✅ Step 1: Review Default System Settings

1️⃣ Check Users

cat /etc/passwd

Check users with login shell:

grep "/bin/bash" /etc/passwd

Check currently logged-in users:

who

2️⃣ Check Running Services

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

3️⃣ Check Open Ports

ss -tulnp

OR

netstat -tulnp

👉 Document:

- Open ports
- Associated services
- Whether required or not

✅ Step 2: Remove Unused Users & Restrict Sudo Access

1️⃣ Remove Unused User

sudo deluser username

Remove with home directory:

sudo deluser --remove-home username

2️⃣ Check Sudo Users

getent group sudo

Remove from sudo group:

sudo deluser username sudo

👉 Principle: **Least Privilege**

✅ **Step 3: Secure SSH Configuration**

Edit SSH config:

sudo nano /etc/ssh/sshd_config

1️⃣ **Disable Root Login**

Find:

PermitRootLogin yes

Change to:

PermitRootLogin no

2️⃣ **Disable Password Authentication (Key-based only)**

PasswordAuthentication no

3️⃣ **Restart SSH**

sudo systemctl restart ssh

4️⃣ **Generate SSH Key (Client Machine)**

ssh-keygen

Copy key:

ssh-copy-id user@server_ip

✅ **Step 4: Update System & Enable Auto Updates**

1️⃣ **Update System**

sudo apt update

sudo apt upgrade -y

2️⃣ **Enable Automatic Updates**

Install:

sudo apt install unattended-upgrades

Enable:

sudo dpkg-reconfigure unattended-upgrades

✅ **Step 5: Configure Firewall (UFW)**

Enable firewall:

sudo ufw enable

Allow SSH:

sudo ufw allow 22

Allow HTTP (if needed):

sudo ufw allow 80

Check status:

sudo ufw status verbose

👉 Only allow required ports.

✅ **Step 6: Disable Unnecessary Services**

Stop service:

sudo systemctl stop servicename

Disable permanently:

sudo systemctl disable servicename

Example:

sudo systemctl disable bluetooth

✅ **Step 7: Secure File Permissions**

1️⃣ **Secure /etc/shadow**

ls -l /etc/shadow

Correct permission:

-rw-r----- 1 root shadow

Fix if required:

sudo chmod 640 /etc/shadow

2️⃣ **Secure SSH Folder**

chmod 700 ~/.ssh

chmod 600 ~/.ssh/authorized_keys

3️⃣ Find World-Writable Files

sudo find / -type f -perm -002 2>/dev/null

✅ Step 8: Review Logs

1️⃣ Authentication Logs

Ubuntu:

sudo cat /var/log/auth.log

Kali:

sudo cat /var/log/auth.log

2️⃣ Failed Login Attempts

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

3️⃣ View System Logs

journalctl -xe