**Proof of Concept**

**Linux Security - Exploitation & Hardening**

**Task 1: User & Permission**

**Misconfigurations**

# Executive Summary

This PoC demonstrates how incorrect permissions on sensitive system files (e.g., /etc/shadow) can allow low-privileged users to access critical information. The task involves creating users, misconfiguring file permissions, exploiting the misconfiguration, and then mitigating the issue by restoring proper permissions and ownership.

# Objectives

**Setup:** Create users and assign incorrect permissions to sensitive files.

**Exploit:** Demonstrate how a low-privileged user can access sensitive files.

**Mitigation:** Fix the permission issues and prevent unauthorized access.

# Setup

**3.1.** Create Users Two users, alan and selvan, were created using the useradd command, and passwords were assigned using the passwd command.

**Commands Used:**

sudo useradd <username>

sudo passwd <username>



**3.2 Assign Incorrect Permissions**

The permissions for the /etc/shadow file were changed to 777 (read, write, and execute for everyone), making it accessible to all users.

**Commands Used:**

sudo chmod 777 /etc/shadow



# Exploitation

**4.1.** Access Sensitive File as Low-Privileged User The user alan alamwas able to switch to their account using the su command and access the /etc/shadow file, which contains encrypted password hashes.

**Commands Used:**

su alan cat

/etc/shadow





# Mitigation

**5.1 Restore Proper Permissions**

The permissions for /etc/shadow were corrected to 640, and ownership was restored to root:shadow.

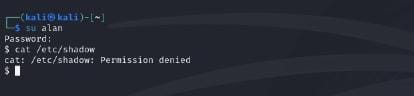
**Commands Used:**

sudo chmod 640 /etc/shadow sudo chown root:shadow /etc/shadow



**5.2 Verify Mitigation**

After fixing the permissions, the user alan was unable to access the /etc/shadow file.



# Conclusion

This PoC successfully demonstrated how incorrect permissions on sensitive files can lead to unauthorized access. By restoring proper permissions and ownership, the security risk was mitigated.

# Recommendations

* Regularly audit file permissions on critical system files.
* Use tools like auditd or tripwire to monitor changes to sensitive files.
* Educate system administrators about the importance of proper file permissions.