🛡 Task 14: Linux Server Hardening & Secure Configuration

Platform: Ubuntu / Kali Linux
Tools: Lynis, CIS Benchmarks

🔐 Introduction

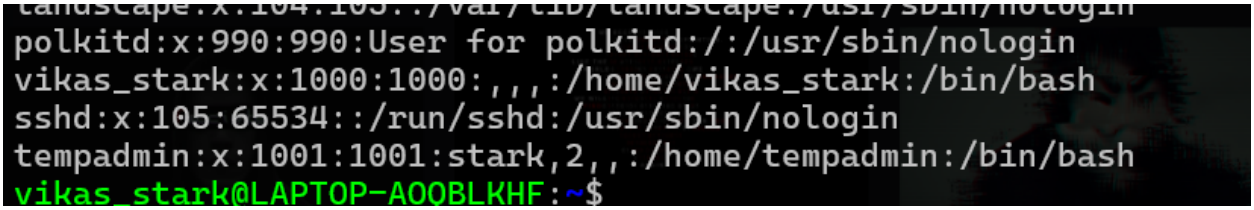
Linux server hardening is the process of securing a server by reducing its attack surface, removing unnecessary components, enforcing strict access control, and configuring services securely. The goal is to protect the system from unauthorized access and common cyberattacks.

📋 Linux Hardening Checklist

1️⃣ Review Default System Configuration

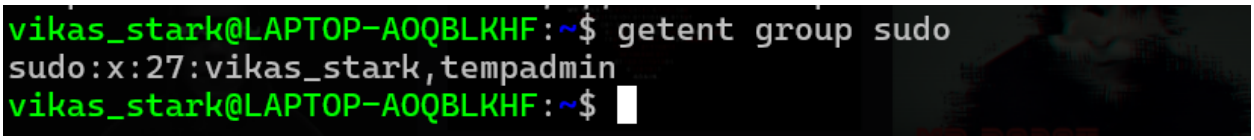
Check Users

cat /etc/passwd



Check Sudo Group

getent group sudo



Check Running Services

systemctl list-units --type=service --state=running

```
vikas_stark@LAPTOP-AOQBLKHF:~$ systemctl list-units --type=service --state=running
  UNIT                          LOAD   ACTIVE SUB     DESCRIPTION
  apache2.service               loaded active running The Apache HTTP Server
  console-getty.service         loaded active running Console Getty
  cron.service                  loaded active running Regular background program processing daemon
  dbus.service                  loaded active running D-Bus System Message Bus
  getty@tty1.service            loaded active running Getty on tty1
  rsyslog.service               loaded active running System Logging Service
  snapd.service                 loaded active running Snap Daemon
  systemd-journald.service      loaded active running Journal Service
  systemd-logind.service        loaded active running User Login Management
  systemd-resolved.service      loaded active running Network Name Resolution
  systemd-timesyncd.service     loaded active running Network Time Synchronization
  systemd-udevd.service         loaded active running Rule-based Manager for Device Events and Files
  unattended-upgrades.service loaded active running Unattended Upgrades Shutdown
  user@1000.service             loaded active running User Manager for UID 1000
  wsl-pro.service               loaded active running Bridge to Ubuntu Pro agent on Windows

Legend: LOAD   → Reflects whether the unit definition was properly loaded.
        ACTIVE → The high-level unit activation state, i.e. generalization of SUB.
        SUB    → The low-level unit activation state, values depend on unit type.

15 loaded units listed.
```

Check Open Ports

ss -tulnp

```
vikas_stark@LAPTOP-AOQBLKHF:~$ ss -tulnp
Netid      State       Recv-Q      Send-Q           Local Address:Port          Peer Address:Port     Process
udp        UNCONN      0           0                    127.0.0.1:323              0.0.0.0:*
udp        UNCONN      0           0                   127.0.0.54:53               0.0.0.0:*
udp        UNCONN      0           0                127.0.0.53%lo:53               0.0.0.0:*
udp        UNCONN      0           0               10.255.255.254:53               0.0.0.0:*
udp        UNCONN      0           0                        [::1]:323                  [::]:*
tcp        LISTEN      0           4096                127.0.0.54:53               0.0.0.0:*
tcp        LISTEN      0           1000            10.255.255.254:53               0.0.0.0:*
tcp        LISTEN      0           4096             127.0.0.53%lo:53               0.0.0.0:*
tcp        LISTEN      0           4096                   0.0.0.0:22               0.0.0.0:*
tcp        LISTEN      0           511                        *:80                     *:*
tcp        LISTEN      0           4096                    [::]:22                  [::]:*
vikas_stark@LAPTOP-AOQBLKHF:~$
```

2️⃣ Remove Unused Users & Restrict Sudo Access

Remove Unused User

sudo deluser viky

```
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo deluser viky
info: Removing crontab ...
info: Removing user `viky' ...
vikas_stark@LAPTOP-AOQBLKHF:~$
```

Edit Sudo Privileges

sudo visudo

Apply **least privilege principle** — give only necessary permissions.

3️⃣ Disable Root Login & Secure SSH

Edit SSH Configuration

sudo nano /etc/ssh/sshd_config

Change:

PermitRootLogin no

PasswordAuthentication no

Enable Key-Based Authentication

ssh-keygen

ssh-copy-id user@server-ip

Restart SSH:

sudo systemctl restart ssh

4️⃣ Update System & Enable Automatic Security Updates

Update Packages

sudo apt update && sudo apt upgrade -y

Install Automatic Updates

sudo apt install unattended-upgrades

sudo dpkg-reconfigure unattended-upgrades

5️⃣ Configure Firewall (UFW)

Enable Firewall

sudo ufw enable

Allow Required Ports

sudo ufw allow 22

sudo ufw allow 80

Check Firewall Status

sudo ufw status verbose

```
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo ufw enable
Firewall is active and enabled on system startup
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo ufw allow 22
sudo ufw allow 80
Skipping adding existing rule
Skipping adding existing rule (v6)
Skipping adding existing rule
Skipping adding existing rule (v6)
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
22                         ALLOW IN    Anywhere
80                         ALLOW IN    Anywhere
443                        ALLOW IN    Anywhere
23                         DENY IN     Anywhere
Anywhere                   ALLOW IN    192.168.1.10
Anywhere                   DENY IN     192.168.1.100
22/tcp (v6)                ALLOW IN    Anywhere (v6)
22 (v6)                    ALLOW IN    Anywhere (v6)
80 (v6)                    ALLOW IN    Anywhere (v6)
443 (v6)                   ALLOW IN    Anywhere (v6)
23 (v6)                    DENY IN     Anywhere (v6)

25                         DENY OUT    Anywhere
25 (v6)                    DENY OUT    Anywhere (v6)
```

6️⃣ Disable Unnecessary Services

List Services

systemctl list-unit-files --type=service

Disable Service

sudo systemctl stop service_name

sudo systemctl disable service_name

7️⃣ Secure File Permissions

Secure Shadow File

sudo chmod 640 /etc/shadow

sudo chown root:shadow /etc/shadow

Find World-Writable Files

sudo find / -perm -2 -type f 2>/dev/null

8️⃣ Review Logs & Monitor Activity

Authentication Logs

sudo cat /var/log/auth.log

Check Failed SSH Attempts

sudo grep "Failed password" /var/log/auth.log

System Logs

sudo journalctl -xe

🔍 Security Audit Tools

🔹 Lynis

Install:

sudo apt install lynis

Run Audit:

sudo lynis audit system

🔹 **Center for Internet Security (CIS Benchmarks)**

Use CIS guidelines to ensure secure configuration standards and compliance.

📄 **Security Configuration Summary**

- Removed unused users
- Restricted sudo access
- Disabled root login
- Enabled SSH key authentication
- Updated system packages
- Enabled automatic security updates
- Configured firewall (UFW)
- Disabled unnecessary services
- Secured sensitive file permissions
- Reviewed logs regularly
- Performed security audit using Lynis