

Linux IAM & Hardening — Remediation Report
Author: Priyanshu Dewangan
Institute: Rungta College of Engineering and Technology
Course: Ethical Hacking Project
Department: Computer Science & Engineering
Submission: November 2025

1. Objective

Implement a minimal, secure IAM model on a Kali Linux lab VM, detect and fix common misconfigurations, and provide evidence and a remediation checklist.

2. Environment

- OS: Kali Linux (Debian-based)
- Test VM: lab snapshot (instructor-provided) or student-created vulnerable snapshot.
- Privileges: sudo

3. Baseline policy

(see baseline_policy.txt)

4. Implementation summary

- Groups created: sysadmin, project, auditor
- Users created: alice (sysadmin), bob, carol (project), dave (auditor)
- Shared folder: /srv/project owned by root:project with setgid and default ACLs
- Sudoers: /etc/sudoers.d/sysadmin created with explicit allowed commands for sysadmin and project.
- Auditing: manual audit entries written to /var/log/manual_audit.log

5. Misconfigurations discovered & remediation (examples)

A. World-writable /etc/cron.d

- Detection: ``ls -ld /etc/cron.d`` showed global write bit
- Fix: ``chmod 755 /etc/cron.d``
- Evidence files: evidence/cron_perms.txt (before/after)

B. Unrestricted sudo (NOPASSWD)

- Detection: ``grep -R "NOPASSWD" /etc/sudoers*``
- Fix: remove NOPASSWD entries, replace with explicit command whitelist
- Evidence files: evidence/nopasswd_check.txt

C. Weak permissions on /etc/passwd or private keys

- Detection: ``ls -l /etc/passwd /etc/shadow``

- Fix: `chmod 644 /etc/passwd` and `chmod 600 /etc/shadow`
- Evidence files: evidence/passwd_perms.txt

6. Evidence collection

Run the script and collect outputs from:

- ~/iam_project/evidence/
- /var/log/manual_audit.log

7. Recommendations

- Replace temporary passwords with SSH keys
- Use auditd or centralized SIEM for production auditing
- Maintain change log for sudo exceptions and review monthly

8. Appendix: Key commands (run on the lab VM)

```
sudo groupadd -f sysadmin project auditor
sudo useradd -m -s /bin/bash -G sysadmin alice
sudo useradd -m -s /bin/bash -G project bob
sudo useradd -m -s /bin/bash -G project carol
sudo useradd -m -s /bin/bash -G auditor dave
sudo chown root:project /srv/project
sudo chmod 2775 /srv/project
sudo setfacl -R -m g:project:rwx /srv/project
sudo tee /etc/sudoers.d/sysadmin <<'EOF'
%sysadmin ALL=(ALL) /usr/sbin/useradd, /usr/sbin/usermod, /usr/sbin/userdel,
/usr/bin/passwd, /bin/systemctl,/usr/bin/apt-get,/bin/journalctl
%project ALL=(root) /bin/systemctl restart myapp.service, /bin/systemctl status
myapp.service
EOF
sudo chmod 0440 /etc/sudoers.d/sysadmin
sudo chmod 644 /etc/passwd
sudo chmod 600 /etc/shadow
```