2025

MAQUINA DEBIAN

EMMANUEL IZAGUIRRE RUIZ

Introducción

Se mostrara el paso a paso de una maquina debian comprometida desde su encendiso, actualizaciones de programas etc etc.

Verificación del estado inicial

Encendemos la maquina debian , usuario: debian , contraseña: 123456.

Para revisar el estado inicial de la maquina después del arranque

Uname -a

```
lebian@debian:~$ uname -a
.inux debian 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26)
 x86_64 GNU/Linux
```

Esto nos muestra versión de la maquina, nombre el host, sistema operativo, arquitectura del sistema, nombre del sistema operativo.

actualización de los repositorios del software.

Sudo apt update

```
Get:12 http://deb.debian.org/debian bookworm-updates/main Translation-en T-2025-
01-14-2009.05-F-2024-11-27-1405.46.pdiff [14.8 kB]
Get:13 http://deb.debian.org/debian bookworm/non-free-firmware Sources [6,436 B]
Get:14 http://deb.debian.org/debian bookworm/main amd64 Packages [8,792 kB]
Get:15 http://deb.debian.org/debian bookworm/main Translation-en [6,109 kB]
Get:16 http://deb.debian.org/debian bookworm/non-free-firmware amd64 Packages [6
,240 B]
Get:17 http://deb.debian.org/debian bookworm-updates/main Sources [16.2 kB]
Fetched 25.3 MB in 4s (6,386 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
149 packages can be upgraded. Run 'apt list --upgradable' to see them.
N: Repository 'http://deb.debian.org/debian bookworm InRelease' changed its 'Ver
sion' value from '12.7' to '12.9'
debian@debian:~$
```

Se actualiza la lista de paquetes disponibles en los repsositorios configurados en el sistema.

Instalando actualización de seguridad.

Sudo apt-get dist-upgrade

```
rsync.service is a disabled or a static unit not running, not starting it.
Setting up espeak-ng-data:amd64 (1.51+dfsg-10+deb12u2) ...
Setting up libsynctex2:amd64 (2022.20220321.62855-5.1+deb12u2) ...
Setting up apache2-utils (2.4.62-1~deb12u2) ...
Setting up python3.11-minimal (3.11.2-6+deb12u5) ...
Setting up libgs10-common (10.0.0~dfsg-11+deb12u6) ...
Setting up gtk-update-icon-cache (3.24.38-2~deb12u3) ...
Setting up openssh-sftp-server (1:9.2p1-2+deb12u5) ...
Setting up gir1.2-gstreamer-1.0:amd64 (1.22.0-2+deb12u1) ...
Setting up php8.2-common (8.2.26-1~deb12u1) ...
Setting up php8.2-mysql (8.2.26-1~deb12u1) ...
Setting up libsoup2.4-1:amd64 (2.74.3-1+deb12u1) ...
Setting up openssh-server (1:9.2p1-2+deb12u5) ...
Configuring openssh-server
--------------------------

A new version (/tmp/tmp.CTIo1Wfnd5) of configuration file /etc/ssh/sshd_config
is available, but the version installed currently has been locally modified.
```

Con este comando se actualizan los paquetes instalados a sus versiones mas recientes. Así como eliminar los paquetes obsoletos si es necesarios.

actualizaciones aplicadas.

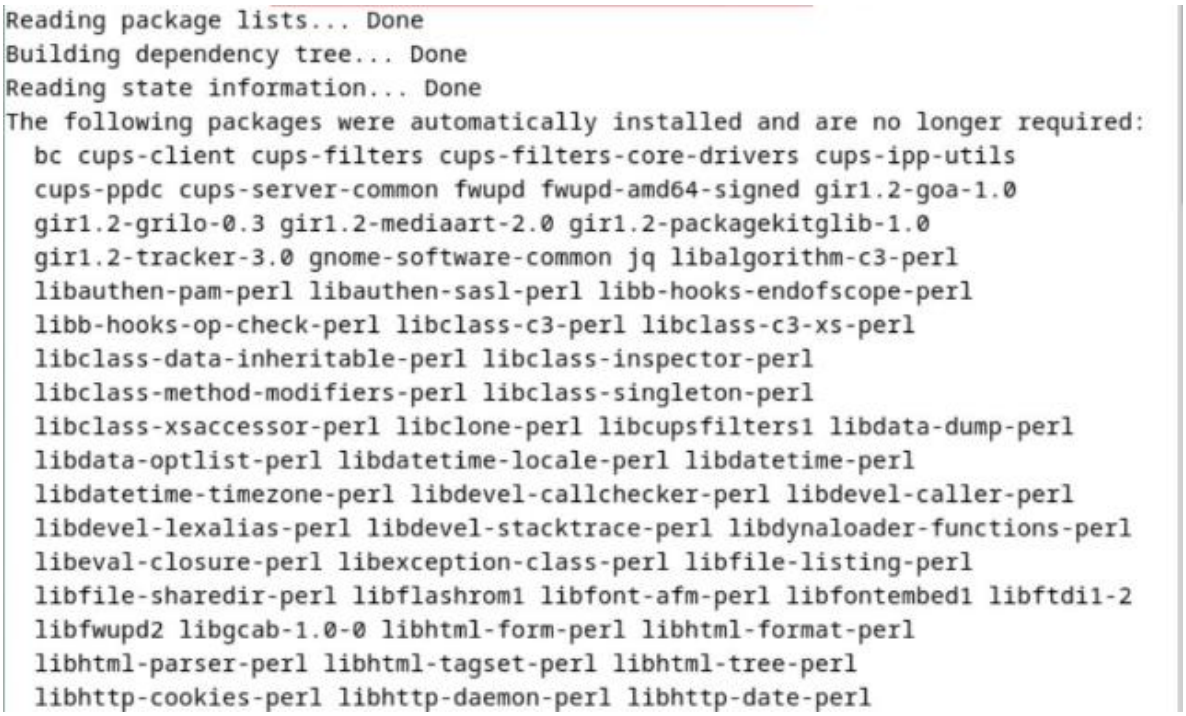
Grep “upgrade” /var/log/dpkg.log

```
7-1+deb12u6
2025-02-22 20:07:11 upgrade libreoffice-common:all 4:7.4.7-1+deb12u5 4:7.4.7-1+d
eb12u6
2025-02-22 20:07:13 upgrade libreoffice-help-en-us:all 4:7.4.7-1+deb12u5 4:7.4.7
-1+deb12u6
2025-02-22 20:07:15 upgrade libreoffice-style-colibre:all 4:7.4.7-1+deb12u5 4:7.
4.7-1+deb12u6
2025-02-22 20:07:15 upgrade libsrt1.5-gnutls:amd64 1.5.1-1 1.5.1-1+deb12u1
2025-02-22 20:07:16 upgrade libsynctex2:amd64 2022.20220321.62855-5.1+deb12u1 20
22.20220321.62855-5.1+deb12u2
2025-02-22 20:07:40 upgrade linux-image-amd64:amd64 6.1.106-3 6.1.128-1
2025-02-22 20:07:41 upgrade openssl:amd64 3.0.14-1~deb12u2 3.0.15-1~deb12u1
2025-02-22 20:07:42 upgrade php8.2:all 8.2.20-1~deb12u1 8.2.26-1~deb12u1
2025-02-22 20:07:42 upgrade python3-pkg-resources:all 66.1.1-1 66.1.1-1+deb12u1
2025-02-22 20:07:43 upgrade python3-urllib3:all 1.26.12-1 1.26.12-1+deb12u1
2025-02-22 20:07:43 upgrade util-linux-locales:all 2.38.1-5+deb12u1 2.38.1-5+deb
12u3
```

Nos poermite ver el historial de paquetes que han sido actualizados en el sistema.

Verificación de actualizaciones de seguridad especificas.

Sudo apt install unattended-upgrades



Con este comando podemos visualizar el estado de las actualizaciones de seguridad de la maquina.

Estado de los servicios

Sudo systemclt status (nombre del servicio) ejemplo apache2.

```
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enab
     Active: active (running) since Fri 2025-02-14 21:14:40 EST; 1 week 2 days
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 653 (apache2)
      Tasks: 6 (limit: 2284)
     Memory: 15.0M
        CPU: 10.958s
     CGroup: /system.slice/apache2.service
             ├─  653 /usr/sbin/apache2 -k start
             ├─15691 /usr/sbin/apache2 -k start
             ├─15692 /usr/sbin/apache2 -k start
             ├─15693 /usr/sbin/apache2 -k start
             ├─15694 /usr/sbin/apache2 -k start
             └─15696 /usr/sbin/apache2 -k start

Feb 14 21:14:40 debian systemd[1]: Starting apache2.service - The Apache HTTP S
Feb 14 21:14:40 debian systemd[1]: Started apache2.service - The Apache HTTP Se
Feb 19 21:56:10 debian systemd[1]: Reloading apache2.service - The Apache HTTP
Feb 19 21:56:11 debian systemd[1]: Reloaded apache2.service - The Apache HTTP S
Feb 21 22:08:44 debian systemd[1]: Reloading apache2.service - The Apache HTTP
Feb 21 22:08:45 debian systemd[1]: Reloaded apache2.service - The Apache HTTP S
Feb 22 00:00:11 debian systemd[1]: Reloading apache2.service - The Apache HTTP
```

Con este comando podemos visualizar el estado del servicio del que queramos revisar. En este ejemplo se visualiza el estado del servficio de apache2

Manteni

```
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enab
     Active: active (running) since Fri 2025-02-14 21:14:40 EST; 1 week 2 days
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 653 (apache2)
      Tasks: 6 (limit: 2284)
     Memory: 15.0M
        CPU: 10.958s
     CGroup: /system.slice/apache2.service
             ├─  653 /usr/sbin/apache2 -k start
             ├─15691 /usr/sbin/apache2 -k start
             ├─15692 /usr/sbin/apache2 -k start
             ├─15693 /usr/sbin/apache2 -k start
             ├─15694 /usr/sbin/apache2 -k start
             └─15696 /usr/sbin/apache2 -k start

Feb 14 21:14:40 debian systemd[1]: Starting apache2.service - The Apache HTTP S
Feb 14 21:14:40 debian systemd[1]: Started apache2.service - The Apache HTTP Se
Feb 19 21:56:10 debian systemd[1]: Reloading apache2.service - The Apache HTTP
Feb 19 21:56:11 debian systemd[1]: Reloaded apache2.service - The Apache HTTP S
Feb 21 22:08:44 debian systemd[1]: Reloading apache2.service - The Apache HTTP
Feb 21 22:08:45 debian systemd[1]: Reloaded apache2.service - The Apache HTTP S
Feb 22 00:00:11 debian systemd[1]: Reloading apache2.service - The Apache HTTP
```

Mantenimiento general de la maquina

Primero para eliminar los paquetes obsoletos ejecutamos el comando

Sudo apt autoremove

Sudo apt clean

Verificación del disco

df -h

```
debian@debian:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            952M     0  952M   0% /dev
tmpfs           197M  1.1M  196M   1% /run
/dev/sda1        29G  7.1G   21G  26% /
tmpfs           984M     0  984M   0% /dev/shm
tmpfs           5.0M  8.0K  5.0M   1% /run/lock
tmpfs           197M  1.4M  196M   1% /run/user/1000
```

Con este comando podemos saber el uso del disco , así como diagnosticar problemas de almacenamiento , evitar que el sistema se quede son espacio y falle.

Comprobar los logs

Sudo jornalctl -xe

```
 Support: https://www.debian.org/support

 A start job for unit phpsessionclean.service has finished successfully.

 The job identifier is 8665.
eb 24 13:40:53 debian sudo[48861]:   debian : TTY=pts/3 ; PWD=/home/debian ; USER=root ; COMMAND
eb 24 13:40:53 debian sudo[48861]: pam_unix(sudo:session): session opened for user root(uid=0) b
eb 24 13:40:53 debian sudo[48861]: pam_unix(sudo:session): session closed for user root
eb 24 13:41:10 debian sudo[48880]:   debian : TTY=pts/3 ; PWD=/home/debian ; USER=root ; COMMAND
eb 24 13:41:10 debian sudo[48880]: pam_unix(sudo:session): session opened for user root(uid=0) b
eb 24 13:41:10 debian sudo[48880]: pam_unix(sudo:session): session closed for user root
eb 24 13:41:44 debian anacron[48634]: Job `cron.daily' started
eb 24 13:41:44 debian anacron[48963]: Updated timestamp for job `cron.daily' to 2025-02-24
eb 24 13:41:44 debian anacron[48634]: Job `cron.daily' terminated
eb 24 13:41:44 debian anacron[48634]: Normal exit (1 job run)
eb 24 13:41:44 debian systemd[1]: anacron.service: Deactivated successfully.
 Subject: Unit succeeded
 Defined-By: systemd
 Support: https://www.debian.org/support

 The unit anacron.service has successfully entered the 'dead' state.
eb 24 13:50:14 debian sudo[49056]:   debian : TTY=pts/3 ; PWD=/home/debian ; USER=root ; COMMAND
eb 24 13:50:14 debian sudo[49056]: pam_unix(sudo:session): session opened for user root(uid=0) b
ines 1990-2012/2012 (END)
```

Escaneo de vulnerabilidad y seguridad

Sudo ss -tuln

```
debian@debian:/$ sudo ss -tuln
Netid State  Recv-Q Send-Q                    Local Address:Port  Peer Address:
Port                                  Process
udp   UNCONN 0      0                            0.0.0.0:45145      0.0.0.0:
*
udp   UNCONN 0      0                            0.0.0.0:5353       0.0.0.0:
*
udp   UNCONN 0      0                               [::]:5353          [::]:
*
udp   UNCONN 0      0      [fe80::a00:27ff:fe8c:9ec2]%enp0s3:546          [::]:
*
udp   UNCONN 0      0                               [::]:49755         [::]:
*
tcp   LISTEN 0      128                        127.0.0.1:631        0.0.0.0:
*
tcp   LISTEN 0      80                         127.0.0.1:3306       0.0.0.0:
*
tcp   LISTEN 0      128                          0.0.0.0:22         0.0.0.0:
*
tcp   LISTEN 0      128                             [::1]:631          [::]:
*
tcp   LISTEN 0      511                                *:80               *:
```

Este comando nos muestra la lista de sockets abiertos en el sistema.

Recuperación y Aseguramiento de una Máquina Debian Comprometida

Introducción

Una máquina Debian comprometida puede presentar signos como:

- Ralentización inusual.
- Servicios que se comportan de forma errónea.
- Conexiones sospechosas en el sistema.

Este proceso consta de cuatro fases principales:

- **Análisis Forense Inicial**
- **Contención del Ataque**
- **Recuperación del Sistema**
- **Aseguramiento del Sistema**

Análisis Forense Inicial

Identificación del ataque

Verificar conexiones sospechosas

```
netstat -antup | grep ESTABLISHED
```

Muestra todas las conexiones activas con detalles de puertos, IP y procesos involucrados. El filtro grep ESTABLISHED destaca conexiones establecidas que pueden indicar actividad sospechosa.

```
debian@debian:~$ netstat -antup | grep ESTABLISHED
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 192.168.100.26:50036    192.178.56.170:443      ESTABLISHED
1424/firefox-esr
tcp        0      0 192.168.100.26:56056    34.107.243.93:443       ESTABLISHED
1424/firefox-esr
tcp        0      0 192.168.100.26:49138    142.251.34.35:443       ESTABLISHED
1424/firefox-esr
tcp6       0      0 2806:261:485:ab9::57994 2606:4700:4400::ac4:443 ESTABLISHED
1424/firefox-esr
tcp6       0      0 2806:261:485:ab9::57224 2606:4700:4400::681:443 ESTABLISHED
1424/firefox-esr
udp        0      0 192.168.100.26:68       192.168.100.1:67        ESTABLISHED
-
debian@debian:~$
```

ss -tuln

Lista puertos en uso mostrando los estados de escucha y conexión activa, ideal para detectar servicios inesperados.

```
debian@debian:~$ ss -tuln
Netid State  Recv-Q Send-Q                    Local Address:Port  Peer Address:
Port                                  Process
udp   UNCONN 0      0                             0.0.0.0:5353       0.0.0.0:
*
udp   UNCONN 0      0                             0.0.0.0:35129      0.0.0.0:
*
udp   UNCONN 0      0                                [::]:43847         [::]:
*
udp   UNCONN 0      0                                [::]:5353          [::]:
*
udp   UNCONN 0      0      [fe80::a00:27ff:fe8c:9ec2]%enp0s3:546           [::]:
*
tcp   LISTEN 0      128                           0.0.0.0:22         0.0.0.0:
*
tcp   LISTEN 0      80                          127.0.0.1:3306       0.0.0.0:
*
tcp   LISTEN 0      128                         127.0.0.1:631        0.0.0.0:
*
tcp   LISTEN 0      511                              *:80               *:
*
tcp   LISTEN 0      32                               *:21               *:
*
tcp   LISTEN 0      128                              [::]:22            [::]:
```

Revisar procesos activos

ps aux --sort=-%cpu

Muestra los procesos activos ordenados por el mayor consumo de CPU. Esto ayuda a identificar posibles procesos maliciosos consumiendo recursos.

```
debian@debian:~$ ps aux --sort=-%cpu
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
debian      2952  3.9 11.5 2620852 232124 ?      Sl   15:43   0:26 /usr/lib/fire
debian       985  3.2  0.6 1441008 14012 ?       S<sl 14:54   1:57 /usr/bin/puls
debian      1424  2.6 16.4 11654460 331656 ?     Sl   14:54   1:37 /usr/lib/fire
root         635  1.3  4.0 493748 82120 tty7     Ssl+ 14:53   0:48 /usr/lib/xorg
debian      1791  0.4 17.3 2824268 350236 ?      Sl   14:54   0:17 /usr/lib/fire
debian      3384  0.3  2.4 558836 49776 ?        Sl   15:52   0:00 mate-terminal
debian      1677  0.3  7.7 2626516 155828 ?      Sl   14:54   0:11 /usr/lib/fire
debian      1606  0.2  5.9 2594004 120160 ?      Sl   14:54   0:09 /usr/lib/fire
debian      1680  0.2  7.7 2617012 156992 ?      Sl   14:54   0:09 /usr/lib/fire
debian      1161  0.2  2.6 393016 54096 ?        Sl   14:54   0:08 /usr/bin/pyth
debian      1386  0.1  0.5 730636 10096 ?        Ssl  14:54   0:04 /usr/bin/spee
mysql        683  0.0  3.1 1349372 63108 ?       Ssl  14:53   0:02 /usr/sbin/mar
debian      1564  0.0  4.7 2456324 96140 ?       Sl   14:54   0:02 /usr/lib/fire
debian      3563  0.0  3.5 2407896 71552 ?       Sl   15:53   0:00 /usr/lib/fire
debian      1518  0.0  3.7 2442828 74588 ?       Sl   14:54   0:01 /usr/lib/fire
root          43  0.0  0.0      0     0 ?        S    14:53   0:01 [kswapd0]
debian      1085  0.0  1.2 469436 25740 ?        Sl   14:54   0:01 marco
debian      1055  0.0  0.1   9516  3420 ?        S    14:54   0:01 /usr/bin/dbus
debian      3335  0.0  3.5 2407880 72028 ?       Sl   15:51   0:00 /usr/lib/fire
debian      3488  0.0  3.5 2407880 71516 ?       Sl   15:53   0:00 /usr/lib/fire
```

Proporciona una interfaz interactiva para monitorear en tiempo real el uso de recursos del sistema.

Identificar archivos recientemente modificados

find / -mtime -1 2>/dev/null

Busca archivos modificados en las últimas 24 horas, permitiendo detectar alteraciones sospechosas.

```
/var/log/Xorg.0.log
/var/log/lightdm
/var/log/journal/41b6de202c3f48fdaa490411748aaaff
/var/log/journal/41b6de202c3f48fdaa490411748aaaff/system.journal
/var/log/journal/41b6de202c3f48fdaa490411748aaaff/user-1000@ce3b2225985f4da8809f
607d89aa2a80-00000000000054c4-000630661546a638.journal
/var/log/journal/41b6de202c3f48fdaa490411748aaaff/system@a48b40a584d44a45941503e
a72502321-00000000000050e3-0006306614945a93.journal
/var/log/journal/41b6de202c3f48fdaa490411748aaaff/user-1000.journal
/var/log/cups/access_log
/var/tmp
/var/tmp/systemd-private-8d978716587b4841be389abb076fd631-apache2.service-A8C9Cf
/var/tmp/systemd-private-8d978716587b4841be389abb076fd631-ModemManager.service-W
erK9Y
/var/tmp/systemd-private-8d978716587b4841be389abb076fd631-upower.service-owgUZm
/var/tmp/systemd-private-8d978716587b4841be389abb076fd631-systemd-logind.service
-2rCv9R
/var/tmp/systemd-private-8d978716587b4841be389abb076fd631-systemd-timesyncd.serv
ice-FfDRJb
/etc
/etc/cups
/etc/cups/subscriptions.conf
/etc/resolv.conf
```

Verificar intentos de acceso fallidos

grep 'Failed password' /var/log/auth.log

Permite identificar intentos de inicio de sesión fallidos, ideal para detectar intentos de fuerza bruta.

Identificar usuarios sospechosos

cat /etc/passwd | tail

```
debian@debian:~$ cat /etc/passwd | tail
pulse:x:106:114:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:x:107:117::/var/lib/saned:/usr/sbin/nologin
lightdm:x:108:118:Light Display Manager:/var/lib/lightdm:/bin/false
polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin
rtkit:x:109:119:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:110:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/no
login
debian:x:1000:1000:4geeks,,,:/home/debian:/bin/bash
mysql:x:111:121:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
ftp:x:113:122:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
```

Muestra las últimas entradas del archivo /etc/passwd, donde se almacenan cuentas de usuario. Cuentas recientes y sospechosas pueden ser un indicio de ataque.

Contención del Ataque

Aislamiento de la máquina

Bloquear direcciones IP sospechosas

iptables -A INPUT -s <IP_Sospechosa> -j DROP

```
iptables -A INPUT -s <IP_Sospechosa> -j DROP
```

Esta regla bloquea el tráfico entrante desde una IP específica, cortando el acceso del atacante.

Desactivar servicios sospechosos

systemctl stop <servicio>

Detiene de inmediato un servicio sospechoso para prevenir que continúe ejecutándose.

systemctl disable <servicio>

Desactiva el servicio para que no se inicie automáticamente al reiniciar el sistema.

Eliminar cuentas no autorizadas

userdel -r <usuario_sospechoso>

Elimina el usuario y su directorio personal. Esto impide que un atacante recupere acceso mediante esta cuenta.

Verificar puertos abiertos

Escanea los puertos locales para detectar servicios abiertos que pueden estar siendo explotados.

Recuperación del Sistema

Restaurar archivos y configuraciones

Restaurar archivos desde una copia de seguridad

rsync -av /ruta/respaldo /ruta/destino

Copia archivos y directorios de forma recursiva, preservando permisos y fechas de modificación.

Reinstalar paquetes comprometidos

apt-get install --reinstall <paquete>

Reinstala un paquete sospechoso asegurando que sus archivos estén limpios y en su estado original.

Verificar la integridad de archivos críticos

dpkg –verify

```
dpkg --verify
```

```
missing     /var/lib/polkit-1/localauthority/30-site.d (Permission denied)
missing     /var/lib/polkit-1/localauthority/50-local.d (Permission denied)
missing     /var/lib/polkit-1/localauthority/90-mandatory.d (Permission denied)
??5?????? c /etc/apache2/apache2.conf
??5?????? c /etc/apache2/sites-available/000-default.conf
missing     /usr/share/polkit-1/rules.d/systemd-networkd.rules (Permission denied)
missing     /usr/share/polkit-1/rules.d/org.freedesktop.NetworkManager.rules (Permis
sion denied)
missing     /var/lib/polkit-1/localauthority (Permission denied)
missing     /var/lib/polkit-1/localauthority/10-vendor.d (Permission denied)
missing     /var/lib/polkit-1/localauthority/10-vendor.d/org.freedesktop.NetworkMana
ger.pkla (Permission denied)
missing     /usr/lib/mysql/plugin/auth_pam_tool_dir/auth_pam_tool (Permission denied
)
missing     /usr/share/polkit-1/rules.d/org.gtk.vfs.file-operations.rules (Permissio
n denied)
missing     /var/cache/cups/rss (Permission denied)
missing     /var/spool/cups/tmp (Permission denied)
????????? c /etc/sudoers
????????? c /etc/sudoers.d/README
??5?????? c /etc/vsftpd.conf
?????????   /usr/lib/cups/backend/cups-brf
missing     /usr/share/polkit-1/rules.d/50-default.rules (Permission denied)
??5?????? c /etc/default/espeakup
```

Compara los archivos de los paquetes instalados con los valores de referencia del sistema, alertando sobre modificaciones.

Aseguramiento del Sistema

Actualización y endurecimiento

apt-get update && apt-get upgrade

```
Get:1 http://deb.debian.org/debian bookworm InRelease [151 kB]
Get:2 http://security.debian.org/debian-security bookworm-security InRelease [48.0
B]
Get:3 http://deb.debian.org/debian bookworm-updates InRelease [55.4 kB]
Get:4 http://security.debian.org/debian-security bookworm-security/main Sources [14
 kB]
Get:5 http://security.debian.org/debian-security bookworm-security/main amd64 Packa
es [247 kB]
Get:6 http://security.debian.org/debian-security bookworm-security/main Translation
en [147 kB]
Get:7 http://deb.debian.org/debian bookworm/main Sources [9,495 kB]
Get:8 http://deb.debian.org/debian bookworm/non-free-firmware Sources [6,440 B]
Get:9 http://deb.debian.org/debian bookworm/main amd64 Packages [8,792 kB]
Get:10 http://deb.debian.org/debian bookworm/main Translation-en [6,109 kB]
Get:11 http://deb.debian.org/debian bookworm/non-free-firmware amd64 Packages [6,24
 B]
Fetched 25.2 MB in 3s (7,960 kB/s)
Reading package lists... Done
N: Repository 'http://deb.debian.org/debian bookworm InRelease' changed its 'Versio
' value from '12.9' to '12.10'
E: Could not open lock file /var/lib/dpkg/lock-frontend - open (13: Permission deni
d)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), are you
oot?
```

Descarga la lista de paquetes actualizados y los instala, corrigiendo vulnerabilidades conocidas.

Estas reglas bloquean el tráfico entrante por defecto, permitiendo solo el tráfico saliente y las conexiones SSH seguras.

Configurar auditoría del sistema

auditctl -a exit,always -F arch=b64 -S execve

Habilita la auditoría del sistema para registrar cada vez que se ejecuta un proceso, facilitando la detección de actividades sospechosas.

Conclusión

- Documentar todo el proceso de respuesta.
- Implementar políticas de contraseñas robustas.
- Realizar copias de seguridad periódicas.
- Capacitar al personal en buenas prácticas de seguridad.