

# **Minor Project 1: Linux IAM and Hardening**

**Om Raj Panday**

**Certified Ethical Hacking**

**6604327**

**5<sup>th</sup> Semester**

**Rungta College Of Engineering and Technology**

# PROJECT OVERVIEW

## Objective:

To design and implement a secure user/group and permission model on an Ubuntu server, detect and fix 3 misconfigurations, and maintain evidence of all configurations and auditing.

## Tools & Environment:

- Ubuntu Server (Lab VM)
- Kali Linux (Attacker VM– for testing)
- sudo access enabled

## Baseline Policy Document

Role	Privileges	Sudo Access	File access
Admin	Manage users, services, and software	useradd, usermod, systemctl, apt	Full access to /srv/project
Dev	Modify project files, restart app service	systemctl restart/status project.service only	Write to /srv/project, read-only for others
Auditor	Read log and audit evidence only	None	Read-only /srv/project, /var/log/audit

## Implementation Steps

- Creating User and Group
  - Sudo groupadd
  - Sudo useradd

- Configuring Sudoers

Created /etc/sudoers.d/roles-admin and /etc/sudoers.d/roles-dev

- Securing Project Directory

```
sudo mkdir-p /srv/project
```

```
sudo chown :proj /srv/project
```

```
sudo chmod 770 /srv/project
```

```
sudo setfacl-m g:dev:rwx /srv/project
```

```
sudo setfacl-m g:auditor:r-x /srv/project
```

- Enabling Auditing

```
sudo apt install auditd-y
```

```
sudo systemctl enable auditd--now
```

```
sudo auditctl-w /etc/passwd-p wa-k identity
```

```
sudo auditctl-w /etc/sudoers-p wa-k identity
```

- Vulnerability

World-writable /etc/cron.d/test	Unauthorized could add jobs	users sudo chmod 600 etc/cron.d/test
Sudo NOPASSWD for dev	Privilege escalation	Removed from /etc/sudoers.d/roles-dev
Weak permissions on /srv/project	Read/write for all users	sudo chmod 770 /srv/project and reset ACL

- Network check

#### **Scanned and Verified**

```
sudo ss-tulpn > ~/evidence/ports_after_closure.txt
```

```
sudo lsof-i-Pn > ~/evidence/open_sockets_after.txt
```

```
sudo nmap-p8080 127.0.0.1 > ~/evidence/nmap_8080_check.txt
```

- Remediation Verification

Task	Status
Remove world-writable files	✓
Disable unnecessary sudo NOPASSWD	✓
Lock down file permissions	✓
Enable audit logging	✓
Close unused ports	✓
Generate evidence folder	✓

- Summary

Users: 3 created (alice, bob, charlie)

Groups: 3 configured (admin, dev, auditor)

Sudorules: verified and validated

ACLs: configured correctly

Audit logs: functioning

Ports: secure, verified closed

## Proofs

### 1. Opening Ports to listen through

```
(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:79:29:b7 brd ff:ff:ff:ff:ff:ff
        inet 192.168.226.131/24 brd 192.168.226.255 scope global dynamic noprefixroute eth0
            valid_lft 1076sec preferred_lft 1076sec
        inet6 fe80::7dc4:ab2c:162:2554/64 scope link noprefixroute
            valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
└─$ sudo ufw allow from 192.168.226.131/24 to any port 22 proto tcp
WARN: Rule changed after normalization
Rules updated

(kali㉿kali)-[~]
└─$ sudo ufw allow from 192.168.226.131/24 to any port 8080 proto tcp
WARN: Rule changed after normalization
Rules updated

(kali㉿kali)-[~]
└─$ sudo ufw enable
Firewall is active and enabled on system startup

(kali㉿kali)-[~]
└─$ sudo ufw status numbered
Status: active

      To                         Action      From
      --                         --          --
[ 1] 22/tcp                     ALLOW IN   192.168.226.0/24
[ 2] 8080/tcp                   ALLOW IN   192.168.226.0/24
```

### 2. Open Ports for Enumerations for system hardening using ss commands

```
(kali㉿kali)-[~]
└─$ sudo ss -tuln
Netid      State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
tcp        LISTEN      0           5           0.0.0.0:8080      0.0.0.0:*
tcp        LISTEN      0           128         0.0.0.0:22       0.0.0.0:*
tcp        LISTEN      0           128         [::]:22        [::]:*
```

### 3. Nmap Scans

```
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.226.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 07:29 EST
Nmap scan report for 192.168.226.1
Host is up (0.00097s latency).
All 1000 scanned ports on 192.168.226.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.226.2
Host is up (0.0030s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:E0:E3:99 (VMware)

Nmap scan report for 192.168.226.254
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.226.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:FB:81:15 (VMware)

Nmap scan report for 192.168.226.131
Host is up (0.0000070s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
8080/tcp  open  http-proxy

Nmap done: 256 IP addresses (4 hosts up) scanned in 8.71 seconds
```

### 4. Nmap Port scans command used to check specific ports (22 and 8080)

on a target host

```
(kali㉿kali)-[~]
$ sudo nmap -Pn -p 22,8080 192.168.226.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 07:34 EST
Nmap scan report for 192.168.226.1
Host is up (0.00074s latency).

PORT      STATE      SERVICE
22/tcp    filtered  ssh
8080/tcp  filtered  http-proxy
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.46 seconds
```

## 5. Verification of service termination and port closure using ss, lsof, and Nmap

### Nmap

```
(kali㉿kali)-[~]
└─$ python3 -m http.server 8080 &
[1] 46224

(kali㉿kali)-[~]
└─$ Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...

(kali㉿kali)-[~]
└─$ sudo ss -tuln | grep 8080
tcp   LISTEN  0      5          0.0.0.0:8080        0.0.0.0:*
(kali㉿kali)-[~]
└─$ sudo lsof -i :8080
COMMAND  PID USER FD   TYPE DEVICE SIZE/OFF NODE NAME
python3  46224 kali  3u  IPv4    96781      0t0  TCP *:http-alt (LISTEN)

(kali㉿kali)-[~]
└─$ sudo nmap -p 8080 127.0.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 07:40 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00014s latency).

PORT      STATE SERVICE
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

(kali㉿kali)-[~]
└─$ ps aux | grep python3
kali      1527  0.0  2.9 603072 60268 ?        Sl  06:11  0:00 /usr/bin/python3 /usr/bin/blueman-applet
kali      1528  0.0  2.0 64724 40408 ?        S    06:11  0:00 /usr/bin/python3 /usr/share/system-config-printer/applet.py
kali     46224  0.0  0.9 32252 19388 pts/0     SN    07:38  0:00 python3 -m http.server 8080
kali     48516  0.0  0.1  6528  2296 pts/0     S+   07:42  0:00 grep --color=auto python3

(kali㉿kali)-[~]
└─$ sudo pkill -f "python3 -m http.server"
[1] + terminated python3 -m http.server 8080

(kali㉿kali)-[~]
└─$ sudo ss -tuln | grep 8080

(kali㉿kali)-[~]
└─$ sudo lsof -i :8080

(kali㉿kali)-[~]
└─$ sudo nmap -p 8080 127.0.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 07:44 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00016s latency).

PORT      STATE SERVICE
8080/tcp  closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

