

Auditoría técnica de seguridad de infraestructura.

1. Análisis de red y descubrimiento de hosts.

Para detectar dispositivos activos en la red local utilizamos:

nmap -sn 192.168.1.0/24

```
AZDINFARISSE@SVR-BASE-AZDINFARISSE: ~  
File Edit View Search Terminal Help  
AZDINFARISSE@SVR-BASE-AZDINFARISSE:~$ nmap -sn 192.168.1.0/24  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 10:30 CEST  
Nmap scan report for 192.168.1.1 (192.168.1.1)  
Host is up (0.0013s latency).  
Nmap scan report for SVR-BASE-AZDINFARISSE (192.168.1.20)  
Host is up (0.00026s latency).  
Nmap scan report for 192.168.1.129 (192.168.1.129)  
Host is up (0.0030s latency).  
Nmap scan report for 192.168.1.132 (192.168.1.132)  
Host is up (0.0065s latency).  
Nmap scan report for 192.168.1.133 (192.168.1.133)  
Host is up (0.063s latency).  
Nmap scan report for 192.168.1.134 (192.168.1.134)  
Host is up (0.16s latency).  
Nmap scan report for 192.168.1.135 (192.168.1.135)  
Host is up (0.16s latency).  
Nmap scan report for 192.168.1.141 (192.168.1.141)  
Host is up (0.015s latency).  
Nmap scan report for 192.168.1.145 (192.168.1.145)  
Host is up (0.061s latency).  
Nmap scan report for 192.168.1.146 (192.168.1.146)  
Host is up (0.12s latency).  
Nmap scan report for 192.168.1.147 (192.168.1.147)  
Host is up (0.0011s latency).
```

Para identificar los puertos abiertos y servicios expuestos:

nmap -sV 192.168.1.20

```
AZDINFARISSE@SVR-BASE-AZDINFARISSE: ~  
File Edit View Search Terminal Help  
AZDINFARISSE@SVR-BASE-AZDINFARISSE:~$ nmap -sV 192.168.1.20/24  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 10:35 CEST  
Nmap scan report for 192.168.1.1 (192.168.1.1)  
Host is up (0.00060s latency).  
Not shown: 996 closed tcp ports (conn-refused)  
PORT      STATE SERVICE VERSION  
22/tcp    filtered ssh  
53/tcp    open  domain Actiontec router dnsd  
80/tcp    open  http   ZTE web server 1.0 ZTE corp 2015.  
443/tcp   open  tcpwrapped  
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :  
_SF-Port80-TCP:V=7.95%I=7%D=7/21%Time=687DFC0F%P=x86_64-unknown-linux-gnu%r  
SF:(GetRequest,1007F,"HTTP/1.0%0x20200%0x200K\r\nServer:%x20ZTE%0x20web%0x20s  
SF:erver%0x201.0%0x20ZTE%0x20corp%0x202015%0\r\nAccept-Ranges:%x20bytes\r\nCo  
SF:nnection:%x20close\r\nX-Frame-Options:%x20SAMEORIGIN\r\nCache-Control:%  
SF:x20no-cache,no-store\r\nContent-Length:%x20153277\r\nSet-Cookie:%x20SID  
SF:=c00b7baab8a7405fab6df141dea7774f2bdf1a637676553e500906270aa18a76;%x20P  
SF:ATH=;%x20HttpOnly\r\nSet-Cookie:%x20_TESTCOOKIE$UPPORT=1;%x20PATH=/;%x  
SF:20HttpOnly\r\nX-Content-Type-Options:%x20nosniff\r\nX-XSS-Protection:%x  
SF:201;%x20mode=block\r\nContent-Security-Policy:%x20frame-ancestors%0x20's  
SF:elf'%x20data:\r\nContent-Type:%x20text/html;%x20charset=utf-8\r\n\r\n<!  
SF:DOCTYPE%0x20HTML%0x20PUBLIC%0x20"-//W3C//DTD%0x20HTML%0x204.01%0x20Transiti  
SF:onal//EN%0x20"http://www.w3.org/TR/html4/transition%0x20dtd">%0x20<htm
```

Para detectar sistemas operativos y versiones:

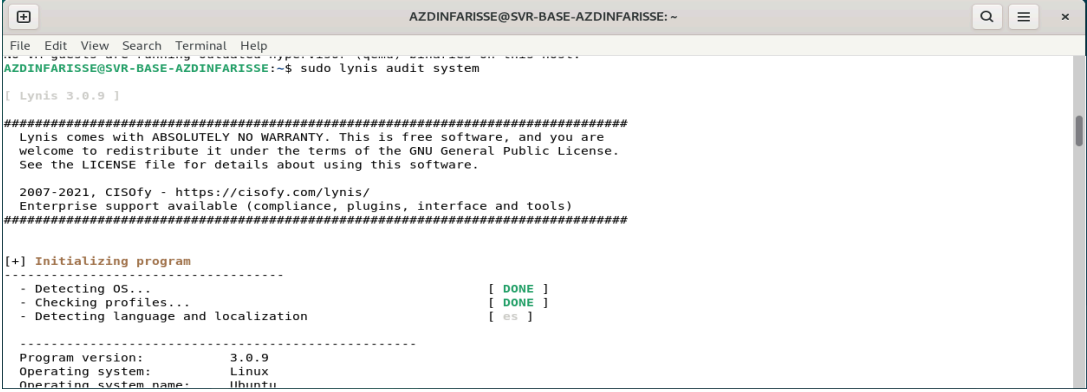
sudo nmap -O 192.168.1.20

```
AZDINFARISSE@SVR-BASE-AZDINFARISSE: ~  
File Edit View Search Terminal Help  
AZDINFARISSE@SVR-BASE-AZDINFARISSE:~$ sudo nmap -O 192.168.1.20  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-21 13:08 CEST  
Nmap scan report for SVR-BASE-AZDINFARISSE (192.168.1.20)  
Host is up (0.000011s latency).  
Not shown: 990 closed tcp ports (reset)  
PORT      STATE SERVICE  
25/tcp    open  smtp  
80/tcp    open  http  
110/tcp   open  pop3  
143/tcp   open  imap  
465/tcp   open  smtps  
587/tcp   open  submission  
993/tcp   open  imaps  
995/tcp   open  pop3s  
2222/tcp  open  EtherNetIP-1  
3128/tcp  open  squid-http  
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  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds
```

2. Evaluación de seguridad en servidores Linux.

Para hacer una auditoría del sistema utilizaremos **lynis**. Para ello lo instalamos y ejecutamos con:

```
sudo apt install lynis  
sudo lynis audit system
```



```
AZDINFARISSE@SVR-BASE-AZDINFARISSE: ~  
File Edit View Search Terminal Help  
AZDINFARISSE@SVR-BASE-AZDINFARISSE:~$ sudo lynis audit system  
[ Lynis 3.0.9 ]  
#####  
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are  
welcome to redistribute it under the terms of the GNU General Public License.  
See the LICENSE file for details about using this software.  
  
2007-2021, CISofy - https://cisofy.com/lynis/  
Enterprise support available (compliance, plugins, interface and tools)  
#####  
[+] Initializing program  
-----  
- Detecting OS... [ DONE ]  
- Checking profiles... [ DONE ]  
- Detecting language and localization [ es ]  
-----  
Program version: 3.0.9  
Operating system: Linux  
Operating system name: ubuntu
```

Esto genera un log que se guarda en:

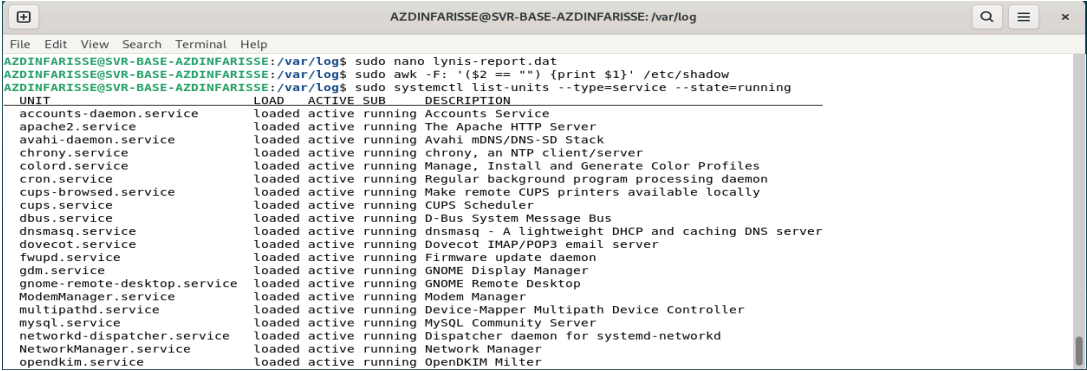
```
/var/log/lynis.log  
/var/log/lynis-report.dat
```

Para buscar si hay usuarios sin contraseña:

```
sudo awk -F: '($2 == "") {print $1}' /etc/shadow
```

Para buscar servicios innecesarios activos:

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



```
AZDINFARISSE@SVR-BASE-AZDINFARISSE: /var/log  
File Edit View Search Terminal Help  
AZDINFARISSE@SVR-BASE-AZDINFARISSE:/var/log$ sudo nano lynis-report.dat  
AZDINFARISSE@SVR-BASE-AZDINFARISSE:/var/log$ sudo awk -F: '($2 == "") {print $1}' /etc/shadow  
AZDINFARISSE@SVR-BASE-AZDINFARISSE:/var/log$ sudo systemctl list-units --type=service --state=running  
UNIT                                LOAD    ACTIVE SUB    DESCRIPTION  
accounts-daemon.service             loaded active running Accounts Service  
apache2.service                     loaded active running The Apache HTTP Server  
avahi-daemon.service                loaded active running Avahi mDNS/DNS-SD Stack  
chrony.service                      loaded active running chrony, an NTP client/server  
colord.service                      loaded active running Manage, Install and Generate Color Profiles  
cron.service                        loaded active running Regular background program processing daemon  
cups-browsed.service                loaded active running Make remote CUPS printers available locally  
cups.service                        loaded active running CUPS Scheduler  
dbus.service                        loaded active running D-Bus System Message Bus  
dnsmasq.service                     loaded active running dnsmasq - A lightweight DHCP and caching DNS server  
dovecot.service                     loaded active running Dovecot IMAP/POP3 email server  
fwupd.service                       loaded active running Firmware update daemon  
gdm.service                         loaded active running GNOME Display Manager  
gnome-remote-desktop.service         loaded active running GNOME Remote Desktop  
ModemManager.service                loaded active running Modem Manager  
multipathd.service                  loaded active running Device-Mapper Multipath Device Controller  
mysql.service                       loaded active running MySQL Community Server  
networkd-dispatcher.service          loaded active running Dispatcher daemon for systemd-networkd  
NetworkManager.service              loaded active running Network Manager  
opendkim.service                    loaded active running OpenDKIM Milter
```

Para valorar si se están aplicando actualizaciones des seguridad correctamente:

```
sudo apt update  
sudo apt list --upgradable  
sudo unattended-upgrades --dry-run
```

Para procesos activos:

```
ps aux --sort=-%mem | head -n 15
```

```
AZDINFARISSE@SVR-BASE-AZDINFARISSE: /var/log
File Edit View Search Terminal Help
/snap/core22/2010/usr/lib/openssh/ssh-keysign
/snap/core22/2010/usr/libexec/polkit-agent-helper-1
/snap/core22/2010/usr/sbin/pam_extrausers_chkpwd
/snap/core22/2010/usr/sbin/unix_chkpwd
/snap/snapd/24718/usr/lib/snapd/snap-confine
AZDINFARISSE@SVR-BASE-AZDINFARISSE: /var/log$ ps aux --sort=-%mem | head -n 15
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
mysql     14734  0.1  9.8 2311896 393916 ?        Ssl   Jul20   1:24 /usr/sbin/mysqld
AZDINF+   3200  0.2  7.1 4456664 287664 ?        Ssl   Jul20   3:31 /usr/bin/gnome-shell
AZDINF+   3372  0.0  4.6 1121920 188392 ?        Sl    Jul20   0:05 /usr/bin/gnome-software --gapplication-service
_rspamd   25662  0.0  3.8 603752 153436 ?        S     00:42   0:00 rspamd: hs_helper process
root      22834  0.0  3.5 188100 144176 ?        Ss    00:41   0:04 /usr/bin/perl -T -w -I /etc/perl -I /usr/lib/x86_64-linux-gnu/perl5/5.38 -I /usr/share/perl5 -I /usr/lib/x86_64-linux-gnu/perl-base -I /usr/lib/x86_64-linux-gnu/perl/5.38 -I /usr/share/perl/5.38 /usr/sbin/sp
amd --pidfile=/run/spamd.pid --create-prefs --max-children 5 --helper-home-dir
root      23630  0.0  3.3 188100 132856 ?        S     00:41   0:00 spamd child
root      23629  0.0  3.3 188100 132852 ?        S     00:41   0:00 spamd child
_rspamd   25253  0.0  2.7 604956 108340 ?        Ss    00:42   0:07 rspamd: main process
_rspamd   25660  0.0  2.5 606056 103344 ?        S     00:42   0:02 rspamd: controller process (localhost:11334)
_rspamd   25661  0.0  2.4 605388 96396 ?        S     00:42   0:01 rspamd: normal process (localhost:11333)
AZDINF+   3397  0.0  2.3 1005484 93184 ?        Sl    Jul20   0:00 /usr/libexec/evolution-data-server/evolution-alarm-notify
_rspamd   22659  0.0  2.2 603880 90008 ?        S     00:42   0:00 rspamd: rspamd_proxy process (localhost:11332)
root      32680  0.0  2.2 279780 90008 pts/26   T+    13:15   0:00 nmap -p 22,80,21,443,25,110,143 -sV 192.168.1.0/24
AZDINF+   30590  0.0  2.1 281196 85892 pts/0    T     10:33   0:01 /snap/nmap/3885/usr/bin/nmap -sV 192.168.1.0/24
AZDINFARISSE@SVR-BASE-AZDINFARISSE: /var/log$
```

Para últimos accesos:
lastlog

```
AZDINFARISSE@SVR-BASE-AZDINFARISSE: /var/log
File Edit View Search Terminal Help
list
irc **Never logged in**
apt **Never logged in**
nobody **Never logged in**
systemd-network **Never logged in**
systemd-timesync **Never logged in**
dhcpcd **Never logged in**
messagebus **Never logged in**
systemd-resolve **Never logged in**
pollinate **Never logged in**
polkitd **Never logged in**
syslog **Never logged in**
uuidd **Never logged in**
tcpdump **Never logged in**
tss **Never logged in**
landscape **Never logged in**
fwupd-refresh **Never logged in**
usbmux **Never logged in**
AZDINFARISSE pts/2 192.168.1.143 jue jun 19 09:40:20 +0200 2025
rtkit **Never logged in**
dnsmasq **Never logged in**
whoopsie **Never logged in**
avahi **Never logged in**
saned **Never logged in**
```

3. Simulación de riesgos internos.

Para identificar vectores de ataque internos, utilizamos el comando:
sudo nmap -sS 192.168.1.0/24

```
AZDINFARISSE@SVR-BASE-AZDINFARISSE: ~
File Edit View Search Terminal Help
AZDINFARISSE@SVR-BASE-AZDINFARISSE:~$ sudo nmap -sS 192.168.1.0/24
[sudo] password for AZDINFARISSE:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-22 07:55 CEST
Nmap scan report for gateway (192.168.1.1)
Host is up (0.00053s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    filtered ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
MAC Address: D8:E8:44:B1:96:60 (zte)

Nmap scan report for 192.168.1.129
Host is up (0.0012s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    filtered ssh
MAC Address: 00:23:C1:3A:FF:2B (Securitas Direct AB)

Nmap scan report for 192.168.1.131
Host is up (0.0017s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
```

- **1. Host: 192.168.1.1**
 - Servicio HTTP sin cifrado expuesto.
 - Riesgo: posible acceso no seguro a la interfaz de administración.
- **2. Host: 192.168.1.132**
 - SSH abierto, posible objetivo de fuerza bruta.
 - HTTP sin cifrado.
- **3. Host: 192.168.1.141**
 - Múltiples puertos altos abiertos (7000, 8001, etc).

- Requiere análisis más profundo (posibles aplicaciones web vulnerables).

- **4. Host: 192.168.1.152**

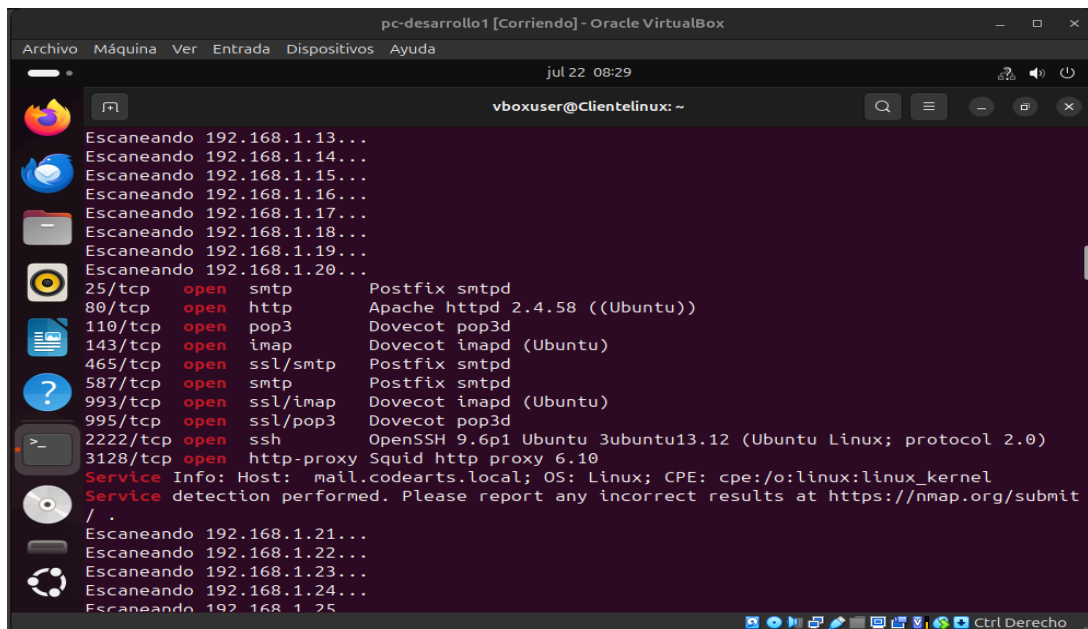
- SOCKS proxy abierto: posible túnel de datos.
- Sun Answerbook: vulnerabilidad conocida.

- **5. Host: 192.168.1.20 (servidor)**

- POP3 e IMAP sin cifrado.
- Riesgo de exposición de credenciales si no está correctamente protegido.

Ahora simulamos la ejecución de un script de escaneo tipo atacante desde el equipo de desarrollo1. Lo hacemos con:

```
for ip in $(seq 1 254); do
  echo "Escaneando 192.168.1.$ip..."
  nmap -sV -T4 192.168.1.$ip | grep -E "open|Service"
done
```



```
pc-desarrollo1 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
jul 22 08:29
vboxuser@Clientlinux: ~
Escaneando 192.168.1.13...
Escaneando 192.168.1.14...
Escaneando 192.168.1.15...
Escaneando 192.168.1.16...
Escaneando 192.168.1.17...
Escaneando 192.168.1.18...
Escaneando 192.168.1.19...
Escaneando 192.168.1.20...
25/tcp open smtp Postfix smtpd
80/tcp open http Apache httpd 2.4.58 ((Ubuntu))
110/tcp open pop3 Dovecot pop3d
143/tcp open imap Dovecot imapd (Ubuntu)
465/tcp open ssl/smtp Postfix smtpd
587/tcp open smtp Postfix smtpd
993/tcp open ssl/imap Dovecot imapd (Ubuntu)
995/tcp open ssl/pop3 Dovecot pop3d
2222/tcp open ssh OpenSSH 9.6p1 Ubuntu 3ubuntu13.12 (Ubuntu Linux; protocol 2.0)
3128/tcp open http-proxy Squid http proxy 6.10
Service Info: Host: mail.codearts.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Escaneando 192.168.1.21...
Escaneando 192.168.1.22...
Escaneando 192.168.1.23...
Escaneando 192.168.1.24...
Escaneando 192.168.1.25...
```

Ahora registramos qué información puede obtener un usuario no privilegiado en la red:

- **Listar dispositivos en red:**

`arp -a`

- **Escaneo de puertos básicos:**

`nmap 192.168.1.0/24`

- **Ver archivos compartidos en red:**

`smbclient -L //IP_DEL_SERVIDOR/ -N`

- **Leer banners de servicios abiertos:**

`nc IP_DEL_SERVIDOR 21 # FTP`

`nc IP_DEL_SERVIDOR 25 # SMTP`

4. Propuestas técnicas de mejora.

- **Tabla de vulnerabilidades detectadas, criticidad y solución:**

IP/Host	Vulnerabilidad	Criticidad	Solución recomendada
192.168.1.1	HTTP sin cifrado (puerto 80)	Media	Redirigir a HTTPS o cerrar servicio si no es necesario.
192.168.1.132	SSH abierto (puerto 22)	Alta	Restringir por firewall y usar solo autenticación por clave pública.
192.168.1.133	Puerto IRC 6668 abierto	Alta	Cerrar puerto si no es usado; posible canal C&C malicioso.
192.168.1.141	Puertos altos (8080, 9999, etc.) abiertos	Alta	Analizar servicios, cerrar si no son esenciales o aplicar autenticación.
192.168.1.152	Proxy SOCKS (1080), sun-answerbook (8888)	Alta	Desactivar servicios obsoletos, actualizar firmware/software del dispositivo.
192.168.1.20 (servidor)	POP3/IMAP sin cifrado (110, 143)	Alta	Forzar uso de IMAPS/POP3S, cerrar versiones inseguras.
192.168.1.20	Múltiples puertos abiertos innecesarios	Media	Desactivar servicios no utilizados.

- **Propuesta de segmentación de red:**

Objetivo: Limitar el acceso entre dispositivos para que un atacante en una subred no pueda moverse lateralmente.

Subred	Descripción	Rango IP sugerido
192.168.1.0/26	Administración/Servidores	192.168.1.0 – 192.168.1.63
192.168.1.64/26	Equipos de empleados	192.168.1.64 – 192.168.1.127
192.168.1.128/26	IoT / Dispositivos inseguros	192.168.1.128 – 192.168.1.191
192.168.1.192/26	Invitados / redes abiertas	192.168.1.192 – 192.168.1.255

Recomendación: aplicar VLANs o reglas de firewall que:

- ❖ Bloqueen acceso entre subredes (excepto desde administración).
- ❖ Impidan conexiones directas desde IoT a servidores.
- ❖ Reduzcan la visibilidad de red interna.

- **Bastionado, cierre de servicios y políticas de logs:**

Bastionado de servidores

- Deshabilitar servicios innecesarios (como POP3 sin cifrado, HTTP, IRC).
- Instalar solo paquetes mínimos necesarios.
- Usar `ufw` o `iptables` para limitar puertos.
- Forzar SSH por clave pública, deshabilitar root remoto.

Políticas de logs y monitorización

- Activar `auditd` para seguimiento de eventos críticos.
- Habilitar logs detallados de autenticación (`/var/log/auth.log`).
- Configurar `rsyslog` para envío centralizado de logs (si hay más de un servidor).
- Revisar accesos sospechosos con `last`, `journalctl`, etc.