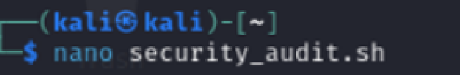
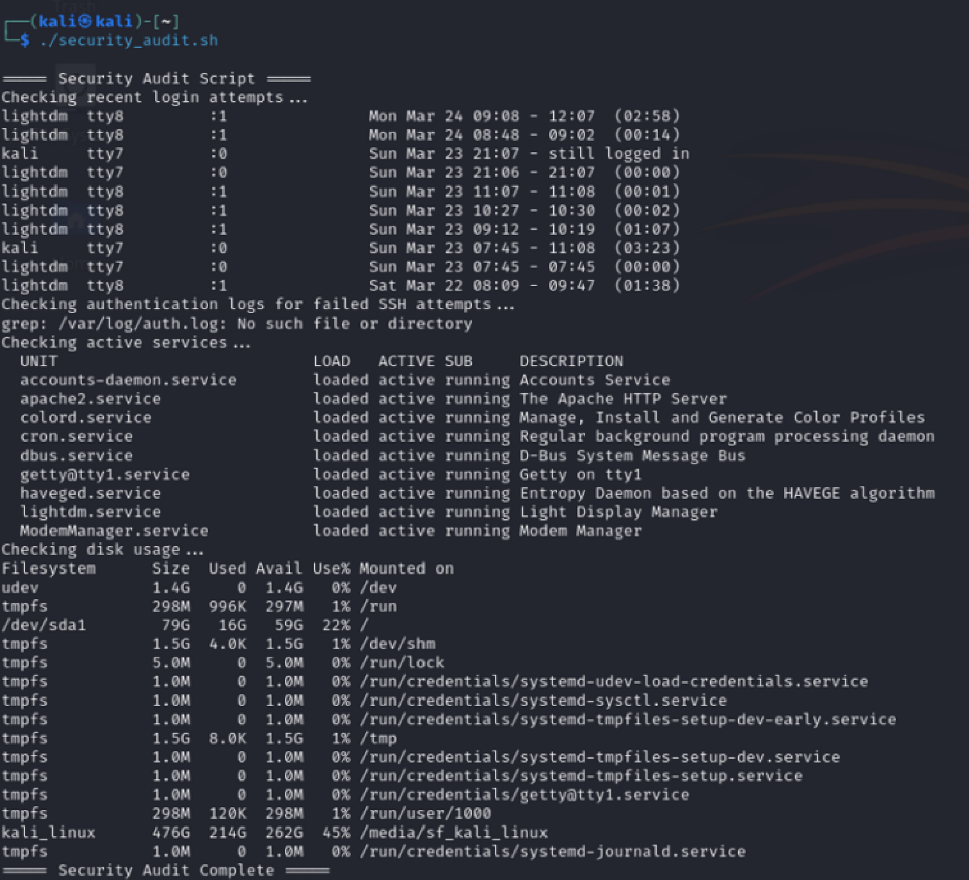
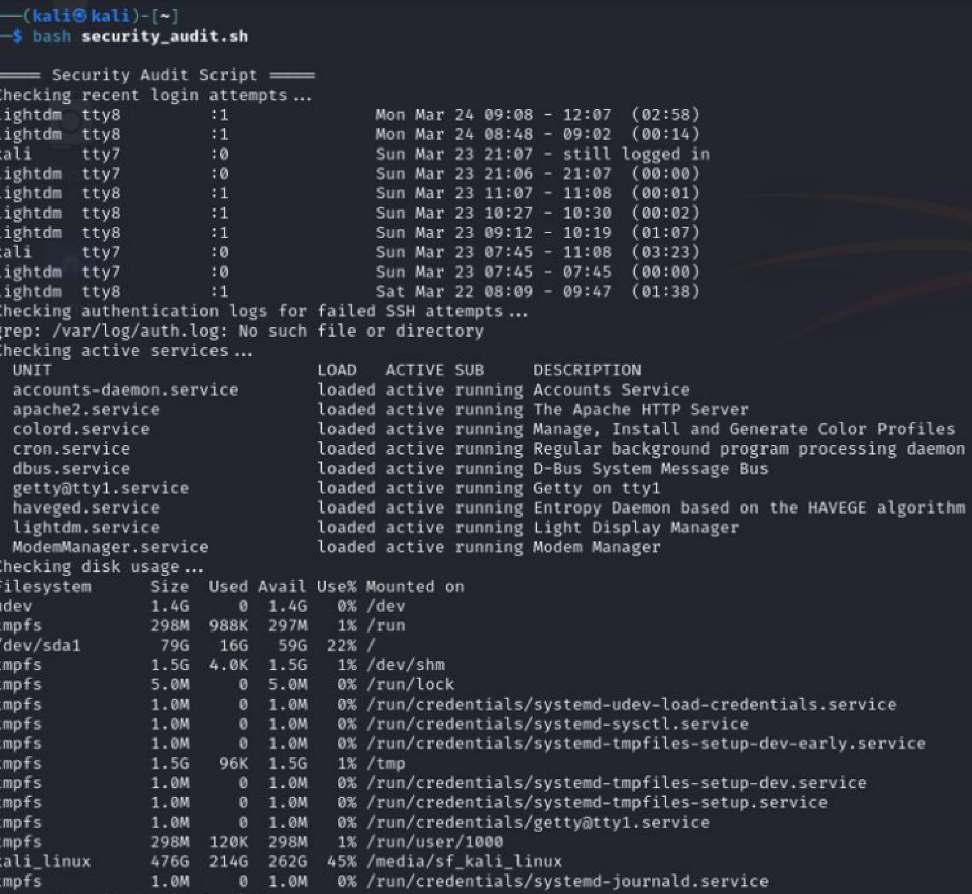
**Task 5: Automated Security Auditing & Scripting**

Step 1: Setup – Write a Security Auditing Bash Script

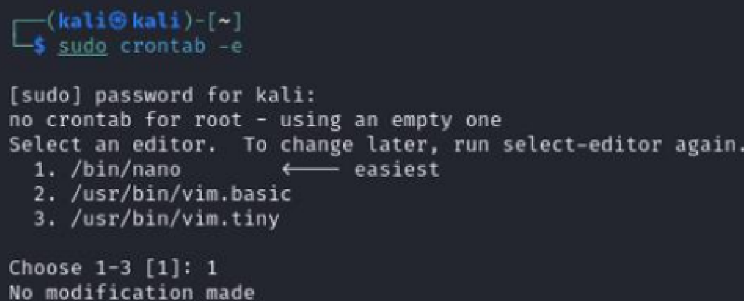


Step 2: Exploit – Identify Weak Configurations

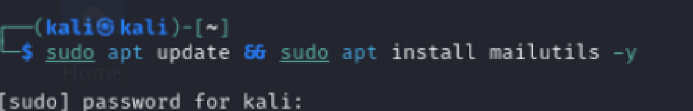




Step 3: Mitigation – Automate & Secure the System



Disable Unused Accounts



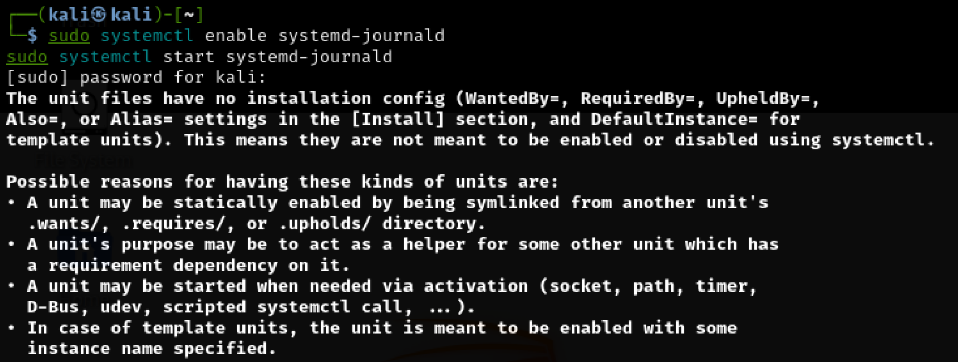
**Summary**

**Setup:** Created a **Bash security audit script**.  
 **Exploit:** Identified **weak accounts & failed SSH attempts**.  
 **Mitigation:** Automated monitoring using **cron & email alerts**.

**Task 6: Log Analysis & Intrusion Detection**

**Step 1: Setup – Enable System Logging & Simulate Attacks**

**1. Enable & View System Logs**



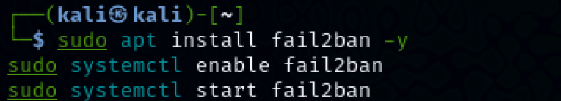
This simulates a **brute-force attack** on SSH.

**Step 2: Exploit – Analyze Logs for Unauthorized Access**

**1. Identify Brute-Force Attempts**



Step 3: Mitigation – Block Attacks with Fail2ban & Log Monitoring





**Summary**

**Setup:** Enabled **system logs & simulated SSH attacks**.  
 **Exploit:** Analyzed **brute-force attempts** in /var/log/auth.log.  
 **Mitigation:** **Configured fail2ban & automated log monitoring**.