Linux Server Hardening Checklist

By : NROUPSINH GOHIL

1. System Information Review

- Checked Linux version using:

```
uname -a

lsb_release -a
```

- Identified running services:

```
systemctl list-units --type=service
```

- Checked open ports:

```
sudo ss -tulnp
```

---

2. User Account Management

- Listed all users:

```
cat /etc/passwd
```

- Removed unused accounts:

```
sudo userdel username
```

- Restricted sudo access by editing:

```
sudo visudo
```

- Applied **Least Privilege Principle**

---

3. Disable Root Login

- Edited SSH config:

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

- Modified:

```
PermitRootLogin no
```

- Restarted SSH:

```
sudo systemctl restart ssh
```

---

4. SSH Key-Based Authentication

- Generated key:

```
ssh-keygen
```

- Copied key to server:

```
ssh-copy-id user@server_ip
```

- Disabled password login:

```
PasswordAuthentication no
```

---

5. Update & Patch System

- Updated packages:

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

- Enabled automatic security updates:

```
sudo apt install unattended-upgrades
```

---

6. Firewall Configuration (UFW)

- Enabled firewall:

```
sudo ufw enable
```

- Allowed SSH:

```
sudo ufw allow 22
```

- Allowed HTTP/HTTPS:

```
sudo ufw allow 80
sudo ufw allow 443
```

- Checked status:

```
sudo ufw status
```

---

7. Disable Unnecessary Services

- Disabled service:

```
sudo systemctl disable service_name
sudo systemctl stop service_name
```

---

8. Secure File Permissions

- Secured SSH directory:

```
chmod 700 ~/.ssh
chmod 600 ~/.ssh/authorized_keys
```

- Checked sensitive files:

```
ls -l /etc/shadow
```

---

9. Log Monitoring

- Viewed authentication logs:

```
sudo cat /var/log/auth.log
```

- Monitored live logs:

```
sudo tail -f /var/log/auth.log
```