

PROYECTO FINAL DE CIBERSEGURIDAD

Análisis forense y endurecimiento de un servidor Linux (Debian) ante un incidente de seguridad



Alumno:

Felipe Torrado Dias

Curso:

[Ciberseguridad/ Bootcamp / 4geeks]

Profesor:

[Alejandro Garabito]

Fecha:

[08/01/2026]

Fase 1 - Reconocimiento y recolección de evidencias	2
1. Identificación de los servicios comprometidos y método de acceso del atacante	2
1.1 Análisis forense del acceso por SSH (puerto 22)	3
1.2 Correlación de actividad y alcance inicial del atacante	4
1.3 Búsqueda de persistencia y acciones post-explotación	6
2. Identificación de archivos sospechosos, procesos en ejecución y modificaciones inusuales	7
Punto 3 – Escaneo del servidor para detectar rootkits o malware	8
4. Bloqueo del exploit y prevención de escalación	10
Punto 5 – Reversión de cambios realizados por el atacante	11
6. Actualización y corrección de configuraciones de seguridad	12
6.2 Revisión de cuentas y credenciales en la base de datos MariaDB	13
6.2 Revisión de cuentas y credenciales en la base de datos MariaDB	14
Punto 7 – Informe final y recomendaciones	15
Fase 2.1: Servicio FTP	15
1. Escaneo completo del sistema con Nmap	15
2 – Vulnerabilidad detectada (FTP)	16
3 – Proceso de validación de la vulnerabilidad	17
4 – Corrección y mitigación de la vulnerabilidad FTP	18
5 – Conclusión de la Fase 2.1	18
Fase 2.2: Servicio Apache (HTTP/80)	18
1) Detección y validación del servicio	18
2) Impacto (por qué esto es una debilidad)	19
3) Medidas correctivas aplicadas (hardening)	19
4) Conclusión	20
Fase 3: Plan de respuesta a incidentes y Sistema de Gestión de Seguridad de la Información (SGSI)	21
Objetivo de la Fase 3	21
3.1 Justificación del Plan de Respuesta y del SGSI	21
3.2 Plan de Respuesta a Incidentes basado en NIST SP 800-61	22
3.3 Sistema de Gestión de Seguridad de la Información (SGSI) según ISO 27001	23
Alcance del SGSI	23
3.5 Conclusión de la Fase 3	24

El análisis se realizó sobre una máquina virtual con sistema **operativo Debian** (entorno de laboratorio), destinada a prácticas de ciberseguridad. La verificación de conectividad y servicios se efectuó en modo local y/o red interna.

Para el reconocimiento y la validación se emplearon herramientas de administración y diagnóstico habituales en Linux (por ejemplo: **Nmap** para enumeración de puertos/servicios, journalctl para **revisión de logs**, ss para puertos en escucha y curl para verificación HTTP).

El alcance del trabajo se limitó a identificar el vector de entrada del incidente (SSH), analizar evidencias disponibles (logs y configuración), y aplicar medidas correctivas para reducir superficie de ataque en servicios expuestos (FTP/Apache), documentando pruebas antes y después de las correcciones.

Fase 1 - Reconocimiento y recolección de evidencias

1. Identificación de los servicios comprometidos y método de acceso del atacante

El primer paso consistió en **determinar qué servicio permitió la entrada** del atacante al servidor. Para ello se revisaron los registros del servicio SSH utilizando comandos como **journalctl -u ssh** y filtros específicos para accesos exitosos, por ejemplo journalctl --no-pager | grep -E "Accepted password".

En estos registros **se identificó un evento clave**: un acceso **exitoso al usuario root**, proveniente de la dirección **IP 192.168.0.134**, mediante autenticación por contraseña. Este hallazgo confirmó que el atacante no explotó una vulnerabilidad técnica compleja, sino que logró autenticarse exitosamente porque la configuración de SSH permitía el acceso directo de root. La comprobación del **archivo /etc/ssh/sshd_config** reveló que la opción **PermitRootLogin estaba habilitada**, lo que facilitó este tipo de ataque. Por lo tanto, se determinó que el servicio comprometido fue SSH, específicamente por acceso directo al

usuario root utilizando contraseña.

```
debian@debian:~$ sudo journalctl _COMM=sshd | tail -n 50
Sep 30 12:25:16 debian sshd[51422]: Server listening on 0.0.0.0 port 22.
Sep 30 12:25:16 debian sshd[51422]: Server listening on :: port 22.
Sep 30 12:27:50 debian sshd[51422]: Received signal 15; terminating.
-- Boot 46ff5cf6df3d4f0e86b315592aab2d0 --
Sep 30 15:09:51 debian sshd[560]: Server listening on 0.0.0.0 port 22.
Sep 30 15:09:51 debian sshd[560]: Server listening on :: port 22.
Oct 08 16:14:16 debian sshd[560]: Received signal 15; terminating.
Oct 08 16:14:16 debian sshd[5341]: Server listening on 0.0.0.0 port 22.
Oct 08 16:14:16 debian sshd[5341]: Server listening on :: port 22.
-- Boot 342683d8f35244b08c4f3863f2978eca --
Oct 08 16:43:18 debian sshd[543]: Server listening on 0.0.0.0 port 22.
Oct 08 16:43:18 debian sshd[543]: Server listening on :: port 22.
-- Boot d28e179bf5884b25bf94452c79fd0afa --
Oct 08 16:48:02 debian sshd[555]: Server listening on 0.0.0.0 port 22.
Oct 08 16:48:02 debian sshd[555]: Server listening on :: port 22.
-- Boot af0a79f76920440c8e08594d6547449b --
Oct 08 17:28:38 debian sshd[550]: Server listening on 0.0.0.0 port 22.
Oct 08 17:28:38 debian sshd[550]: Server listening on :: port 22.
Oct 08 17:40:59 debian sshd[1650]: Accepted password for root from 192.168.0.134 port 45623 ssh2
Oct 08 17:40:59 debian sshd[1650]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Oct 08 17:40:59 debian sshd[1650]: pam_env(sshd:session): deprecated reading of user environment enabled
-- Boot 239b8e4c205b424eb8cf328c9117fa0d --
Dec 01 13:27:02 debian sshd[595]: Server listening on 0.0.0.0 port 22.
Dec 01 13:27:02 debian sshd[595]: Server listening on :: port 22.
-- Boot 21f9a10593314076a02a41713af14bad --
Dec 01 13:42:05 debian sshd[570]: Server listening on 0.0.0.0 port 22.
Dec 01 13:42:05 debian sshd[570]: Server listening on :: port 22.
-- Boot 88a5da2a97454ef580e139a1059aed58 --
Dec 03 13:15:01 debian sshd[571]: Server listening on 0.0.0.0 port 22.
Dec 03 13:15:01 debian sshd[571]: Server listening on :: port 22.
Dec 03 13:41:30 debian sshd[571]: Received signal 15; terminating.
Dec 03 13:41:30 debian sshd[45532]: Server listening on 0.0.0.0 port 22.
Dec 03 13:41:30 debian sshd[45532]: Server listening on :: port 22.
-- Boot d002be6861e94b128b7b7607cc80ef1c --
Dec 03 13:57:17 debian sshd[548]: Server listening on 0.0.0.0 port 22.
Dec 03 13:57:17 debian sshd[548]: Server listening on :: port 22.
-- Boot be99ac7fa28d408496b8742f08df651f --
Dec 03 13:59:50 debian sshd[564]: Server listening on 0.0.0.0 port 22.
Dec 03 13:59:50 debian sshd[564]: Server listening on :: port 22.
debian@debian:~$ █
```

1.1 Análisis forense del acceso por SSH (puerto 22)

Durante la fase de reconocimiento, se priorizó la **revisión de evidencias del servicio SSH** por tratarse del **principal vector de entrada**. Para ello se consultaron los registros del servicio mediante “journalctl -u ssh”, observándose un evento de autenticación exitosa con contraseña para el usuario root desde una IP de la red local (por ejemplo, “Accepted password for root from 192.168.0.134 ... ssh2”). Este hallazgo confirma que el atacante consiguió credenciales válidas y no dependió de una explotación de software en ese momento, sino de autenticación directa. Además, **se revisaron cierres y reinicios del servicio** (mensajes tipo “Starting/Stopping ssh.service” y “Received signal 15”), lo cual permite correlacionar cambios operativos del daemon SSH con la actividad observada en el sistema.

```

debian@debian:~$ sudo journalctl _COMM=sshd --no-pager
[sudo] password for debian:
Sep 30 12:25:16 debian sshd[51422]: Server listening on 0.0.0.0 port 22.
Sep 30 12:25:16 debian sshd[51422]: Server listening on :: port 22.
Sep 30 12:27:58 debian sshd[51422]: Received signal 15; terminating.
-- Boot 46ff5c6df3d4f0e86b315592aabazd0 --
Sep 30 15:09:51 debian sshd[560]: Server listening on 0.0.0.0 port 22.
Sep 30 15:09:51 debian sshd[560]: Server listening on :: port 22.
Oct 08 16:14:16 debian sshd[560]: Received signal 15; terminating.
Oct 08 16:14:16 debian sshd[5341]: Server listening on 0.0.0.0 port 22.
Oct 08 16:14:16 debian sshd[5341]: Server listening on :: port 22.
-- Boot 342683d87f35244b08c4f3863f2978eca --
Oct 08 16:43:18 debian sshd[543]: Server listening on 0.0.0.0 port 22.
Oct 08 16:43:18 debian sshd[543]: Server listening on :: port 22.
-- Boot d28e179bf5884b25bf94452c79fd0fa --
Oct 08 16:48:02 debian sshd[555]: Server listening on 0.0.0.0 port 22.
Oct 08 16:48:02 debian sshd[555]: Server listening on :: port 22.
-- Boot af0a79f76920440c8e05994d6547449b --
Oct 08 17:28:38 debian sshd[558]: Server listening on 0.0.0.0 port 22.
Oct 08 17:28:38 debian sshd[558]: Server listening on :: port 22.
Oct 08 17:40:59 debian sshd[1050]: Accepted password for root from 192.168.0.134 port 45623 ssh2
Oct 08 17:40:59 debian sshd[1050]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Oct 08 17:40:59 debian sshd[1050]: pam_env(sshd:session): deprecated reading of user environment enabled
-- Boot 239b8e4c205b424eb8cf328c9117fa0d --
Dec 01 13:27:02 debian sshd[595]: Server listening on 0.0.0.0 port 22.
Dec 01 13:27:02 debian sshd[595]: Server listening on :: port 22.
-- Boot 21f9a10593314076a02841713af14bad --
Dec 01 13:42:05 debian sshd[570]: Server listening on 0.0.0.0 port 22.
Dec 01 13:42:05 debian sshd[570]: Server listening on :: port 22.
-- Boot 88a5da2a97454ef580e139a1059aed58 --
Dec 03 13:15:04 debian sshd[571]: Server listening on 0.0.0.0 port 22.
Dec 03 13:15:04 debian sshd[571]: Server listening on :: port 22.
Dec 03 13:41:38 debian sshd[571]: Received signal 15; terminating.
Dec 03 13:41:38 debian sshd[45532]: Server listening on 0.0.0.0 port 22.
Dec 03 13:41:38 debian sshd[45532]: Server listening on :: port 22.
-- Boot d002b0a861e04b1287b507cc80ef1 --
Dec 03 13:41:17 debian sshd[548]: Server listening on 0.0.0.0 port 22.
Dec 03 13:41:17 debian sshd[548]: Server listening on :: port 22.
-- Boot be99ac7fa28d408496b742f08d0651f --
Dec 03 13:59:50 debian sshd[564]: Server listening on 0.0.0.0 port 22.
Dec 03 13:59:50 debian sshd[564]: Server listening on :: port 22.
Dec 08 11:34:47 debian sshd[564]: Received signal 15; terminating.
Dec 08 11:34:47 debian sshd[6473]: Server listening on 0.0.0.0 port 22.
Dec 08 11:34:47 debian sshd[6473]: Server listening on :: port 22.
Dec 08 11:56:24 debian sshd[6643]: Connection closed by ::1 port 38744 [preauth]
Dec 08 11:56:53 debian sshd[6710]: Connection closed by ::1 port 52338 [preauth]
Dec 10 13:46:49 debian sshd[10383]: error: kex_exchange_identification: Connection closed by remote host
Dec 10 13:46:49 debian sshd[10383]: Connection closed by 127.0.0.1 port 47360
Dec 10 13:46:57 debian sshd[10401]: Unable to negotiate with 127.0.0.1 port 42802: no matching host key type found. Their offer: ssh-dss [pxauth]
Dec 10 13:46:57 debian sshd[10414]: Unable to negotiate with 127.0.0.1 port 42812: no matching host key type found. Their offer: ssh-rsa [pxauth]
Dec 10 13:46:58 debian sshd[10421]: Connection closed by 127.0.0.1 port 42828 [preauth]

```

1.2 Correlación de actividad y alcance inicial del atacante

Una vez **confirmada la entrada por SSH**, se realizó una correlación básica para estimar el alcance del acceso. **Se revisaron intentos fallidos y patrones de fuerza bruta** en registros (por ejemplo con búsquedas en “/var/log/auth.log” si está disponible), así como el historial de sesiones con “last/lastb” para identificar otras conexiones relevantes.

Paralelamente, se **verificó la existencia de mecanismos de persistencia típicos** asociados a SSH: presencia de claves no autorizadas en “/root/.ssh/authorized_keys”, modificaciones en “/etc/ssh/sshd_config” (parámetros como PermitRootLogin o PasswordAuthentication) y creación de usuarios anómalos en “/etc/passwd”. Con estas comprobaciones se buscó determinar si el **atacante solo obtuvo acceso interactivo** puntual o si dejó el sistema preparado para accesos futuros.

```
-----  
debian@debian:~$ cat /etc/passwd  
cat /etc/group  
root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin  
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin  
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin  
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin  
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin  
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin  
avahi-autoipd:x:101:110:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin  
usbmux:x:102:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin  
dnsmasq:x:103:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin  
avahi:x:104:112:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin  
speech-dispatcher:x:105:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false  
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/nologin  
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  
vboxadd:x:999:1::/var/run/vboxadd:/bin/false  
Debian-exim:x:114:123::/var/spool/exim4:/usr/sbin/nologin  
root:x:0:  
daemon:x:1:  
bin:x:2:  
sys:x:3:  
adm:x:4:  
tty:x:5:  
disk:x:6:  
lp:x:7:  
mail:x:8:  
news:x:9:  
uucp:x:10:  
man:x:12:  
proxy:x:13:  
kmem:x:15:  
dialout:x:20:  
fax:x:21:  
voice:x:22:  
cdrom:x:24:debian  
floppy:x:25:debian  
tape:x:26:  
sudo:x:27:  
audio:x:29:pulse,debian  
dip:x:30:debian  
www-data:x:33:  
backup:x:34:  
operator:x:37:  
list:x:38:  
irc:x:39:  
src:x:40:  
shadow:x:42:  
utmp:x:43:  
video:x:44:debian  
-----
```

1.3 Búsqueda de persistencia y acciones post-explotación

Con el objetivo de responder a la pregunta “**¿qué hizo el atacante después de entrar?**”, se revisaron fuentes de persistencia comunes: **tareas programadas de cron** (crontab del root y directorios /etc/cron.*), servicios habilitados en systemd y timers activos. También se revisó la evidencia de **comandos ejecutados mediante el historial de root** (por ejemplo “/root/.bash_history”) cuando existe y no ha sido eliminado. Como verificación adicional, se enumeraron cambios recientes en rutas sensibles (como /etc, /root, /tmp y /var/tmp) mediante búsquedas por fecha de modificación, con el fin de identificar ficheros añadidos recientemente, scripts, backdoors o configuraciones alteradas. Este conjunto de controles permite aportar un análisis forense más sólido incluso cuando no se observa un “payload” evidente en ejecución.

```
debian@debian:~$ sudo crontab -l
sudo ls -la /etc/cron*
no crontab for root
-rw-r--r-- 1 root root 1042 Mar  2  2023 /etc/crontab

/etc/cron.d:
total 32
drwxr-xr-x  2 root root  4096 Dec  3 13:32 .
drwxr-xr-x 122 root root 12288 Dec 10 13:46 ..
-rw-r--r--  1 root root   285 Jan 10  2023 anacron
-rw-r--r--  1 root root   201 Mar  4  2023 e2scrub_all
-rw-r--r--  1 root root   712 Jul 13  2022 php
-rw-r--r--  1 root root   102 Mar  2  2023 .placeholder

/etc/cron.daily:
total 56
drwxr-xr-x  2 root root  4096 Dec  8 11:22 .
drwxr-xr-x 122 root root 12288 Dec 10 13:46 ..
-rwrxr-xr-x  1 root root   311 Jan 10  2023 anacron
-rwrxr-xr-x  1 root root   539 Jul  1  2024 apache2
-rwrxr-xr-x  1 root root  1478 May 25  2023 apt-compat
-rwrxr-xr-x  1 root root   161 Mar 12  2023 chkrootkit
-rwrxr-xr-x  1 root root   123 Mar 26  2023 dpkg
-rwrxr-xr-x  1 root root  4722 Jun 17  2024 exim4-base
-rwrxr-xr-x  1 root root   377 Dec 14  2022 logrotate
-rwrxr-xr-x  1 root root  1395 Mar 12  2023 man-db
-rw-r--r--  1 root root   102 Mar  2  2023 .placeholder

/etc/cron.hourly:
total 20
drwxr-xr-x  2 root root  4096 Jul 31  2024 .
drwxr-xr-x 122 root root 12288 Dec 10 13:46 ..
-rw-r--r--  1 root root   102 Mar  2  2023 .placeholder

/etc/cron.monthly:
total 24
drwxr-xr-x  2 root root  4096 Jul 31  2024 .
drwxr-xr-x 122 root root 12288 Dec 10 13:46 ..
-rwrxr-xr-x  1 root root   313 Jan 10  2023 anacron
-rw-r--r--  1 root root   102 Mar  2  2023 .placeholder

/etc/cron.weekly:
total 28
drwxr-xr-x  2 root root  4096 Jul 31  2024 .
drwxr-xr-x 122 root root 12288 Dec 10 13:46 ..
-rwrxr-xr-x  1 root root   312 Jan 10  2023 anacron
-rwxi-xr-x  1 root root   1055 Mar 12  2023 man-db
-rw-r--r--  1 root root   102 Mar  2  2023 .placeholder

/etc/cron.yearly:
total 20
drwxr-xr-x  2 root root  4096 Jul 31  2024 .
drwxr-xr-x 122 root root 12288 Dec 10 13:46 ..
-rw-r--r--  1 root root   102 Mar  2  2023 .placeholder
```

2. Identificación de archivos sospechosos, procesos en ejecución y modificaciones inusuales

Después de identificar el vector de entrada, se procedió a analizar el comportamiento del sistema para **detectar alteraciones sospechosas**. Se revisaron los procesos en ejecución mediante **ps aux --sort=-%cpu | head**, comprobando que todos correspondían a servicios legítimos del sistema, como Xorg, speech-dispatcher, caja, mate-terminal y MariaDB. También se verificaron los **puertos abiertos** a través del comando **ss -tulnp**, confirmando

que no existían servicios adicionales escuchando en puertos desconocidos ni backdoors activos en el sistema. Finalmente, mediante last, se revisaron los **accesos registrados** en el historial de sesiones para **confirmar la ausencia de entradas anómalas** posteriores al incidente. **No se detectaron archivos modificados manualmente** por el atacante ni creación de nuevos usuarios, y no se observaron comportamientos inusuales que indiquen persistencia maliciosa.

```
debian@debian:~$ ps aux --sort=-%cpu | head -n 20
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START  TIME COMMAND
debian    1661  0.7  1.6 1703292 32304 ?        S<sl 10:44  0:34 /usr/bin/pulseaudio --daemonize=no --log-target=journal
debian    2159  0.5  0.9 730648 18816 ?        Ssl  10:44  0:24 /usr/bin/speech-dispatcher --spawn --communication-method unix_socket --
socket-path /run/user/1000/speech-dispatcher/speechd.sock --port 6560
root     1462  0.4 12.2 805632 245912 tty7     Ssl+ 10:44  0:18 /usr/lib/xorg/Xorg :0 -seat seat0 -auth /var/run/lightdm/root/:0 -nolist
en tcp vt7  novtswitch
debian   1912  0.2  3.3 389384 67824 ?        Sl  10:44  0:12 /usr/bin/python3 /usr/bin/orca
debian   2245  0.2  2.5 559996 50768 ?        Sl  10:44  0:09 mate-terminal
debian   1747  0.1  0.1 217368 2192 ?        Sl  10:44  0:07 /usr/bin/VBoxClient --draganddrop
debian   2153  0.1  0.6 109008 12512 ?        Sl  10:44  0:07 /usr/lib/speech-dispatcher-modules/sd_espeak-ng /etc/speech-dispatcher/m
odules/espeak-ng.conf
debian   1852  0.0  3.6 815596 72892 ?        Sl  10:44  0:02 /usr/bin/caja
debian   1808  0.0  2.4 745040 49564 ?        Sl  10:44  0:01 marco
root    1158  0.0  0.0 349848 1084 ?        Sl  10:44  0:01 /usr/bin/VBoxDRMClient
debian   1743  0.0  0.1 216852 2192 ?        Sl  10:44  0:01 /usr/bin/VBoxClient --seamless
debian   1778  0.0  0.2 9552 4732 ?        S  10:44  0:01 /usr/bin/dbus-daemon --config-file=/usr/share/default/at-spi2/accessibi
lity.conf --nofork --print-address 11 --address=unix:path=/run/user/1000/at-spi/bus_0
root    6589  0.0  0.0 0 0 ?        I  11:50  0:00 [kworker/1:2-ata_sff]
root    6608  0.0  0.0 0 0 ?        I  11:55  0:00 [kworker/1:0-events]
root    1 0.0  0.6 102864 12732 ?        Ss  10:43  0:00 /sbin/init splash
mysql   736  0.0  6.9 1349652 140540 ?        Ssl 10:43  0:00 /usr/sbin/mariadb
debian   1826  0.0  2.2 552328 45588 ?        Sl  10:44  0:00 mate-panel
debian   1802  0.0  0.4 164532 9612 ?        Sl  10:44  0:00 /usr/libexec/at-spi2-registryd --use-gnome-session
debian   1800  0.0  2.0 1140216 41404 ?        Sl  10:44  0:00 /usr/bin/mate-settings-daemon

debian@debian:~$ sudo ss -tulnp
[sudo] password for debian:
Netid      State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
Process
jdp      UNCONN      0          0          0.0.0.0:5353      0.0.0.0:*
users:(("avahi-daemon",pid=492,fd=12))
jdp      UNCONN      0          0          0.0.0.0:60265      0.0.0.0:*
users:(("avahi-daemon",pid=492,fd=14))
jdp      UNCONN      0          0          [:]:5353      [:]:*
users:(("avahi-daemon",pid=492,fd=13))
jdp      UNCONN      0          0          [:]:56124      [:]:*
users:(("avahi-daemon",pid=492,fd=15))
tcp      LISTEN      0          20          127.0.0.1:25      0.0.0.0:*
users:(("exim4",pid=4987,fd=4))
tcp      LISTEN      0          128         0.0.0.0:22      0.0.0.0:*
users:(("sshd",pid=6473,fd=3))
tcp      LISTEN      0          80          127.0.0.1:3306      0.0.0.0:*
users:(("mariadb",pid=736,fd=31))
tcp      LISTEN      0          128         127.0.0.1:631      0.0.0.0:*
users:(("cupsd",pid=3211,fd=7))
tcp      LISTEN      0          511         *:80          *:*
users:(("apache2",pid=3210,fd=3),("apache2",pid=3209,fd=3),("apache2",pid=3208,fd=3),("apache2",pid=3207,fd=3),("apache2",pid=3206,fd=3),
"apache2",pid=660,fd=3))
tcp      LISTEN      0          32          *:21          *:*
users:(("vsftpd",pid=546,fd=3))
tcp      LISTEN      0          128         [:]:22      [:]:*
users:(("sshd",pid=6473,fd=4))
tcp      LISTEN      0          128         [:]:631      [:]:*
users:(("cupsd",pid=3211,fd=6))
tcp      LISTEN      0          20          [:]:25      [:]:*
users:(("exim4",pid=4987,fd=51))
```

Punto 3 – Escaneo del servidor para detectar rootkits o malware

Con el objetivo de detectar posibles rootkits o malware persistente en el sistema, se realizó un escaneo completo utilizando la herramienta chkrootkit. El análisis revisó binarios críticos

del sistema, procesos en ejecución, módulos del kernel y directorios comúnmente utilizados por malware conocido.

El resultado del escaneo **no evidenció la presencia de rootkits conocidos** ni de binarios alterados. Se mostraron algunas advertencias relacionadas con archivos y procesos legítimos del sistema, como componentes de LibreOffice y NetworkManager, los cuales fueron analizados manualmente y correlacionados con paquetes oficiales instalados en el sistema.

Tras esta verificación adicional, no se encontraron indicios concluyentes de infección activa, por lo que se determinó que el sistema **no presentaba malware persistente** en el momento del análisis.

```
debian@debian:~$ sudo chkrootkit
ROOTDIR is '/'
Checking `amd'...                                not found
Checking `basename'...                            not infected
Checking `biff'...                               not found
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 `fingerd'...                            not infected
Checking `gpm'...                                not found
Checking `grep'...                               not found
Checking `hdparm'...                            not infected
Checking `su'...                                 not found
Checking `ifconfig'...                           not infected
Checking `inetd'...                             not infected
Checking `inetdconf'...                          not found
Checking `identd'...                            not found
Checking `init'...                               not infected
Checking `killall'...                            not infected
Checking `ldpreload'...                           not infected
Checking `login'...                             not infected
Checking `ls'...                                 not infected
Checking `lsof'...                               not infected
Checking `mail'...                               not infected
Checking `mingetty'...                           not found
Checking `netstat'...                            not infected
Checking `named'...                             not found
Checking `passwd'...                            not infected
Checking `pidof'...                             not infected
Checking `pop2'...                               not found
Checking `pop3'...                               not found
Checking `ps'...                                 not infected
Checking `pstree'...                            not infected
Checking `rpcinfo'...                           not found
Checking `rlogind'...                           not found
Checking `rshd'...                               not found
Checking `slogin'...                            not infected
Checking `sendmail'...                           not infected
```

```

Searching for CrossRAT...                                not found
Searching for Hidden Cobra...                           not found
Searching for Rocke Miner rootkit...                  not found
Searching for PWNLNX4 lkm rootkit...                 not found
Searching for PWNLNX6 lkm rootkit...                 not found
Searching for Umreon lirk...                           not found
Searching for Kinsing.a backdoor rootkit...          not found
Searching for RotaJakiro backdoor rootkit...         not found
Searching for Syslogk LKM rootkit...                 not found
Searching for Kovid LKM rootkit...                   not tested
Searching for suspect PHP files...                  not found
Searching for zero-size shell history files...      not found
Searching for hardlinked shell history files...     not found
Checking 'aliens'...                                 finished
Checking 'asp'...                                    not infected
Checking 'bindshell'...                            not found
Checking 'lkm'...                                   started
Searching for Adore LKM...                           not tested
Searching for sebek LKM (Adore based)...          not tested
Searching for knark LKM rootkit...                 not found
Searching for for hidden processes with chkproc... not found
Searching for for hidden directories using chkdirs... not found
Checking 'lkm'...                                 finished
Checking 'rexedcs'...                            not found
Checking 'sniffer'...                            WARNING
WARNING: Output from ifpromisc:
lo: not promisc and no packet sniffer sockets
enp0s3: PACKET SNIFFER(/usr/sbin/NetworkManager[509], /usr/sbin/NetworkManager[509])

Checking 'w55808'...                                not found
Checking 'wted'...                                 not found
Checking 'scalper'...                            not found
Checking 'slapper'...                            not found
Checking 'z2'...                                    not found
Checking 'chkutmp'...                            not found
Checking 'OSX_RSPLUG'...                          not tested
debian@debian:~$ ip link show enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 08:00:27:a6:d3:0b brd ff:ff:ff:ff:ff:ff
debian@debian:~$ sudo lsof -n | grep PACKET
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1000/doc
      Output information may be incomplete.
systemd      1          root    81u   unix 0x00000000a3d673a1      0t0    13687 /run/udev/control type=SEQPACKET (LISTEN)
systemd-u  273          root    3u   unix 0x00000000a3d673a1      0t0    13687 /run/udev/control type=SEQPACKET (LISTEN)
debian@debian:~$ dpkg -V network-manager
missing      /usr/share/polkit-1/rules.d/org.freedesktop.NetworkManager.rules (Permission 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.NetworkManager.pkla (Permission denied)

```

4. Bloqueo del exploit y prevención de escalación

Una vez **confirmado** que el **atacante obtuvo acceso al servidor mediante SSH** utilizando la contraseña del **usuario root**, la medida de contención más inmediata consistió en bloquear el vector de entrada. Para ello, se revisó y modificó la configuración del servicio SSH, deshabilitando por completo el inicio de sesión remoto del usuario root mediante la directiva **PermitRootLogin no**. Esta acción impide que futuros intentos de autenticación directa como root puedan realizarse, incluso si un atacante conoce o adivina la contraseña.

```

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication

```

Además, se reforzaron las políticas de autenticación del servicio SSH, **reduciendo la superficie de ataque** y evitando que la vulnerabilidad inicial pudiera ser explotada nuevamente. Durante esta fase se confirmó que ningún otro servicio del sistema mostraba señales de compromiso y que no existían procesos sospechosos en ejecución.

Punto 5 – Reversión de cambios realizados por el atacante

Como parte de la fase de **contención y erradicación**, se procedió a **revisar posibles cambios realizados por el atacante** durante el acceso no autorizado. Para ello, se verificó el archivo de cuentas del sistema con el fin de identificar usuarios adicionales o modificaciones en cuentas existentes.

El análisis no mostró la existencia de usuarios no autorizados ni cuentas con privilegios elevados fuera de las esperadas. Asimismo, se revisaron servicios activos, procesos en ejecución y puertos en escucha, confirmando que **no se habían creado backdoors** ni servicios persistentes adicionales.

```
debian@debian:~$ cat /etc/passwd | tail -n 20
systemd-network:x:998:998:systemd Network Management::/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization::/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:101:110:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:102:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:103:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:104:112:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:x:105:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
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/nologin
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
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
Debian-exim:x:114:123::/var/spool/exim4:/usr/sbin/nologin
```

```
debian@debian:~$ sudo ss -tulnp
Netid      State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
tcp        UNCONN      0          0          0.0.0.0:5353      0.0.0.0:*
tcp        UNCONN      0          0          0.0.0.0:60265     0.0.0.0:*
tcp        UNCONN      0          0          [::]:5353       [::]:*
tcp        UNCONN      0          0          [::]:56124      [::]:*
tcp        LISTEN      0          20         127.0.0.1:25      0.0.0.0:*
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       [::]:*
tcp        LISTEN      0          128        [::]:631      [::]:*
tcp        LISTEN      0          20          [::]:25       [::]:*
users:(("exim4",pid=4987,fd=4))
```

6. Actualización y corrección de configuraciones de seguridad

Con el fin de mejorar la postura de seguridad y evitar futuros incidentes, se aplicaron varias medidas correctivas. En primer lugar, se actualizaron todos los paquetes del sistema mediante **apt update** y **apt upgrade**, asegurando que no quedaran vulnerabilidades conocidas sin parchear. Se modificaron las credenciales críticas, especialmente las del usuario root, utilizando contraseñas más robustas. Adicionalmente, se reforzó la **configuración del firewall para limitar la exposición de servicios** y se aumentó la

seguridad del servicio SSH deshabilitando accesos inseguros y estableciendo parámetros más restrictivos. Estas medidas garantizaron que el sistema quedara significativamente más protegido que antes del incidente.

```
debian@debian:~$ sudo apt update
sudo apt upgrade -y
Get:1 http://deb.debian.org/debian bookworm InRelease [48.0 kB]
Get:2 http://security.debian.org/debian-security bookworm-security InRelease [55.4 kB]
Get:3 http://deb.debian.org/debian bookworm-updates InRelease [195 kB]
Get:4 http://security.debian.org/debian-security bookworm-security/main Sources [195 kB]
Get:5 http://security.debian.org/debian-security bookworm-security/main amd64 Packages [290 kB]
Get:6 http://security.debian.org/debian-security bookworm-security/main Translation-en [176 kB]
Fetched 764 kB in 1s (1,401 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
3 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libdaxt1 libndctl16 libpmem1 linux-image-6.1.0-22-amd64 linux-image-6.1.0-23-amd64
Use 'sudo apt autoremove' to remove them.
The following packages will be upgraded:
  libjavascriptcoregtk-4.1-0 libpng16-16 libwebkit2gtk-4.1-0
3 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 30.2 MB of archives.
After this operation, 67.6 kB of additional disk space will be used.
Get:1 http://security.debian.org/debian-security bookworm-security/main amd64 libpng16-16 amd64 1.6.39-2+deb12u1 [276 kB]
Get:2 http://security.debian.org/debian-security bookworm-security/main amd64 libwebkit2gtk-4.1-0 amd64 2.50.3-1-deb12u1 [22.6 MB]
Get:3 http://security.debian.org/debian-security bookworm-security/main amd64 libjavascriptcoregtk-4.1-0 amd64 2.50.3-1-deb12u1 [7,242 kB]
Fetched 30.2 MB in 1s (22.3 MB/s)
apt-listchanges: Reading changelogs...
(Reading database ... 197908 files and directories currently installed.)
Preparing to unpack .../libpng16-16_1.6.39-2+deb12u1_amd64.deb ...
Unpacking libpng16-16:amd64 (1.6.39-2+deb12u1) over (1.6.39-2) ...
Preparing to unpack .../libwebkit2gtk-4.1-0_2.50.3-1-deb12u1_amd64.deb ...
Unpacking libwebkit2gtk-4.1-0:amd64 (2.50.3-1-deb12u1) over (2.50.1-1-deb12u1) ...
Preparing to unpack .../libjavascriptcoregtk-4.1-0_2.50.3-1-deb12u1_amd64.deb ...
Unpacking libjavascriptcoregtk-4.1-0:amd64 (2.50.3-1-deb12u1) over (2.50.1-1-deb12u1) ...
Setting up libpng16-16:amd64 (1.6.39-2+deb12u1) ...
Setting up libwebkit2gtk-4.1-0:amd64 (2.50.3-1-deb12u1) ...
Processing triggers for libc-bin (2.36-9+deb12u1) ...

#!/usr/sbin/nft -f

table inet filter {
    chain input {
        type filter hook input priority 0;

        # Permitir loopback (necessário para o sistema)
        iif "lo" accept

        # Permitir tráfego já estabelecido
        ct state established,related accept

        # Permitir ICMP (ping)
        ip protocol icmp accept

        # Permitir conexões SSH (porta 22)
        tcp dport 22 accept

        # Rejeitar todo o resto
        reject
    }
}
```

6.2 Revisión de cuentas y credenciales en la base de datos MariaDB

Durante la revisión de configuraciones de seguridad, se identificó una debilidad en los permisos del sistema de archivos asociados al servicio Apache. El directorio raíz del servicio web (/var/www/html) presentaba permisos excesivamente permisivos, permitiendo lectura y escritura a cualquier usuario del sistema.

Esta configuración supone un riesgo relevante, ya que facilita el acceso no autorizado a ficheros de configuración, código fuente y posibles credenciales almacenadas en el entorno

web, incrementando la probabilidad de manipulación del contenido o de exposición de información sensible.

Como medida correctiva, se procedió a aplicar el principio de mínimo privilegio, restringiendo los permisos del directorio y sus ficheros para que únicamente el usuario del servicio Apache (www-data) tuviera acceso. Tras la corrección, los directorios fueron configurados con permisos 750 y los ficheros con permisos 640, eliminando el acceso innecesario para otros usuarios del sistema.

Estas acciones reducen significativamente la superficie de ataque del servicio web y refuerzan la seguridad del entorno Apache frente a accesos locales no autorizados.

```
debian@debian:~$ ps aux | grep apache
root      12341  0.0  1.6 268720 33612 ?        Ss   10:43   0:00 /usr/sbin/apache2 -k start
www-data   13617  0.0  0.7 269320 15216 ?        S    11:43   0:00 /usr/sbin/apache2 -k start
www-data   13618  0.0  0.7 269320 15216 ?        S    11:43   0:00 /usr/sbin/apache2 -k start
www-data   13620  0.0  0.7 269320 15216 ?        S    11:43   0:00 /usr/sbin/apache2 -k start
www-data   13621  0.0  0.7 269320 15216 ?        S    11:43   0:00 /usr/sbin/apache2 -k start
www-data   13622  0.0  0.7 269320 15216 ?        S    11:43   0:00 /usr/sbin/apache2 -k start
debian    13771  0.0  0.1  6340  2120 pts/0    S+   11:50   0:00 grep apache
debian@debian:~$ ls -la /var/www
total 12
drwxr-xr-x  3 root      root      4096 Sep 30  2024 .
drwxr-xr-x 12 root      root      4096 Sep 30  2024 ..
drwxrwxrwx  5 www-data  www-data  4096 Dec 10 13:47 [redacted]
```

6.2 Revisión de cuentas y credenciales en la base de datos MariaDB

Como parte del proceso de endurecimiento del sistema, se realizó una auditoría de las cuentas configuradas en el servicio de base de datos MariaDB. Durante esta revisión se identificó la existencia de una cuenta genérica (user) con privilegios administrativos globales (ALL PRIVILEGES sobre todas las bases de datos) y capacidad de delegar permisos (GRANT OPTION).

La presencia de este tipo de cuentas genéricas representa una mala práctica de seguridad, especialmente cuando se combina con credenciales débiles, ya que permite el acceso total al sistema de bases de datos sin una adecuada separación de responsabilidades.

Tras verificar que dicha cuenta no era utilizada por la aplicación (WordPress), se procedió a su eliminación. Se mantuvo únicamente el usuario específico de la aplicación (wordpressuser), limitado exclusivamente a la base de datos necesaria y con privilegios restringidos.

Esta corrección elimina el riesgo asociado a credenciales débiles y privilegios excesivos en el sistema gestor de bases de datos, alineando la configuración con buenas prácticas de seguridad y el principio de mínimo privilegio.

```
MariaDB [(none)]> DROP USER 'user'@'localhost';
Query OK, 0 rows affected (0.010 sec)

MariaDB [(none)]>
```

Punto 7 – Informe final y recomendaciones

Las medidas aplicadas durante esta fase permitieron mitigar de forma efectiva el acceso no autorizado detectado inicialmente y reducir la superficie de ataque del sistema. **El bloqueo del acceso remoto** directo al usuario root, junto con la revisión de servicios y procesos activos, contribuyó a reforzar la postura de seguridad del servidor.

Como recomendaciones adicionales para prevenir incidentes similares en el futuro, se sugiere implementar autenticación basada en claves para SSH, limitar el acceso por dirección IP cuando sea posible, mantener un monitoreo continuo de logs de autenticación y aplicar actualizaciones de seguridad de manera periódica. Asimismo, se recomienda realizar auditorías regulares de servicios expuestos para evitar configuraciones innecesarias o inseguras.

Fase 2.1: Servicio FTP

1. Escaneo completo del sistema con Nmap

Para identificar nuevos vectores de ataque, se realizó un escaneo exhaustivo del sistema empleando la herramienta Nmap con detección avanzada de servicios:

```
sudo nmap -A -p- localhost
```

```

debian@debian:~$ sudo nmap -A -p- localhost
Starting Nmap 7.93 ( https://nmap.org ) at 2025-12-10 13:46 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00005s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 65524 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
| ftp-syst:
|_ STAT:
| FTP server status:
|   Connected to ::ffff:127.0.0.1
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 1
|   vsFTPD 3.0.3 - secure, fast, stable
_|End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh     OpenSSH 9.2p1 Debian 2+deb12u7 (protocol 2.0)
| ssh-hostkey:
|_ 256 aaf839b3ce63ac96079bc6c647ff5a (EDDSA)
|_ 256 43caa9c9317b82d903ff40f2a3714083 (ED25519)
25/tcp    open  smtp   Exim smtpd 4.96
| ssl-cert: Subject: commonName=debian.debian.org/organizationName=Exim Developers/countryName=UK
| Not valid before: 2025-12-10T18:19:10
|_Not valid after: 2025-12-10T20:19:10
|_ssl-date: TLS randomness does not represent time
| smtp-commands: debian.debian Hello localhost [127.0.0.1], SIZE 52428800, 8BITMIME, PIPELINING, PIPECONNECT, CHUNKING, STARTTLS, PRDR, HELO
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
80/tcp    open  http   Apache httpd 2.4.65 ((Debian))
|_http-server-header: Apache/2.4.65 (Debian)
|_http-title: Apache2 Debian Default Page: It works
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
631/tcp   open  ipp    CUPS 2.4
|_http-server-header: CUPS/2.4 IPP/2.1
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Home - CUPS 2.4
3306/tcp  open  mysql MySQL 5.5.5-10.11.14-MariaDB-0+deb12u2
| mysql-info:
| Protocol: 10
| Version: 5.5.5-10.11.14-MariaDB-0+deb12u2
| Thread ID: 32
| Capabilities flags: 63486
| Some Capabilities: SupportsLoadDataLocal, DontAllowDatabaseTableColumn, ConnectWithDatabase, IgnoreSpaceBeforeParenthesis, IgnoreSigpipe, SupportsTransactions, ODBCClient, InteractiveClient, LongColumnFlag, SupportsCompression, FoundRows, Speaks41ProtocolNew, Speaks41ProtocolOld, Support41Auth, SupportsMultipleStatements, SupportsMultipleResults, SupportsAuthPlugins
| Status: Autocommit

```

El análisis reveló **varios servicios expuestos**, entre ellos SSH (22), Apache (80), MySQL (3306), Exim (25), CUPS (631) y **FTP (21)**. Dentro de estos servicios, el hallazgo más relevante fue el **puerto 21/tcp**, donde se ejecutaba **vsFTPD 3.0.3**, permitiendo acceso FTP anónimo, lo cual representa una vulnerabilidad significativa por exposición innecesaria de información. Esta superficie de ataque no estaba relacionada con el incidente anterior y constituía un objetivo válido para análisis forense y explotación controlada.

2 – Vulnerabilidad detectada (FTP)

Durante el **escaneo del sistema se detectó el servicio FTP** (vsFTPD 3.0.3) escuchando en el puerto 21, el cual permitía autenticación anónima. Esta configuración constituye una mala práctica de seguridad, ya que expone un servicio innecesario y amplía la superficie de ataque del sistema.

No obstante, al verificar el acceso otorgado al usuario anónimo, se comprobó que el directorio disponible se encontraba vacío y que no existían permisos de escritura. Por lo tanto, no se evidenció exposición directa de información sensible ni capacidad de modificación de archivos en el estado actual del sistema.

A pesar de ello, se considera una vulnerabilidad de configuración con riesgo potencial, ya que cambios futuros en permisos o la presencia de archivos podrían derivar en una exposición real.

```
debian@debian:~$ ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.3)
Name (localhost:debian): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
drwxr-xr-x    2 0          122        4096 Oct  08  2024 .
drwxr-xr-x    2 0          122        4096 Oct  08  2024 ..
226 Directory send OK.
```

3 – Proceso de validación de la vulnerabilidad

Con el objetivo de evaluar el impacto real de la vulnerabilidad detectada, se realizó una validación controlada del servicio FTP mediante autenticación anónima. Durante esta prueba se accedió al servicio y se ejecutaron comandos básicos de navegación para verificar el contenido accesible y los permisos asignados al usuario anónimo.

El análisis confirmó que el directorio accesible se encontraba vacío y que el usuario anónimo no disponía de permisos de escritura ni de capacidad para subir archivos al servidor. Asimismo, no fue posible acceder a otros directorios del sistema ni ejecutar acciones que permitieran escalar privilegios.

Estos resultados permitieron concluir que, si bien el servicio **FTP se encontraba expuesto** de forma innecesaria, no existía un compromiso efectivo del sistema ni una explotación práctica de la vulnerabilidad en el estado actual del entorno.

4 – Corrección y mitigación de la vulnerabilidad FTP

Dado que el servicio FTP no era necesario para el funcionamiento del sistema y representaba una exposición innecesaria, se decidió eliminar completamente este vector de ataque como medida preventiva. **Para ello, el servicio fue detenido, deshabilitado para su inicio automático** y posteriormente **enmascarado**, garantizando que no pudiera ser iniciado de forma accidental.

Tras la aplicación de estas medidas, se realizó una verificación del estado de los puertos del sistema, confirmando que el puerto 21 dejó de encontrarse en escucha. Con esta acción se redujo de forma efectiva la superficie de ataque del servidor y se eliminó el riesgo potencial asociado a la configuración insegura detectada.

5 – Conclusión de la Fase 2.1

En esta fase se identificó y analizó una vulnerabilidad distinta al incidente inicial de SSH, relacionada con la exposición innecesaria del servicio FTP. Aunque no se evidenció un compromiso efectivo del sistema, el análisis permitió detectar una configuración insegura que incrementaba el riesgo potencial.

La vulnerabilidad fue corregida eliminando el servicio expuesto y verificando posteriormente la reducción de la superficie de ataque. Este enfoque preventivo permite fortalecer la seguridad del sistema y demuestra la importancia de revisar periódicamente los servicios activos, incluso cuando no presentan explotación inmediata.

Fase 2.2: Servicio Apache (HTTP/80)

1) Detección y validación del servicio

Tras el escaneo previo del sistema, se confirmó que el servicio HTTP estaba accesible en el puerto 80. Para identificar la versión instalada se verificó el binario de Apache mediante la ruta completa, obteniendo como resultado Apache/2.4.65 (Debian).

A continuación, se revisó la información expuesta por cabeceras HTTP mediante una petición HEAD, observando que el servidor revelaba metadatos del producto (cabecera "Server"). Por último, se consultó el contenido publicado y se confirmó que el sitio mostraba la página por defecto de Apache en Debian, indicador de configuración inicial/no endurecida.

```
debian@debian:~$ sudo /usr/sbin/apache2 -v
Server version: Apache/2.4.65 (Debian)
Server built:   2025-07-29T20:18:46
debian@debian:~$ curl -I http://localhost
HTTP/1.1 200 OK
Date: Fri, 12 Dec 2025 18:44:01 GMT
Server: Apache/2.4.65 (Debian)
Last-Modified: Mon, 30 Sep 2024 14:44:22 GMT
ETag: "29cd-623573d915b52"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Content-Type: text/html
```

2) Impacto (por qué esto es una debilidad)

La exposición de metadatos del servidor (producto/versión y estado por defecto) constituye un caso de information disclosure. Aunque no implica ejecución remota por sí misma, facilita el reconocimiento del atacante, la selección de exploits compatibles y la priorización de vectores de ataque. Además, mantener la página por defecto aporta pistas sobre estructura y configuración del servicio web.

3) Medidas correctivas aplicadas (hardening)

Para mitigar la fuga de información, se ajustó la configuración de seguridad de Apache en el fichero /etc/apache2/conf-enabled/security.conf, aplicando directivas de endurecimiento:

ServerTokens Prod (minimiza la información de versión)

ServerSignature Off (evita firmas del servidor en páginas generadas)

TraceEnable Off (deshabilita el método TRACE)

Tras los cambios, se validó nuevamente la cabecera “Server” mediante petición HEAD para comprobar que ya no se expone la versión completa.

```
GNU nano 7.2                                         /etc/apache2/conf-enabled/security.conf *
# Changing the following options will not really affect the security of the
# server, but might make attacks slightly more difficult in some cases.

#
## ServerTokens
## This directive configures what you return as the Server HTTP response
## Header. The default is 'Full' which sends information about the OS-type
## and compiled in modules.
## Set to one of: Full | OS | Minimal | Minor | Major | Prod
## where Full conveys the most information, and Prod the least.
##ServerTokens Minimal
ServerTokens Prod
##ServerTokens Full

#
## Optionally add a line containing the server version and virtual host
## name to server-generated pages (internal error documents, FTP directory
## listings, mod_status and mod_info output etc., but not CGI generated
## documents or custom error documents).
## Set to "EMail" to also include a mailto: link to the ServerAdmin.
## Set to one of: On | Off | EMail
##ServerSignature off
ServerSignature Off

#
## Allow TRACE method
##
## Set to "extended" to also reflect the request body (only for testing and
## diagnostic purposes).
##
## Set to one of: On | Off | extended
TraceEnable Off
##TraceEnable On

#
## Forbid access to version control directories
##
## If you use version control systems in your document root, you should
## probably deny access to their directories.
##
## Examples:
##
##RedirectMatch 404 /\.git
##RedirectMatch 404 /\.svn

#
## Setting this header will prevent MSIE from interpreting files as something
## else than declared by the content type in the HTTP headers.
## Requires mod_headers to be enabled.
##
##Header set X-Content-Type-Options: "nosniff"

#
## Setting this header will prevent other sites from embedding pages from this
## site as frames. This defends against clickjacking attacks.
## Requires mod_headers to be enabled.
##
##Header set Content-Security-Policy "frame-ancestors 'self';"
```

```
debian@debian:~$ curl http://localhost
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/1999/xhtml">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Apache2 Debian Default Page: It works</title>
<style type="text/css" media="screen">
* {
margin: 0px 0px 0px 0px;
padding: 0px 0px 0px 0px;
}
body, html {
padding: 3px 3px 3px 3px;
background-color: #D8DBE2;
font-family: Verdana, sans-serif;
font-size: 11pt;
text-align: center;
}
div.main_page {
position: relative;
display: table;
width: 800px;
margin-bottom: 3px;
margin-left: auto;
margin-right: auto;
padding: 0px 0px 0px;
```

4) Conclusión

Se identificó una debilidad de configuración en Apache relacionada con exposición de metadatos y estado por defecto. La mitigación aplicada redujo la información revelada por el servicio y, por tanto, disminuyó la superficie de reconocimiento para un posible atacante. Como mejora adicional, se recomienda reemplazar la página por defecto, revisar módulos habilitados y mantener un ciclo de actualizaciones periódicas.

```
debian@debian:~$ curl -I http://localhost
HTTP/1.1 200 OK
Date: Fri, 12 Dec 2025 18:49:58 GMT
Server: Apache
Last-Modified: Mon, 30 Sep 2024 14:44:22 GMT
ETag: "29cd-623573d915b52"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Content-Type: text/html
```

Fase 3: Plan de respuesta a incidentes y Sistema de Gestión de Seguridad de la Información (SGSI)

Objetivo de la Fase 3

El objetivo de esta fase es diseñar un plan de respuesta a incidentes basado en buenas prácticas reconocidas, así como establecer un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001. Este planteamiento permite transformar los hallazgos técnicos identificados en las Fases 1 y 2 en medidas

organizativas, preventivas y correctivas que reduzcan el riesgo de futuros incidentes de seguridad.

3.1 Justificación del Plan de Respuesta y del SGSI

Durante las fases anteriores se **identificó un acceso no autorizado mediante el servicio SSH** y la exposición de servicios adicionales como **FTP y Apache**, los cuales **presentaban configuraciones inseguras**. Aunque **no se detectó una exfiltración de información sensible ni una escalada de privilegios avanzada**, los hallazgos evidencian debilidades en la configuración y en la gestión de los servicios del sistema.

Estos incidentes justifican la necesidad de implantar un plan formal de respuesta a incidentes y un SGSI que permita gestionar la seguridad de forma estructurada, proactiva y alineada con estándares internacionales.

3.2 Plan de Respuesta a Incidentes basado en **NIST SP 800-61**

El **plan de respuesta a incidentes** se ha diseñado siguiendo las recomendaciones del estándar NIST SP 800-61, adaptándolo al contexto del sistema analizado.

Identificación

La **identificación del incidente** se realizó mediante el **análisis de registros del sistema**, especialmente los **logs del servicio SSH**, donde se detectó un **acceso exitoso al usuario root** desde una dirección IP interna. Asimismo, los escaneos de servicios permitieron identificar la exposición de servicios adicionales que ampliaban la superficie de ataque.

Contención

Como medida de **contención inmediata**, se procedió a reforzar la configuración del servicio SSH, **deshabilitando el acceso remoto directo al usuario root** y **limitando los vectores de entrada**. Además, se aplicaron **reglas de firewall** para restringir el tráfico entrante únicamente a los servicios estrictamente necesarios y se **detuvo el servicio FTP**, que permitía acceso anónimo.

Erradicación

En la fase de erradicación se revisaron las configuraciones de los servicios expuestos, eliminando opciones inseguras y reduciendo la información revelada por los servicios. Se confirmó la ausencia de malware o rootkits mediante herramientas de análisis forense y se verificó que no existían usuarios no autorizados ni procesos sospechosos activos.

Recuperación

Tras aplicar las medidas correctivas, los servicios necesarios fueron restaurados con configuraciones reforzadas. Se validó la estabilidad del sistema y se verificó que los accesos quedaran correctamente limitados, asegurando la continuidad operativa sin comprometer la seguridad.

Lecciones aprendidas

El incidente evidenció la importancia de aplicar configuraciones seguras desde la instalación inicial de los servicios, así como la necesidad de monitorizar de forma continua los accesos y los servicios expuestos. La documentación y revisión periódica de los controles de seguridad se consideran esenciales para evitar incidentes similares en el futuro.

3.3 Sistema de Gestión de Seguridad de la Información (SGSI) según ISO 27001

Alcance del SGSI

El SGSI propuesto abarca el servidor Linux analizado, incluyendo los servicios SSH, FTP, Apache y los datos gestionados por dichos servicios. El alcance se centra en **proteger la confidencialidad, integridad y disponibilidad de la información** y de los sistemas asociados.

Análisis de riesgos

El análisis de riesgos identifica como activos críticos el acceso administrativo al sistema, los servicios de red y la información alojada en el servidor. Las principales amenazas detectadas incluyen accesos no autorizados, configuraciones inseguras y exposición innecesaria de servicios. El **impacto potencial se considera medio**, mientras que la probabilidad se reduce mediante la aplicación de controles adecuados.

Controles de seguridad

Entre los controles implementados destacan el **principio de mínimo privilegio**, el **endurecimiento de servicios críticos**, la **segmentación del tráfico** mediante **firewall**, la **actualización periódica del sistema** y la **restricción de accesos administrativos**. Estos controles reducen significativamente la superficie de ataque y el riesgo asociado.

Protección de la información

La protección de la información se basa en el **control de accesos**, la **limitación de privilegios**, la correcta gestión de configuraciones y la recomendación de copias de seguridad periódicas. Estas medidas garantizan la recuperación del sistema ante incidentes y evitan la pérdida o alteración de datos críticos.

Mejora continua

El SGSI contempla un **proceso de mejora continua** mediante **revisiones periódicas**, auditorías internas y actualización de políticas de seguridad. Este enfoque permite adaptar las medidas de protección a nuevos riesgos y amenazas emergentes.

3.4 Relación entre el Incidente y el SGSI

El incidente analizado demuestra que incluso sistemas sin una explotación avanzada pueden presentar riesgos significativos si no se gestionan adecuadamente. La implantación del SGSI permite pasar de una gestión reactiva de la seguridad a un modelo preventivo y estructurado, alineando las medidas técnicas con políticas organizativas claras.

3.5 Conclusión de la Fase 3

La combinación de un plan de respuesta a incidentes y un SGSI conforme a **ISO 27001** proporciona un **marco sólido para la gestión de la seguridad de la información**. Las medidas propuestas permiten prevenir la recurrencia de incidentes similares, mejorar la postura de seguridad del sistema y garantizar una gestión responsable y profesional de los riesgos de seguridad.