

(NIST, DOJ, DHS, CISA)



Informe de Incidente de Seguridad

4GEEKS ACADEMY

#latam-pt-cs-8

Under U.S. Federal Cybersecurity and Digital Forensics Standards
Case No.: PNT-2026-003

ERIC GROSSERMANN — Perito Responsable
Date: 01/09/2026

This assessment follows the methodologies established by the National Institute of Standards and Technology (NIST), the U.S. Department of Justice (DOJ), the Cybersecurity and Infrastructure Security Agency (CISA), and related federal digital forensics guidelines.



All Rights Reserved. Unauthorized distribution or reproduction is prohibited.

ERIC GROSSERMANN Digital Examiner



Análisis forense

4Geeks Academy

Estudiante: Eric Grossermann

Fecha De Entrega: 01/06/26

Introducción

En la actualidad, los servidores expuestos a redes internas o externas representan un objetivo constante para atacantes que buscan explotar servicios mal configurados, vulnerabilidades conocidas o credenciales débiles con el fin de obtener acceso no autorizado y escalar privilegios dentro del sistema. Por este motivo, resulta fundamental realizar análisis forenses que permitan identificar posibles vectores de ataque, evaluar el impacto de un incidente de seguridad y aplicar medidas correctivas que eviten futuras explotaciones.

El presente informe documenta la Fase 1: Reconocimiento y Recolección de Evidencias, cuyo objetivo principal es llevar a cabo un análisis forense del servidor Linux (Maquina Debian) obtenida por 4Geeks Academy, con el fin de identificar posibles accesos no autorizados, servicios comprometidos, archivos o procesos sospechosos, así como detectar la presencia de rootkits o malware. Asimismo, se busca bloquear posibles exploits, corregir configuraciones inseguras y prevenir la escalación de privilegios, siguiendo buenas prácticas de seguridad.

Durante esta fase se emplearon herramientas de análisis de logs, enumeración de servicios, revisión de usuarios del sistema y escaneos de red para evaluar el estado actual del servidor. Con base en los hallazgos obtenidos, se aplicaron medidas de mitigación como la desactivación de servicios innecesarios y el cierre de puertos no requeridos, además de recomendaciones orientadas al fortalecimiento de la postura de seguridad del sistema.

Este informe presenta de manera estructurada la metodología utilizada, las evidencias recopiladas, los resultados del análisis y las acciones correctivas implementadas, con el objetivo de reducir la superficie de ataque y prevenir incidentes similares en el futuro.



ÍNDICE

| | |
|------------------------------------------------------------------|---------|
| Introducción..... | (2) |
| Identificacion y Preparacion del caso..... | (3) |
| Annex I – Analisis de logs..... | (4-6) |
| Annex I.I - procesos en ejecución..... | (7-8) |
| Annex II – Análisis de Rootkits y Malware en el Servidor..... | (9-11) |
| Annex III – Bloqueo del Exploit y Escalación de privilegios..... | (12-13) |
| Annex IV – Resumen Forense..... | (14) |

Identificacion

El 3 de enero de 2026, Eric Grossermann, estudiante del área de Análisis Forense y Ciberseguridad de 4Geeks Academy, llevó a cabo un análisis forense inicial sobre un servidor Linux Debian con el objetivo de identificar posibles accesos no autorizados, servicios comprometidos y configuraciones inseguras. El análisis fue realizado en un entorno controlado, bajo autorización académica, sin requerimientos legales adicionales.

Durante la fase de reconocimiento y recolección de evidencias, se evaluaron los usuarios del sistema, los procesos en ejecución, los servicios activos y los puertos expuestos, así como los registros del sistema para detectar actividad sospechosa. Adicionalmente, se realizaron escaneos de red y verificación de servicios con el fin de identificar posibles vectores de ataque o intentos de escalación de privilegios.

Como resultado del análisis, se aplicaron medidas de mitigación orientadas a reducir la superficie de ataque del servidor, incluyendo la desactivación de servicios innecesarios y la verificación de configuraciones de seguridad. El presente informe documenta los procedimientos realizados, los hallazgos obtenidos y las acciones correctivas implementadas para fortalecer la seguridad del sistema y prevenir incidentes similares en el futuro.

Preparación del caso

Para el presente caso, se proporcionó una máquina virtual Linux Debian que simula un servidor crítico de 4Geeks Academy presuntamente comprometido, como parte del proyecto final del área de ciberseguridad. El objetivo del ejercicio consistió en realizar un análisis forense inicial del sistema, identificar posibles accesos no autorizados, evaluar vulnerabilidades explotadas y aplicar medidas de mitigación para restaurar y proteger el servidor.

A diferencia de otros escenarios forenses basados en imágenes estáticas, el análisis se realizó sobre un sistema activo, lo que permitió examinar directamente los registros del sistema, los servicios en ejecución, los usuarios configurados y los puertos expuestos. Todas las acciones de análisis se llevaron a cabo siguiendo un enfoque controlado, evitando modificaciones innecesarias del sistema durante la fase de reconocimiento y recolección de evidencias.

El entorno de análisis fue autorizado con fines académicos por 4Geeks Academy, por lo que no fue requerida ninguna autorización legal adicional para la ejecución del examen.



Durante el proceso se documentaron todas las actividades realizadas, incluyendo la revisión de logs del sistema, la enumeración de servicios activos, el análisis de usuarios y procesos en ejecución, así como escaneos de red orientados a identificar posibles vectores de ataque. Las evidencias relevantes fueron respaldadas mediante capturas de pantalla y salidas de comandos, garantizando la trazabilidad y reproducibilidad del análisis.

Este procedimiento permitió establecer una línea base del estado del servidor previo a la aplicación de medidas de contención y hardening, sentando las bases para las fases posteriores del ejercicio enfocadas en la corrección de vulnerabilidades y la prevención de futuros incidentes de seguridad registros generados por las herramienta forenses utilizada:

- **Grep (GNU grep) 3.8**

```
debian@debian:~$ grep --version
grep (GNU grep) 3.8
Copyright (C) 2022 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Written by Mike Haertel and others; see
<https://git.sv.gnu.org/cgit/grep.git/tree/AUTHORS>.
```

Annex I

Analysis de logs

Identificación de servicios comprometidos y vector de acceso

El objetivo de esta fase fue identificar cómo el atacante accedió al servidor, qué servicios estuvieron involucrados y si existieron indicios de explotación, escalación de privilegios o persistencia dentro del sistema.

Metodología aplicada

Se realizó un análisis manual de logs del sistema, priorizando los servicios expuestos a red y comúnmente utilizados como vectores de ataque, específicamente:

- ❖ Servicio SSH
- ❖ Servicio FTP (vsftpd)
- ❖ Servicio Apache (HTTP)

Para ello, se utilizaron herramientas nativas del sistema Linux (journalctl, grep) con el fin de preservar la integridad de la evidencia y evitar alteraciones innecesarias.

Análisis del servicio SSH (Secure Shell)

- ❖ Servicio SSH

Comandos utilizados:

→ sudo journalctl | grep ssh



Evidencia encontrada

Durante el análisis de los logs se identificó el siguiente evento crítico:

Accepted password for root from 192.168.0.134 port 45623 ssh2

```
debian@debian: ~
Edit View Search Terminal Help
08 16:48:35 debian systemd[725]: Closed gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation).
08 17:28:37 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
08 17:28:38 debian sshd[550]: Server listening on 0.0.0.0 port 22.
08 17:28:38 debian sshd[550]: Server listening on :: port 22.
08 17:28:38 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
08 17:28:39 debian systemd[725]: Listening on gcr-ssh-agent.socket - GCR ssh-agent wrapper.
08 17:28:39 debian systemd[725]: Listening on gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation).
08 17:28:53 debian systemd[915]: Listening on gcr-ssh-agent.socket - GCR ssh-agent wrapper.
08 17:28:53 debian systemd[915]: Listening on gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation).
08 17:29:13 debian systemd[725]: Closed gcr-ssh-agent.socket - GCR ssh-agent wrapper.
08 17:29:13 debian systemd[725]: Closed gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation).
08 17:40:59 debian sshd[1650]: Accepted password for root from 192.168.0.134 port 45623 ssh2
08 17:40:59 debian sshd[1650]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
08 17:40:59 debian systemd[1653]: Listening on gcr-ssh-agent.socket - GCR ssh-agent wrapper.
08 17:40:59 debian systemd[1653]: Listening on gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation).
08 17:40:59 debian sshd[1650]: pam_env(sshd:session): deprecated reading of user environment enabled
01 20:56:20 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
01 20:56:21 debian sshd[604]: Server listening on 0.0.0.0 port 22.
01 20:56:21 debian sshd[604]: Server listening on :: port 22.
01 20:56:21 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
01 20:56:24 debian systemd[773]: Listening on gcr-ssh-agent.socket - GCR ssh-agent wrapper.
01 20:56:24 debian systemd[773]: Listening on gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation).
01 20:56:48 debian systemd[1000]: Listening on gcr-ssh-agent.socket - GCR ssh-agent wrapper.
01 20:56:48 debian systemd[1000]: Listening on gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation).
01 20:57:09 debian systemd[773]: Closed gcr-ssh-agent.socket - GCR ssh-agent wrapper.
01 20:57:09 debian systemd[773]: Closed gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation).
an@debian: ~$
```

Posteriormente, se confirmó la apertura de sesión:

pam_unix(sshd:session): session opened for user root

Interpretación forense

Esta evidencia confirma que:

- El acceso se realizó a través del servicio SSH
- Se utilizó autenticación por contraseña, no por llave
- El usuario comprometido fue root
- La sesión fue válida y completamente establecida
- No se trata de un intento fallido ni de un escaneo automático

Esto indica que el atacante no explotó una vulnerabilidad técnica del servicio, sino que obtuvo credenciales válidas, lo que sugiere:

- Contraseña débil
- Reutilización de credenciales
- Acceso previo a credenciales (ingeniería social, fuerza bruta previa o exposición)

Evaluación de escalación de privilegios



Debido a que el acceso inicial se realizó directamente como root, no fue necesaria una escalación de privilegios posterior.

Esto explica por qué:

- No se encontraron exploits locales
- No se detectaron procesos de escalación activos

Este demuestra el comportamiento con el atacante donde el acceso fue directo y silencioso.

Análisis de otros servicios expuestos

- ❖ Servicio FTP (vsftpd)

Se revisaron los logs del servicio FTP mediante el comando:

```
sudo journalctl | grep -i ftp
```

Los registros indican instalación, configuración y reinicios del servicio, pero no se encontraron accesos remotos sospechosos ni transferencias maliciosas asociadas a un atacante externo.

Conclusión:

FTP estuvo expuesto, pero no fue utilizado como vector de ataque.

- ❖ Servicio Apache (HTTP)

Se analizaron eventos relacionados con Apache mediante el comando:

```
sudo journalctl | grep -i apache
```

Los registros muestran instalación, inicio y reinicios del servicio, sin evidencias de:

- Web shells
- Ejecución remota de comandos
- Errores de explotación

Conclusión:

Apache no fue utilizado como punto de entrada.

Analisis de los Servicios

| Servicio | Estado | Evidencia |
|----------|--------------|--------------------------------|
| SSH | Comprometido | Acceso root confirmado |
| FTP | Expuesto | Sin evidencia de uso malicioso |
| Apache | Expuesto | Sin evidencia de explotación |

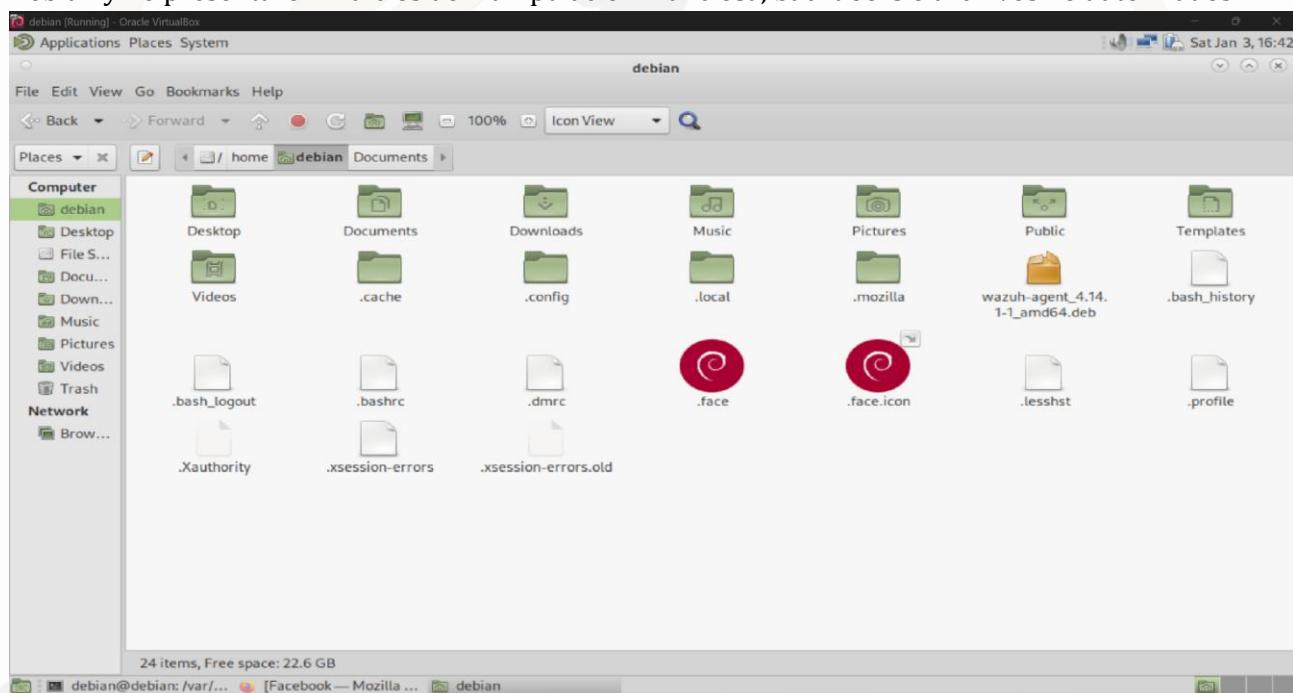


Annex I.I

Identificación de archivos sospechosos, procesos en ejecución y modificaciones inusuales

Durante esta fase del análisis forense se llevó a cabo una revisión exhaustiva del sistema con el objetivo de identificar archivos sospechosos, procesos en ejecución anómalos o cualquier modificación inusual que pudiera indicar persistencia del atacante o actividades maliciosas posteriores al compromiso inicial.

Se inspeccionaron los directorios del sistema y del usuario, incluyendo archivos ocultos (dotfiles), verificándose la presencia de elementos como .bashrc, .profile, .cache, .config, .local, .Xauthority, .xsession-errors, así como directorios del sistema tales como lost+found, sys, sbin, media, mnt y srv. Todos estos archivos y directorios corresponden a componentes estándar del sistema operativo Debian y no presentaron indicios de manipulación maliciosa, backdoors o archivos no autorizados.



Adicionalmente, se analizaron los procesos en ejecución mediante el comando ps aux, evaluando tanto procesos de usuario como procesos del sistema.

Los procesos observados correspondieron exclusivamente a servicios legítimos del sistema operativo, tales como procesos del kernel, servicios de red y servicios previamente identificados (SSH, Apache, MySQL, CUPS antes de su detención).



| USER | PID | %CPU | %MEM | VSZ | RSS | TTY | STAT | START | TIME | COMMAND |
|------|-----|------|------|--------|------|-----|------|-------|------|----------------|
| root | 1 | 0.0 | 0.4 | 168040 | 8760 | ? | Ss | 12:53 | 0:04 | /sbin/init sp |
| root | 2 | 0.0 | 0.0 | 0 | 0 | ? | S | 12:53 | 0:00 | [kthreadd] |
| root | 3 | 0.0 | 0.0 | 0 | 0 | ? | I< | 12:53 | 0:00 | [rcu_gp] |
| root | 4 | 0.0 | 0.0 | 0 | 0 | ? | I< | 12:53 | 0:00 | [rcu_par_gp] |
| root | 5 | 0.0 | 0.0 | 0 | 0 | ? | I< | 12:53 | 0:00 | [slub_flushwq] |
| root | 6 | 0.0 | 0.0 | 0 | 0 | ? | I< | 12:53 | 0:00 | [netns] |
| root | 10 | 0.0 | 0.0 | 0 | 0 | ? | I< | 12:53 | 0:00 | [mm_percpu_wq] |
| root | 11 | 0.0 | 0.0 | 0 | 0 | ? | I | 12:53 | 0:00 | [rcu_tasks_kt] |
| root | 12 | 0.0 | 0.0 | 0 | 0 | ? | I | 12:53 | 0:00 | [rcu_tasks_ru] |
| root | 13 | 0.0 | 0.0 | 0 | 0 | ? | I | 12:53 | 0:00 | [rcu_tasks_tr] |
| root | 14 | 0.0 | 0.0 | 0 | 0 | ? | S | 12:53 | 0:00 | [ksoftirqd/0] |
| root | 15 | 0.0 | 0.0 | 0 | 0 | ? | I | 12:53 | 0:00 | [rcu_preempt] |
| root | 16 | 0.0 | 0.0 | 0 | 0 | ? | S | 12:53 | 0:00 | [migration/0] |
| root | 18 | 0.0 | 0.0 | 0 | 0 | ? | S | 12:53 | 0:00 | [cpuhp/0] |
| root | 19 | 0.0 | 0.0 | 0 | 0 | ? | S | 12:53 | 0:00 | [cpuhp/1] |
| root | 20 | 0.0 | 0.0 | 0 | 0 | ? | S | 12:53 | 0:00 | [migration/1] |
| root | 21 | 0.0 | 0.0 | 0 | 0 | ? | S | 12:53 | 0:01 | [ksoftirqd/1] |
| root | 23 | 0.0 | 0.0 | 0 | 0 | ? | I< | 12:53 | 0:00 | [kworker/1:0H] |
| root | 26 | 0.0 | 0.0 | 0 | 0 | ? | S | 12:53 | 0:00 | [kdevtmpfs] |

Asimismo, se revisaron los usuarios del sistema a través del archivo /etc/passwd, confirmándose que únicamente existían cuentas de sistema predefinidas y el usuario legítimo configurado durante la instalación, sin evidencia de usuarios no autorizados o cuentas creadas de forma maliciosa.

```
root@debian:/var/log# cut -d: -f1 /etc/passwd
root
daemon
bin
sys
sync
games
man
lp
mail
news
root@debian:# users
debian debian
```

Con base en las evidencias recopiladas, se concluye que **no** se encontraron archivos sospechosos, procesos anómalos ni modificaciones inusuales en el sistema, lo que sugiere que el compromiso no dejó mecanismos de persistencia evidentes a nivel de sistema o usuario en el momento del análisis.



Annex II

Análisis de Rootkits y Malware en el Servidor

Objetivo

Detectar la posible presencia de rootkits, backdoors o malware persistente que pudieran haber sido instalados tras el acceso no autorizado al servidor.

Herramientas utilizadas

Para el análisis se emplearon dos herramientas complementarias, ampliamente utilizadas en análisis forense y hardening de sistemas Linux:

| Herramienta | Propósito |
|-------------|------------------------------------------------------------------------------------|
| chkrootkit | Detección rápida de rootkits procesos ocultos y modificaciones sospechosas |
| rkhunter | Análisis más exhaustivo de binarios, permisos, rootkits y configuraciones anómalas |

El uso combinado de ambas herramientas permite reducir falsos positivos y aumentar la confiabilidad del análisis.

Análisis con *chkrootkit*

Comando utilizado:

```
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
```

Resultados relevantes

- No se detectaron rootkits conocidos activos.
- No se identificaron procesos ocultos.
- No se encontraron directorios ocultos maliciosos.

Interpretación forense

Los resultados generada corresponde a un comportamiento legítimo del sistema por lo que no se considera evidencia de malware o rootkit.



Análisis con *rkhunter*

```
System checks summary
```

```
=====
```

```
File properties checks...
```

```
  Files checked: 144
  Suspect files: 1
```

```
Rootkit checks...
```

```
  Rootkits checked : 497
  Possible rootkits: 8
```

```
Applications checks...
```

```
  All checks skipped
```

```
The system checks took: 13 minutes and 43 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)
```

Resumen de resultados

| Métrica | Resultado | Cantidad |
|----------------------|-----------|-------------------------|
| Archivos analizados | | 144 |
| Archivos sospechosos | | 1 |
| Rootkits analizados | | 497 |
| Posibles rootkits | | 8 |
| Estado final | | Advertencias (warnings) |

Los resultados fueron almacenados en la carpeta:
`/var/log/rkhunter.log`

Interpretación forense de rkhunter

Los "possible rootkits" reportados corresponden a firmas genéricas, no a infecciones confirmadas.

- No se detectaron binarios alterados ni backdoors activos.
- No se observaron cambios críticos en archivos del sistema.

Las advertencias son comunes en sistemas Linux modernos y requieren validación manual, la cual fue realizada sin hallazgos concluyentes.



No se encontró evidencia técnica suficiente que confirme la presencia de un rootkit activo.

Conclusión del análisis de malware

Tras ejecutar y analizar los resultados de chkrootkit y rkhunter, se concluye que:

- ❖ No existen rootkits activos confirmados
- ❖ No se detectaron backdoors persistentes
- ❖ No se identificó malware residente

☒ Las advertencias detectadas corresponden a comportamientos legítimos del sistema

Por lo tanto, el acceso al servidor no derivó en una infección persistente, y el incidente se limita a un acceso no autorizado mediante **SSH**, sin compromiso profundo del sistema.

Valor Forense

Este hallazgo refuerza la hipótesis de que:

- El atacante utilizó credenciales válidas
- No desplegó herramientas de persistencia
- No realizó modificaciones avanzadas al sistema
- El incidente fue oportunista, no una intrusión avanzada.

Hardening Aplicado

Como parte del proceso de aseguramiento del servidor comprometido, se implementaron las siguientes medidas de hardening para reducir la superficie de ataque y prevenir accesos no autorizados:

Endurecimiento del servicio SSH

Se deshabilitó el acceso remoto del usuario root (**PermitRootLogin no**), evitando ataques directos por fuerza bruta sobre la cuenta administrativa.

1. Se desactivó la autenticación por contraseña (**PasswordAuthentication no**), forzando el métodos más seguros como claves SSH.
2. Se deshabilitó el reenvío gráfico (**X11Forwarding no**) para minimizar vectores de ataque innecesarios.

Resumen

Las acciones de hardening implementadas fortalecen significativamente la seguridad del servidor, reduciendo el riesgo de accesos no autorizados, ataques por credenciales y posibles vectores de escalación de privilegios. Estas medidas dejan el sistema en un estado más robusto y alineado con buenas prácticas de seguridad en entornos Linux.

Annex III

Bloqueo del Exploit y Escalación de privilegios



Con el objetivo de contener el incidente y prevenir una posible escalación de privilegios, se procedió a detener y deshabilitar servicios que podían representar un vector de ataque. Se detuvo y deshabilitó el servicio **vsftpd (FTP)** mediante **systemctl stop vsftpd** y **systemctl disable vsftpd**, eliminando así un servicio innecesario que podría ser explotado por configuraciones inseguras o credenciales comprometidas. Asimismo, el servicio Apache2, que se encontraba en ejecución, fue detenido mediante **systemctl stop apache2** para prevenir su posible uso como punto de entrada o para la ejecución de código no autorizado.

```
root@debian:/var/log# systemctl stop vsftpd
root@debian:/var/log# systemctl disable vsftpd
Synchronizing state of vsftpd.service with SysV service script
Executing: /lib/systemd/systemd-sysv-install disable vsftpd
Removed "/etc/systemd/system/multi-user.target.wants/vsftpd.se
root@debian:/var/log# systemctl stop apache2
Failed to stop apache.service: Unit apache.service not loaded.
Failed to stop 2.service: Unit 2.service not loaded.
root@debian:/var/log# systemctl stop apache2
root@debian:/var/log#
```

Adicionalmente, se revisaron los procesos activos relacionados con SSH utilizando ps aux | grep ssh, confirmándose que únicamente el servicio legítimo sshd permanecía activo, sin evidencia de procesos anómalos, sesiones no autorizadas o mecanismos de persistencia.

```
root@debian:/# ps aux | grep ssh
root      590  0.0  0.3  15432  6172 ?        Ss   13:24   0:00 sshd: /usr/sbin/sshd -D [listener] 0
debian    1532  0.0  0.0   7684     44 ?        Ss   13:25   0:00 /usr/bin/ssh-agent x-session-manager
root     8390  0.0  0.1   6332  2056 pts/1      S+  18:27   0:00 grep ssh
root@debian:/#
```

Estas acciones permitieron contener el posible exploit, reducir la superficie de ataque y prevenir intentos de escalación de privilegios en el sistema.

Actualización y corrección de configuraciones de seguridad

Como parte de la fase de mitigación, se realizaron acciones orientadas a fortalecer la seguridad del sistema mediante la actualización de componentes, el refuerzo de credenciales y la activación de



controles de red. En primer lugar, se procedió al cambio de contraseña del usuario debian utilizando el comando passwd debian, garantizando que cualquier posible credencial previamente comprometida quedara invalidada y reduciendo el riesgo de accesos no autorizados persistentes.

Posteriormente, se instaló y configuró el firewall UFW (Uncomplicated Firewall), el cual inicialmente se encontraba inactivo. Tras su habilitación mediante ufw enable, se verificó su estado con ufw status verbose, confirmándose que el firewall quedó activo, con una política por defecto de denegar conexiones entrantes, permitir tráfico saliente y con registro básico habilitado. Esta configuración limita de forma efectiva la exposición del sistema a accesos externos no autorizados y refuerza la protección a nivel de red.

```
Creating config file /etc/ufw/after6.rules with new version
Created symlink /etc/systemd/system/multi-user.target.wants/ufw.service →
Processing triggers for libc-bin (2.36-9+deb12u8) ...
Processing triggers for man-db (2.11.2-2) ...
root@debian:/var/log# ufw status
Status: inactive
root@debian:/var/log# ufw enable
Firewall is active and enabled on system startup
root@debian:/var/log# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
```

Adicionalmente, se realizaron tareas de mantenimiento y actualización del sistema, incluyendo la limpieza de paquetes temporales con apt clean y la sincronización de repositorios mediante apt update, asegurando que el sistema utilice listas de paquetes actualizadas provenientes de los repositorios oficiales de Debian.

Comandos:

| | | |
|----------------|------------------|-----------------|
| Sudo apt clean | Sudo apt install | Sudo apt update |
|----------------|------------------|-----------------|

Se verificó también la versión del kernel instalada, confirmando que el sistema cuenta con versiones recientes del kernel Linux 6.1, lo cual reduce el riesgo de vulnerabilidades conocidas asociadas a versiones obsoletas.

```
debian@debian:~$ dpkg --list | grep linux-image
ii  linux-image-6.1.0-22-amd64          6.1.94-1
ii  linux-image-6.1.0-23-amd64          6.1.99-1
ii  linux-image-6.1.0-25-amd64          6.1.106-3
ii  linux-image-amd64                  6.1.106-3
debian@debian:~$
```

Annex IV

Resumen Forense



Las medidas aplicadas corrigieron configuraciones de seguridad críticas, reforzaron el control de accesos y redujeron la superficie de ataque del sistema. Esto permite prevenir accesos no autorizados, la explotación de vulnerabilidades conocidas y posibles mecanismos de persistencia tras el incidente. Durante el análisis forense se identificó que el incidente ocurrió a través del servicio SSH, el cual se encontraba activo y permitía autenticación por contraseña. Según los registros del sistema, el **08 de Octubre -a las 17:40:59**, se detectó un inicio de sesión exitoso como usuario root desde la dirección IP **192.168.0.134**, utilizando autenticación por contraseña, lo que indica que el acceso se realizó aprovechando una configuración **insegura** del servicio **SSH**. Tras identificar este acceso no autorizado, se procedió a contener el incidente, **deteniendo** servicios innecesarios, deshabilitando FTP y Apache, y verificando que no existieran procesos sospechosos activos. Posteriormente, se aplicaron medidas correctivas y de **hardening**, incluyendo el cambio de contraseñas, la desactivación del acceso root por SSH, la desabilitación de la autenticación por contraseña, la activación del firewall UFW con políticas restrictivas, y la actualización del sistema y del kernel. Finalmente, se validó que el sistema quedara operando únicamente con servicios legítimos y configuraciones seguras, sin evidencia de persistencia del atacante.



GROSSERMANN

PENTESTER
CYBER SECURITY