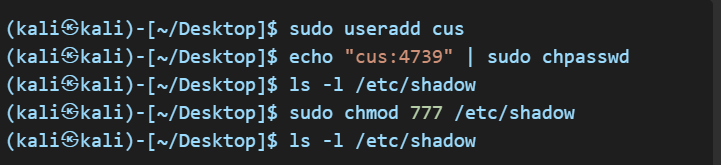
**POC TASKS**

**Task 1: User & Permission Misconfigurations**

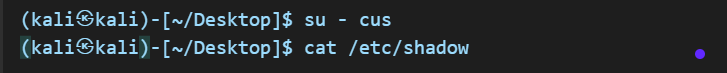
**Description:**

Improper file permissions can allow unauthorized users to access sensitive system files, leading to privilege escalation. This task demonstrates how weak permissions pose security risks and how to secure them properly.

**Setup: Creating Users & Misconfiguring Permissions**



**Exploitation: Accessing Sensitive Files**

**Mitigation: Fixing Security Issues**

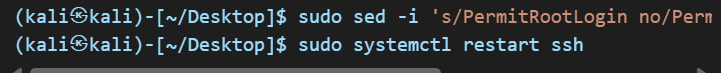


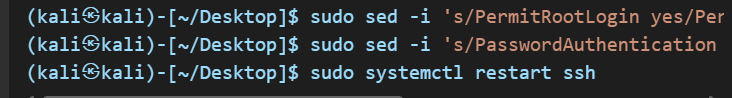
**Task 2: Remote Access & SSH Hardening**

**Description:**

Weak SSH configurations can allow unauthorized users to gain system access. This task covers common SSH vulnerabilities and best practices for securing remote access.

**Setup: Weak SSH Configuration**

****

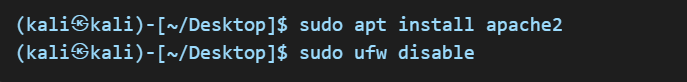
**Mitigation: Secure SSH**

**Task 3: Firewall & Network Security**

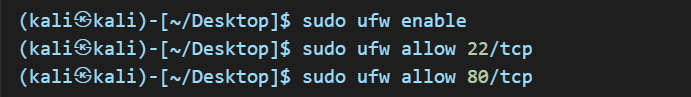
**Description:**

A misconfigured firewall can expose a system to unauthorized access. This task demonstrates how to scan open ports and configure firewall rules for security.

**Setup: Open Ports & Firewall Misconfigurations**

****

**Mitigation: Restrict Access**



**Task 4: SUID & Privilege Escalation**

**Description:**

SUID binaries can be abused to gain unauthorized root access. This task highlights how attackers exploit SUID permissions and how to secure these files.

**Setup: Exploitable SUID Permissions**

**Exploitation: Escalating Privileges**



**Mitigation: Remove Unnecessary SUID**



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

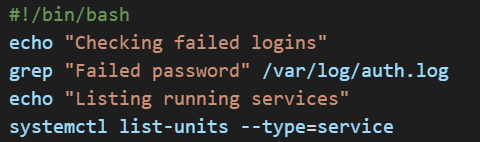
**Description:**

Automated security monitoring helps detect vulnerabilities in real time. This task focuses on writing scripts to monitor login attempts and running services.

**Setup: Writing a Security Audit Script**

**security\_check.sh:**

**Mitigation: Automate Security Checks**

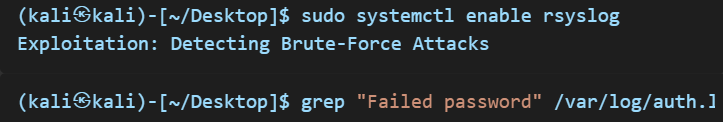


**Task 6: Log Analysis & Intrusion Detection**

**Description:**

System logs provide crucial insights into security threats. This task demonstrates how to analyze logs for failed authentication attempts and implement preventive measures.

**Setup: Enabling System Logs**



**Mitigation: Use Fail2Ban**

