Linux IAM & Hardening Mini — Full Project Report

Student: Abhay Raj
Course: B.Tech | Branch: CSE (Core)
Erp no – 6604180
Semester-5th sem
Instructor: Anshul Kaundal
Date: 05 Nov 2025

1. Objective

Design and implement a secure user/group and permission model on an Ubuntu server, identify and fix three misconfigurations in a deliberately vulnerable lab VM, enable auditing, and produce a remediation report with evidence.

2. Baseline Policy (One Page Summary)

Purpose: Define secure roles, sudo rules, and file access for a small team working on an Ubuntu server.

Roles & Responsibilities

- **Admins**: Limited administrative commands via sudo (no NOPASSWD). Two approvers required for admin group membership.
- **Developers (devs)**: Work on /srv/project; allowed specific service restarts (e.g., systemctl restart myapp.service) via limited sudo. No full sudo.
- **Auditors**: Read-only access to logs and configs; cannot modify.
- **Ops**: Deployment operators; allowed to run deployment scripts via sudo for fixed paths only.

File & Folder Access

- /srv/project: group 'project' owns. SGID set so newly created files inherit group. project members haverwx; auditors placed in project_readers group with rx via ACLs.
- Sensitive files (/etc/sudoers, /etc/shadow): root-owned, strict permissions (0640 or more restrictive),monitored by auditd.

3. Commands & Scripts (copy-paste to lab VM)

3.1 Create groups and users

```
# Groups groupadd admin
groupadd devs groupadd
auditors groupadd ops
groupadd project
groupadd project_readers

# Users (examples) useradd -m -s /bin/bash -G
admin,project alice useradd -m -s /bin/bash -G
devs,project bob useradd -m -s /bin/bash -G devs,project
carol useradd -m -s /bin/bash -G
auditors,project_readers dave useradd -m -s
/usr/sbin/nologin -G ops svc-deploy

# Set passwords interactively (or use chpasswd in automation)
passwd alice passwd bob passwd carol passwd dave
passwd -l svc-deploy  # lock service account
```

3.2 Sudoers (use visudo or /etc/sudoers.d files)

```
# Example /etc/sudoers.d/10-admins (edit with visudo -f)
%admin ALL=(ALL) /usr/sbin/useradd, /usr/sbin/userdel, /usr/sbin/usermod, /usr/bin/systemctl, /usr/bin/apt
%devs ALL=(root) NOPASSWD: /usr/bin/systemctl restart myapp.service, /usr/bin/systemctl status myapp.service
%ops ALL=(root) NOPASSWD: /usr/local/bin/deploy.sh
# Notes: prefer no NOPASSWD; use only when necessary and for specific commands.
```

3.3 Shared project folder: POSIX + ACLs

```
mkdir -p /srv/project chown root:project /srv/project
chmod 2770 /srv/project   # setgid so files inherit group
setfacl -m g:project_readers:rx /srv/project getfacl
/srv/project ls -ld /srv/project
```

3.4 Enable auditd & persistent rules

```
apt update && apt install -y auditd audispd-plugins

cat > /etc/audit/rules.d/50-security.rules <<'EOF' -
w /etc/sudoers -p wa -k sudoers_changes
-w /etc/sudoers.d -p wa -k sudoers_d_changes
-w /etc/passwd -p wa -k passwd_changes
-w /etc/group -p wa -k group_changes
-w /etc/shadow -p wa -k shadow_changes
EOF

service auditd restart #
Verify rules auditctl -l #
Search logs (example) ausearch
-k sudoers_changes -i
```

4. Vulnerable Snapshot Analysis: 3 Misconfigurations

Misconfiguration A — World-writable sensitive files

Description: A sensitive configuration directory or file (e.g., /etc/cron.d or files in /etc/sudoers.d) is world-writable allowing local privilege escalation or planting cron jobs. Detection commands:
find /etc -xdev -type f -perm -0002 -ls
ls -ld /etc/cron.d
Fix commands:
chmod o-w /etc/cron.d
find /etc/sudoers.d -type f -exec chmod 0440 {} \;
chown root:root /etc/sudoers.d/*
Verification:
ls -ld /etc/cron.d find /etc -xdev -type f -perm -0002 -ls (should be empty
for sensitive files)

Misconfiguration B — Unrestricted sudo NOPASSWD

Description: Sudoers contains a broad rule like '%wheel ALL=(ALL) NOPASSWD: ALL' allowing passwordless root access. Detection:
grep -R "NOPASSWD" /etc/sudoers /etc/sudoers.d || true
Fix:
Use visudo to edit offending file, and replace broad rules with command-specific entries or remove NOPASSWD.
Validation: visudo -c grep -R "NOPASSWD" /etc/sudoers* -n || echo "no
NOPASSWD entries"

Misconfiguration C — Weak permissions on sensitive files

Description: Files like /etc/passwd, /etc/shadow, or /root/.ssh/authorized_keys have weak permissions or incorrect ownership. Detection:
stat -c "%n %a %U:%G" /etc/passwd /etc/shadow /etc/group
ls -ld /root /root/.ssh /root/.ssh/authorized_keys || true Fix
commands:
chmod 0644 /etc/passwd chown
root:root /etc/passwd chmod
0640 /etc/shadow chown

root:shadow /etc/shadow
chmod 700 /root/.ssh
chmod 600 /root/.ssh/authorized_keys
chown root:root /root/.ssh/authorized_keys
Verification: use stat and ls -ld to prove corrected modes and owners.

6. Remediation Checklist (Final Deliverable)

1) Remove world-writable bits from system config dirs. 2) Remove/limit NOPASSWD. 3) Fix perms on passwd/shadow. 4) Lock service accounts & nologin. 5) Configure /srv/project with SGID+ACLs. 6) Enable auditd watches. 7) Sudoers in /etc/sudoers.d with visudo -c. 8) Enforce password policy & quarterly reviews. 9) Automate detection via cron/monitoring. 10) Onboard/offboard documented.

10. Final State Summary

Least-privilege model applied; shared resources protected with POSIX+ACL; auditd monitors critical files; misconfigurations remediated and validated with before/after evidence.