Linux IAM & System Hardening — Secure User, Group & Permissions

✔■ *Objective*

Design and implement secure IAM model, enforce least privilege, configure sudo restrictions, apply file permissions & ACLs, enable auditd, identify misconfigurations, test using attacker VM.

✔■ *Tools*

Ubuntu VM, Kali VM, VirtualBox/VMware, auditd, sudo, useradd, visudo, chmod, ACL tools

✔■ *Role-Based Access*

Admin: limited sudo | Developer: restart app only | Auditor: read-only | Project Team: shared folder access

✔■ *Security Policies*

Root login disabled, strong passwords, no NOPASSWD sudo, secure file permissions (/etc/passwd 644, /etc/shadow 640), 2775 shared dir permissions

✔■ *Audit Rules*

-w /etc/sudoers -p wa -k sudoers_changes

-w /etc/passwd -p wa -k passwd_changes

✔■ *Misconfig Fixes*

• World-writable cron file → chmod o-w

• NOPASSWD sudo → remove entry

• /etc/shadow readable → chmod 640

✔■ *Testing*

SSH access verified, unauthorized sudo blocked, audit logs tested, attacker VM validation

✔■ *Outcome*

Completed secure Linux hardening with IAM, ACL, sudo restrictions, and auditing