

Linux IAM & System Hardening

Name: **Sanjana Thawait**

ERP: **6604710**

Course: **B.Tech CSE (Cybersecurity)**

Semester: **5th**

Section: **CY5A**

Date: **05/11/2025**

1. INTRODUCTION

This project demonstrates how Identity and Access Management (IAM) and system hardening are implemented on a Linux-based server environment. IAM ensures that users have the correct amount of access depending on their role, while hardening focuses on reducing vulnerabilities. We simulate a real organization scenario with:

- Admins – full administrative privileges
- Developers – limited access only to required commands
- Auditors – read-only monitoring access

2. PROJECT OBJECTIVE

- Build a secure user access model in Linux using IAM concepts
- Apply least privilege through sudo and ACLs
- Create a vulnerable lab intentionally and exploit it using Kali
- Fix vulnerabilities and produce a remediation report

3. THEORY OF PROJECT

IAM ensures the right user gets the right access. Linux implements IAM using:

- Users and Groups (RBAC)
- Sudo permissions (Least Privilege)
- POSIX/ACL permissions
- auditd monitoring

Hardening removes misconfigurations that allow privilege escalation.

4. TOOLS USED

- Ubuntu VM (Target)
- Kali Linux VM (Attacker)
- ACL, POSIX Permissions
- auditd (log monitoring)
- SSH & nmap for attack simulation

Creating Users & Assigning Groups

Users assigned into admins, devs, auditors (RBAC).

```
ubuntu 2 - VMware Workstation
File Edit View VM Tabs Help || 
File Home X ubuntu 1 X My Computer X ubuntu 2 X kali-linux-2025-2-vmware-amd64 X
Nov 5 12:23
sanjanathawat2@sanjanathawat2:~$ sudo groupadd admins
sanjanathawat2@sanjanathawat2:~$ sudo groupadd devs
sanjanathawat2@sanjanathawat2:~$ sudo groupadd auditors
sanjanathawat2@sanjanathawat2:~$ getent group admins devs auditors
admins:x:1001:
devs:x:1002:
auditors:x:1003:
sanjanathawat2@sanjanathawat2:~$ sudo useradd -m -s /bin/bash -G admins alice sudo passwd alice
Usage: useradd [options] LOGIN
      useradd -D
      useradd -O
      useradd -D [options]

Options:
  --badname          do not check for bad names
  -b, --base-dir BASE_DIR   base directory for the home directory of the new account
  -c, --comment COMMENT    comment for the new account
  -d, --home-dir HOME_DIR  home directory for the new account
  -e, --expiredate EXPIRE_DATE
                           expiration date of the new account
  -f, --inactive INACTIVE   password inactivity period of the new account
  -F, --add-subuids-for-system
                           add entries to subuid/subgid even when adding a system user
  -g, --gid GROUP          name or ID of the primary group of the new account
  -G, --groups GROUPS      list of supplementary groups of the new account
  -h, --help              display this help message and exit
  -k, --skel SKEL_DIR      use this alternative skeleton directory
  -K, --key KEY=VALUE      override /etc/login.defs defaults
  -l, --no-log-init        do not add the user to the lastlog and faillog databases
  -m, --create-home        create the user's home directory
  -M, --no-create-home     do not create the user's home directory
  -N, --no-user-group      do not create a group with the same name as
To direct input to this VM, click inside or press Ctrl+G.
23°C Clear Search ENG IN 12:23 05-11-2025
```

Applying ACL Permissions on /srv/project

ACL ensures only devs write; auditors read-only access.

```
ubuntu 2 - VMware Workstation
File Edit View VM Tabs Help || 
File Home X ubuntu 1 X My Computer X ubuntu 2 X kali-linux-2025-2-vmware-amd64 X
Nov 5 12:24
sanjanathawat2@sanjanathawat2:~$ sudo useradd -m -s /bin/bash -G admins alice sudo passwd alice
New PASSWORD:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: password updated successfully
sanjanathawat2@sanjanathawat2:~$ sudo useradd -m -s /bin/bash -G admins bob sudo passwd bob
New password:
Retype new password:
passwd: password updated successfully
sanjanathawat2@sanjanathawat2:~$ sudo useradd -m -s /bin/bash -G devs carol sudo passwd carol
New password:
Retype new password:
passwd: password updated successfully
sanjanathawat2@sanjanathawat2:~$ sudo useradd -m -s /bin/bash -G devs dave sudo passwd dave
New password:
Retype new password:
passwd: password updated successfully
sanjanathawat2@sanjanathawat2:~$ sudo useradd -m -s /bin/bash -G auditors eve sudo passwd eve
New password:
Retype new password:
passwd: password updated successfully
sanjanathawat2@sanjanathawat2:~$ getent group admins devs auditors
admins:x:1001:alice,bob
devs:x:1002:carol,dave
auditors:x:1003:eve
sanjanathawat2@sanjanathawat2:~$ echo "%admins ALL=(ALL:ALL) ALL" | sudo tee /etc/sudoers.d/admins
To direct input to this VM, click inside or press Ctrl+G.
23°C Clear Search ENG IN 12:24 05-11-2025
```

Configuring Restricted Sudo Permissions

Developers allowed only specific sudo actions (least privilege).

```

File Edit View Search Terminal Help
sanjanathawat2@sanjanathawat2:~$ echo "%admin ALL=(ALL:ALL) ALL" | sudo tee /etc/sudoers.d/admins
tee: /etc/sudoers.d/admins: No such file or directory
%admin ALL=(ALL:ALL) ALL
sanjanathawat2@sanjanathawat2:~$ sudo tee /etc/sudoers.d/devs>/dev/null << 'EOF'
%devs ALL=(root) /bin/systemctl restart myapp.service, /bin/journalctl -u myapp.service EOF
>
> sudo chmod 440 /etc/sudoers.d/*
> sudo visudo -c
> %admin
sanjanathawat2@sanjanathawat2:~$ sudo nano /etc/sudoers.d/devs
sanjanathawat2@sanjanathawat2:~$ sudo visudo -c
/etc/sudoers: parsed OK
/etc/sudoers.d/README: parsed OK
/etc/sudoers.d/devs: bad permissions, should be mode 0440
sanjanathawat2@sanjanathawat2:~$ sudo mkdir /srv/project
sanjanathawat2@sanjanathawat2:~$ sudo chown root:dev /srv/project
chown: invalid group: 'root:dev'
sanjanathawat2@sanjanathawat2:~$ sudo chown root:dev /srv/project
sanjanathawat2@sanjanathawat2:~$ sudo chmod 2770 /srv/project
sanjanathawat2@sanjanathawat2:~$ sudo setfacl -m g:admin:rwx /srv/project
sudo: setfacl: command not found
sanjanathawat2@sanjanathawat2:~$ sudo setfacl -n g:admin:rwx /srv/project
sanjanathawat2@sanjanathawat2:~$ sudo setfacl -n g:admin:rwx /srv/project
sanjanathawat2@sanjanathawat2:~$ sudo setfacl -n g:admin:rwx /srv/project
sanjanathawat2@sanjanathawat2:~$ ls -l /srv/project
drwxrws--- 2 root devs 4096 Nov  4 21:39 /srv/project
sanjanathawat2@sanjanathawat2:~$ sudo apt install auditd -y
Reading package lists... done
Building dependency tree... done
Reading status information... done
The following package was automatically installed and is no longer required:
  liblawn19
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libuparse0t64

To direct input to this VM, click inside or press Ctrl+G.
23°C Clear
ENG IN 1224 05-11-2025

```

Enabling auditd Monitoring

auditd logs privileged changes.

```

File Edit View Search Terminal Help
sanjanathawat2@sanjanathawat2:~$ sudo systemctl enable --now auditd
Synchronizing state of auditd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable auditd
sanjanathawat2@sanjanathawat2:~$ sudo nano /etc/audit/rules.d/project.rules
sanjanathawat2@sanjanathawat2:~$ sudo nano /etc/audit/rules.d/project.rules
sanjanathawat2@sanjanathawat2:~$ sudo augenrules --load
No rules
enabled 1
file 1
pid 5129
rate_limit 0
backlog_limit 8192
lost 0
backlog 2
backlog_wait_time 60000
backlog_wait_time_actual 0
enabled 1
file 1
pid 5129
rate_limit 0
backlog_limit 8192
lost 0
backlog 0
backlog_wait_time 60000
backlog_wait_time_actual 0
enabled 1
file 1
pid 5129
rate_limit 0
backlog_limit 8192
lost 0
backlog 1
backlog_wait_time 60000
backlog_wait_time_actual 0
To direct input to this VM, click inside or press Ctrl+G.
23°C Clear
ENG IN 1224 05-11-2025

```

World-Writable Cron Vulnerability

Cron was intentionally made writable (vulnerability).

ubuntu 2 - VMware Workstation

File Edit View VM Tabs Help

Home X ubuntu 1 X My Computer X ubuntu 2 X kali-linux 2023.2-vmware-0mds X

Nov 5 12:25

sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop

```
File Edit View Search Terminal Help
backlog_limit 8192
lost 0
backlog 2
backlog_wait_time 60000
A backlog_wait_time_actual 0
enabled 1
failure 1
pid 5129
rate_limit 0
backlog_limit 8192
lost 0
backlog 0
backlog_wait_time 60000
backlog_wait_time_actual 0
enabled 1
failure 1
pid 5129
rate_limit 0
backlog_limit 8192
lost 0
backlog 1
backlog_wait_time 60000
backlog_wait_time_actual 0
sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop$ sudo auditctl -l
sudo: auditctl: command not found
sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop$ sudo auditctl -l
Option -l is invalid
There was an error while processing parameters
sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop$ sudo auditctl -l
-w /etc/audited -p wa -k sudoers_change
-w /etc/sudoers.d -p wa -k sudoers_change
-w /etc/passwd -p wa -k passwd_change
-w /etc/shadow -p wa -k shadow_change
-w /srv/project -p wa -k passwd_access
sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop$
```

To direct input to this VM, click inside or press Ctrl+G.

23°C Clear

ENG IN 12:25 05-11-2025

NOPASSWD sudo Misconfiguration

NOPASSWD provided unrestricted sudo access.

ubuntu 2 - VMware Workstation

File Edit View VM Tabs Help

Home X ubuntu 1 X My Computer X ubuntu 2 X kali-linux 2023.2-vmware-0mds X

Nov 5 12:28

sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop

```
> 0 * *
> sudo tee /etc/cron.d/backup >/dev/null <<'EOF'
* * * * root /bin/true
> EOF
A [sudo] password for sanjanathawait2:
Sorry, try again.
[sudo] password for sanjanathawait2:
Sorry, try again.
[sudo] password for sanjanathawait2:
sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop$ sudo chmod 0777 /etc/cron.d/backup
sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop$ ls -l /etc/cron.d/backup
total 4
-rwxrwxrwx 1 root root 82 Nov 4 23:08 /etc/cron.d/backup
sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop$ sudo tee /etc/sudoers.d/unsafe >/dev/null <<'EOF'
> %dev ALL=(ALL) NOPASSWD: ALL
> EOF
sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop$ sudo chmod 440 /etc/sudoers.d/unsafe
sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop$ sudo visudo -c
/etc/sudoers.d/README: parsed OK
/etc/sudoers.d/devs: bad permissions, should be mode 844
/etc/sudoers.d/unsafe: parsed OK
sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop$ sudo mkdir -p /root/secrets
sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop$ sudo tee /root/secrets/id_rsa_test >/dev/null << 'EOF'
> -----BEGIN PRIVATE KEY-----
> FAKE-TEST-KEY-FOR-LAB
> -----END PRIVATE KEY-----
> EOF
sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop$ sudo chmod 644 /root/secrets/id_rsa_test
sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop$ ls -l /root/secrets/id_rsa_test
ls: cannot access '/root/secrets/id_rsa_test': Permission denied
sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop$ sudo chmod 440 /etc/sudoers.d/devs
sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop$ sudo visudo -c
```

To direct input to this VM, click inside or press Ctrl+G.

23°C Clear

ENG IN 12:28 05-11-2025

Weak SSH Private Key Permissions

Weak key permissions allowed unauthorized access.

```

sanjanathawat2@sanjanathawat2:~$ ls -l /root/secrets/id_rsa_test
ls: cannot access '/root/secrets/id_rsa_test': Permission denied
sanjanathawat2@sanjanathawat2:~$ sudo chmod 440 /etc/sudoers.d/devs
sanjanathawat2@sanjanathawat2:~$ sudo visudo -c
/etc/sudoers: parsed OK
A /etc/sudoers.d/README: parsed OK
/etc/sudoers.d/devs: parsed OK
/etc/sudoers.d/unsafe: parsed OK
B sanjanathawat2@sanjanathawat2:~$ hostname -I
192.168.63.131 192.168.74.131
C sanjanathawat2@sanjanathawat2:~$ ip a
1: lo</loopback,UP,LOWER_UP> brd 0:00:00:00:00:00 state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        netet 127.0.0.1/8 scope host noprefixroute
            valid_lft forever preferred_lft forever
        netet :1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: ens33:<BROADCAST,MULTICAST,UP,LOWER_UP> brd 192.168.63.255 state UP group default qlen 1000
    link/ether 00:0c:29:47:eb:51 brd ffffff:ffff:ffff:ffff
        altname enp3s0
        netet fe80::c839:691f:15de:8847/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
3: ens37:<BROADCAST,MULTICAST,UP,LOWER_UP> brd 192.168.63.255 state UP group default qlen 1000
    link/ether 00:0c:29:47:eb:51 brd ffffff:ffff:ffff:ffff
        altname enp2s0
        netet 192.168.74.131/24 brd 192.168.74.255 scope global dynamic noprefixroute ens37
            valid_lft forever preferred_lft 1770sec
            netet fe80::20c:29ff:fe47:eb51/64 scope link
                valid_lft forever preferred_lft forever
sanjanathawat2@sanjanathawat2:~$ sudo chmod 644 /etc/cron.d/backup
[sudo] password for sanjanathawat2:
chmod: cannot access '/etc/cron.d/backup': No such file or directory
D sanjanathawat2@sanjanathawat2:~$ sudo chmod 644 /etc/cron.d/backup
E sanjanathawat2@sanjanathawat2:~$ sudo chmod root:root /etc/cron.d/backup
F To direct input to this VM, click inside or press Ctrl+G.

```

To direct input to this VM, click inside or press Ctrl+G.

23°C Clear ENG IN 12:29 05-11-2025

Kali Scanning using nmap

Kali attacker scans system.

```

sanjanathawat2@sanjanathawat2:~$ nmap -A -O 192.168.63.0/24
Nmap 7.6.1 (https://nmap.org) starting ...
[+] Nmap done: 256 hosts (0 up, 256 down) at 2023-11-05 12:29 (rate: 100.00 ports/s)
sanjanathawat2@sanjanathawat2:~$ sudo chmod 644 /etc/cron.d/backup
[sudo] password for sanjanathawat2:
chmod: cannot access '/etc/cron.d/backup': No such file or directory
sanjanathawat2@sanjanathawat2:~$ sudo chmod 644 /etc/cron.d/backup
sanjanathawat2@sanjanathawat2:~$ sudo chmod root:root /etc/cron.d/backup
H     Try 'chmod --help' for more information.
sanjanathawat2@sanjanathawat2:~$ sudo chown root:root /etc/cron.d/backup
sanjanathawat2@sanjanathawat2:~$ sudo rm /etc/sudoers.d/unsafe
sanjanathawat2@sanjanathawat2:~$ sudo visudo -c
/etc/sudoers: parsed OK
A /etc/sudoers.d/README: parsed OK
/etc/sudoers.d/devs: parsed OK
/etc/sudoers.d/unsafe: parsed OK
B sanjanathawat2@sanjanathawat2:~$ sudo chmod 600 /root/secrets/id_rsa_test
C sanjanathawat2@sanjanathawat2:~$ ls -l
total 0
D sanjanathawat2@sanjanathawat2:~$ sudo chmod 600 /root/secrets/id_rsa_test
E sudo: command not found
sanjanathawat2@sanjanathawat2:~$ sudo chmod 644 /etc/cron.d/backup
sanjanathawat2@sanjanathawat2:~$ sudo chmod 644 /etc/cron.d/backup
F chmod: missing operand after '644/etc/cron.d/backup'
Try 'chmod --help' for more information.
sanjanathawat2@sanjanathawat2:~$ sudo chmod 644 /etc/cron.d/backup
sanjanathawat2@sanjanathawat2:~$ ls -l /etc/cron.d/backup
!`rm -rf /`root root 62 Nov 4 23:08 /etc/cron.d/backup
sanjanathawat2@sanjanathawat2:~$ sudo ausearch -k sudoers
...
time=Tue Nov 4 21:54:57 2023
type=PROCTITLE msg=audit(1762273497.934:303): prctl(t=2F7362696E2F617564697463746C020520802F6574632F61756469742E72756C6573
type=SYSCALL msg=audit(1762273497.934:303): arch=c000003e syscall=44 success=yes exit=1084 a0=3 a1=7ff9e626d400 a2=43c a3=0 items=0 ppid=5624 pid=5638 auid=1000 uid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty pts1 sess3 comm="audtctl" exe="/usr/sbin/audtctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1762273497.934:303): auid=1000 ses=3 subj=unconfined op=add_rule key="sudoers_change" list=4 res=1
...
E To direct input to this VM, click inside or press Ctrl+G.

```

To direct input to this VM, click inside or press Ctrl+G.

23°C Clear ENG IN 12:29 05-11-2025

SSH Access Exploitation

Attacker connects via SSH.

```

Processing triggers for fw (0.36-2.6) ...
[sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop]$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/ssh.service → /usr/lib/systemd/system/ssh.service.
[sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop]$ sudo systemctl start ssh
[sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop]$ sudo ss -tulpn | grep :22
tcp  LISTEN  0      4996          0.0.0.0:22           0.0.0.0:*          users:(("sshd",pid=9026,fd=3),("systemd",pid=1,fd=114)) ino:65807 sk:8 cgroup:/system.slice/sshd.socket <-
tcp  LISTEN  0      4996          0.0.0.0:4996         0.0.0.0:*          users:(("sshd",pid=9026,fd=4),("systemd",pid=1,fd=115)) ino:65809 sk:9 cgroup:/system.slice/sshd.socket v6only:1 <-
ls: cannot access '/etc/cron.d/*': No such file or directory
[sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop]$ ls -l /etc/cron.d/* backup
-rw-r--r-- 1 root  root 82 Nov  4 23:08 /etc/cron.d/backup
[sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop]$ ls -l /tmp/cron_proof_by_attacker 2>/dev/null || echo "NO_PROFILE"
[sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop]$ sudo grep -R 'NOPASSWD' /etc/sudoers /etc/sudoers.d/*
[sudo] password for sanjanathawait2:
NO_PROFILE
[sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop]$ sudo password for sanjanathawait2:
Sorry, try again.
[sudo] password for sanjanathawait2:
Sorry, try again.
[sudo] password for sanjanathawait2:
Sorry, try again.
[sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop]$ sudo ausearch -k sudoers_change -i > ~/lab_evidence/ausearch_sudoers_ftter.txt 2>&1 || true
[sudo] password for sanjanathawait2:
To direct input to this VM, click inside or press Ctrl+G.
23°C Clear Search ENG IN 12:30 05-11-2025

```

Privilege Escalation via cron

Privilege escalation achieved using cron.

```

Processing triggers for fw (0.36-2.6) ...
[sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop]$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/ssh.service → /usr/lib/systemd/system/ssh.service.
[sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop]$ sudo systemctl start ssh
[sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop]$ sudo ss -tulpn | grep :22
tcp  LISTEN  0      4996          0.0.0.0:22           0.0.0.0:*          users:(("sshd",pid=9026,fd=3),("systemd",pid=1,fd=114)) ino:65807 sk:8 cgroup:/system.slice/sshd.socket <-
tcp  LISTEN  0      4996          0.0.0.0:4996         0.0.0.0:*          users:(("sshd",pid=9026,fd=4),("systemd",pid=1,fd=115)) ino:65809 sk:9 cgroup:/system.slice/sshd.socket v6only:1 <-
ls: cannot access '/etc/cron.d/*': No such file or directory
[sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop]$ ls -l /etc/cron.d/* backup
-rw-r--r-- 1 root  root 82 Nov  4 23:08 /etc/cron.d/backup
[sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop]$ ls -l /tmp/cron_proof_by_attacker 2>/dev/null || echo "NO_PROFILE"
[sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop]$ sudo grep -R 'NOPASSWD' /etc/sudoers /etc/sudoers.d/*
[sudo] password for sanjanathawait2:
NO_PROFILE
[sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop]$ sudo password for sanjanathawait2:
Sorry, try again.
[sudo] password for sanjanathawait2:
Sorry, try again.
[sudo] password for sanjanathawait2:
Sorry, try again.
[sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop]$ sudo ausearch -k sudoers_change -i > ~/lab_evidence/ausearch_sudoers_ftter.txt 2>&1 || true
[sudo] password for sanjanathawait2:
[sanjanathawait2@sanjanathawait2-VMware-Virtual-Platform:~/Desktop]$ sudo ausearch -k sudoers_change -i > ~/lab_evidence/ausearch_sudoers_ftter.txt 2>&1 || true
To direct input to this VM, click inside or press Ctrl+G.
23°C Clear Search ENG IN 12:30 05-11-2025

```

Fix: Correcting Cron Permissions

Corrected ownership and permissions.

```

[sudo] password for sanjanathawalt2:
NO_PASWD_FOUND
sanjanathawalt2@sanjanathawalt2:~/Desktop$ sudo ls -l /root/secrets/ | grep id_rsa_test
sanjanathawalt2@sanjanathawalt2:~/Desktop$ sudo ls -l /root/secrets/ | grep id_rsa_test > /dev/null || echo "NO_KEY_FILE"
sanjanathawalt2@sanjanathawalt2:~/Desktop$ sudo mkdir -p ~/lab_evidence
sanjanathawalt2@sanjanathawalt2:~/Desktop$ sudo ls -l /etc/cron.d/backup > ~/lab_evidence/cron_after.txt 2>&1
sanjanathawalt2@sanjanathawalt2:~/Desktop$ sudo ls -l /etc/sudoers.d/ > ~/lab_evidence/sudoersd_after.txt 2>&1
sanjanathawalt2@sanjanathawalt2:~/Desktop$ sudo ls -l /root/secrets/ | grep id_rsa_test > ~/lab_evidence/key_after.txt 2>&1 || true
[?] password for sanjanathawalt2:
Sorry, try again.
[?] password for sanjanathawalt2:
Sorry, try again.
[?] password for sanjanathawalt2:
Sorry, try again.
[?] password for sanjanathawalt2:
sanjanathawalt2@sanjanathawalt2:~/Desktop$ sudo ausearch -k sudoers_change -i > ~/lab_evidence/ausearch_sudoers_stfer.txt 2>&1 || true
sanjanathawalt2@sanjanathawalt2:~/Desktop$ sudo ausearch -k sudoers_change -i > ~/lab_evidence/ausearch_sudoers_after.txt 2>&1 || true
sanjanathawalt2@sanjanathawalt2:~/Desktop$ sudo ausearch -k project_access -i > ~/lab_evidence/ausearch_project_after.txt 2>&1 || true
sanjanathawalt2@sanjanathawalt2:~/Desktop$ sudo ausearch -k summary -i > ~/lab_evidence/ausearch_summary.txt 2>&1 || true
sanjanathawalt2@sanjanathawalt2:~/Desktop$ sudo ausearch -k summary -i > ~/lab_evidence/ausearch_summary.txt 2>&1 || true
sanjanathawalt2@sanjanathawalt2:~/Desktop$ sudo journalctl -u ssh -n 200 --no-pager > ~/lab_evidence/journal_ssh_last200.txt || true
sanjanathawalt2@sanjanathawalt2:~/Desktop$ sudo journalctl -u cron -n 200 --no-pager > ~/lab_evidence/journal_cron_last200.txt || true
sanjanathawalt2@sanjanathawalt2:~/Desktop$ ls -lah ~/lab_evidence
total 68K
drwxrwxr-x 2 sanjanathawalt2 sanjanathawalt2 4.0K Nov 5 01:43 .
drwxr-xr-x 16 sanjanathawalt2 sanjanathawalt2 4.0K Nov 5 01:30 ..
-rw-rw-r-- 1 sanjanathawalt2 sanjanathawalt2 261 Nov 5 01:40 auseport_summary.txt
-rw-rw-r-- 1 sanjanathawalt2 sanjanathawalt2 13 Nov 5 01:39 ausearch_project_after.txt
-rw-rw-r-- 1 sanjanathawalt2 sanjanathawalt2 5.1K Nov 5 01:38 ausearch_sudoers_after.txt
-rw-rw-r-- 1 sanjanathawalt2 sanjanathawalt2 5.1K Nov 5 01:38 ausearch_sudoers_stfer.txt
-rw-rw-r-- 1 sanjanathawalt2 sanjanathawalt2 58 Nov 5 01:31 cron_after.txt
-rw-rw-r-- 1 sanjanathawalt2 sanjanathawalt2 260 Nov 5 01:43 journal_cron_last200.txt
-rw-rw-r-- 1 sanjanathawalt2 sanjanathawalt2 726 Nov 5 01:42 journal_ssh_last200.txt
-rw-rw-r-- 1 sanjanathawalt2 sanjanathawalt2 36 Nov 5 01:35 key_after.txt
-rw-rw-r-- 1 sanjanathawalt2 sanjanathawalt2 102 Nov 5 01:33 sudoersd_after.txt
sanjanathawalt2@sanjanathawalt2:~/Desktop$ tar -czvf ~/lab_evidence_after.tar.gz -c ~ lab_evidence

```

To direct input to this VM, click inside or press Ctrl+G.

23°C Clear ENG IN 12:31 05-11-2025

Fix: Securing Private Key

Private key secured using chmod 600.

```

sanjanathawalt2@sanjanathawalt2:~/Desktop$ tar -zcvf ~/lab_evidence_after.tar.gz -c ~ lab_evidence
tar: Removing leading '/' from member names
/home/sanjanathawalt2/.sudo_as_admin_successful
tar: Removing leading '/' from hard link targets
/home/sanjanathawalt2/.Xauthority
/home/sanjanathawalt2/.lab_evidence/
/home/sanjanathawalt2/lab_evidence/ausearch_project_after.txt
/home/sanjanathawalt2/lab_evidence/key_after.txt
/home/sanjanathawalt2/lab_evidence/journal_ssh_last200.txt
/home/sanjanathawalt2/lab_evidence/ausearch_summary.txt
/home/sanjanathawalt2/lab_evidence/sudoersd_after.txt
/home/sanjanathawalt2/lab_evidence/ausearch_sudoers_stfer.txt
/home/sanjanathawalt2/lab_evidence/journal_cron_last200.txt
/home/sanjanathawalt2/lab_evidence/ausearch_sudoers_after.txt
/home/sanjanathawalt2/lab_evidence/cron_after.txt
/home/sanjanathawalt2/Desktop/
/home/sanjanathawalt2/.snap/
/home/sanjanathawalt2/.snap/snappy/
/home/sanjanathawalt2/.snap/snappy/desktop-integration/
/home/sanjanathawalt2/.snap/snappy/desktop-integration/common/
/home/sanjanathawalt2/.snap/snappy/desktop-integration/common/.cache/

```

To direct input to this VM, click inside or press Ctrl+G.

23°C Clear ENG IN 12:32 05-11-2025

Fix: Validating sudo rules

sudo validated using visudo.

Audit Log Evidence

auditd captured change logs.

Conclusion

This project demonstrated the complete lifecycle of Linux IAM and System Hardening.

First, a secure baseline was implemented:

- Role Based Access Control was enforced using users and groups
- Least privilege principle applied through restricted sudo rules
- ACLs secured the project directory allowing controlled access
- auditd was configured for monitoring high risk configuration changes

Second, security weaknesses were intentionally introduced:

- Writable cron allowed privilege escalation
- NOPASSWD enabled unrestricted sudo privilege
- Weak permissions on a private key allowed unauthorized access

Third, using Kali Linux as an attacker:

- Reconnaissance was performed (nmap scan)
- Exploitation succeeded, proving privilege escalation to root

Finally, remediation:

- Misconfigurations were fixed (chmod, removing NOPASSWD)
- auditd logs confirmed tracking of privileged operations

Learning Outcome:

This project reinforced how misconfigurations, not software vulnerabilities, are the biggest root cause of security breaches.

By enforcing IAM, least privilege, ACL, and auditing, the attack surface drastically reduces.

Securing Linux is not only about tools — it is about discipline and correct configuration.