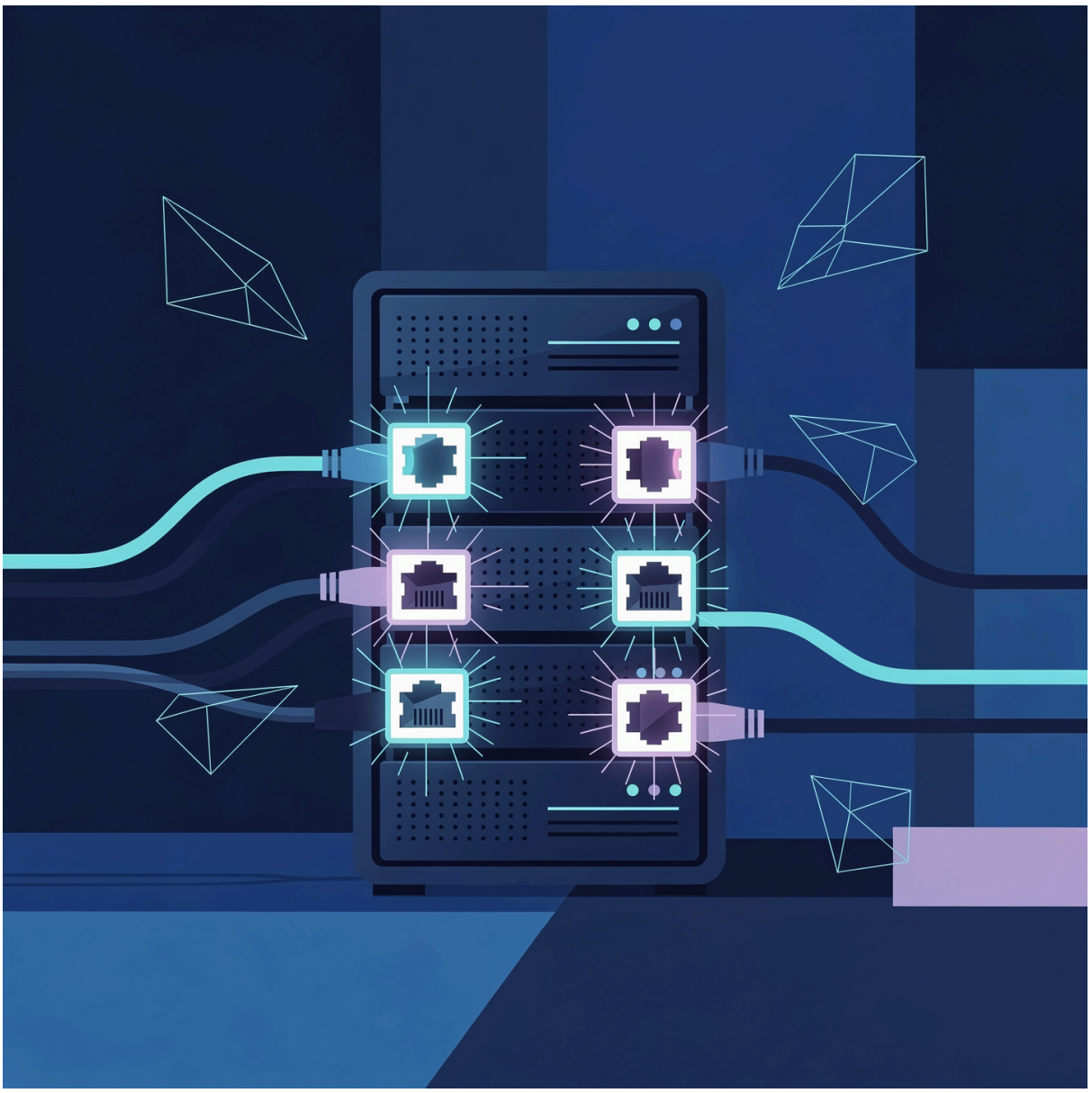
Informe de incidente de seguridad



Análisis forense, detección de riesgos y acciones correctivas

Nombre: Gerardo Ernesto Aguilar López

1. Introducción

El presente informe tiene como objetivo documentar el análisis de seguridad realizado sobre un servidor Debian GNU/Linux 12. El trabajo combina técnicas de pentesting defensivo, análisis de incidentes y endurecimiento del sistema, con el fin de identificar vulnerabilidades, evaluar posibles riesgos y aplicar medidas correctivas.

El análisis se llevó a cabo en un entorno controlado y se centró en la revisión de servicios activos, configuraciones inseguras, permisos de archivos críticos, análisis de logs del sistema y detección de malware o rootkits.

2. Alcance del análisis

El análisis incluyó los siguientes puntos:

- Identificación y documentación de vulnerabilidades
- Verificación de configuraciones inseguras
- Escaneo de puertos y servicios
- Revisión de permisos de archivos sensibles
- Análisis forense de logs del sistema
- Detección de malware y rootkits
- Aplicación de soluciones y medidas correctivas

3. Escaneo de puertos y servicios activos

Como primer paso del pentesting, se realizó un escaneo local de los puertos y servicios activos para identificar la superficie de ataque del servidor.

```
debian@debian:~$ ss -tulnp
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                                         0.0.0.0:45297              0.0.0.0:*
udp      UNCONN     0          0                                            [::]:5353                  [::]:*
udp      UNCONN     0          0                                            [::]:53518                 [::]:*
udp      UNCONN     0          0              [fe80::a00:27ff:fe02:911d]%enp0s3:546                    [::]:*
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                       *:*
tcp      LISTEN     0          128                                           [::]:22                    [::]:*
tcp      LISTEN     0          32                                               *:21                       *:*
debian@debian:~$
```

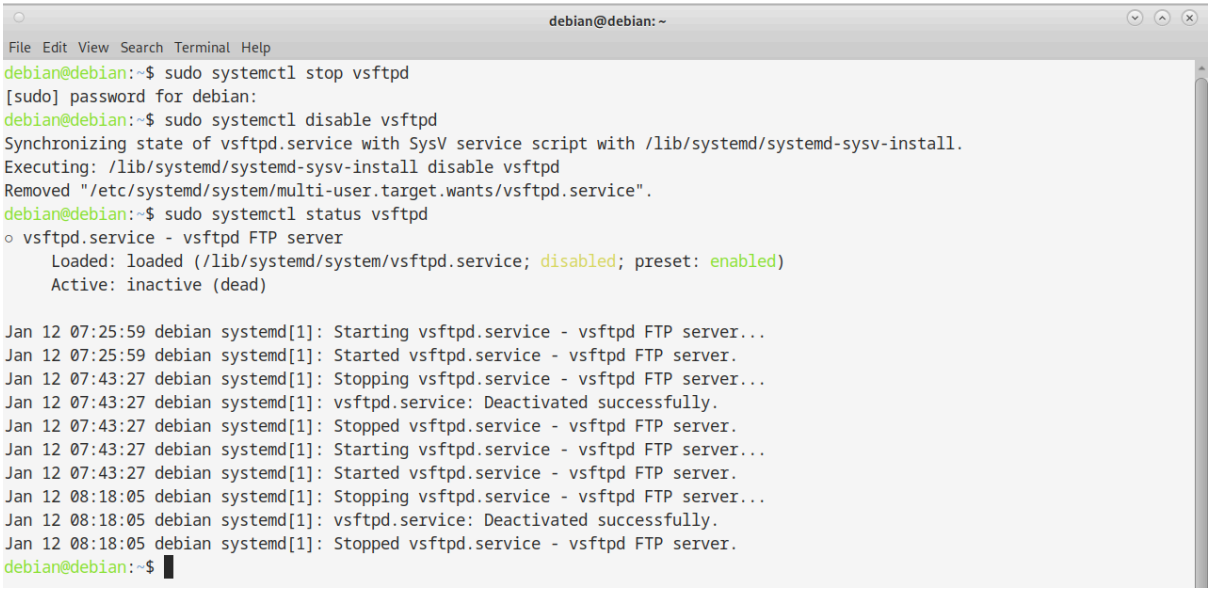
A partir del escaneo se identificaron los siguientes servicios relevantes:

- SSH en el puerto 22
- Apache en el puerto 80
- MariaDB escuchando solo en localhost
- Servicio FTP (vsftpd) en el puerto 21

4. Identificación y corrección del servicio FTP inseguro

Se detectó que el servicio FTP (vsftpd) estaba activo, lo cual representa un riesgo si no es estrictamente necesario, especialmente si permite accesos inseguros.

Se observó que el servicio estaba habilitado y permitía escritura, por lo que se decidió tomar medidas para mejorar la seguridad del servidor.



5. Revisión de permisos en archivos críticos (WordPress)

Se revisaron los permisos del archivo wp-config.php, el cual contiene información sensible como credenciales de base de datos.

Se detectó que el archivo tiene permisos demasiado permisivos. Para corregirlo, se limitaron los permisos únicamente al propietario.

6. Endurecimiento del servidor web (Apache)

Se revisó la configuración del servidor Apache para evitar el listado de directorios, una vulnerabilidad común en servidores web mal configurados.

Así que se modifica la directiva correspondiente para mejorar el servidor.

7. Implementación de firewall (UFW)

Para reducir la exposición del servidor, se configuró un firewall con UFW, permitiendo únicamente los servicios necesarios.

Comandos utilizados:

sudo ufw default deny incoming

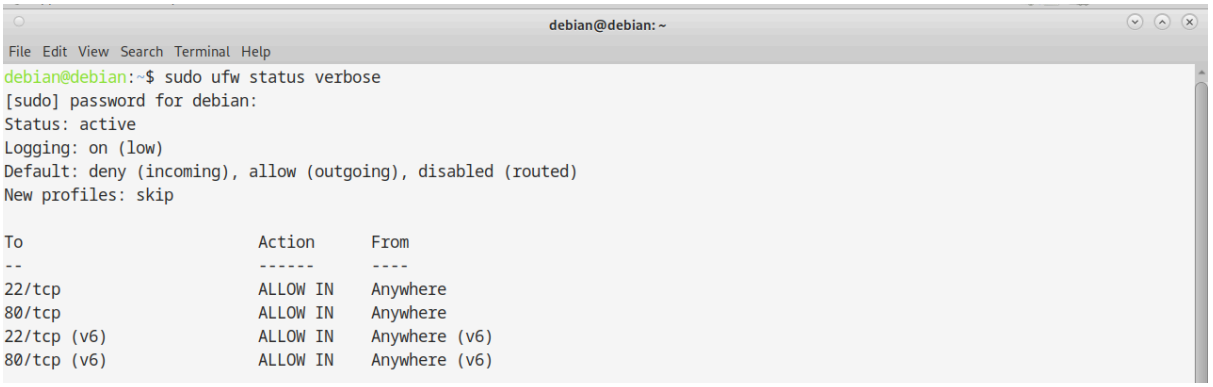
sudo ufw default allow outgoing

sudo ufw allow 22/tcp

sudo ufw allow 80/tcp

sudo ufw enable

sudo ufw status verbose



8. Escaneo de malware y rootkits

Como parte del análisis de seguridad, se realizó un escaneo del sistema para detectar malware o rootkits utilizando la herramienta rkhunter.

```
[Press <ENTER> to continue]



System checks summary
=====================

File properties checks...
    Files checked: 144
    Suspect files: 1

Rootkit checks...
    Rootkits checked : 497
    Possible rootkits: 5

Applications checks...
    All checks skipped

The system checks took: 6 minutes and 11 seconds

All results have been written to the log file: /var/log/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)
```

El escaneo no detectó rootkits activos. Únicamente se generaron advertencias menores que fueron revisadas manualmente.

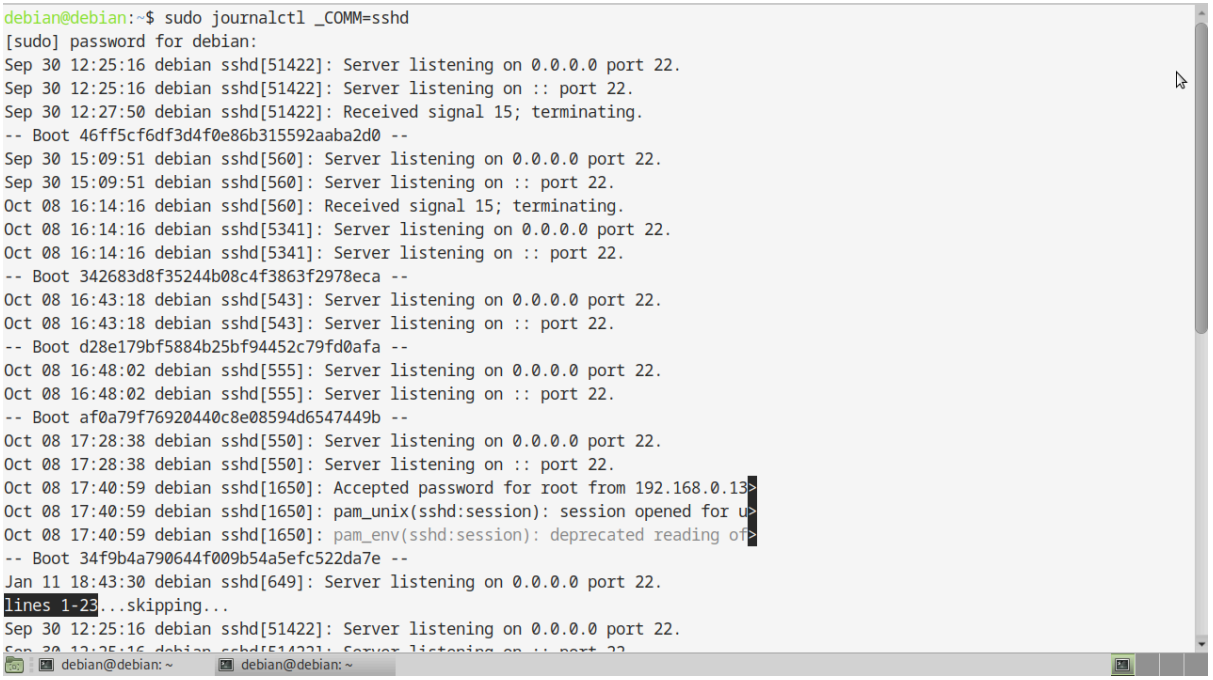
```
[09:15:56] Running Rootkit Hunter version 1.4.6 on debian
[09:15:56]
[09:15:56] Info: Start date is Mon Jan 12 09:15:56 AM EST 2026
[09:15:56]
[09:15:56] Checking configuration file and command-line options...
[09:15:56] Info: Detected operating system is 'Linux'
[09:15:56] Info: Found O/S name: Debian GNU/Linux 12 (bookworm)
[09:15:56] Info: Command line is /usr/bin/rkhunter --check
[09:15:56] Info: Environment shell is /bin/bash; rkhunter is using dash
[09:15:56] Info: Using configuration file '/etc/rkhunter.conf'
[09:15:56] Info: Installation directory is '/usr'
[09:15:56] Info: Using language 'en'
[09:15:56] Info: Using '/var/lib/rkhunter/db' as the database directory
[09:15:56] Info: Using '/usr/share/rkhunter/scripts' as the support script direc
tory
[09:15:56] Info: Using '/usr/local/sbin /usr/local/bin /usr/sbin /usr/bin /sbin
/bin /usr/libexec' as the command directories
[09:15:56] Info: Using '/var/lib/rkhunter/tmp' as the temporary directory
[09:15:56] Info: No mail-on-warning address configured
[09:15:56] Info: X will be automatically detected
[09:15:56] Info: Using second color set
[09:15:56] Info: Found the 'basename' command: /usr/bin/basename
[09:15:56] Info: Found the 'diff' command: /usr/bin/diff
/var/log/rkhunter.log
```

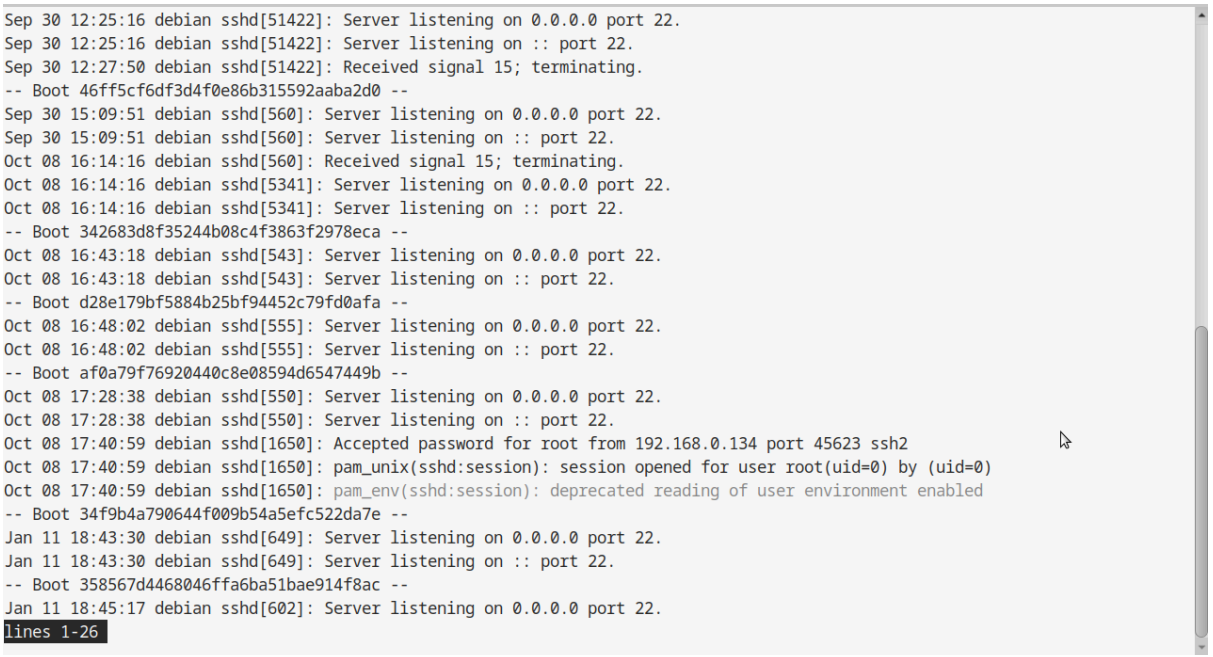
9. Análisis forense de logs del sistema

Durante el análisis forense se observó que el servidor utiliza systemd-journal en lugar de los archivos clásicos como auth.log.

```
debian@debian: ~
File  Edit  View  Search  Terminal  Help
debian@debian:~$ ls /var/log
alternatives.log    boot.log.2  dpkg.log.1      lastlog       speech-dispatcher
alternatives.log.1  boot.log.3  exim4           lightdm       vsftpd.log
apache2             btmp        faillog         private       wtmp
apt                 btmp.1      fontconfig.log  README        Xorg.0.log
boot.log            cups        installer       rkhunter.log  Xorg.0.log.old
boot.log.1          dpkg.log    journal         runit
debian@debian:~$ cat /var/log/README
You are looking for the traditional text log files in /var/log, and they are
gone?

Here's an explanation on what's going on:

You are running a systemd-based OS where traditional syslog has been replaced
with the Journal. The journal stores the same (and more) information as classic
syslog. To make use of the journal and access the collected log data simply
invoke "journalctl", which will output the logs in the identical text-based
format the syslog files in /var/log used to be. For further details, please
refer to journalctl(1).

Alternatively, consider installing one of the traditional syslog
implementations available for your distribution, which will generate the
classic log files for you. Syslog implementations such as syslog-ng or rsyslog
may be installed side-by-side with the journal and will continue to function
the way they always did.

Thank you!
debian@debian: ~
```

Posteriormente, se analizaron los eventos relacionados con SSH usando journalctl





Durante el análisis forense de los registros del sistema mediante journalctl, se identificó un acceso exitoso a la cuenta root desde una dirección IP interna perteneciente al entorno.

Este acceso fue realizado de forma intencionada y controlada como parte de las pruebas, con el objetivo de verificar el comportamiento del servicio SSH y confirmar cómo se registran los eventos de autenticación en sistemas basados en systemd.

No se recomienda entrar con usuario root, se entró así en un entorno de prueba

10. Evaluación del incidente

No se encontraron evidencias de compromiso del sistema ni de malware activo. Sin embargo, se identificaron configuraciones inseguras que podrían haber sido explotadas en un entorno real, tales como:

- Servicios innecesarios activos (FTP)
- Permisos inseguros en archivos críticos
- Acceso SSH como root
- Falta inicial de firewall

Todas estas debilidades fueron corregidas durante el proyecto.

11. Conclusiones finales

El análisis realizado permitió identificar y corregir múltiples vulnerabilidades antes de que se convirtieran en incidentes reales. El servidor quedó correctamente asegurado mediante la reducción de servicios activos, la aplicación de un firewall, la corrección de permisos y el análisis forense de logs.

Este informe demuestra la importancia de aplicar buenas prácticas de seguridad, realizar auditorías periódicas y comprender el funcionamiento interno del sistema para una correcta respuesta ante incidentes.

12. Comandos utilizados durante el análisis

Escaneo de puertos y servicios:

sudo ss -tulnp

sudo ss -tulnp | grep :21

Revisión de configuración del servicio FTP:

sudo grep -E "^(anonymous_enable|local_enable|write_enable)" /etc/vsftpd.conf

Gestión del servicio FTP:

sudo systemctl stop vsftpd

sudo systemctl disable vsftpd

sudo systemctl status vsftpd

Revisión de permisos en archivos críticos:

ls -l /var/www/html/wp-config.php

sudo chmod 600 /var/www/html/wp-config.php

sudo chown www-data:www-data /var/www/html/wp-config.php

Revisión y aplicación de cambios en Apache:

sudo nano /etc/apache2/apache2.conf

sudo systemctl reload apache2

Configuración del firewall (UFW):

sudo ufw default deny incoming

sudo ufw default allow outgoing

sudo ufw allow 22/tcp

sudo ufw allow 80/tcp

sudo ufw enable

sudo ufw status verbose

Análisis de malware y rootkits:

sudo rkhunter --update

sudo rkhunter --check

sudo less /var/log/rkhunter.log

Análisis forense de logs del sistema:

ls /var/log

cat /var/log/README

sudo journalctl _COMM=sshd