

PROJECT: Linux IAM & Hardening mini

Submitted By:

Name: Kaushal Jung Thapa

ERP: 6604309

Course: CEH

1. 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

2. 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 logs and audit evidence only | None | Read-only /srv/project, /var/log/audit |

3. Implementation Steps

a) User and group creation

commands:

```
sudo groupadd
```

```
sudo useradd
```

b) Configure Sudoers (Least Privilege)

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

c) Step 3: Secure 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
```

Verification:

```
getfacl /srv/project
```

d) Enable 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
```

e) Vulnerability Discovery & Fixes

| | | |
|--------------------------------------------------|--------------------------------------|----------------------------------------------|
| ¹ World-writable /etc/cron.d/test | Unauthorized users could add jobs | sudo chmod 600 /etc/cron.d/test |
| ² Sudo NOPASSWD for devs | Privilege escalation | Removed from /etc/sudoers.d/roles- dev |
| ³ Weak permissions on /srv/project | Read/write for all users | sudo chmod 770 /srv/project and reset ACL |

f) Network Check

Scanned and Verified

```
sudo ss -tuln > ~/evidence/ports_after_closure.txt  
sudo lsof -i -Pn > ~/evidence/open_sockets_after.txt  
sudo nmap -p 8080 127.0.0.1 > ~/evidence/nmap_8080_check.txt
```

g) Remediation Checklist

| Task | Status |
|-----------------------------------|-------------------------------------|
| Remove world-writable files | <input checked="" type="checkbox"/> |
| Disable unnecessary sudo NOPASSWD | <input checked="" type="checkbox"/> |
| Lock down file permissions | <input checked="" type="checkbox"/> |
| Enable audit logging | <input checked="" type="checkbox"/> |
| Close unused ports | <input checked="" type="checkbox"/> |
| Generate evidence folder | <input checked="" type="checkbox"/> |

h) Summary

Users: 3 created (alice, bob, charlie)

Groups: 3 configured (admin, dev, auditor)

Sudo rules: verified and validated

ACLs: configured correctly

Audit logs: functioning

Ports: secure, verified closed

Supporting ScreenShots:

- 1) Opening ports to listen through

```
root@agent-virtual-machine: /home/agent
[1]+ 00:29:26:f8:9a brd ff:ff:ff:ff:ff:ff
altname enp2s1
inet 192.168.81.135/24 brd 192.168.81.255 scope global dynamic noarp
prefixroute ens33
    valid_lft 1378sec preferred_lft 1378sec
inet6 fe80::2ed0:df9c:93c:57b0/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
root@agent-virtual-machine:/home/agent# sudo ufw allow from 192.168.81.0/24 to any port 22 proto tcp
Rules updated
root@agent-virtual-machine:/home/agent# sudo ufw allow from 192.168.56.10 to any port 8080 proto tcp
Rules updated
root@agent-virtual-machine:/home/agent# sudo ufw enable
Firewall is active and enabled on system startup
root@agent-virtual-machine:/home/agent# sudo ufw status numbered
Status: active

      To                         Action      From
      --                         -----      ---
[ 1] 22/tcp                     ALLOW IN   192.168.81.0/24
[ 2] 8080/tcp                   ALLOW IN   192.168.56.10

root@agent-virtual-machine:/home/agent#
```

2) Open Ports Enumeration for System Hardening using ss Command

```
root@agent-virtual-machine:/home/agent# sudo ss -tuln
Netid State  Recv-Q Send-Q      Local Address:Port      Peer Address:Port Process
udp   UNCONN 0        0          127.0.0.53%lo:53      0.0.0.0:*
udp   UNCONN 0        0          0.0.0.0:631         0.0.0.0:*
udp   UNCONN 0        0          0.0.0.0:33601        0.0.0.0:*
udp   UNCONN 0        0          0.0.0.0:5353        0.0.0.0:*
udp   UNCONN 0        0          [::]:53837          [::]:*
udp   UNCONN 0        0          [::]:5353          [::]:*
tcp   LISTEN 0       128        0.0.0.0:1514        0.0.0.0:*
tcp   LISTEN 0       128        0.0.0.0:1515        0.0.0.0:*
tcp   LISTEN 0       128        127.0.0.1:631       0.0.0.0:*
tcp   LISTEN 0      2048       0.0.0.0:55000       0.0.0.0:*
tcp   LISTEN 0       511        0.0.0.0:443        0.0.0.0:*
tcp   LISTEN 0      4096       127.0.0.53%lo:53      0.0.0.0:*
tcp   LISTEN 0      4096       [::ffff:127.0.0.1]:9200  *:*
tcp   LISTEN 0      2048       [::]:55000          [::]:*
tcp   LISTEN 0       128        [::1]:631          [::]:*
tcp   LISTEN 0      4096       [::ffff:127.0.0.1]:9300  *:*
```

3) Nmap scan

```
Starting Nmap 7.80 ( https://nmap.org ) at 2025-11-04 23:23 IST
Nmap scan report for 192.168.81.1
Host is up (0.0019s latency).

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

Nmap scan report for _gateway (192.168.81.2)
Host is up (0.00061s latency).

PORT      STATE    SERVICE
22/tcp    closed   ssh
8080/tcp  closed   http-proxy
MAC Address: 00:50:56:EB:29:82 (VMware)

Nmap scan report for 192.168.81.128
Host is up (0.0022s latency).

PORT      STATE    SERVICE
22/tcp    closed   ssh
8080/tcp  closed   http-proxy
MAC Address: 00:0C:29:82:A5:0F (VMware)

Nmap scan report for 192.168.81.254
Host is up (0.00035s latency).

PORT      STATE    SERVICE
22/tcp    filtered ssh
8080/tcp  filtered http-proxy
MAC Address: 00:50:56:EF:2A:67 (VMware)

Nmap scan report for agent-virtual-machine (192.168.81.135)
Host is up (0.000057s latency).

PORT      STATE    SERVICE
22/tcp    closed   ssh
8080/tcp  closed   http-proxy

Nmap done: 256 IP addresses (5 hosts up) scanned in 3.51 seconds
root@agent-virtual-machine:/home/agent#
```

4) Nmap port scan command used to check specific ports (22 and 8080) on a target host

```
root@agent-virtual-machine:/home/agent# nmap -Pn -p 22,8080 192.168.56.20 -oN ~/evidence/nmap_sc
an.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2025-11-04 23:24 IST
Nmap scan report for 192.168.56.20
Host is up.

PORT      STATE    SERVICE
22/tcp    filtered ssh
8080/tcp  filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 3.16 seconds
```

5) Nmap scan from KALI LINUX

```
File Actions Edit View Help
└$ nmap -Pn -p 22,8080 1 + -oN ~/evidence/nmap_to_labvm.txt
Failed to open normal output file /home/kali/evidence/nmap_to_labvm.txt for writing: No such
file or directory (2)

└─(kali㉿kali)-[~]
└$ ping -c 4 192.16
PING 192.168.56.20 (192.168.56.20) 56(84) bytes of data.

— 192.168.56.20 ping statistics —
4 packets transmitted, 0 received, 100% packet loss, time 3082ms

└─(kali㉿kali)-[~]
└$ ^[[200~nman -Pn -p 192.168.56.20 + -oN ~/evidence/nmap_to_lab.txt
zsh: bad substitution
└─(kali㉿kali)-[~]
└$ nmap -Pn -p 22,8080 192.168.56.20 + -oN ~/evidence/nmap_to_lab.txt
cat ~/evidence/nmap_to_lab.txt
Failed to open normal output file /home/kali/evidence/nmap_to_lab.txt for writing: No such f
ile or directory (2)
cat: /home/kali/evidence/nmap_to_lab.txt: No such file or directory

└─(kali㉿kali)-[~]
└$ nmap -Pn -p 22,8080 192.168.56.20 + -oN ~/evidence/nmap_to_lab.txt
Failed to open normal output file /home/kali/evidence/nmap_to_lab.txt for writing: No such f
ile or directory (2)

└─(kali㉿kali)-[~]
└$ curl -I http://192.168.56.20:8080 --max-time 5
curl: (28) Connection timed out after 5002 milliseconds

└─(kali㉿kali)-[~]
└$
```

6) Verification of Service Termination and Port Closure using ss, lsof, and Nmap

```
root@agent-virtual-machine:/home/agent# sudo systemctl stop project.service
sudo systemctl disable project.service
sudo systemctl status project.service --no-pager
Failed to stop project.service: Unit project.service not loaded.
Failed to disable unit: Unit file project.service does not exist.
Unit project.service could not be found.
root@agent-virtual-machine:/home/agent# sudo systemctl stop project.service
Failed to stop project.service: Unit project.service not loaded.
root@agent-virtual-machine:/home/agent# sudo ss -tulpn | sed -n '1,200p'
Netid State Recv-Q Send-Q Local Address:Port Peer Address:PortProcess
udp UNCONN 0 0 127.0.0.53%lo:53 0.0.0.0:*
users:(("systemd-resolve",pid=675,fd=13))
udp UNCONN 0 0 0.0.0.0:631 0.0.0.0:*
users:(("cups-browsed",pid=1032,fd=7))
udp UNCONN 0 0 0.0.0.0:33601 0.0.0.0:*
users:(("avahi-daemon",pid=858,fd=14))
udp UNCONN 0 0 0.0.0.0:5353 0.0.0.0:*
users:(("avahi-daemon",pid=858,fd=12))
udp UNCONN 0 0 [:]:53837 [:]:*
users:(("avahi-daemon",pid=858,fd=15))
udp UNCONN 0 0 [:]:5353 [:]:*
users:(("avahi-daemon",pid=858,fd=13))
tcp LISTEN 0 128 0.0.0.0:1514 0.0.0.0:*
users:(("wazuh-remoted",pid=1948,fd=4))
tcp LISTEN 0 128 0.0.0.0:1515 0.0.0.0:*
users:(("wazuh-authd",pid=1834,fd=3))
tcp LISTEN 0 128 127.0.0.1:631 0.0.0.0:*
users:(("cupsd",pid=963,fd=7))
tcp LISTEN 0 2048 0.0.0.0:55000 0.0.0.0:*
users:(("python3",pid=1779,fd=42))
tcp LISTEN 0 511 0.0.0.0:443 0.0.0.0:*
users:(("node",pid=912,fd=19))
tcp LISTEN 0 4096 127.0.0.53%lo:53 0.0.0.0:*
users:(("systemd-resolve",pid=675,fd=14))
tcp LISTEN 0 4096 [:ffff:127.0.0.1]:9200 *:*
users:(("java",pid=1038,fd=618))
tcp LISTEN 0 2048 [:]:55000 [:]:*
users:(("python3",pid=1779,fd=44))
tcp LISTEN 0 128 [:]:631 [:]:*
users:(("cupsd",pid=963,fd=6))
tcp LISTEN 0 4096 [:ffff:127.0.0.1]:9300 *:*
users:(("java",pid=1038,fd=616))
root@agent-virtual-machine:/home/agent# sudo ss -tulpn | grep ':8080'
root@agent-virtual-machine:/home/agent# sudo lsof -i :8080 -Pn
root@agent-virtual-machine:/home/agent# sudo nmap -p 8080 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2025-11-04 23:42 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00012s latency).

PORT      STATE SERVICE
8080/tcp  closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
root@agent-virtual-machine:/home/agent# sudo ss -tulpn > ~/evidence/ports_after_closure.txt
sudo lsof -i -Pn > ~/evidence/open_sockets_after.txt
sudo nmap -p 8080 127.0.0.1 > ~/evidence/nmap_8080_check.txt
root@agent-virtual-machine:/home/agent#
```