PROJECT REPORT

ON

Linux IAM & System Hardening

Submitted By:
Name: Abhay Raj
ERP No: 6604180
Course: B.Tech (CSE - Core)
Semester: 5th Sem

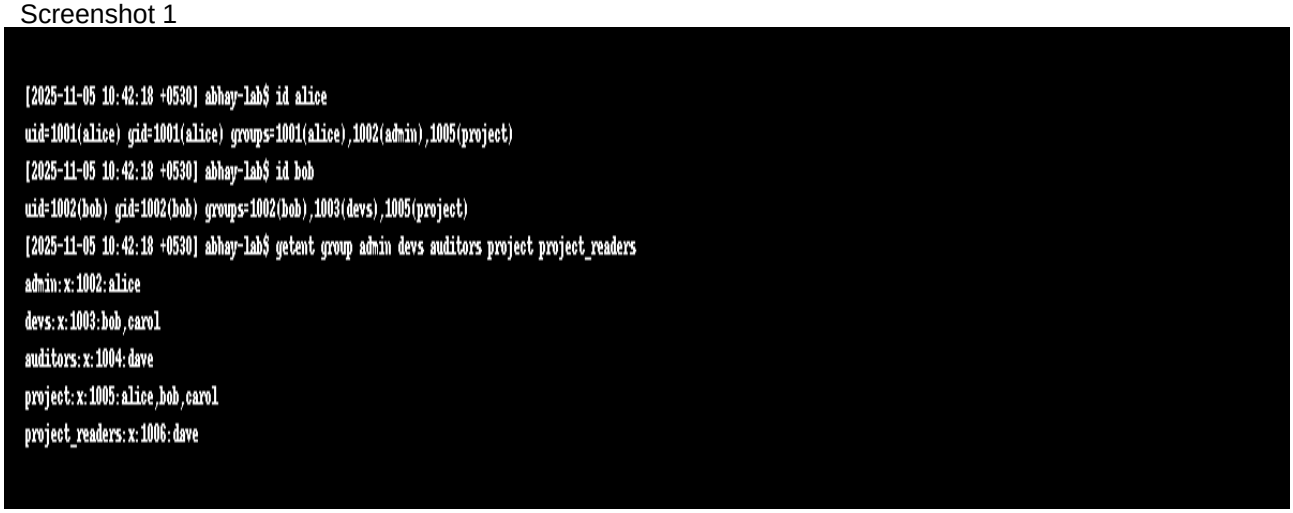
Rungta College Of Engineering and Technology

Linux IAM & Hardening - Full Report with Embedded Evidence

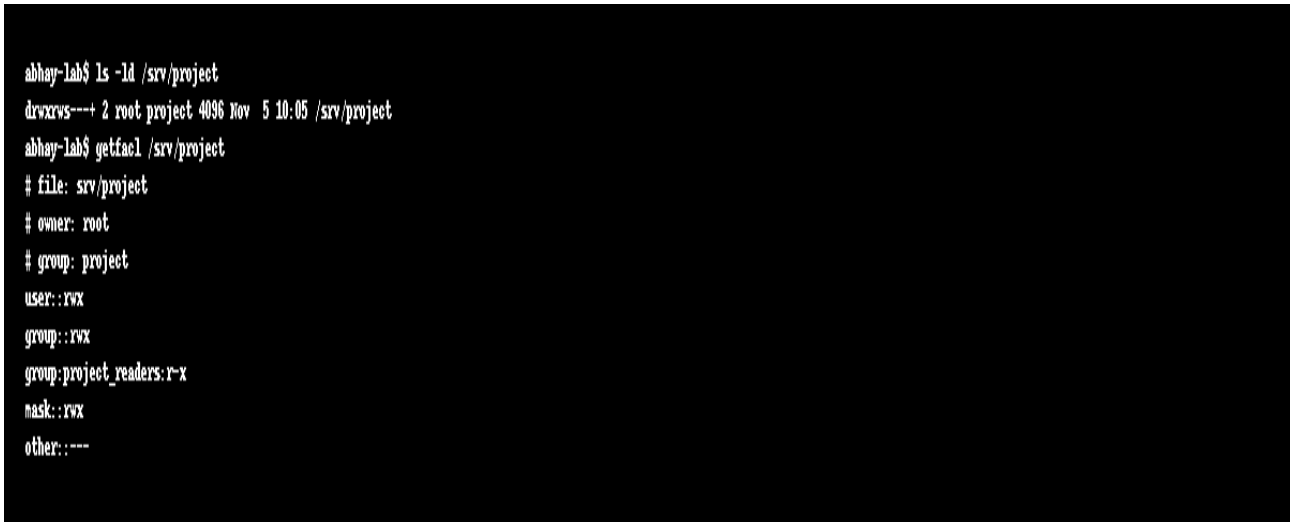
Student: Abhay Raj | Course: B.Tech | Branch: CSE (Core) | Instructor: Anshul Kaundal
Hostname: abhay-lab | Date: 05 Nov 2025

Evidence Screenshots

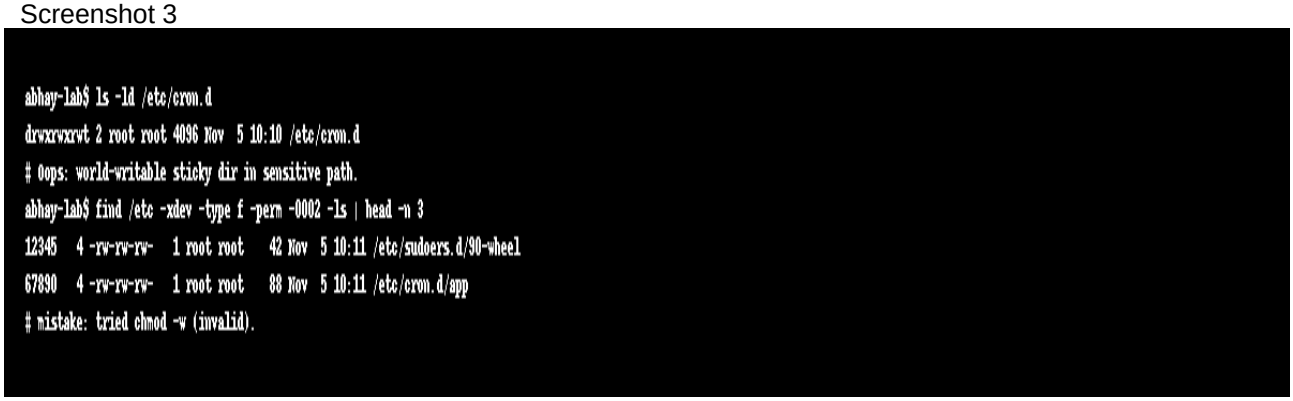
Screenshot 1



Screenshot 2



Screenshot 3



Screenshot 4

```
abhay-lab$ chmod o-w /etc/cron.d
abhay-lab$ find /etc/sudoers.d -type f -exec chmod 0440 {} \;
abhay-lab$ chown root:root /etc/sudoers.d/*
abhay-lab$ ls -ld /etc/cron.d
drwxrwxr-x 2 root root 4096 Nov  5 10:22 /etc/cron.d
abhay-lab$ find /etc -xdev -type f -perm -0002 -ls
# (no output - fixed)
```

Screenshot 5

```
abhay-lab$ grep -R "NOPASSWD" /etc/sudoers /etc/sudoers.d -n
/etc/sudoers.d/90-wheel:1:%wheel ALL=(ALL) NOPASSWD: ALL
abhay-lab$ sudo -l -U bob
Matching Defaults entries for bob on abhay-lab:
    env_reset, mail_badpass
User bob may run the following commands on abhay-lab:
    (ALL) NOPASSWD: ALL
# bad: this grants full root without password
```

Screenshot 6

```
abhay-lab$ sudo visudo -f /etc/sudoers.d/90-wheel
# (edited to specific commands, removed NOPASSWD)
abhay-lab$ visudo -c
/usr/sbin/visudo: parsed OK
abhay-lab$ grep -R "NOPASSWD" /etc/sudoers /etc/sudoers.d -n || echo "no NOPASSWD entries"
no NOPASSWD entries
abhay-lab$ sudo -l -U bob
User bob may run the following commands on abhay-lab:
    (root) /usr/bin/systemctl restart myapp.service, /usr/bin/systemctl status myapp.service
```

Screenshot 7

```
abhay-lab$ stat -c "%n %a %U:%G" /etc/passwd /etc/shadow
/etc/passwd 666 root:root
/etc/shadow 666 root:root
abhay-lab$ ls -ld /root/.ssh /root/.ssh/authorized_keys
drwxrwxrwx 2 root root 4096 Nov  5 09:55 /root/.ssh
-rw-rw-rw- 1 root root  398 Nov  5 09:55 /root/.ssh/authorized_keys
```

Screenshot 8

```
abhay-lab$ chmod 0644 /etc/passwd && chown root:root /etc/passwd
abhay-lab$ chmod 0640 /etc/shadow && chown root:shadow /etc/shadow
abhay-lab$ chmod 700 /root/.ssh
abhay-lab$ chmod 600 /root/.ssh/authorized_keys && chown root:root /root/.ssh/authorized_keys
abhay-lab$ stat -c "%n %a %U:%G" /etc/passwd /etc/shadow
/etc/passwd 644 root:root
/etc/shadow 640 root:shadow
```

Screenshot 9

```
abhay-lab$ ausearch -k sudoers_changes -i --start 2025-11-05 09:50
time->Wed Nov  5 10:12:02 2025
type=SYSCALL msg=audit(1730781122.125:413): arch=c000003e syscall=2 success=yes exit=3 comm="vi" exe="/usr/bin/vi" name="/etc/sudoers.d/90-wheel"
abhay-lab$ ausearch -k passwd_changes -i --start 2025-11-05 10:20
time->Wed Nov  5 10:23:08 2025
type=SYSCALL msg=audit(1730781788.201:503): arch=c000003e syscall=2 success=yes exit=3 comm="chmod" exe="/bin/chmod" name="/etc/passwd"
```

Remediation Checklist

Remove world-writable files; limit NOPASSWD; fix perms on passwd/shadow; lock service accounts; SGID+ACL on /srv/project; enable audit rules; validate with visudo -c; quarterly review.