**# Proof of Concept (PoC): Linux Security - Exploitation & Hardening**

## **Task 1: User & Permission Misconfigurations**

### **Objective:**

This PoC demonstrates how improper user permissions can lead to security vulnerabilities in Linux systems. We will exploit misconfigured file permissions and then implement mitigation techniques to secure the system.

## **Step 1: Setup - Creating Users & Misconfiguring Permissions**

**Create multiple users**

**Assign incorrect permissions to sensitive files  
**

* + The above commands make /etc/shadow and /etc/passwd files world-readable and writable, which can allow unauthorized users to manipulate authentication-related information.

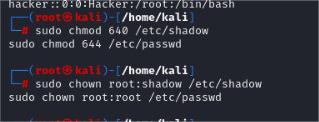
## **Step 2: Exploitation - Demonstrating Unauthorized Access**

**Switch to a low-privileged user and access sensitive files**

**Attempt privilege escalation by modifying /etc/passwd**

* + This creates a backdoor root account (hacker) by adding a user with UID and GID of 0 (root privileges).
  + Exploiting this misconfiguration allows an attacker to gain unauthorized root access.

## **Step 3: Mitigation - Fixing Permission Issues**

**Correct permissions using chmod  
**

**Set correct ownership**

**Restrict sudo access using visudo** sudo visudo

* + Remove unnecessary sudo privileges for users to prevent unauthorized privilege escalation.

## **Deliverables**

1. **Report:**
   * Commands executed
   * Screenshots demonstrating unauthorized access and applied fixes
2. **Video:**
   * Screen recording showing misconfigurations, exploitation, and mitigation in action

## **Conclusion:**

This PoC highlights the risks of improper file permissions and demonstrates how attackers can exploit misconfigurations to escalate privileges. By applying security best practices such as **restricting file permissions, enforcing correct ownership, and managing sudo access**, we can significantly enhance the security posture of Linux systems.