

Informe de Pentesting del Servidor Debian

Identificación y explotación de vulnerabilidades

Autor:

Alejandro Winter

Contenido:

Este documento recoge los resultados del escaneo de seguridad, las vulnerabilidades encontradas y su validación mediante pruebas prácticas.

INFORME DE SUPERFICIE DE ATAQUE Y EXPLOTACIÓN DE SERVICIOS

Para verificar un **reconocimiento completo** de todo el servidor **comprometido**, he usado **tres herramientas** proporcionadas por la **VM Kali Linux**. Las **vulnerabilidades** de **WordPress, FTP y Apache** no fueron necesariamente utilizadas por el **atacante identificado** en la Fase 1, pero fueron **descubiertas** mediante pentesting para evaluar otros vectores que habrían permitido comprometer el sistema.

-Nmap

Se realizó un escaneo de puertos y servicios mediante Nmap con el fin de identificar los servicios expuestos y sus versiones, detectando servicios como FTP, SSH y HTTP accesibles desde la red.

```
[kali㉿kali]:~$ sudo nmap -sS -sV -sC -O -p 21,22,80 192.168.151.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-15 13:19 EST
Nmap scan report for 192.168.151.3
Host is up (0.002s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_ STAT:
|   FTP server status:
|     Connected to ::ffff:192.168.151.10
|     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
```

Hallazgos clave de riesgo alto:

Puerto 21 – FTP (vsftpd 3.0.3)

Anonymous FTP login allowed
Control connection is plain text

¿Por qué es grave?

- Acceso **anónimo sin credenciales**
- Transferencia en **texto plano**
- Robo de información
- Subida de ficheros maliciosos
- Enumeración del sistema

Se detectó el servicio **FTP (vsftpd 3.0.3)** con acceso anónimo habilitado y sin cifrado, lo que supone un riesgo elevado al permitir el acceso no autenticado y la posible exposición o manipulación de archivos.

Puerto 22 – SSH (OpenSSH 9.2p1)

- Servicio actualizado
- Claves modernas (ECDSA / ED25519)

No es vulnerable por sí solo, pero:

- Está expuesto a red
- Puede ser objetivo de fuerza bruta

```
22/tcp open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
| 256 aa:f8:39:b3:ce:e6:3a:c9:60:79:bc:6c:06:47:ff:5a (ECDSA)
| 256 43:ca:a9:c9:31:7b:82:d9:03:ff:40:f2:a3:71:40:83 (ED25519)
```

Aunque la versión de **OpenSSH** y los algoritmos criptográficos eran modernos, la configuración de autenticación era **insegura**, ya que permitía el login del **usuario root** mediante contraseña. Esta política **expuso** el servicio a ataques de fuerza bruta o credenciales comprometidas y fue el vector utilizado en el incidente analizado.

Puerto 80 – HTTP (Apache 2.4.62)

```
80/tcp open http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_ http-robots.txt: 1 disallowed entry
|_ /wp-admin/
|_ http-title: Apache2 Debian Default Page: It works
MAC Address: 08:00:27:35:1A:50 (PCS Systemtechnik/Oracle VirtualBox virt NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results
https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 25.11 seconds
```

Hallazgo:

- Página por defecto activa
- robots.txt presente
- Rastro de WordPress
- Ruta /wp-admin/ detectada

Riesgo medio-alto

Apache por defecto + WordPress = **superficie de ataque amplia**.

Whatweb

Mediante WhatWeb se realizó un fingerprinting del servicio web con el objetivo de identificar tecnologías y configuraciones que pudieran suponer una superficie de ataque.

Resultado:

Apache/2.4.62 (Debian)
Apache2 Debian Default Page

```
(kali㉿kali)-[~]
$ whatweb http://192.168.151.3

http://192.168.151.3 [200 OK] Apache[2.4.62], Country[RESERVED][ZZ], HTT
ver[Debian Linux][Apache/2.4.62 (Debian)], IP[192.168.151.3], Title[Apac
Debian Default Page: It works]
```

Aunque el riesgo sea **bajo**, es **importante** porque revela el **software exacto**, facilita la búsqueda de **exploits** y confirma el entorno por defecto.

Nikto

Se ejecutó Nikto para la detección de vulnerabilidades conocidas en el servidor web, identificando posibles configuraciones inseguras y validando el nivel de exposición del servicio.

```
(kali㉿kali)-[~]
$ nikto -h http://192.168.151.3

- Nikto v2.5.0
+ Target IP:      192.168.151.3
+ Target Hostname: 192.168.151.3
+ Target Port:     80
+ Start Time:     2025-12-15 13:22:17 (GMT-5)

+ Server: Apache/2.4.62 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: h
://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the
agent to render the content of the site in a different fashion to the M
type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerab
les/missing-content-type-header/
+ /KtYY4LP.pldir: Drupal Link header found with value: <http://localho
ndex.php/wp-json/>; rel="https://api.w.org/". See: https://www.drupal.or
```

Nikto encontró:

- /wp-login.php
- /wp-admin/
- /wp-content/uploads/ **indexable**
- wp-app.log
- license.txt
- Headers típicos de WordPress

WordPress está instalado y expuesto, aunque no se vea en la página principal.

Directory listing en uploads

/wp-content/uploads/: Directory indexing found

Riesgo alto

Para validar la explotación de esta vulnerabilidad, se accedió al directorio

/wp-content/uploads/, comprobando que era posible listar y descargar archivos sin autenticación.

```
index.php/wp-json/>; rel="https://api.w.org/". See: https://www.drupal.org/KtYYg4LP.: Uncommon header 'x-redirect-by' found, with contents: Word
s.
+ No CGI Directories found (use '-C all' to force check all possible dir
+ /robots.txt: contains 2 entries which should be manually viewed. See:
s://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /: Server may leak inodes via ETags, header found with file /, inode:
, size: 623573d915b52, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cv
e.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ /wp-links-opml.php: This WordPress script reveals the installed versio
+ /license.txt: License file found may identify site software.
+ /wp-app.log: Wordpress' wp-app.log may leak application/system details
+ /wordpress/wp-app.log: Wordpress' wp-app.log may leak application/syst
etails.
+ /wordpress/: A Wordpress installation was found.
+ /wp-login.php?action=register: Cookie wordpress_test_cookie created wi
t the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/H
Cookies
+ /wp-content/uploads/: Directory indexing found.
+ /wp-content/uploads/: Wordpress uploads directory is browsable. This m
eveal sensitive information.
+ /wp-login.php: Wordpress login found.
+ 8106 requests: 0 error(s) and 16 item(s) reported on remote host
+ End Time: 2025-12-15 13:31:16 (GMT-5) (539 seconds)
+ 1 host(s) tested
```

Se identificaron archivos subidos previamente, confirmando una exposición directa de datos y la posibilidad de obtener backups, imágenes o ficheros con metadatos sensibles.

Headers de seguridad ausentes

Faltan:

X-Frame-Options, X-Content-Type-Options, Cookies sin HttpOnly.

Esto permite:

Clickjacking, MIME sniffing, Robo de cookies.

El escaneo con **Nikto** reveló la presencia de una instalación de WordPress expuesta, junto con múltiples configuraciones inseguras como directorios navegables, ausencia de cabeceras de seguridad y posibles fugas de información, aumentando significativamente la superficie de ataque del sistema.

Tras revisar las **respuestas** de ambos comandos e intentar detectar algún archivo sospechoso, proceso en ejecución o cualquier modificación inusual en el sistema, carecen de algún significado relevante pues son procesos normales del sistema

- ✓ No existen backdoors.
 - ✓ No existen shells añadidas.
 - ✓ No existe malware persistente.
 - ✓ No hay modificaciones del atacante.

```
File Edit View Search Terminal Help
auto mode
Processing triggers for man-db (2.11.2-2) ...
Processing triggers for libc-bin (2.36-9+deb12u13) ...
debian@debian:~$ sudo chkrootkit
ROOTDIR is '/'
Checking `and'...
Checking `basename'...
Checking `biff'...
Checking `chfn'...
Checking `chsh'...
Checking `cron'...
Checking `crontab'...
Checking `date'...
Checking `du'...
Checking `dirname'...
Checking `echo'...
Checking `egrep'...
Checking `env'...
Checking `find'...
Checking `fingerprint'...
Checking `gpm'...
Checking `grep'...
Checking `hdparm'...
Checking `su'...
not found
not infected
not found
not infected
not found
not found
not infected
not found
not infected
```

-Realizaremos un escaneo del servidor para detectar rootkits o malware.

Chkrootkit no reportó evidencia de rootkits conocidos. Esto **reduce la probabilidad** de compromiso persistente, aunque no lo descarta, por lo que se recomienda complementar con revisión de integridad, logs y monitoreo.

Únicamente se reportaron dos advertencias:

Un directorio oculto asociado a LibreOffice (`/usr/lib/libreoffice/share/.registry`), considerado legítimo tras su revisión.

Un aviso de interfaz en modo promiscuo gestionada por **NetworkManager**, atribuible a la propia configuración de red de la máquina virtual.

No se han detectado binarios del sistema modificados ni procesos ocultos.