LINUX SERVER HARDENING CHECKLIST



BLUE

CHECKLIST V1

BY CRISTOPHER MEJIA

STEP 1: KEEP PACKAGES UPDATED

- [ ] sudo apt update && sudo apt upgrade -y

STEP 2: CONFIGURE A FIREWALL (UFW/IPTABLES)

- [ ] sudo ufw default deny incoming
- [ ] sudo ufw default allow outgoing
- [ ] sudo ufw allow OpenSSH
- [ ] sudo ufw allow ssh
- [ ] sudo ufw enable

STEP 3: DISABLE SSH ROOT LOGIN

- [ ] sudo sed -i 's/^#\?PermitRootLogin.*/PermitRootLogin no/' /etc/ssh/sshd_config
- [ ] sudo systemctl restart ssh

STEP 4: USE SSH KEY AUTHENTICATION AND DISABLE PASSWORDS

- [ ] ssh-keygen -t ed25519 -C "your_email@example.com"
- [ ] ssh-copy-id user@server_ip
- [ ] sudo sed -i 's/^#\?PasswordAuthentication.*/PasswordAuthentication no/' /etc/ssh/sshd_config
- [ ] sudo sed -i 's/^#\ChallengeResponseAuthentication.*/ChallengeResponseAuthentication no/' /etc/ssh/sshd_config
- [ ] sudo systemctl restart ssh

FASE 5: INSTALL AND CONFIGURE FAIL2BAN

- [ ] sudo apt install fail2ban -y
- [ ] sudo tee /etc/fail2ban/jail.local >/dev/null <<'EOF'
  [sshd]
  enabled = true
  port   = ssh
  filter = sshd
  logpath = /var/log/auth.log
  maxretry = 5
  bantime = 1h
  findtime = 10m
  EOF
- [ ] sudo systemctl enable --now fail2ban
- [ ] sudo fail2ban-client status
- [ ] sudo fail2ban-client status sshd

STEP 6: REMOVE UNNECESSARY SERVICES

- [ ] systemctl list-units --type=service --state=running
- [ ] sudo systemctl disable --now service_name

STEP 7: SET PROPER PERMISSIONS AND LEAST PRIVILEGE

- [ ] Lsudo find / -type f -perm -o+w 2>/dev/null | head
- [ ] sudo find / -type d -perm -o+w 2>/dev/null | head

STEP 8: AUDIT PROCESSES AND OPEN PORTS

- [ ] systemctl list-units --type=service --state=running
- [ ] sudo systemctl disable --now service_name

STEP 9: ENABLE LOGGING AND BASIC MONITORING

- [ ] systemctl list-units --type=service --state=running
- [ ] sudo systemctl disable --now service_name

STEP 10: REGULAR BACKUPS AND TESTED RESTORES

- [ ] sudo tar -czf /backups/etc-$(date +%F).tar.gz /etc
- [ ] sudo crontab -e   # schedule backups

Linux Server Hardening in Action

By Cristopher Mejia

1. Update packages

sudo apt update && sudo apt upgrade -y

```
cristo1256@cristo1256:~$ sudo apt update && sudo apt upgrade -y
[sudo] password for cristo1256:
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Hit:3 http://ec.archive.ubuntu.com/ubuntu noble InRelease
Hit:4 http://ec.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:5 http://ec.archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
41 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: https://artifacts.elastic.co/packages/8.x/apt/dists/stable/InRelease: Key is stored in
 legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-ke
y(8) for details.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

2. Configure firewall (UFW)

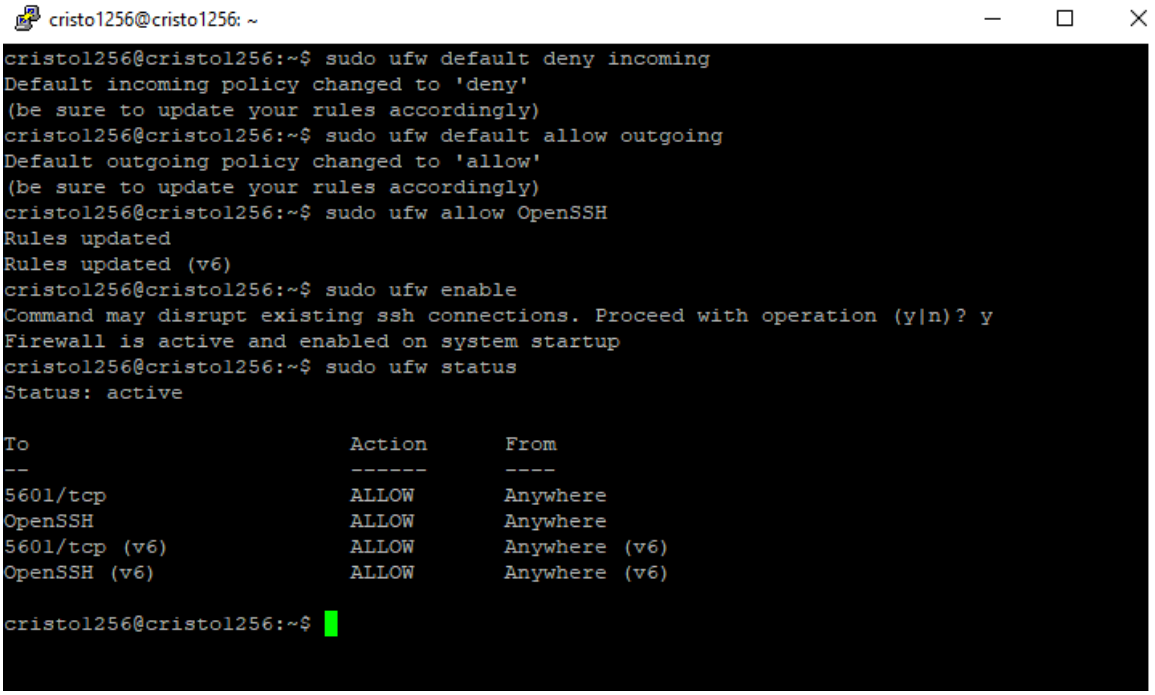
sudo ufw default deny incoming

sudo ufw default allow outgoing

sudo ufw allow OpenSSH

sudo ufw enable

sudo ufw status



3. Disable SSH root login

sudo sed -i 's/^#\?PermitRootLogin.*/PermitRootLogin no/' /etc/ssh/sshd_config

sudo systemctl restart ssh

```
cristol256@cristol256:~$ sudo sed -i 's/^#\?PermitRootLogin.*/PermitRootLogin no/' /etc/s
sh/sshd_config
cristol256@cristol256:~$ sudo systemctl restart ssh
```

4. Use SSH key authentication (disable passwords)

ssh-keygen -t ed25519 -C "your_email@example.com"

ssh-copy-id user@server_ip

sudo sed -i 's/^#\?PasswordAuthentication.*/PasswordAuthentication no/' /etc/ssh/sshd_config

sudo sed -i 's/^#\?ChallengeResponseAuthentication.*/ChallengeResponseAuthentication no/' /etc/ssh/sshd_config

sudo systemctl restart ssh

```
cristol256@cristol256:~$ ssh-keygen -t ed25519 -C "your_email@example.co
m"
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/cristol256/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/cristol256/.ssh/id_ed25519
Your public key has been saved in /home/cristol256/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:5TYClbQXdvI/KwhAXvaRlrtaANkpmGcVMppewmluFB8 your_email@example.co
m
The key's randomart image is:
+--[ED25519 256]--+
|      ▄▄▄▄▄▄▄▄▄  |
|      ++O**B.*   |
|      .@oo*.. o  |
|      =.+o o . . |
|       ▄▄▄▄▄ ...|
|      .  o...o  o|
|           .o. . |
|           .  .  |
|                 |
+----[SHA256]-----+
cristol256@cristol256:~$
```

5. Install and configure Fail2Ban

sudo apt install fail2ban -y

sudo tee /etc/fail2ban/jail.local >/dev/null <<'EOF'

[sshd]

enabled = true

port = ssh

filter = sshd

logpath = /var/log/auth.log

maxretry = 5

bantime = 1h

findtime = 10m

EOF

sudo systemctl enable --now fail2ban

sudo fail2ban-client status

sudo fail2ban-client status sshd

```
cristo1256@cristo1256:~$ sudo apt install fail2ban -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-pyasyncore python3-pyinotify whois
Suggested packages:
  mailx monit sqlite3 python-pyinotify-doc
The following NEW packages will be installed:
  fail2ban python3-pyasyncore python3-pyinotify whois
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 496 kB of archives.
After this operation, 2,572 kB of additional disk space will be used.
Get:1 http://ec.archive.ubuntu.com/ubuntu noble/main amd64 python3-pyasyncore all 1.0.2-2 [10.1
Get:2 http://ec.archive.ubuntu.com/ubuntu noble-updates/universe amd64 fail2ban all 1.0.2-3ubunt
 kB]
```

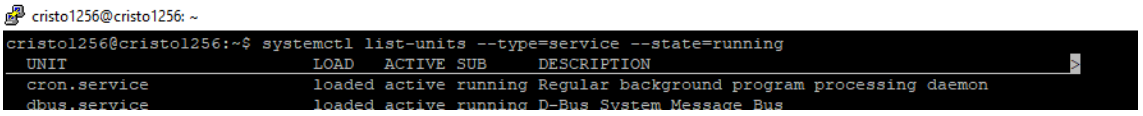
cristo1256@cristo1256: ~

```
cristo1256@cristo1256:~$ sudo tee /etc/fail2ban/jail.local >/dev/null <<'EOF'
> [sshd]
enabled = true
port    = ssh
filter  = sshd
logpath = /var/log/auth.log
maxretry = 5
bantime = 1h
findtime = 10m
EOF
```

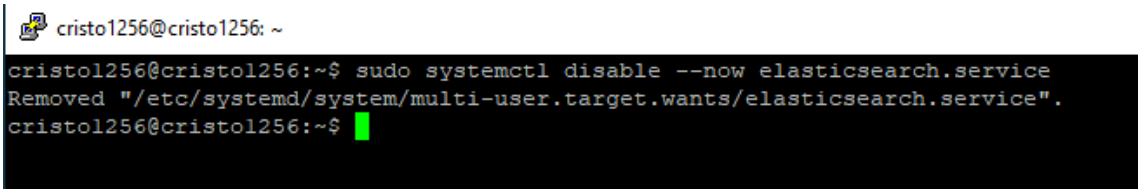
```
cristo1256@cristo1256:~$ sudo systemctl enable --now fail2ban
Synchronizing state of fail2ban.service with SysV service script with /usr/lib/systemd/systemd-sysv-insta
ll.
Executing: /usr/lib/systemd/systemd-sysv-install enable fail2ban
cristo1256@cristo1256:~$ sudo fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
cristo1256@cristo1256:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
cristo1256@cristo1256:~$
```

6. Remove unnecessary services

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

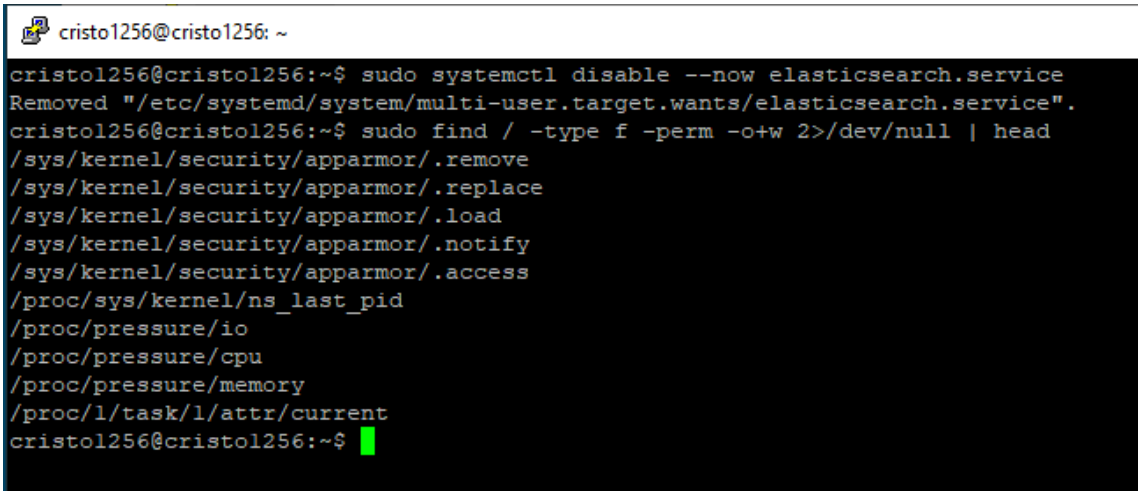


sudo systemctl disable --now service_name

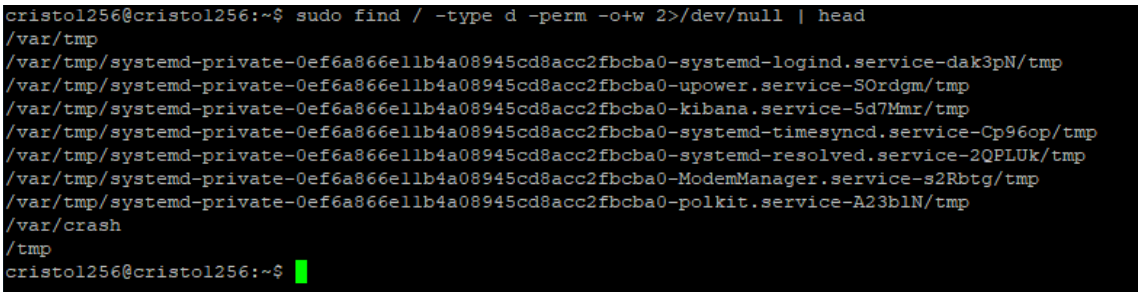


7. Audit permissions

sudo find / -type f -perm -o+w 2>/dev/null | head

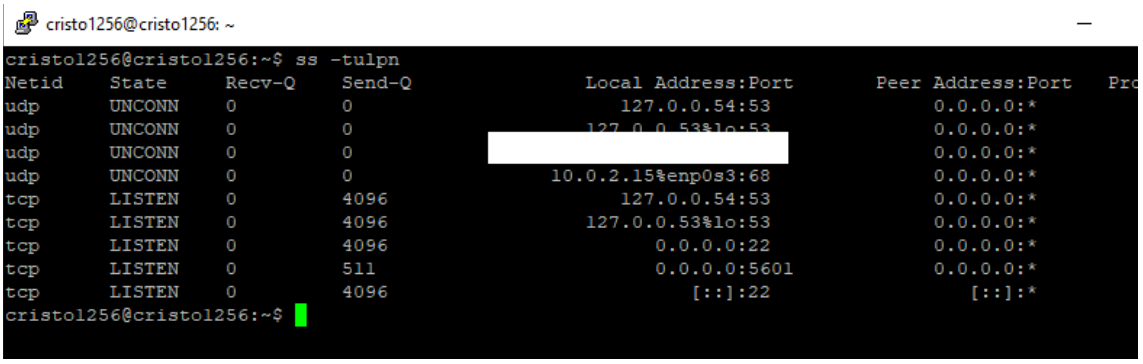


sudo find / -type d -perm -o+w 2>/dev/null | head



8. Audit processes and open ports

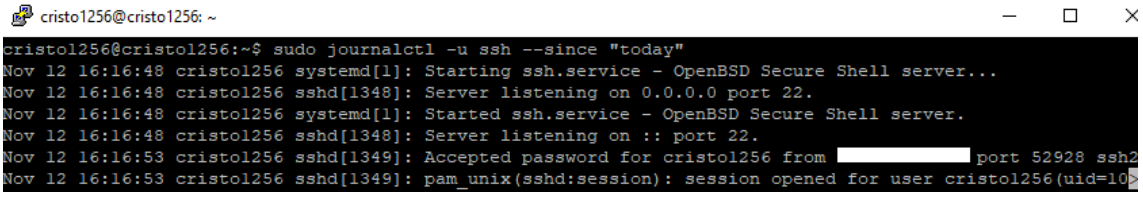
ss -tulpn



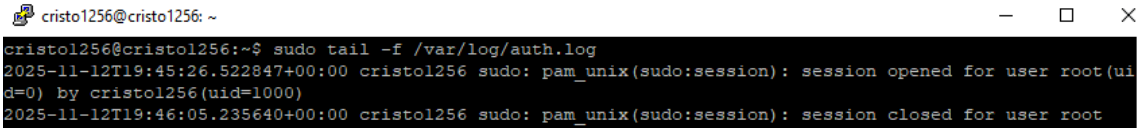
ps aux --sort=-%cpu | head

9. Check logs

sudo journalctl -u ssh --since "today"



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



10. Backup test

sudo tar -czf /backups/etc-$(date +%F).tar.gz /etc

ls -lh /backups/

