

# Linux IAM & System Hardening

Name: Vikash Kumar

ERP: 6604703

Course: B.Tech CSE (Cybersecurity)

Semester: 5th | Section: CY5A

## **1. INTRODUCTION**

This project focuses on implementing Identity and Access Management (IAM) and Linux system hardening. IAM ensures correct access control based on user roles while hardening minimizes security risks by removing vulnerabilities. This project simulates Admin, Developer, and Auditor roles.

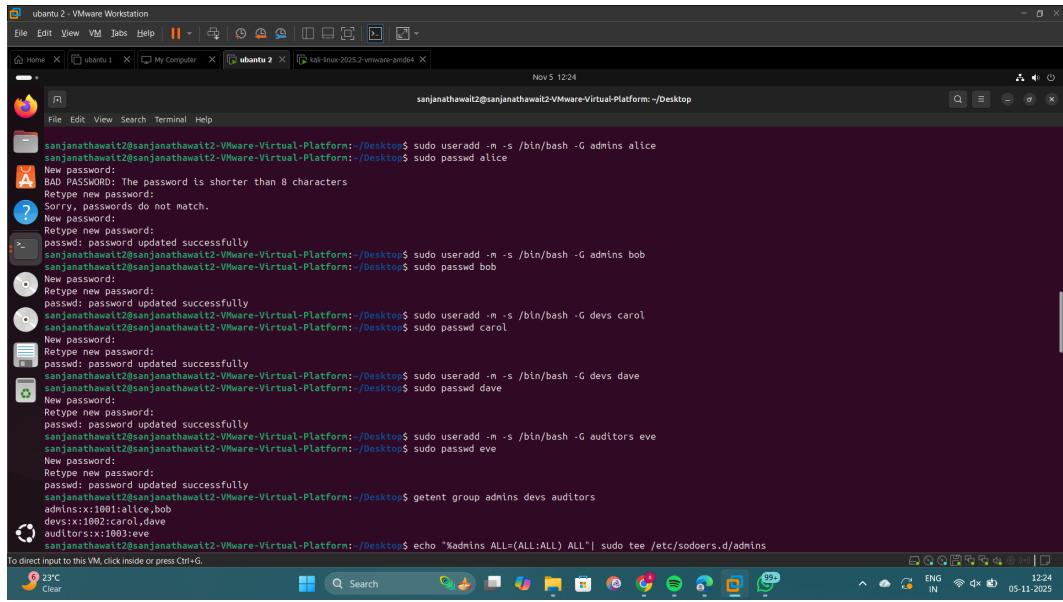
## **2. PROJECT OBJECTIVE**

- To configure secure role-based access control in Linux.
- To implement least privilege access using sudo and ACL.
- To simulate real-world attack scenario using Kali Linux.
- To identify security weaknesses and apply system hardening.
- To document results with proof of execution.

## **3. TOOLS USED**

- Ubuntu Linux (Target System)
- Kali Linux (Attacker System)
- User and Group Management Utilities
- sudo and ACL Permissions
- auditd Monitoring Service
- SSH, nmap and basic networking utilities

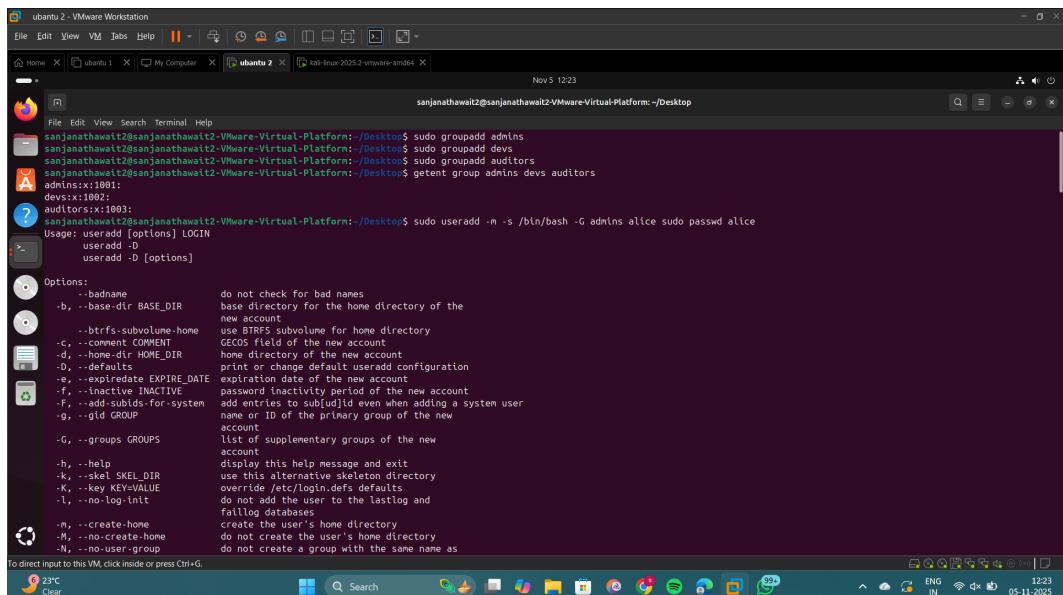
## 4. PRACTICAL EXECUTION EVIDENCE



The screenshot shows a terminal window titled "ubuntu 2 - VMware Workstation". The terminal session is running on a Kali Linux 2023.2 VM. The user is creating multiple new users:

```
sanjanathawitz@sanjanathawitz:~/Desktop$ sudo useradd -m -s /bin/bash -G admins alice
sanjanathawitz@sanjanathawitz:~/Desktop$ sudo passwd alice
New password:
Re-type new password:
passwd: password updated successfully
sanjanathawitz@sanjanathawitz:~/Desktop$ sudo useradd -m -s /bin/bash -G admins bob
sanjanathawitz@sanjanathawitz:~/Desktop$ sudo passwd bob
New password:
Re-type new password:
passwd: password updated successfully
sanjanathawitz@sanjanathawitz:~/Desktop$ sudo useradd -m -s /bin/bash -G devs carol
sanjanathawitz@sanjanathawitz:~/Desktop$ sudo passwd carol
New password:
Re-type new password:
passwd: password updated successfully
sanjanathawitz@sanjanathawitz:~/Desktop$ sudo useradd -m -s /bin/bash -G devs dave
sanjanathawitz@sanjanathawitz:~/Desktop$ sudo passwd dave
New password:
Re-type new password:
passwd: password updated successfully
sanjanathawitz@sanjanathawitz:~/Desktop$ sudo useradd -m -s /bin/bash -G auditors eve
sanjanathawitz@sanjanathawitz:~/Desktop$ sudo passwd eve
New password:
Re-type new password:
passwd: password updated successfully
sanjanathawitz@sanjanathawitz:~/Desktop$ getent group admins devs auditors
admins:x:1001:alice,bob
devs:x:1002:carol,dave
auditors:x:1003:eve
sanjanathawitz@sanjanathawitz:~/Desktop$ echo "%admins ALL=(ALL:ALL) ALL" | sudo tee /etc/sudoers.d/admins
```

### Proof of Execution



The screenshot shows a terminal window titled "ubuntu 2 - VMware Workstation". The terminal session is running on a Kali Linux 2023.2 VM. The user is creating a new user "alice" and then listing all users to verify the addition:

```
sanjanathawitz@sanjanathawitz:~/Desktop$ sudo groupadd admins
sanjanathawitz@sanjanathawitz:~/Desktop$ sudo groupadd devs
sanjanathawitz@sanjanathawitz:~/Desktop$ sudo groupadd auditors
sanjanathawitz@sanjanathawitz:~/Desktop$ getent group admins devs auditors
admins:x:1001:
devs:x:1002:
auditors:x:1003:
sanjanathawitz@sanjanathawitz:~/Desktop$ sudo useradd -m -s /bin/bash -G admins alice sudo passwd alice
Usage: useradd [options] LOGIN
      useradd -D
      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
  --btrfs-subvolume-home   use BTRFS subvolume for home directory
  -c, --comment COMMENT    GECOS field of the new account
  -d, --home-dir HOME_DIR   home directory of the new account
  -D, --no-create-home     prevent creation of the user's home directory
  --expiredate EXPIRE_DATE  pre-configuration of the expiration date of the new account
  -f, --inactive INACTIVE   password inactivity period of the new account
  --add-subuids-for-system add entries to subuid1d 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
                            falllog databases
  -n, --create-home        create the user's home directory
  -N, --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
```

### Proof of Execution

## Proof of Execution

Proof of Execution

```

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-amd64 X
Nov 5 12:25
sanjanathawaltz@sanjanathawaltz:~/Desktop$ sudo auditctl -l
auditctl: command not found
sanjanathawaltz@sanjanathawaltz:~/Desktop$ sudo auditctl -l
Option -i is invalid
There was an error while processing parameters
sanjanathawaltz@sanjanathawaltz:~/Desktop$ sudo auditctl -l
-W /etc/sudoers -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 /etc/group -p wa -k group_change
-W /etc/cron.d -p wa -k password_access
sanjanathawaltz@sanjanathawaltz:~/Desktop$ 

```

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

23°C Clear 12:25 ENG IN 05-11-2025

## Proof of Execution

```

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-amd64 X
Nov 5 12:28
sanjanathawaltz@sanjanathawaltz:~/Desktop$ sudo tee /etc/cron.d/backup >/dev/null <<'EOF'
0 * * * * root /bin/true
> EOF
[sudo] password for sanjanathawaltz:
Sorry, try again.
[sudo] password for sanjanathawaltz:
[Sudo] password for sanjanathawaltz:
[sudo] password for sanjanathawaltz:
sanjanathawaltz@sanjanathawaltz:~/Desktop$ sudo chmod 0777 /etc/cron.d/backup
sanjanathawaltz@sanjanathawaltz:~/Desktop$ ls -l /etc/cron.d/backup
ls: invalid option -- '/'
Try `ls --help' for more information.
sanjanathawaltz@sanjanathawaltz:~/Desktop$ ls -l /etc/cron.d/backup
-rw-rw-rw- 1 root root 92 Nov 4 23:08 /etc/cron.d/backup
sanjanathawaltz@sanjanathawaltz:~/Desktop$ sudo tee /etc/sudoers.d/unsafe > /dev/null <<'EOF'
> $devs ALL:(ALL) NOPASSWD: ALL
> EOF
sanjanathawaltz@sanjanathawaltz:~/Desktop$ sudo chmod 440 /etc/sudoers.d/unsafe
sanjanathawaltz@sanjanathawaltz:~/Desktop$ sudo visudo -c
/etc/sudoers: parsed OK
/etc/sudoers.d/unsafe: parsed OK
/etc/sudoers.d/unsafe: bad permissions, should be mode 0440
/etc/sudoers.d/unsafe: parsed OK
sanjanathawaltz@sanjanathawaltz:~/Desktop$ sudo mkdir -p /root/secrets
sanjanathawaltz@sanjanathawaltz:~/Desktop$ sudo tee /root/secrets/id_rsa_test > /dev/null <<'EOF'
> -----BEGIN PRIVATE KEY-----
> FAKE-TEST-KEY-FOR-LAB
> -----END PRIVATE KEY-----
> EOF
sanjanathawaltz@sanjanathawaltz:~/Desktop$ sudo chmod 644 /root/secrets/id_rsa_test
sanjanathawaltz@sanjanathawaltz:~/Desktop$ ls -l /root/secrets/id_rsa_test
ls: cannot access '/root/secrets/id_rsa_test': Permission denied
sanjanathawaltz@sanjanathawaltz:~/Desktop$ sudo chmod 440 /etc/sudoers.d/devs
sanjanathawaltz@sanjanathawaltz:~/Desktop$ sudo visudo -c

```

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

23°C Clear 12:28 ENG IN 05-11-2025

## Proof of Execution

## Proof of Execution

Proof of Execution

```
ubuntu 2 - VMware Workstation
File Edit View VM Tabs Help || Back Forward Home ubuntu 1 My Computer ubuntu 2 kali-linux:2025.2-vmware-amd64 Nov 5 12:30
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:~/Desktop$ sudo systemctl enable ssh
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:~/Desktop$ sudo systemctl start ssh
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:~/Desktop$ sudo systemctl status ssh
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:~/Desktop$ sudo systemctl start ssh
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:~/Desktop$ sudo ss -tulpn | grep :22
? [TCP] LISTEN 0 4096 0.0.0.0:22 0.0.0.0:*
users:(("sshd",pid=9026,fd=3),("systemd",pid=1,fd=11)) ino:65807 sk:b cgroup:/system.slice/sshd.socket <-->
? [TCP] LISTEN 0 4096 0.0.0.0:22 0.0.0.0:*
users:(("sshd",pid=9026,fd=4),("systemd",pid=1,fd=15)) ino:65809 sk:b cgroup:/system.slice/sshd.socket vonly:1 <-->
? [TCP] LISTEN 0 4096 0.0.0.0:22 0.0.0.0:*
users:(("sshd",pid=9026,fd=4),("systemd",pid=1,fd=15)) ino:65809 sk:b cgroup:/system.slice/sshd.socket vonly:1 <-->
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:~/Desktop$ ls -l /etc/cron.d/baackup
ls: cannot access '/etc/cron.d/baackup': No such file or directory
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:~/Desktop$ ls -l /etc/cron.d/baackup
ls: cannot access '/etc/cron.d/baackup': No such file or directory
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:~/Desktop$ ls -l /etc/cron.d/backups
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:~/Desktop$ ls -l /tmp/cron_probe_by_attacker 2>/dev/null || echo "NO_PROOF_FILE"
NO_PROOF_FILE
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:~/Desktop$ sudo grep -R "NOPASSWD" /etc/sudoers /etc/sudoers.d/* -n 2>/dev/null || echo "NO_PASSWD_FOUND"
[sudo] password for sanjanathawat2:
Sorry, try again.
[sudo] password for sanjanathawat2:
NO_PASSWD_FOUND
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:~/Desktop$ sudo ls -l /root/secrets/id_rsa_test 2>/dev/null || echo "NO_KEY_FILE"
NO_KEY_FILE
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:~/Desktop$ mkdir -p ~/lab_evidence
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:~/Desktop$ ls -l /etc/cron.d/backup > ~/lab_evidence/cron_after.txt 2>&1
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:~/Desktop$ ls -l /etc/sudoers.d/* > ~/lab_evidence/sudoersd_after.txt 2>&1
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:~/Desktop$ sudo ls -l /root/secrets/id_rsa_test > ~/lab_evidence/key_after.txt 2>&1 || true
[sudo] password for sanjanathawat2:
Sorry, try again.
[sudo] password for sanjanathawat2:
Sorry, try again.
[sudo] password for sanjanathawat2:
[sudo] password for sanjanathawat2:
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:~/Desktop$ sudo ausearch -k sudoers_change -l > ~/lab_evidence/ausearch_sudoers_fster.txt 2>&1 || true
[sudo] password for sanjanathawat2:
To direct input to this VM, click inside or press Ctrl+G.
```

## Proof of Execution

```
ubuntu 2 : VMware Workstation
File Edit View VM Help || | X Home X ubuntu 1 X My Computer X ubuntu 2 X kali-linux-2025.2-vmware-amd64 X Nov 5 12:30
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:/Desktop$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemctl-sysv-install.
Executing: /usr/lib/systemd/systemctl-sysv-install enable ssh
Created symlink /etc/systemd/system/ssh.service → /usr/lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /usr/lib/systemd/system/ssh.service.
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:/Desktop$ sudo systemctl start ssh
[sudo] password for sanjanathawat2:
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:/Desktop$ sudo su -l julpun | grep -i22
tcp  LISTEN  0      4096   0.0.0.0    0.0.0.0    users:(("sshd",pid=9826,fd=1),("systemd",pid=1,fd=14))  lno:65887 sk:8 cgroup:/system.slice/sshd.socket <-->
tcp  LISTEN  0      4096   0.0.0.0    0.0.0.0    users:(("sshd",pid=9826,fd=4),("systemd",pid=1,fd=15))  lno:65889 sk:b cgroup:/system.slice/sshd.socket vonly:1 <-->
?    ls: cannot access '/etc/cron.d/baekcup': No such file or directory
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:/Desktop$ ls -l /etc/cron.d/baekcup
ls: cannot access '/etc/cron.d/baekcup': No such file or directory
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:/Desktop$ ls -l /etc/cron.d/backup
ls: cannot access '/etc/cron.d/backup': No such file or directory
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:/Desktop$ ls -l /tmp/cron_prob_by_attacker 2>/dev/null || echo "NO_PROFILE_FILE"
NO_PROFILE_FILE
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:/Desktop$ sudo grep -R "NOPASSWD" /etc/sudoers /etc/sudoers.d/* -n 2>/dev/null || echo "NO_PASSWD_FOUND"
[sudo] password for sanjanathawat2:
Sorry, try again.
[sudo] password for sanjanathawat2:
NO_PASSWD_FOUND
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:/Desktop$ sudo ls -l /root/secrets/id_rsa_test 2>/dev/null || echo "NO_KEY_FILE"
NO_KEY_FILE
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:/Desktop$ mkdir -p ~/lab_evidence
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:/Desktop$ ls -l ~/etc/cron.d/backup > ~/lab_evidence/cron_after.txt 2>&1
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:/Desktop$ ls -l ~/etc/sudoers.d/ > ~/lab_evidence/sudoersd_after.txt 2>&1
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:/Desktop$ sudo ls -l /root/secrets/id_rsa_test > ~/lab_evidence/key_after.txt 2>&1 || true
[sudo] password for sanjanathawat2:
Sorry, try again.
[sudo] password for sanjanathawat2:
Sorry, try again.
[sudo] password for sanjanathawat2:
[sudo] password for sanjanathawat2:
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:/Desktop$ sudo ausearch -k sudoers_change -i -> ~/lab_evidence/ausearch_sudoers_fster.txt 2>&1 ||true
sanjanathawat2@sanjanathawat2:~/VMware-Virtual-Platform:/Desktop$ sudo ausearch -k sudoers_change -i -> ~/lab_evidence/ausearch_sudoers_after.txt 2>&1 ||true
To direct input to this VM, click inside or press Ctrl+G.
```

Proof of Execution

```

ubuntu 2 - VMware Workstation
File Edit View VM Tabs Help || Home X | My Computer X | ubuntu 2 X | kali-linux-2023.2-vmware-amd64 X
Nov 5 12:32

sanjanathawalt2@sanjanathawalt2:~/lab_evidence$ journalctl -u ssh -n 200 --no-pager > /lab_evidence/journal_ssh_last200.txt || true
total 68K
drwxr-x--x 2 sanjanathawalt2 sanjanathawalt2 4.0K Nov 5 01:43 .
drwxr-x--x 16 sanjanathawalt2 sanjanathawalt2 4.0K Nov 5 01:30 ..
-rw-rw-r-- 1 sanjanathawalt2 sanjanathawalt2 261 Nov 5 01:39 aureport_summary.txt
-rw-rw-r-- 1 sanjanathawalt2 sanjanathawalt2 13 Nov 5 01:39 auresearch_project_after.txt
-rw-rw-r-- 1 sanjanathawalt2 sanjanathawalt2 5.1K Nov 5 01:38 auresearch_sudoers_after.txt
-rw-rw-r-- 1 sanjanathawalt2 sanjanathawalt2 5.1K Nov 5 01:38 auresearch_sudoers_sfter.txt
-rw-rw-r-- 1 sanjanathawalt2 sanjanathawalt2 58 Nov 5 01:31 cron_after.txt
-rw-rw-r-- 1 sanjanathawalt2 sanjanathawalt2 28K 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:~/lab_evidence$ tar -czvf ~/lab_evidence_after.tar.gz -c - lab_evidence
tar: Removing leading '/' from member names
/home/sanjanathawalt2/
/home/sanjanathawalt2/.sudo_as_admin_successful
/home/sanjanathawalt2/.profile
/home/sanjanathawalt2/.xsession-errors
/home/sanjanathawalt2/lab_evidence/aureport_summary.txt
/home/sanjanathawalt2/lab_evidence/aureport_project_after.txt
/home/sanjanathawalt2/lab_evidence/aureport_key_after.txt
/home/sanjanathawalt2/lab_evidence/journal_ssh.last200.txt
/home/sanjanathawalt2/lab_evidence/sudoersd_after.txt
/home/sanjanathawalt2/lab_evidence/aureport_sudoers.sfter.txt
/home/sanjanathawalt2/lab_evidence/aureport_sudoers_after.txt
/home/sanjanathawalt2/lab_evidence/journal_cron.last200.txt
/home/sanjanathawalt2/lab_evidence/cron_after.txt
/home/sanjanathawalt2/Desktop/
/home/sanjanathawalt2/snap/
/home/sanjanathawalt2/snap/dsnapd-desktop-integration/
/home/sanjanathawalt2/snap/dsnapd-desktop-integration/common/
/home/sanjanathawalt2/snap/dsnapd-desktop-integration/common/.cache/

```

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

23°C Clear 12:32 ENG IN 05-11-2025

## Proof of Execution

```

ubuntu 2 - VMware Workstation
File Edit View VM Tabs Help || Home X | My Computer X | ubuntu 2 X | kali-linux-2023.2-vmware-amd64 X
Nov 5 12:31

[sudo] password for sanjanathawalt2:
NO_KEY_FILE
sanjanathawalt2@sanjanathawalt2:~/lab_evidence$ sudo ls -l /root/secrets/id_rsa_test 2>/dev/null || echo "NO_KEY_FILE"
[sudo] password for sanjanathawalt2:
sanjanathawalt2@sanjanathawalt2:~/lab_evidence$ mkdir -p ~/lab_evidence
[sudo] password for sanjanathawalt2:
sanjanathawalt2@sanjanathawalt2:~/lab_evidence$ ls -l /etc/cron.d/backup > ~/lab_evidence/cron_after.txt 2>&1
[sudo] password for sanjanathawalt2:
sanjanathawalt2@sanjanathawalt2:~/lab_evidence$ ls -l /etc/sudoers.d/ > ~/lab_evidence/sudoersd_after.txt 2>&1
[sudo] password for sanjanathawalt2:
[sudo] password for sanjanathawalt2:
Sorry, try again.
[sudo] password for sanjanathawalt2:
Sorry, try again.
[sudo] password for sanjanathawalt2:
[sudo] password for sanjanathawalt2:
sanjanathawalt2@sanjanathawalt2:~/lab_evidence$ sudo ausearch -k sudoers_change -i > ~/lab_evidence/ausearch_sudoers_sfter.txt 2>&1 ||true
[sudo] password for sanjanathawalt2:
sanjanathawalt2@sanjanathawalt2:~/lab_evidence$ sudo ausearch -k sudoers_change -i > ~/lab_evidence/ausearch_sudoers_after.txt 2>&1 ||true
sanjanathawalt2@sanjanathawalt2:~/lab_evidence$ sudo ausearch -k project_access -i > ~/lab_evidence/ausearch_project_after.txt 2>&1 ||true
sanjanathawalt2@sanjanathawalt2:~/lab_evidence$ sudo auseport -summary -file > ~/lab_evidence/aureport_summary.txt 2>&1 ||true
bash: /home/sanjanathawalt2/labevidence/aureport_summary.txt: No such file or directory
sanjanathawalt2@sanjanathawalt2:~/lab_evidence$ sudo auseport -summary -file > ~/lab_evidence/aureport_summary.txt 2>&1 ||true
sanjanathawalt2@sanjanathawalt2:~/lab_evidence$ journalctl -u ssh -n 200 --no-pager > ~/lab_evidence/journal_ssh.last200.txt || true
sanjanathawalt2@sanjanathawalt2:~/lab_evidence$ journalctl -u cron -n 200 --no-pager > ~/lab_evidence/journal_cron.last200.txt || true
sanjanathawalt2@sanjanathawalt2:~/lab_evidence$ tar -czvf ~/lab_evidence_after.tar.gz -c - lab_evidence
total 68K
drwxr-x--x 2 sanjanathawalt2 sanjanathawalt2 4.0K Nov 5 01:43 .
drwxr-x--x 16 sanjanathawalt2 sanjanathawalt2 4.0K Nov 5 01:30 ..
-rw-rw-r-- 1 sanjanathawalt2 sanjanathawalt2 261 Nov 5 01:43 aureport_summary.txt
-rw-rw-r-- 1 sanjanathawalt2 sanjanathawalt2 13 Nov 5 01:39 auresearch_project_after.txt
-rw-rw-r-- 1 sanjanathawalt2 sanjanathawalt2 5.1K Nov 5 01:38 auresearch_sudoers_after.txt
-rw-rw-r-- 1 sanjanathawalt2 sanjanathawalt2 5.1K Nov 5 01:38 auresearch_sudoers_sfter.txt
-rw-rw-r-- 1 sanjanathawalt2 sanjanathawalt2 58 Nov 5 01:31 cron_after.txt
-rw-rw-r-- 1 sanjanathawalt2 sanjanathawalt2 28K 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

```

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

23°C Clear 12:31 ENG IN 05-11-2025

## Proof of Execution

```
kali@kali: ~[~/Desktop]
$ ping -c 3 192.168.63.131
nmap -sV 192.168.63.131
ssh carol@192.168.63.131
ping: connect: Network is unreachable
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-04 13:18 EST
setup_target: failed to determine route to 192.168.63.131
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.16 seconds
ssh: connect to host 192.168.63.131 port 22: Network is unreachable

[kali㉿kali: ~[~/Desktop]
$ ping -c 3 192.168.63.131
nmap -sV 192.168.63.131
ssh carol@192.168.63.131
ping: connect: Network is unreachable
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-04 13:28 EST
setup_target: failed to determine route to 192.168.63.131
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.87 seconds
ssh: connect to host 192.168.63.131 port 22: Network is unreachable

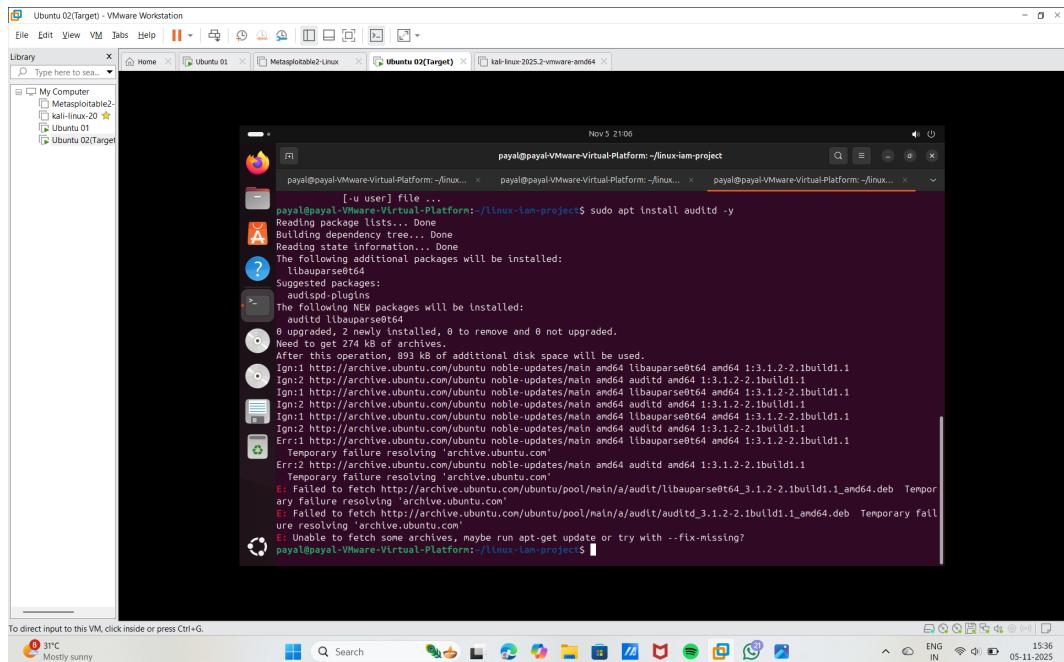
[kali㉿kali: ~[~/Desktop]
$ ping -c 3 192.168.74.131
nmap -sV 192.168.74.131
ssh carol@192.168.74.131
PING 192.168.74.131 (192.168.74.131) 56(64) bytes of data.
64 bytes from 192.168.74.131: icmp_seq=1 ttl=64 time=13.0 ms
64 bytes from 192.168.74.131: icmp_seq=2 ttl=64 time=2.65 ms
64 bytes from 192.168.74.131: icmp_seq=3 ttl=64 time=4.72 ms

--- 192.168.74.131 ping statistics --
```

## Proof of Execution

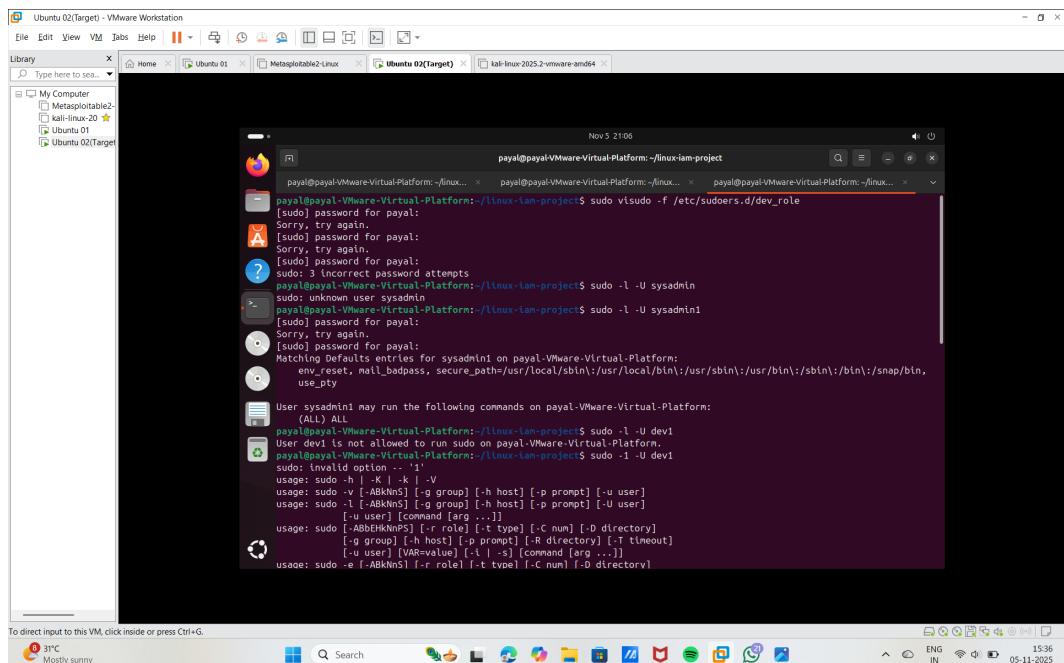
Proof of Execution

## 5. UPDATED PRACTICAL EXECUTION (ADDITIONAL)



```
[u user] file ...
payal@payal-VMware-Virtual-Platform:~/linux-iam-project$ sudo apt install auditd -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libltparser0 libauditd-plugins
Suggested packages:
auditd-sudo-plugins
The following NEW packages will be installed:
auditd libltparser0t64
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 274 kB of archives.
After this operation, 1.0 MB of additional disk space will be used.
Ign1: http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libltparser0t64 amd64 1:3.1.2-2.1build1.1
Ign1: https://archive.ubuntu.com/ubuntu noble-updates/main amd64 auditd amd64 1:3.1.2-2.1build1.1
Ign1: https://archive.ubuntu.com/ubuntu noble-updates/main amd64 libltparser0t64 amd64 1:3.1.2-2.1build1.1
Ign2: http://archive.ubuntu.com/ubuntu noble-updates/main amd64 auditd amd64 1:3.1.2-2.1build1.1
Ign2: https://archive.ubuntu.com/ubuntu noble-updates/main amd64 libltparser0t64 amd64 1:3.1.2-2.1build1.1
Err1: http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libltparser0t64 amd64 1:3.1.2-2.1build1.1
Temporary failure resolving 'archive.ubuntu.com'
Err1: Failed to fetch http://archive.ubuntu.com/ubuntu/pool/main/a/audit/libltparser0t64_1:3.1.2-2.1build1.1_amd64.deb Temporary failure resolving 'archive.ubuntu.com'
Err1: Failed to fetch http://archive.ubuntu.com/ubuntu/pool/main/a/audit/auditd_3.1.2-2.1build1.1_amd64.deb Temporary failure resolving 'archive.ubuntu.com'
Err1: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
payal@payal-VMware-Virtual-Platform:~/linux-iam-project$
```

### Proof of Execution



```
[sudo] password for payal:
Sorry, try again.
[sudo] password for payal:
Sorry, try again.
[sudo] password for payal:
sudo: 1 incorrect password attempt
payal@payal-VMware-Virtual-Platform:~/linux-iam-project$ sudo -l -U sysadmin
sudo: unknown user sysadmin
payal@payal-VMware-Virtual-Platform:~/linux-iam-project$ sudo -l -U sysadmin
[sudo] password for payal:
Sorry, try again.
[sudo] password for payal:
Matching Defaults entries for sysadmin on payal-VMware-Virtual-Platform:
    env_reset, mail_badpass, secure_path/usr/local/sbin/:usr/local/bin:/usr/sbin:/bin:/sbin:/snap/bin,
    use_pty
User sysadmin may run the following commands on payal-VMware-Virtual-Platform:
    (ALL) ALL
payal@payal-VMware-Virtual-Platform:~/linux-iam-project$ sudo -l -U dev1
User dev1 is not allowed to run sudo on payal-VMware-Virtual-Platform.
payal@payal-VMware-Virtual-Platform:~/linux-iam-project$ sudo -l -U dev1
sudo: dev1 is not in sudoers file
usage: sudo -h [-K] [-k] [-V]
usage: sudo -v [-ABKnS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-ABKnS] [-g group] [-h host] [-p prompt] [-U user]
           [-u user] [command [arg ...]]
usage: sudo [-ABbhNnPS] [-r role] [-t type] [-C num] [-D directory]
           [-g group] [-h host] [-p prompt] [-R directory] [-T timeout]
           [-u user] [VAR=value] [-l | -s] [command [arg ...]]
usage: sudo -e [-ABKnS] [-r role] [-t type] [-C num] [-D directory]
```

### Proof of Execution

```

Nov 5 21:07
payal@payal:~/VMware-Virtual-Platform: ~/linux-iam-project
payal@payal:~/VMware-Virtual-Platform: ~/linux-iam-project          payal@payal:~/VMware-Virtual-Platform: ~/linux-iam-project
GNU nano 7.2                                baseline_iam_policy.md *

## Baseline IAM Policy

## Roles
- **Admin** -> System management, limited sudo for system & apt.
- **Developer** -> Application restart, no root access.
- **Auditor** -> Read-only access to logs and project folders.

## Groups
- admin
- dev
- auditor
- devproj (shared project folders)

## Permissions
- -> /project -> owned by root:devproj
- Devs:Read+Write
- Auditors: Read-only via ACL

## Security Rules
- No 'NOPASSWD' in sudoers
- no world-writable system files
- Enable auditing on '/etc/passwd', '/etc/sudoers', '/srv/project'
cat baseline_iam_policy.md


```

## Proof of Execution

```

Nov 5 21:21
payal@payal:~/VMware-Virtual-Platform: ~/linux-iam-project
payal@payal:~/VMware-Virtual-Platform: ~/linux-iam-project          payal@payal:~/VMware-Virtual-Platform: ~/linux-iam-project
Need to get 274 kB of archives.
After this operation, 893 kB of additional disk space will be used.
Do you want to continue [Y/n]?
Ign:1 https://archive.ubuntu.com/ubuntu noble-updates/main amd64 liblbauparse0t64 amd64 1:3.1.2-2.1build1.1
Ign:2 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 audited amd64 1:3.1.2-2.1build1.1
Ign:3 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 liblbauparse0t64 amd64 1:3.1.2-2.1build1.1
Ign:4 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 audited amd64 1:3.1.2-2.1build1.1
Ign:5 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 liblbauparse0t64 amd64 1:3.1.2-2.1build1.1
Ign:6 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 liblbauparse0t64 amd64 1:3.1.2-2.1build1.1
Err:7 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 liblbauparse0t64 amd64 1:3.1.2-2.1build1.1
Temporary failure resolving 'archive.ubuntu.com'
Err:8 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 audited amd64 1:3.1.2-2.1build1.1
Temporary failure resolving 'archive.ubuntu.com'
E: Failed to fetch http://archive.ubuntu.com/ubuntu/pool/main/a/audit/liblbauparse0t64_3.1.2-2.1build1.1_amd64.deb  Temporary failure resolving 'archive.ubuntu.com'
E: Failed to fetch http://archive.ubuntu.com/ubuntu/pool/main/a/audit/audited_3.1.2-2.1build1.1_amd64.deb  Temporary failure resolving 'archive.ubuntu.com'
E: Unable to fetch some archives. Maybe run apt-get update or try with --fix-missing?
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
coreutils is already the newest version (9.4-3ubuntu6).
coreutils set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
payal@payal:~/VMware-Virtual-Platform: ~/linux-iam-project$ sudo augenrules --load
sudo: augenrules: command not found
payal@payal:~/VMware-Virtual-Platform: ~/linux-iam-project$ sudo auditcti -i
sudo: auditcti: command not found
payal@payal:~/VMware-Virtual-Platform: ~/linux-iam-project$
```

## Proof of Execution

```
Nov 5 21:27
payal@payal:~/VMware-Virtual-Platform: ~/linux-lan-project
payal@payal:~/VMware-Virtual-Platform: ~/linux... payal@payal:~/VMware-Virtual-Platform: ~/linux...
payal@payal:~/VMware-Virtual-Platform: ~/linux-lan-project$ ls -1
--help      list one file per line
--version   output version information and exit
A?          The SIZE argument is an integer and optional unit (example: 10K is 10*1024),
Units are K,M,G,T,P,E,Z,Y,R,Q (powers of 1024) or KB,MB,... (powers of 1000).
Binary prefixes can be used, too: KB=K, MIB=M, and so on.

The TIME_STYLE argument can be full-iso, long-iso, iso, locale, or +FORMAT.
FORMAT is interpreted like in date(1). If FORMAT is FORMAT1+newline+FORMAT2,
then FORMAT1 applies to non-recent files and FORMAT2 to recent files.
TIME_STYLE prefixed with 'posix-' takes effect only outside the POSIX locale.
Also the TIME_STYLE environment variable sets the default style to use.

The WHEN argument defaults to 'always' and can also be 'auto' or 'never'.

Using color to distinguish file types is disabled both by default and
with --color=never. With --color=auto, ls emits color codes only when
standard output is connected to a terminal. The LS_COLORS environment
variable can change the settings. Use the dircolors(1) command to set it.

Exit status:
0 if OK,
1 if minor problems (e.g., cannot access subdirectory),
2 if serious trouble (e.g., cannot access command-line argument).

GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Full documentation: <https://www.gnu.org/software/coreutils/ls>
or available locally via: info '(coreutils) ls invocation'
payal@payal:~/VMware-Virtual-Platform: ~/linux-lan-project$
```

## Proof of Execution

```
Nov 5 21:33
payal@payal:~/VMware-Virtual-Platform: ~/linux-lan-project
payal@payal:~/VMware-Virtual-Platform: ~/linux... payal@payal:~/VMware-Virtual-Platform: ~/linux...
payal@payal:~/VMware-Virtual-Platform: ~/linux-lan-project$ sudo chmod 755 /etc/cron.d
payal@payal:~/VMware-Virtual-Platform: ~/linux-lan-project$ sudo rm /etc/sudoers.d/99-weak
sudo: /etc/sudoers.d/99-weak: command not found
payal@payal:~/VMware-Virtual-Platform: ~/linux-lan-project$ sudo rm /etc/sudoers.d/99-weak
rm: cannot remove '/etc/sudoers.d/99-weak': No such file or directory
payal@payal:~/VMware-Virtual-Platform: ~/linux-lan-project$ ls -l
total 0
payal@payal:~/VMware-Virtual-Platform: ~/linux-lan-project$
```

## Proof of Execution

## CONCLUSION

Linux IAM and system hardening ensure that user privileges remain controlled and attackers cannot exploit misconfigurations. By applying ACL rules, strict sudo permissions, secure SSH settings and monitoring using auditd, the risk of privilege escalation is significantly reduced. This project demonstrates how proper configuration defends against attacks, proving security depends more on discipline than just tools.