Cybersecurity Checklist for Linux Support

1.Keep your System Updated

Command in terminal: “ sudo apt update && sudo apt upgrade”

```
imad-baraja@cyberdawg:~$ sudo apt update && sudo apt upgrade
```

Why ?

To keep your system protected from unknown vulnerabilities and to install the latest patches and improvements.

2. Use Strong Passwords

- At least 12 chars
- Mix of uppercase, lowercases, numbers, and special symbols
- No personal info or common words

Why ?

Strong passwords prevent brute-force and dictionary attacks. Change them regularly.

3. Enable the Firewall

Command in terminal: “ sudo ufw enable”

```
imad-baraja@cyberdawg:~$ sudo ufw enable
```

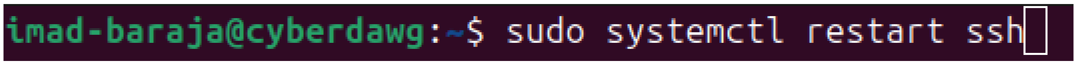
Why ?

Blocks unwanted incoming connections and helps control traffic. Always check with: “ sudo ufw status

```
imad-baraja@cyberdawg:~$ sudo ufw status
```

4. Disable Root Login Over SSH

File to Edit:
/etc/ssh/sshd_config
Change this line: “PermitRootLogin no”
Command in terminal: “ sudo systemctl restart ssh”



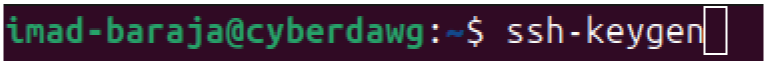
```
imad-baraja@cyberdawg:~$ sudo systemctl restart ssh
```

Why ?

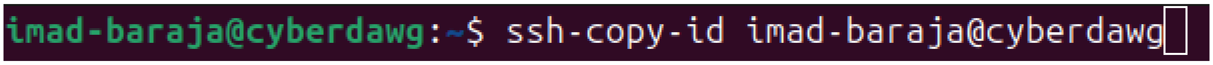
Prevent attackers from gaining full control via root access. Always use non-root user logins.

5. Use SSH Keys Instead of Passwords

Command in terminal: “ ssh-keygen
Ssh-copy-id username@server-ip



```
imad-baraja@cyberdawg:~$ ssh-keygen
```



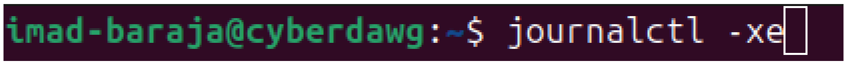
```
imad-baraja@cyberdawg:~$ ssh-copy-id imad-baraja@cyberdawg
```

Why ?

SSH keys are more secure than passwords and help protect against remote brute-force attacks.

6. Bonus Tips

- Lock your screen when away
- Don’t run unnecessary services
- Don’t plug in shady USBs
- Use antivirus like ClamAV if handling external files
- Check logs often “journalctl -xe”



```
imad-baraja@cyberdawg:~$ journalctl -xe
```