INFOTACT
SOLUTIONS

INTERNSHIP REPORT

PROJECT 3 – SECURE LINUX SERVER SETUP & HARDENING

INFOTACT
SOLUTIONS

JULY 2025 - AUGUST 2025

SUBMITTED BY
Ranjith M C

Project 3 - Secure Linux Server Setup & Hardening

Platform: Ubuntu Server 22.04 (VMware)

Tools Used: SSH, UFW, Fail2Ban, auditd, Nmap, CIS Benchmark

Step 1: Deploy Linux Server (Ubuntu 22.04)

- A virtual machine was created using VMware Workstation.
- Ubuntu Server 22.04 was installed.
- A non-root user was created during installation.

The server was updated using the command:

```
sudo apt update && sudo apt upgrade -y
```

Step 2: Secure SSH Configuration

Commands Used:

```
sudo nano /etc/ssh/sshd_config
```

Changes Made:

- Disabled root login:
  `PermitRootLogin no`
- Enabled key-based authentication:
  `PasswordAuthentication no`
- Restarted SSH service:
  `sudo systemctl restart ssh`

Step 3: Setup UFW Firewall

Commands Used:

```
sudo apt install ufw

sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw allow OpenSSH
sudo ufw enable
sudo ufw status
```

Step 4: Install and Configure Fail2Ban

Commands Used:

```
sudo apt install fail2ban
sudo systemctl enable fail2ban
sudo systemctl start fail2ban
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
sudo nano /etc/fail2ban/jail.local
```

Fail2Ban Jail Config:

```
[sshd]
        enabled = true
        port = ssh
        filter = sshd
        logpath = /var/log/auth.log
        maxretry = 5
```

Step 5: Setup auditd for System Auditing

Commands Used:

```
sudo apt install auditd
sudo systemctl enable auditd
sudo systemctl start auditd
sudo auditctl -l
```

Step 6: Manual Checks with CIS Benchmarks

Verified:

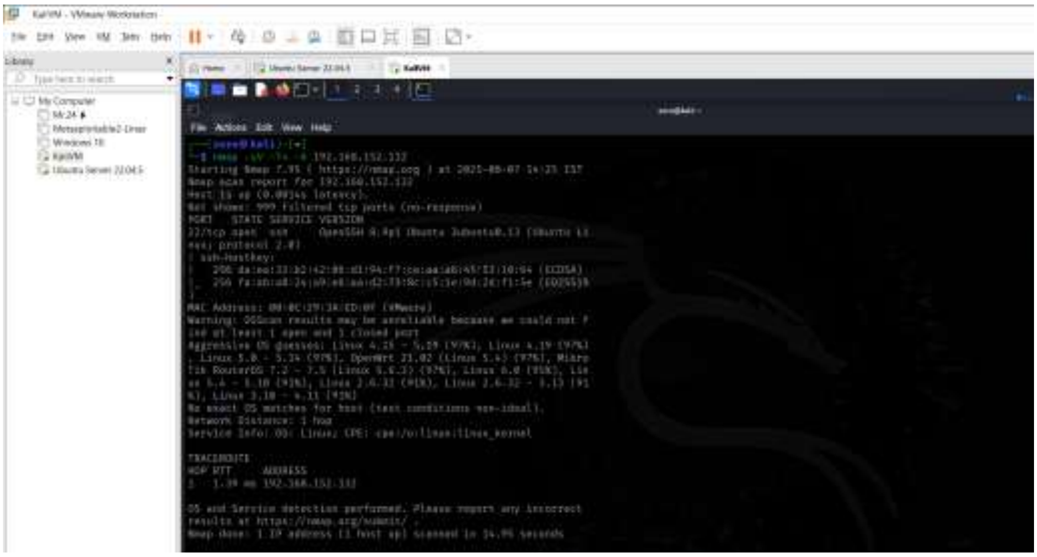
- Root login disabled via SSH
- Password-based login disabled
- UFW active and configured
- Fail2Ban working correctly
- auditd running and logging important events

Step 7: Perform Vulnerability Scan with Nmap (from Kali Linux)

Command Used:

```
ifconfig (Ubuntu Server)
```

```
nmap -sV -T4 -A 192.168.152.132 (Kali Linux)
```



```
┌──(user㉿kali)-[~]
└─$ nmap -sV -T4 -A 192.168.152.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 14:23 IST
Nmap scan report for 192.168.152.132
Host is up (0.00034s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Li
nux; protocol 2.0)
| ssh-hostkey:
|   256 da:ee:33:b2:42:88:d1:94:f7:ce:aa:a6:45:33:10:64 (ECDSA)
|_  256 fa:ab:a8:24:a9:e8:aa:d2:73:8c:15:1e:9d:2d:f1:5e (ED25519
)
MAC Address: 00:0C:29:3A:ED:0F (VMware)
Warning: OSScan results may be unreliable because we could not f
ind at least 1 open and 1 closed port
Aggressive OS guesses: Linux 4.15 - 5.19 (97%), Linux 4.19 (97%)
, Linux 5.0 - 5.14 (97%), OpenWrt 21.02 (Linux 5.4) (97%), Mikro
Tik RouterOS 7.2 - 7.5 (Linux 5.6.3) (97%), Linux 6.0 (95%), Lin
ux 5.4 - 5.10 (91%), Linux 2.6.32 (91%), Linux 2.6.32 - 3.13 (91
%), Linux 3.10 - 4.11 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.39 ms 192.168.152.132

OS and Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.95 seconds
```

Example Output:

- Port 22 open: SSH (OpenSSH 8.9p1)
- No other unnecessary open ports
- OS Detection: Linux Kernel 4.15 - 5.19

Step 8: Patch and Harden Server

Commands Used:

```
sudo apt update && sudo apt upgrade -y
```

Common updated services:

- openssh-server
- libc6
- auditd
- ufw
- grub-pc

Final Remediation Checklist ✅

Task	Status
SSH secured (no root login, key only)	✓
UFW configured with strict rules	✓
Fail2Ban protects SSH	✓
auditd enabled	✓
System packages up to date	✓
Vulnerability scan complete	✓

Conclusion

The Ubuntu server was securely deployed and hardened using best practices including SSH hardening, firewall configuration, brute-force protection, system auditing, and vulnerability scanning. These security measures significantly reduce the risk of unauthorized access and misconfiguration. This hardened system serves as a secure foundation for enterprise workloads.