Hardening server Linux

SS

ssh -V
OpenSSH_9.6p1 Ubuntu-3ubuntu13.14, OpenSSL 3.0.13 30 Jan 2024

lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:	Ubuntu 24.04.3 LTS
Release:	24.04
Codename:	noble

uname -r
6.8.0-84-generic

uptime
20:41:17 up 43 min, 2 users, load average: 0.00, 0.00, 0.00

sudo ss -tuln | grep -E "LISTEN|UNCONN"
[sudo] password for admin:
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   10.0.2.15%enp0s3:68   0.0.0.0:*
tcp   LISTEN 0   4096   0.0.0.0:22   0.0.0.0:*
tcp   LISTEN 0   4096   127.0.0.53%lo:53   0.0.0.0:*
tcp   LISTEN 0   4096   127.0.0.54:53   0.0.0.0:*
tcp   LISTEN 0   4096   [::]:22   [::]:*

sudo nmap -sV -O 127.0.0.1

Starting Nmap 7.94SVN (https://nmap.org) at 2025-09-30 20:45 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000033s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.73 seconds

sudo chkrootkit | grep -i "infected"
Checking basename'... not infected Checking chfn'...
not infected
Checking chsh'... not infected Checking cron'...
not infected
Checking crontab'... not infected Checking date'...
not infected
Checking du'... not infected Checking dirname'...
not infected
Checking echo'... not infected Checking egrep'...
not infected
Checking env'... not infected Checking find'...
not infected
Checking grep'... not infected Checking hdparm'...
not infected
Checking su'... not infected Checking ifconfig'...
not infected
Checking inetd'... not infected Checking init'...

not infected
Checking killall'... not infected Checking ldsopreload'...
not infected
Checking login'... not infected Checking ls'...
not infected
Checking lsof'... not infected Checking mail'...
not infected
Checking netstat'... not infected Checking passwd'...
not infected
Checking pidof'... not infected Checking ps'...
not infected
Checking pstree'... not infected Checking slogin'...
not infected
Checking sendmail'... not infected Checking sshd'...
not infected
Checking tar'... not infected Checking tcpdump'...
not infected
Checking top'... not infected Checking vdir'...
not infected
Checking w'... not infected Checking write'...
not infected
Checking `asp'... not infected

sudo rkhunter --check --sk
/var/log/rkhunter.log

sudo grep -i "fail|invalid" /var/log/auth.log
grep: /var/log/auth.log: binary file matches

sudo journalctl _SYSTEMD_UNIT=ssh.service | tail -50
Sep 30 19:37:24 server sshd[9219]: Server listening on 0.0.0.0 port 22.
Sep 30 19:37:24 server sshd[9219]: Server listening on :: port 22.
Sep 30 19:42:49 server sshd[9219]: Received signal 15; terminating.
-- Boot 155c4ab708084767aba9289969aa8f45 --
Sep 30 19:45:28 server sshd[1035]: Server listening on 0.0.0.0 port 22.
Sep 30 19:45:28 server sshd[1035]: Server listening on :: port 22.

-- Boot 642bef6a0065416ba91c9d85d719f1a4 --
Sep 30 19:55:32 server sshd[650]: Server listening on 0.0.0.0 port 22.
Sep 30 19:55:32 server sshd[650]: Server listening on :: port 22.
-- Boot e0fe4ed3ed834ddf8125780145db44c2 --
Sep 30 19:58:15 server sshd[630]: Server listening on 0.0.0.0 port 22.
Sep 30 19:58:16 server sshd[630]: Server listening on :: port 22.
Sep 30 20:03:13 server sshd[630]: Received signal 15; terminating.
Sep 30 20:03:13 server sshd[1138]: Server listening on 0.0.0.0 port 22.
Sep 30 20:03:13 server sshd[1138]: Server listening on :: port 22.
Sep 30 20:15:57 server sshd[1264]: Accepted password for admin from 192.168.50.15 port 49830 ssh2
Sep 30 20:15:57 server sshd[1264]: pam_unix(sshd:session): session opened for user admin(uid=1000) by admin(uid=0)
Sep 30 20:45:32 server sshd[1640]: Connection closed by 127.0.0.1 port 33424
Sep 30 21:04:07 server sshd[41663]: Connection closed by authenticating user admin 192.168.50.15 port 32782 [preauth]
Sep 30 21:05:01 server sshd[41669]: Accepted password for admin from 192.168.50.15 port 54576 ssh2
Sep 30 21:05:01 server sshd[41669]: pam_unix(sshd:session): session opened for user admin(uid=1000) by admin(uid=0)
Sep 30 21:05:02 server sshd[41669]: pam_unix(sshd:session): session closed for user admin

==========

sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)

sudo ufw allow OpenSSH
Rules updated
Rules updated (v6)

sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)?

y
Firewall is active and enabled on system startup

sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To	Action	From
22/tcp (OpenSSH)	ALLOW IN	Anywhere
22/tcp (OpenSSH (v6))	ALLOW IN	Anywhere (v6)

sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.bak

sudo sed -i 's/#Port 22/Port 2222/' /etc/ssh/sshd_config

sudo sed -i 's/PermitRootLogin yes/PermitRootLogin no/' /etc/ssh/sshd_config

========== problema conexion ssh con cambio de puerto

Perfecto, aquí va la **guía resumida y funcional** para cambiar el puerto de SSH a 2222 en Ubuntu Server 24, manteniendo la activación por socket y sin perder acceso:

1️⃣ Crear directorio para configuración personalizada del socket

```
sudo mkdir -p /etc/systemd/system/ssh.socket.d
```

2️⃣ Crear archivo de configuración `listen.conf`

```
sudo nano /etc/systemd/system/ssh.socket.d/listen.conf
```

Contenido:

```
[Socket]
# Borra cualquier puerto previo
ListenStream=
# Escucha explícitamente en IPv4 y IPv6
ListenStream=0.0.0.0:2222
ListenStream=[::]:2222
```

Guardá y cerrá (`Ctrl+O`, `Enter`, `Ctrl+X`).

3️⃣ Recargar systemd y reiniciar el socket

```
sudo systemctl daemon-reload
sudo systemctl restart ssh.socket
```

Verificar que escucha:

```
sudo ss -tuln | grep 2222
```

Deberías ver algo como:

```
tcp   LISTEN  0      4096  0.0.0.0:2222      0.0.0.0:*
tcp   LISTEN  0      4096  [::]:2222         [::]:*
```

4️⃣ Abrir el puerto en el firewall

```
sudo ufw allow 2222/tcp
sudo ufw reload
```

Verificar:

```
sudo ufw status
```

5️⃣ Probar conexión SSH

Desde otra terminal:

```
ssh -p 2222 usuario@IP_DEL_SERVIDOR
```

- Para pruebas locales: `ssh -p 2222 usuario@127.0.0.1`
- Debería conectarse sin problema.

✅ Notas importantes

- **No se modifica el archivo original** `/lib/systemd/system/ssh.socket`, se usa la configuración personalizada para evitar problemas con actualizaciones del sistema.
- **IPv4 e IPv6 asegurados**: así evitamos "connection refused" por solo escuchar en IPv6.
- **Prueba antes de cerrar sesión**: siempre recomendable para no perder acceso.

---

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:

Servicios que **normalmente puedes deshabilitar en un Ubuntu Server minimal** (seguro si no los usás):

- **apport.service** → sistema de reportes de errores de Ubuntu. Innecesario en un server.

- **pollinate.service** → servicio de Ubuntu para generar entropía/semillas criptográficas en la nube. No suele hacer falta.
- **gpu-manager.service** → gestiona drivers gráficos. En un server sin entorno gráfico, sobra.
- **ModemManager.service** → solo sirve si usás un módem USB 3G/4G. Si estás en VM o ethernet, lo podés quitar.
- **open-vm-tools.service** → solo útil si usás VMware. Si estás en VirtualBox, podés deshabilitarlo.
- **vboxadd.service / vboxadd-service.service / vgauth.service** → al revés: solo sirven en VirtualBox. Si no estás en VirtualBox, fuera.
- **cloud-init**(cloud-config.service, cloud-final.service, cloud-init.service, etc.) → solo necesarios si tu VM viene de una imagen cloud (AWS, Azure, etc.). En local, podés deshabilitarlos si no los usás.
- **snapd**(snapd.service y relacionados) → gestor de paquetes snap. Si no usás snaps, podés deshabilitarlo para ahorrar memoria/CPU.
- **thermald.service** → gestiona temperatura del procesador. En VM no hace falta, en baremetal podría ser útil.
- **multipathd.service / open-iscsi.service / iscsid.service** → solo si usás almacenamiento iSCSI o multipath. Si no, deshabilitables.
- **postfix.service** → servidor de correo. Solo necesario si enviás correos desde el server. En la mayoría de los casos, se puede deshabilitar.
- **uuidd.service** → generador de UUIDs, normalmente innecesario salvo aplicaciones muy específicas.
- **unattended-upgrades.service** → instala actualizaciones automáticas. Lo podés deshabilitar si preferís controlar las updates manualmente.
- **sysstat.service** → recolecta estadísticas del sistema (iostat, sar). Si no lo usás, sobra.

Servicios que **conviene dejar habilitados:**

- **ssh.service** (obvio, acceso remoto).
- **systemd-networkd.service** y relacionados (manejo de red).
- **systemd-resolved.service** (resolución DNS).

- **ufw.service** (firewall).
- **fail2ban.service** (cuando lo dejes funcionando).
- **rsyslog.service** (logs).
- **systemd-timesyncd.service** (sincronización de hora).
- **apparmor.service** (seguridad obligatoria, mejor dejarlo).
- **cron.service** (tareas programadas).
- **e2scrub_reap.service** (limpieza de filesystems, útil en ext4).
- **secureboot-db.service** (solo si usás secure boot).
- **lvm2-monitor.service** (si usás LVM en tus discos).

Sugerencias aplicadas de Lynis:

MAIL-8818

AUTH-9262
AUTH-9286
AUTH-9328

SSH-7408

BOOT-5122
KRNL-5820
NETW-3200

ACCT-9628
PKGS-7370
PKGS-7394