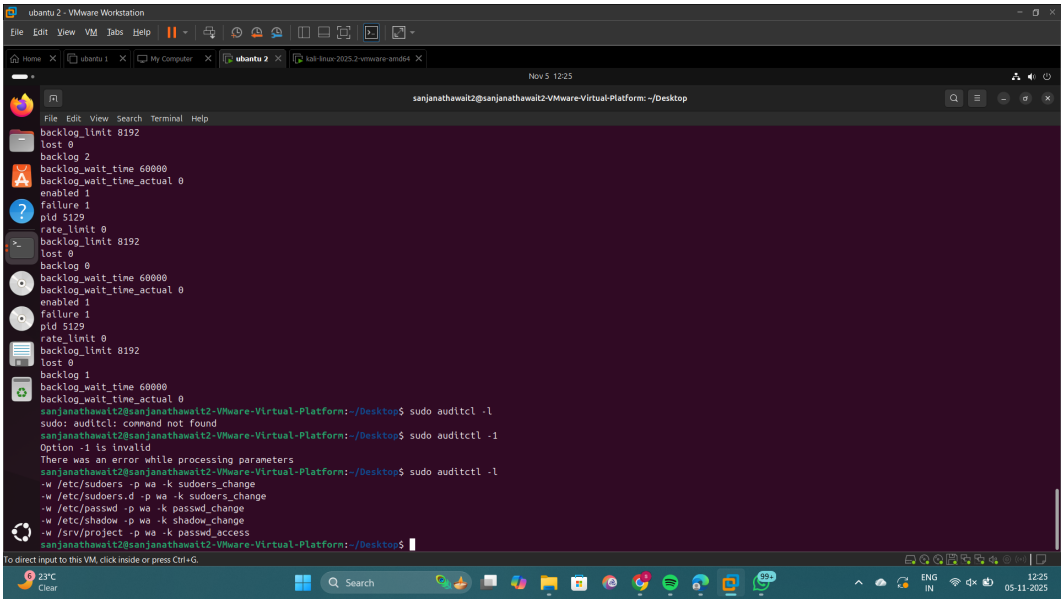
Proof of Execution



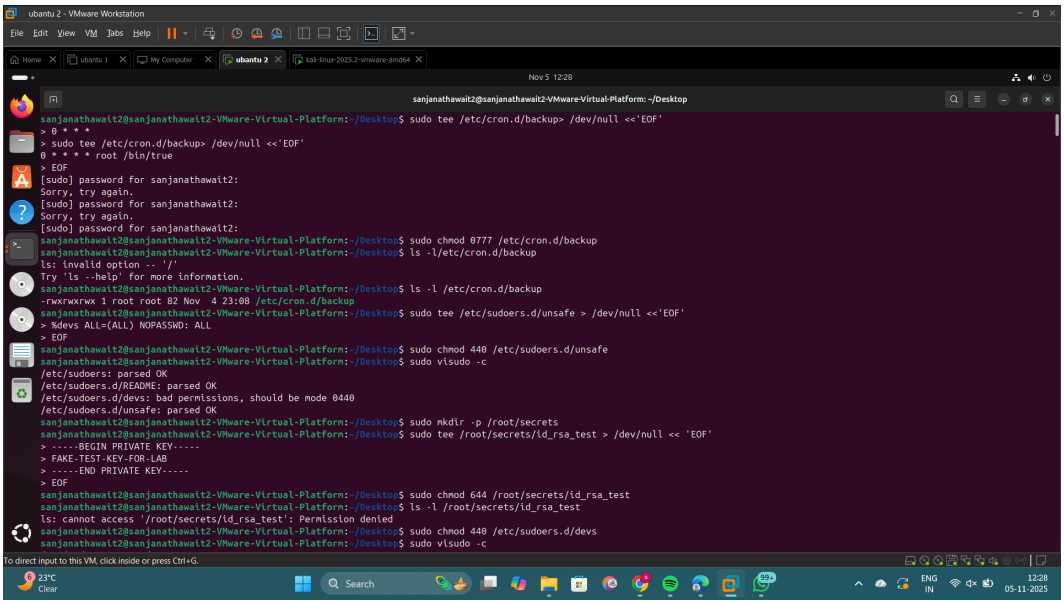
Proof of Execution



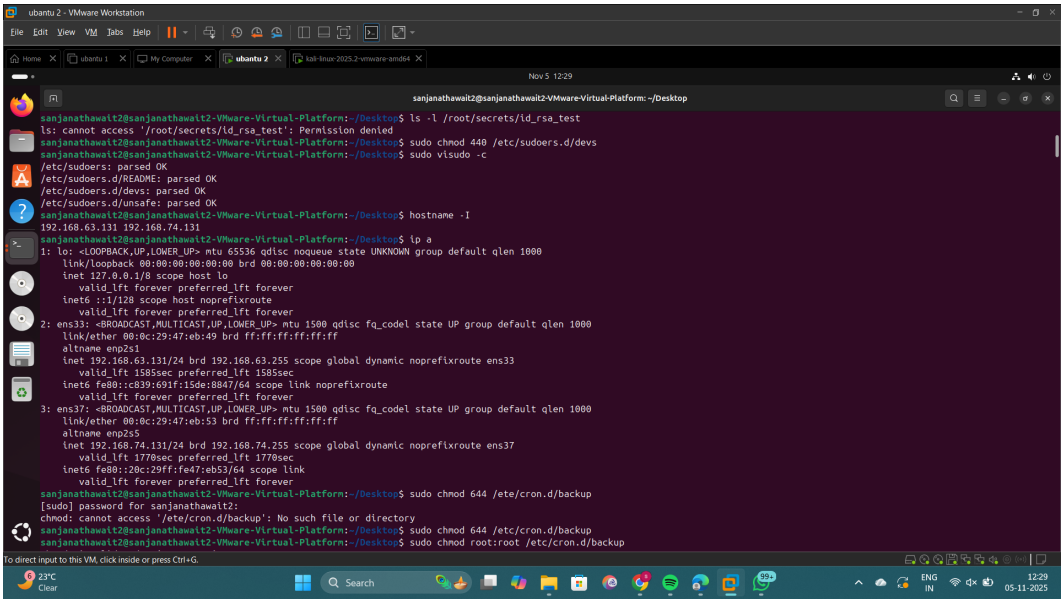
Proof of Execution



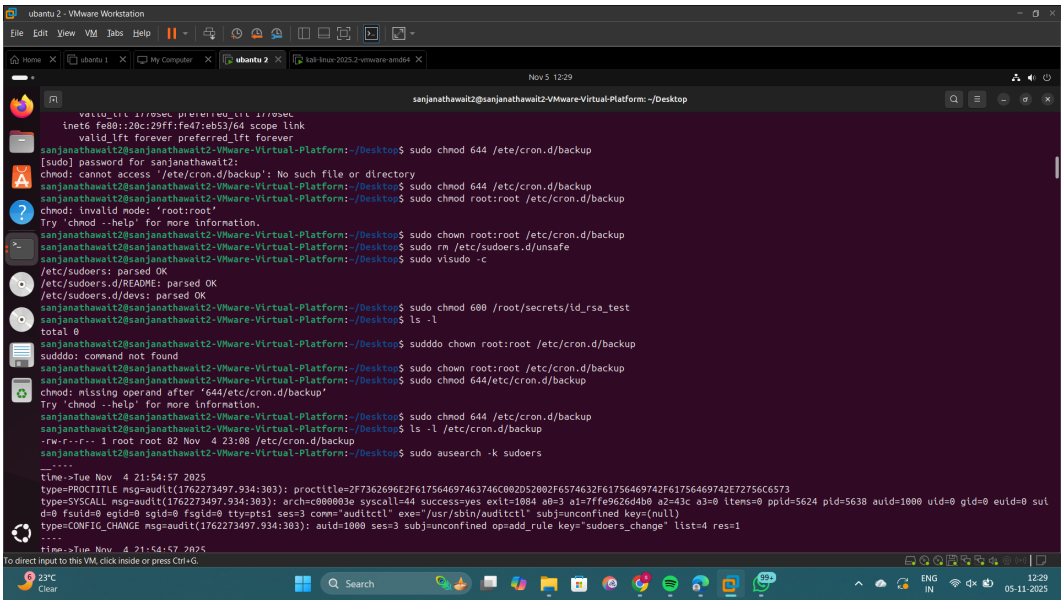
Proof of Execution



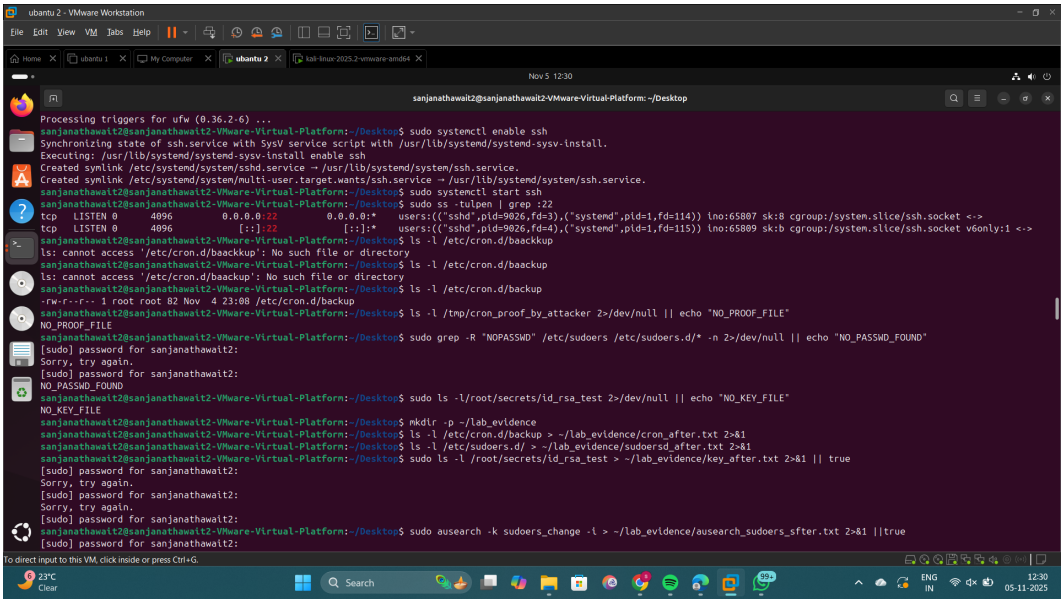
Proof of Execution



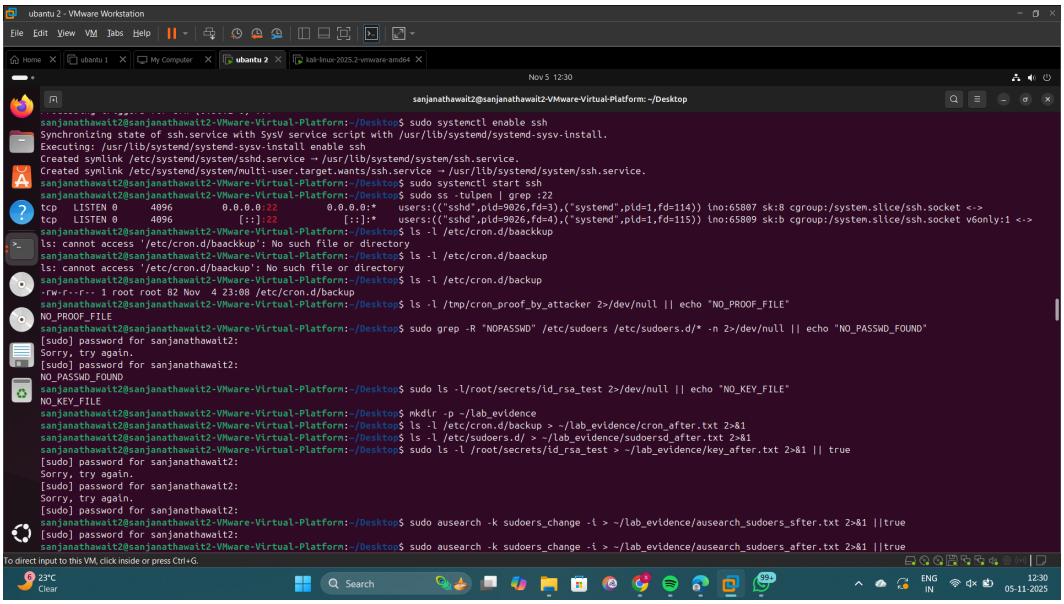
Proof of Execution



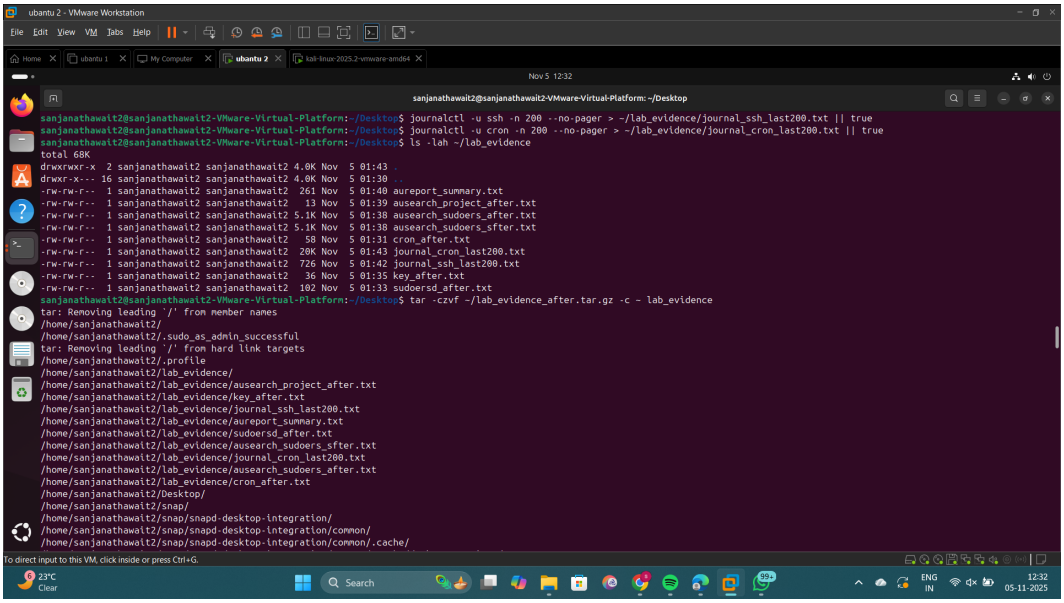
Proof of Execution



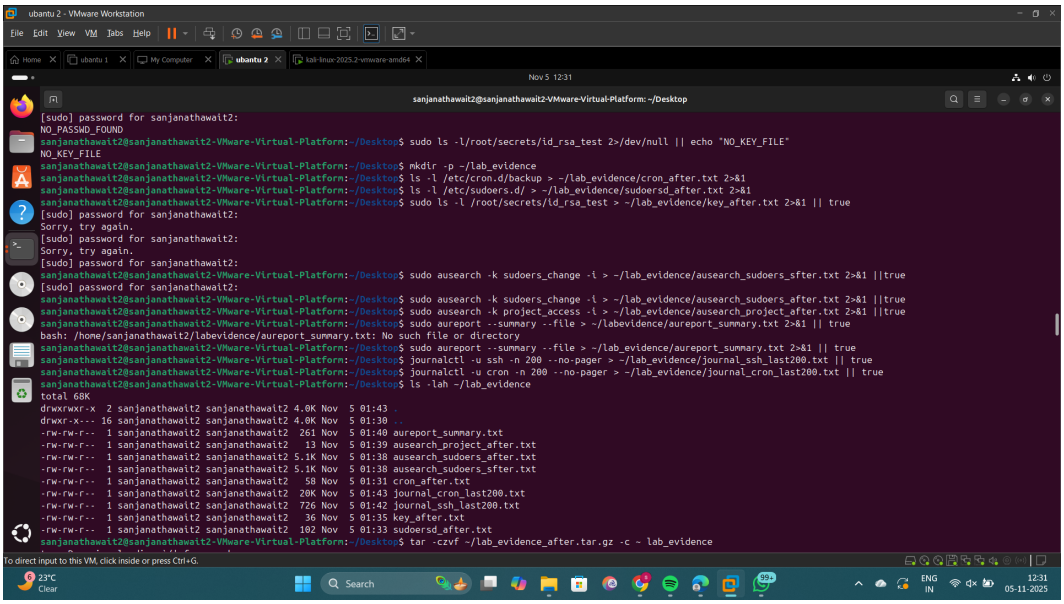
Proof of Execution



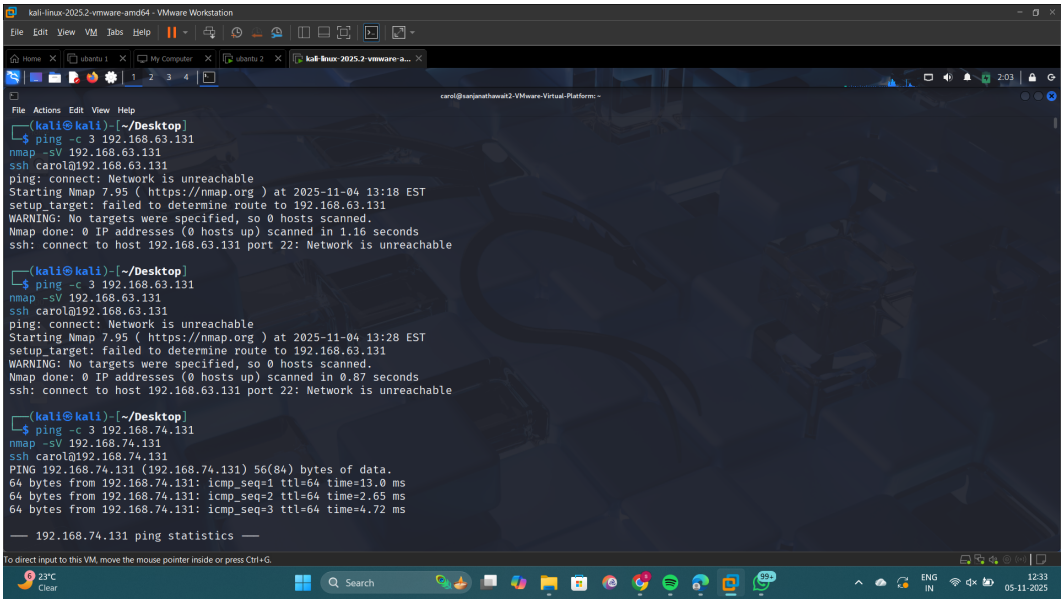
Proof of Execution



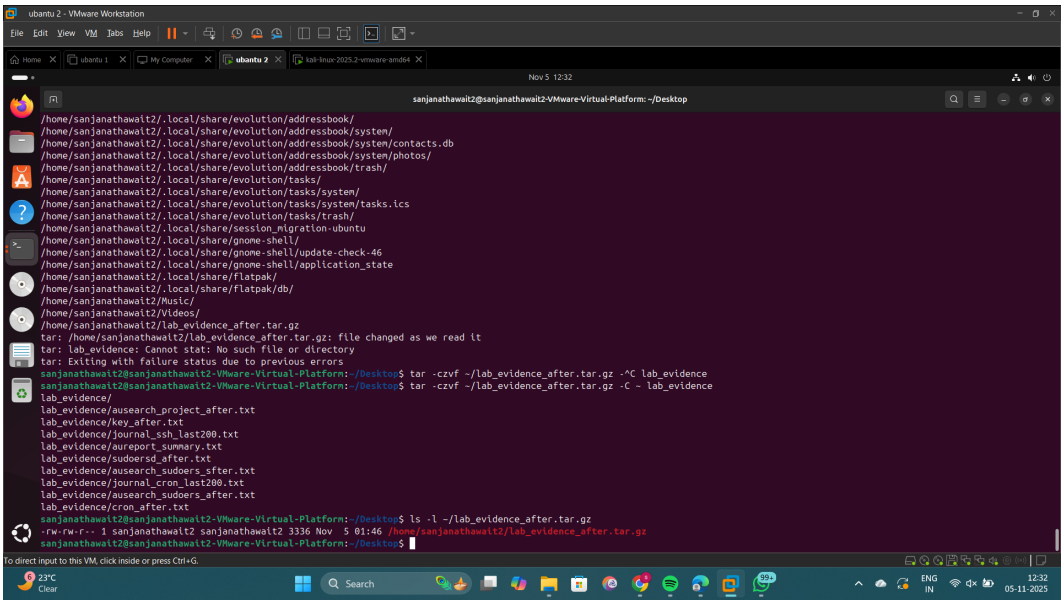
Proof of Execution



Proof of Execution

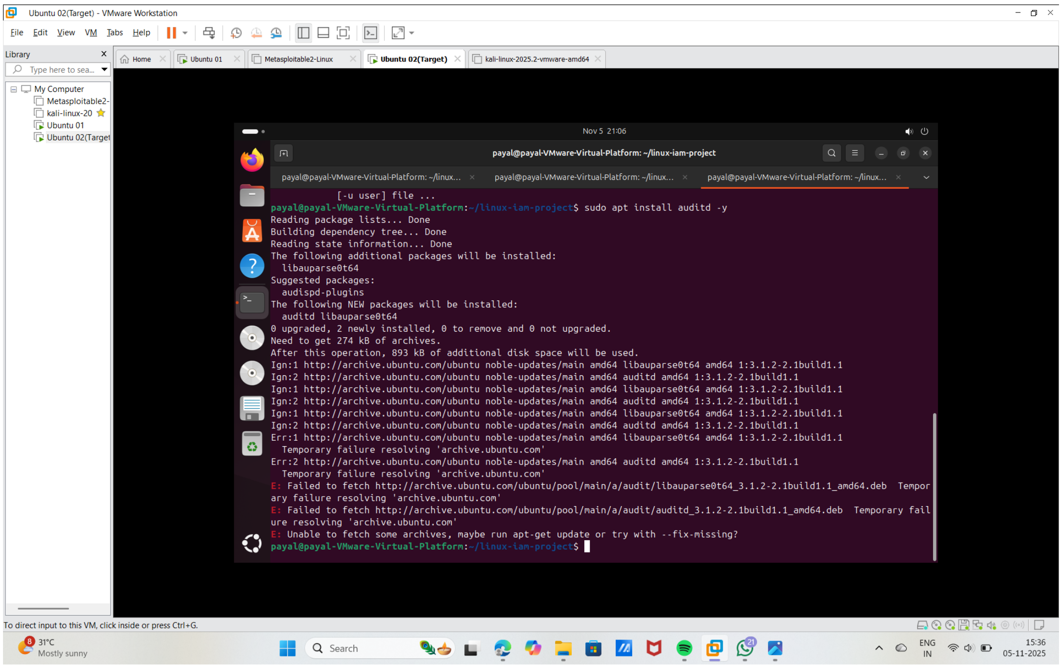


Proof of Execution

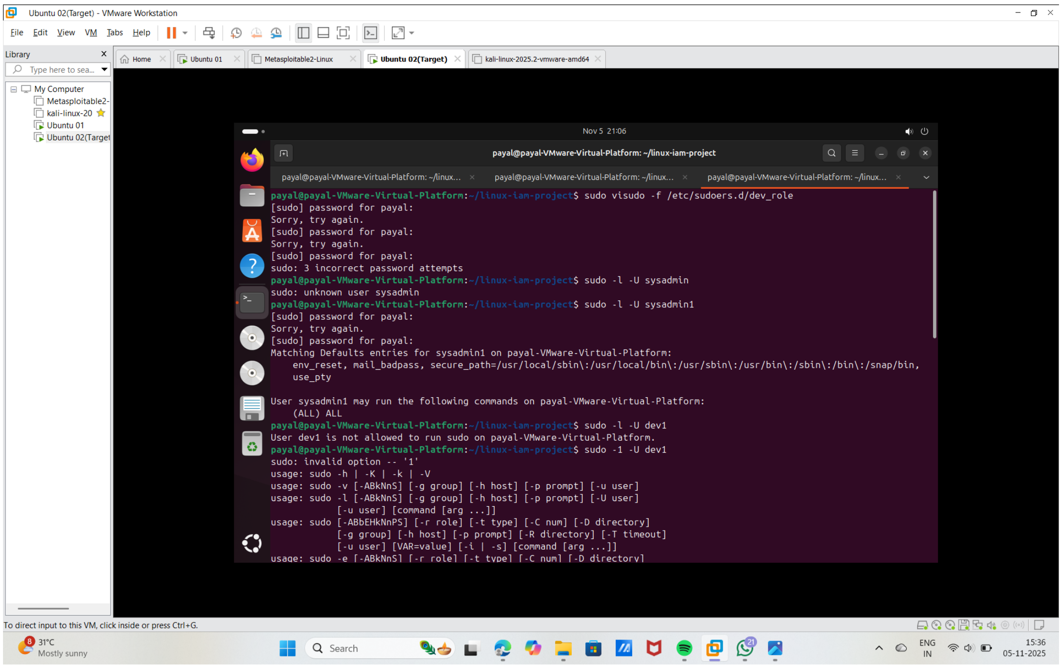


Proof of Execution

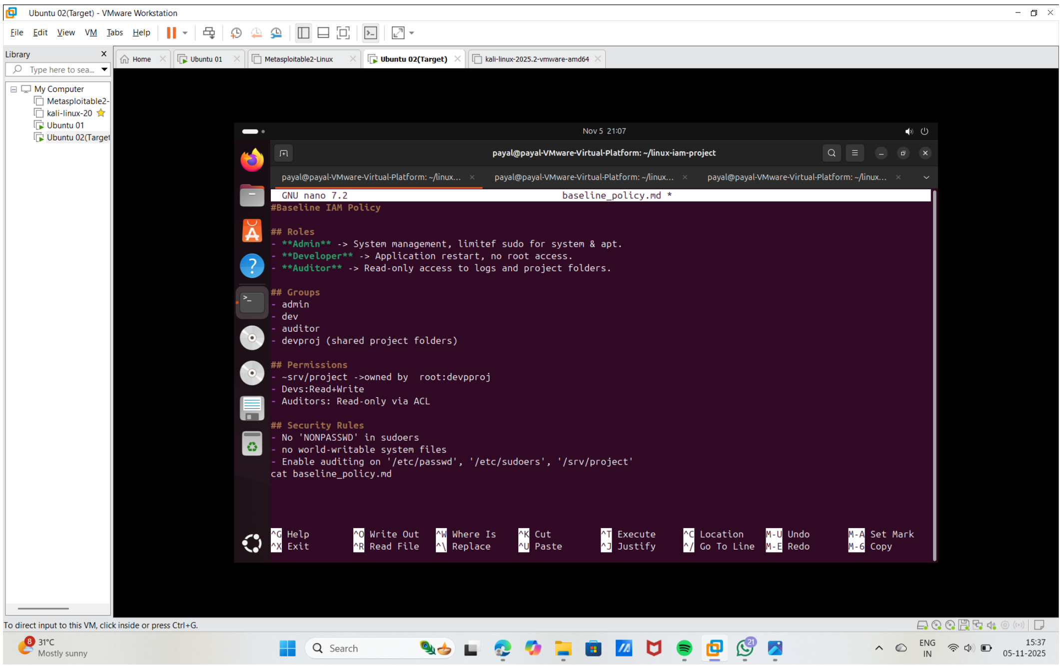
5. UPDATED PRACTICAL EXECUTION (ADDITIONAL)



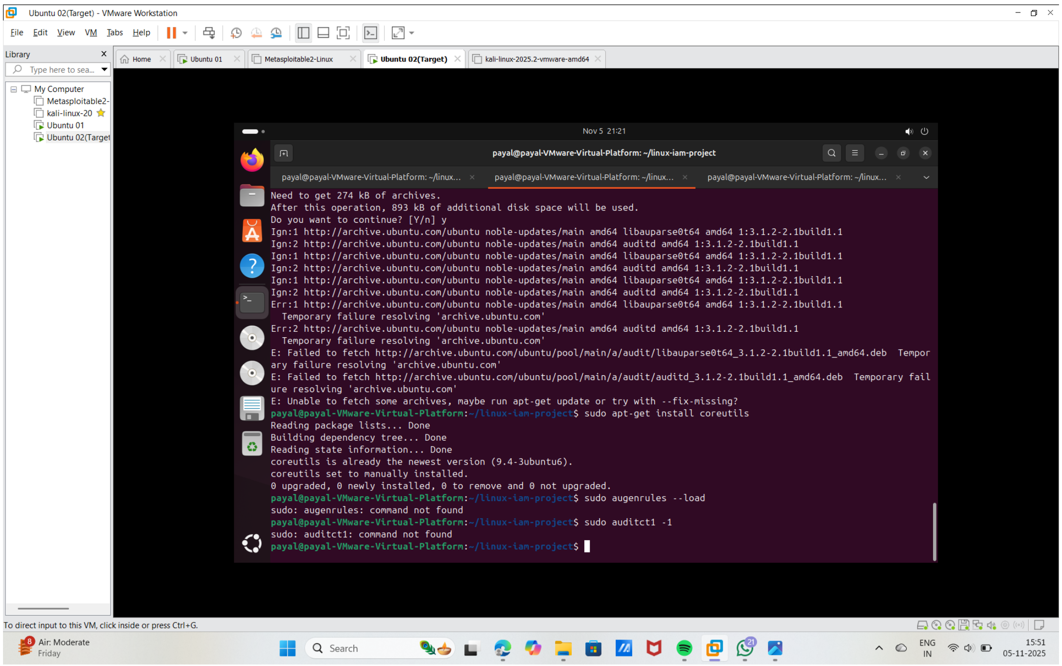
Proof of Execution



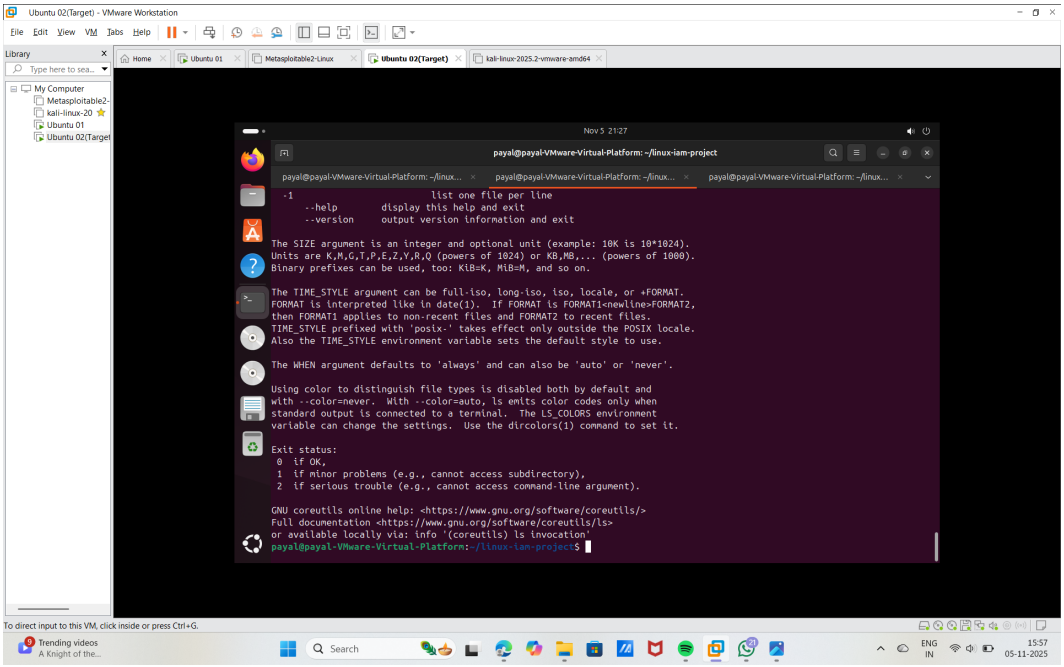
Proof of Execution



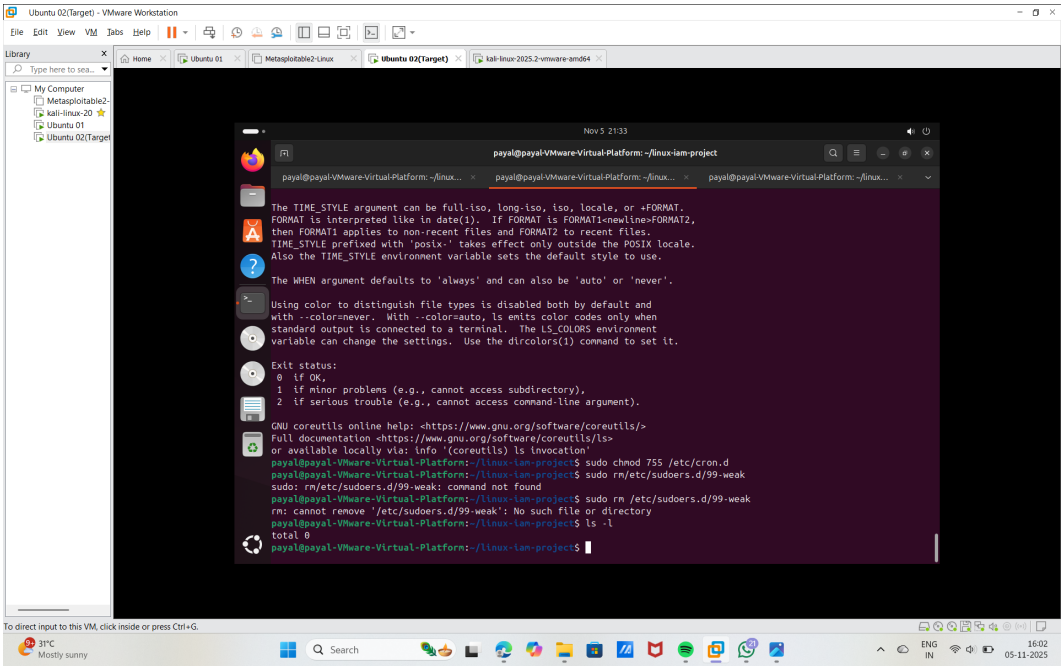
Proof of Execution



Proof of Execution



Proof of Execution



Proof of Execution

CONCLUSION

Linux IAM and system hardening ensure that user privileges remain controlled and attackers cannot exploit misconfigurations. By applying ACL rules, strict sudo permissions, secure SSH settings and monitoring using auditd, the risk of privilege escalation is significantly reduced. This project demonstrates how proper configuration defends against attacks, proving security depends more on discipline than just tools.