Fase 1. Reconocimiento y recolección de evidencias

Reporte de Análisis Forense: Detección de Vulnerabilidades

Introducción

Este reporte documenta el análisis forense realizado sobre una máquina comprometida con el objetivo de identificar vulnerabilidades explotadas y evidencias relacionadas con actividades maliciosas. A pesar de no determinar cómo el atacante comprometió inicialmente el sistema, se recopilaron numerosos indicios de actividades sospechosas que se detallan a continuación. Este documento incluye evidencias específicas encontradas y secciones detalladas para proporcionar un análisis completo del incidente.

---

1. Reconocimiento y Recolección de Evidencias

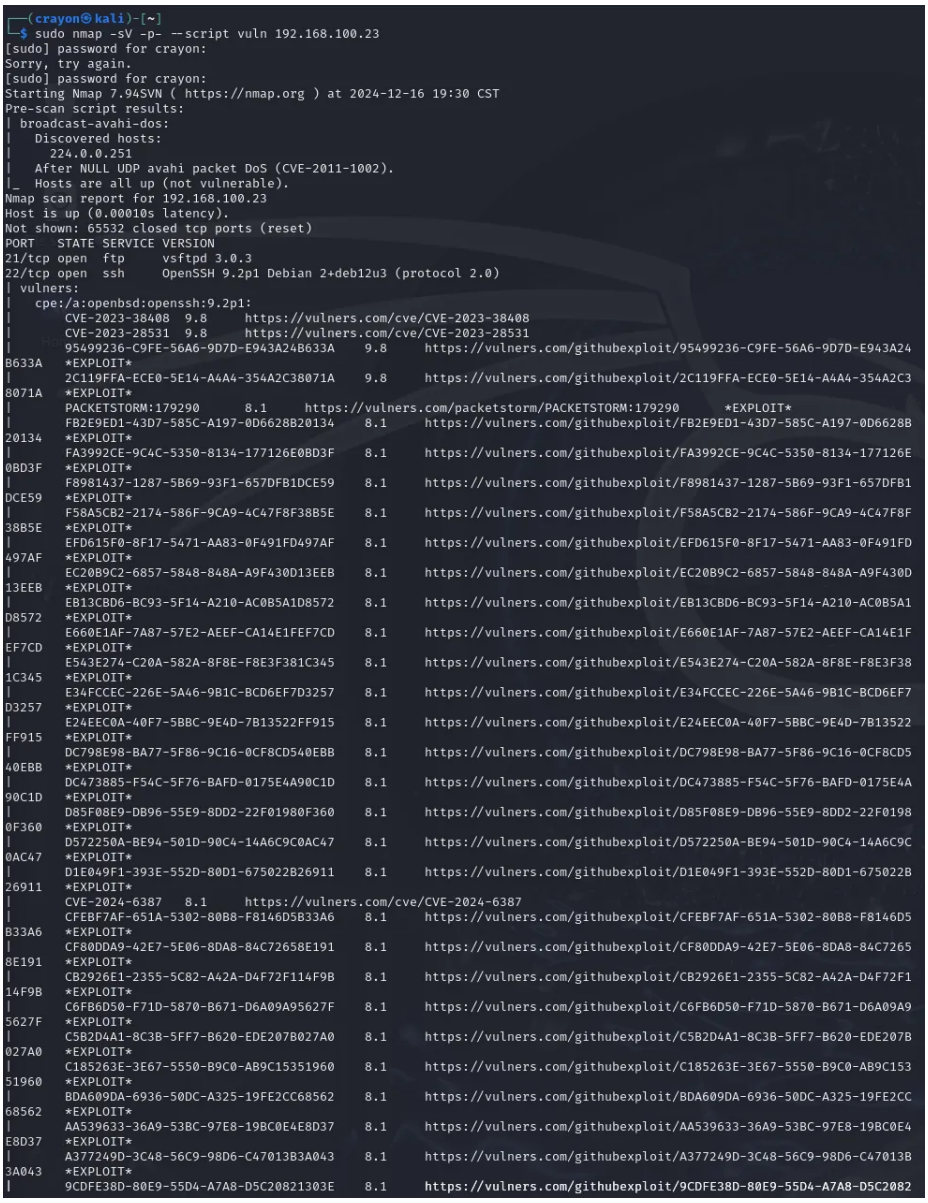
1.1 Análisis con Nmap

Se ejecutó el comando `sudo nmap -sV -p- --script vuln 192.168.100.23` para obtener una evaluación completa de los servicios y puertos expuestos en la máquina objetivo. Este escaneo permite identificar tanto las versiones de los servicios en ejecución como las vulnerabilidades conocidas asociadas. Las principales tareas realizadas incluyeron:

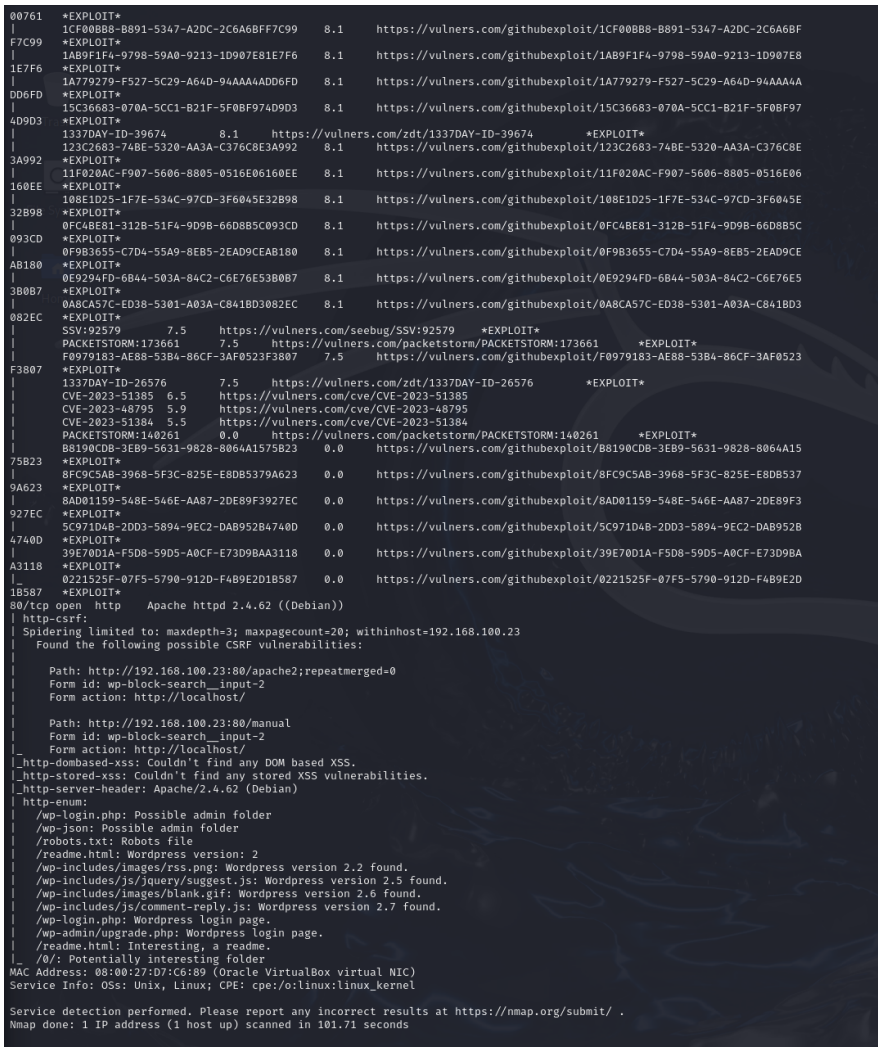
1. **Detección de versiones de servicios:** Esto permite asociar las versiones encontradas con vulnerabilidades conocidas y parches disponibles.
2. **Escaneo de todos los puertos abiertos:** Este enfoque garantiza que ningún servicio quede fuera del alcance del análisis.
3. **Uso de scripts para identificar vulnerabilidades conocidas:** Los scripts de Nmap son herramientas poderosas que automatizan la detección de problemas de seguridad comunes.

Principales hallazgos del escaneo:

- **Puertos abiertos y versiones detectadas:**
  - FTP (vsftpd 3.0.3) en el puerto 21/tcp: Se identificó una versión vulnerable que ha estado asociada con problemas de seguridad en el pasado. Esto representa un riesgo significativo, especialmente si las configuraciones por defecto no se han ajustado.
  - SSH (OpenSSH 9.2p1): Esta versión presenta vulnerabilidades críticas, incluyendo ejecución remota de código (CVE-2023-38408), lo que la convierte en un objetivo principal para atacantes.
  - HTTP (Apache HTTPD 2.4.62): La configuración detectada expone al servidor a ataques como CSRF y XSS, lo que podría permitir el robo de información o la manipulación de datos del usuario.



```
┌──(crayon㉿kali)-[~]
└─$ sudo nmap -sV -p- --script vuln 192.168.100.23
[sudo] password for crayon:
Sorry, try again.
[sudo] password for crayon:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 19:30 CST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.100.23
Host is up (0.00010s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:9.2p1:
|       CVE-2023-38408  9.8     https://vulners.com/cve/CVE-2023-38408
|       CVE-2023-28531  9.8     https://vulners.com/cve/CVE-2023-28531
|       95499236-C9FE-56A6-9D7D-E943A24B633A    9.8     https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24
B633A   *EXPLOIT*
|       2C119FFA-ECE0-5E14-A4A4-354A2C38071A    9.8     https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C3
8071A   *EXPLOIT*
|       PACKETSTORM:179290      8.1     https://vulners.com/packetstorm/PACKETSTORM:179290      *EXPLOIT*
|       FB2E9ED1-43D7-585C-A197-0D6628B20134    8.1     https://vulners.com/githubexploit/FB2E9ED1-43D7-585C-A197-0D6628B
20134   *EXPLOIT*
|       FA3992CE-9C4C-5350-8134-177126E0BD3F    8.1     https://vulners.com/githubexploit/FA3992CE-9C4C-5350-8134-177126E
0BD3F   *EXPLOIT*
|       F8981437-1287-5B69-93F1-657DFB1DCE59    8.1     https://vulners.com/githubexploit/F8981437-1287-5B69-93F1-657DFB1
DCE59   *EXPLOIT*
|       F58A5CB2-2174-586F-9CA9-4C47F8F38B5E    8.1     https://vulners.com/githubexploit/F58A5CB2-2174-586F-9CA9-4C47F8F
38B5E   *EXPLOIT*
|       EFD615F0-8F17-5471-AA83-0F491FD497AF    8.1     https://vulners.com/githubexploit/EFD615F0-8F17-5471-AA83-0F491FD
497AF   *EXPLOIT*
|       EC20B9C2-6857-5848-848A-A9F430D13EEB    8.1     https://vulners.com/githubexploit/EC20B9C2-6857-5848-848A-A9F430D
13EEB   *EXPLOIT*
|       EB13CBD6-BC93-5F14-A210-AC0B5A1D8572    8.1     https://vulners.com/githubexploit/EB13CBD6-BC93-5F14-A210-AC0B5A1
D8572   *EXPLOIT*
|       E660E1AF-7A87-57E2-AEEF-CA14E1FEF7CD    8.1     https://vulners.com/githubexploit/E660E1AF-7A87-57E2-AEEF-CA14E1F
EF7CD   *EXPLOIT*
|       E543E274-C20A-582A-8F8E-F8E3F381C345    8.1     https://vulners.com/githubexploit/E543E274-C20A-582A-8F8E-F8E3F38
1C345   *EXPLOIT*
|       E34FCCEC-226E-5A46-9B1C-BCD6EF7D3257    8.1     https://vulners.com/githubexploit/E34FCCEC-226E-5A46-9B1C-BCD6EF7
D3257   *EXPLOIT*
|       E24EEC0A-40F7-5BBC-9E4D-7B13522FF915    8.1     https://vulners.com/githubexploit/E24EEC0A-40F7-5BBC-9E4D-7B13522
FF915   *EXPLOIT*
|       DC798E98-BA77-5F86-9C16-0CF8CD540EBB    8.1     https://vulners.com/githubexploit/DC798E98-BA77-5F86-9C16-0CF8CD5
40EBB   *EXPLOIT*
|       DC473885-F54C-5F76-BAFD-0175E4A90C1D    8.1     https://vulners.com/githubexploit/DC473885-F54C-5F76-BAFD-0175E4A
90C1D   *EXPLOIT*
|       D85F08E9-DB96-55E9-8DD2-22F01980F360    8.1     https://vulners.com/githubexploit/D85F08E9-DB96-55E9-8DD2-22F0198
0F360   *EXPLOIT*
|       D572250A-BE94-501D-90C4-14A6C9C0AC47    8.1     https://vulners.com/githubexploit/D572250A-BE94-501D-90C4-14A6C9C
0AC47   *EXPLOIT*
|       D1E049F1-393E-552D-80D1-675022B26911    8.1     https://vulners.com/githubexploit/D1E049F1-393E-552D-80D1-675022B
26911   *EXPLOIT*
|       CVE-2024-6387   8.1     https://vulners.com/cve/CVE-2024-6387
|       CFEBF7AF-651A-5302-80B8-F8146D5B33A6    8.1     https://vulners.com/githubexploit/CFEBF7AF-651A-5302-80B8-F8146D5
B33A6   *EXPLOIT*
|       CF80DDA9-42E7-5E06-8DA8-84C72658E191    8.1     https://vulners.com/githubexploit/CF80DDA9-42E7-5E06-8DA8-84C7265
8E191   *EXPLOIT*
|       CB2926E1-2355-5C82-A42A-D4F72F114F9B    8.1     https://vulners.com/githubexploit/CB2926E1-2355-5C82-A42A-D4F72F1
14F9B   *EXPLOIT*
|       C6FB6D50-F71D-5870-B671-D6A09A95627F    8.1     https://vulners.com/githubexploit/C6FB6D50-F71D-5870-B671-D6A09A9
5627F   *EXPLOIT*
|       C5B2D4A1-8C3B-5FF7-B620-EDE207B027A0    8.1     https://vulners.com/githubexploit/C5B2D4A1-8C3B-5FF7-B620-EDE207B
027A0   *EXPLOIT*
|       C185263E-3E67-5550-B9C0-AB9C15351960    8.1     https://vulners.com/githubexploit/C185263E-3E67-5550-B9C0-AB9C153
51960   *EXPLOIT*
|       BDA609DA-6936-50DC-A325-19FE2CC68562    8.1     https://vulners.com/githubexploit/BDA609DA-6936-50DC-A325-19FE2CC
68562   *EXPLOIT*
|       AA539633-36A9-53BC-97E8-19BC0E4E8D37    8.1     https://vulners.com/githubexploit/AA539633-36A9-53BC-97E8-19BC0E4
E8D37   *EXPLOIT*
|       A377249D-3C48-56C9-98D6-C47013B3A043    8.1     https://vulners.com/githubexploit/A377249D-3C48-56C9-98D6-C47013B
3A043   *EXPLOIT*
|       9CDFE38D-80E9-55D4-A7A8-D5C20821303E    8.1     https://vulners.com/githubexploit/9CDFE38D-80E9-55D4-A7A8-D5C2082
```



```
00761   *EXPLOIT*
|       1CF00BB8-B891-5347-A2DC-2C6A6BFF7C99    8.1     https://vulners.com/githubexploit/1CF00BB8-B891-5347-A2DC-2C6A6BF
F7C99   *EXPLOIT*
|       1AB9F1F4-9798-59A0-9213-1D907E81E7F6    8.1     https://vulners.com/githubexploit/1AB9F1F4-9798-59A0-9213-1D907E8
1E7F6   *EXPLOIT*
|       1A779279-F527-5C29-A64D-94AAA4ADD6FD    8.1     https://vulners.com/githubexploit/1A779279-F527-5C29-A64D-94AAA4A
DD6FD   *EXPLOIT*
|       15C36683-070A-5CC1-B21F-5F0BF974D9D3    8.1     https://vulners.com/githubexploit/15C36683-070A-5CC1-B21F-5F0BF97
4D9D3   *EXPLOIT*
|       1337DAY-ID-39674        8.1     https://vulners.com/zdt/1337DAY-ID-39674        *EXPLOIT*
|       123C2683-74BE-5320-AA3A-C376C8E3A992    8.1     https://vulners.com/githubexploit/123C2683-74BE-5320-AA3A-C376C8E
3A992   *EXPLOIT*
|       11F020AC-F907-5606-8805-0516E06160EE    8.1     https://vulners.com/githubexploit/11F020AC-F907-5606-8805-0516E06
160EE   *EXPLOIT*
|       108E1D25-1F7E-534C-97CD-3F6045E32B98    8.1     https://vulners.com/githubexploit/108E1D25-1F7E-534C-97CD-3F6045E
32B98   *EXPLOIT*
|       0FC4BE81-312B-51F4-9D9B-66D8B5C093CD    8.1     https://vulners.com/githubexploit/0FC4BE81-312B-51F4-9D9B-66D8B5C
093CD   *EXPLOIT*
|       0F9B3655-C7D4-55A9-8EB5-2EAD9CEAB180    8.1     https://vulners.com/githubexploit/0F9B3655-C7D4-55A9-8EB5-2EAD9CE
AB180   *EXPLOIT*
|       0E9294FD-6B44-503A-84C2-C6E76E53B0B7    8.1     https://vulners.com/githubexploit/0E9294FD-6B44-503A-84C2-C6E76E5
3B0B7   *EXPLOIT*
|       0A8CA57C-ED38-5301-A03A-C841BD3082EC    8.1     https://vulners.com/githubexploit/0A8CA57C-ED38-5301-A03A-C841BD3
082EC   *EXPLOIT*
|       SSV:92579       7.5     https://vulners.com/seebug/SSV:92579    *EXPLOIT*
|       PACKETSTORM:173661      7.5     https://vulners.com/packetstorm/PACKETSTORM:173661      *EXPLOIT*
|       F0979183-AE88-53B4-86CF-3AF0523F3807    7.5     https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523
F3807   *EXPLOIT*
|       1337DAY-ID-26576        7.5     https://vulners.com/zdt/1337DAY-ID-26576        *EXPLOIT*
|       CVE-2023-51385  6.5     https://vulners.com/cve/CVE-2023-51385
|       CVE-2023-48795  5.9     https://vulners.com/cve/CVE-2023-48795
|       CVE-2023-51384  5.5     https://vulners.com/cve/CVE-2023-51384
|       PACKETSTORM:140261      0.0     https://vulners.com/packetstorm/PACKETSTORM:140261      *EXPLOIT*
|       B8190CDB-3EB9-5631-9828-8064A1575B23    0.0     https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A15
75B23   *EXPLOIT*
|       8FC9C5AB-3968-5F3C-825E-E8DB5379A623    0.0     https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB537
9A623   *EXPLOIT*
|       8AD01159-548E-546E-AA87-2DE89F3927EC    0.0     https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3
927EC   *EXPLOIT*
|       5C971D4B-2DD3-5894-9EC2-DAB952B4740D    0.0     https://vulners.com/githubexploit/5C971D4B-2DD3-5894-9EC2-DAB952B
4740D   *EXPLOIT*
|       39E70D1A-F5D8-59D5-A0CF-E73D9BAA3118    0.0     https://vulners.com/githubexploit/39E70D1A-F5D8-59D5-A0CF-E73D9BA
A3118   *EXPLOIT*
|_      0221525F-07F5-5790-912D-F4B9E2D1B587    0.0     https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D
1B587   *EXPLOIT*
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.100.23
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.100.23:80/apache2;repeatmerged=0
|     Form id: wp-block-search__input-2
|     Form action: http://localhost/
|
|     Path: http://192.168.100.23:80/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-server-header: Apache/2.4.62 (Debian)
| 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:D7:C6:89 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 101.71 seconds
```

1.2 Análisis con Nessus

Para complementar los hallazgos de Nmap, se realizó un escaneo de vulnerabilidades utilizando Nessus desde una máquina Kali Linux. Nessus es una herramienta reconocida por su capacidad de evaluar sistemáticamente el estado de seguridad de un sistema. El escaneo detectó un total de 28 vulnerabilidades, de las cuales destacan las siguientes:

- **ICMP Timestamp Request Remote Date Disclosure:** Aunque clasificada como de baja severidad, esta vulnerabilidad permite a un atacante determinar la hora del sistema, facilitando ataques de sincronización o inferencias sobre la actividad del servidor.
- **Apache HTTP Server Version:** La versión de Apache identificada presenta riesgos asociados a vulnerabilidades conocidas, incrementando la posibilidad de explotar fallas si no se han aplicado los parches correspondientes.
- **Backported Security Patch Detection:** Este hallazgo indica que las versiones de FTP y SSH utilizan parches de seguridad retroportados, lo que puede implicar una exposición residual a fallas no completamente mitigadas.

Vulnerabilities Total: 28

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
LOW	2.1*	2.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	39519	Backported Security Patch Detection (FTP)
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	10092	FTP Server Detection
INFO	N/A	-	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	181418	OpenSSH Detection
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	11153	Service Detection (HELP Request)
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	10302	Web Server robots.txt Information Disclosure
INFO	N/A	-	-	66717	mDNS Detection (Local Network)
INFO	N/A	-	-	52703	vsftpd Detection

Estos hallazgos resaltan la necesidad de mantener actualizados los servicios y de realizar configuraciones adecuadas para mitigar riesgos potenciales.

1.3 Evidencias Adicionales

Durante el análisis, se recopilaron informaciones complementarias que aportan un contexto profundo sobre el estado general del sistema y las posibles vulnerabilidades:

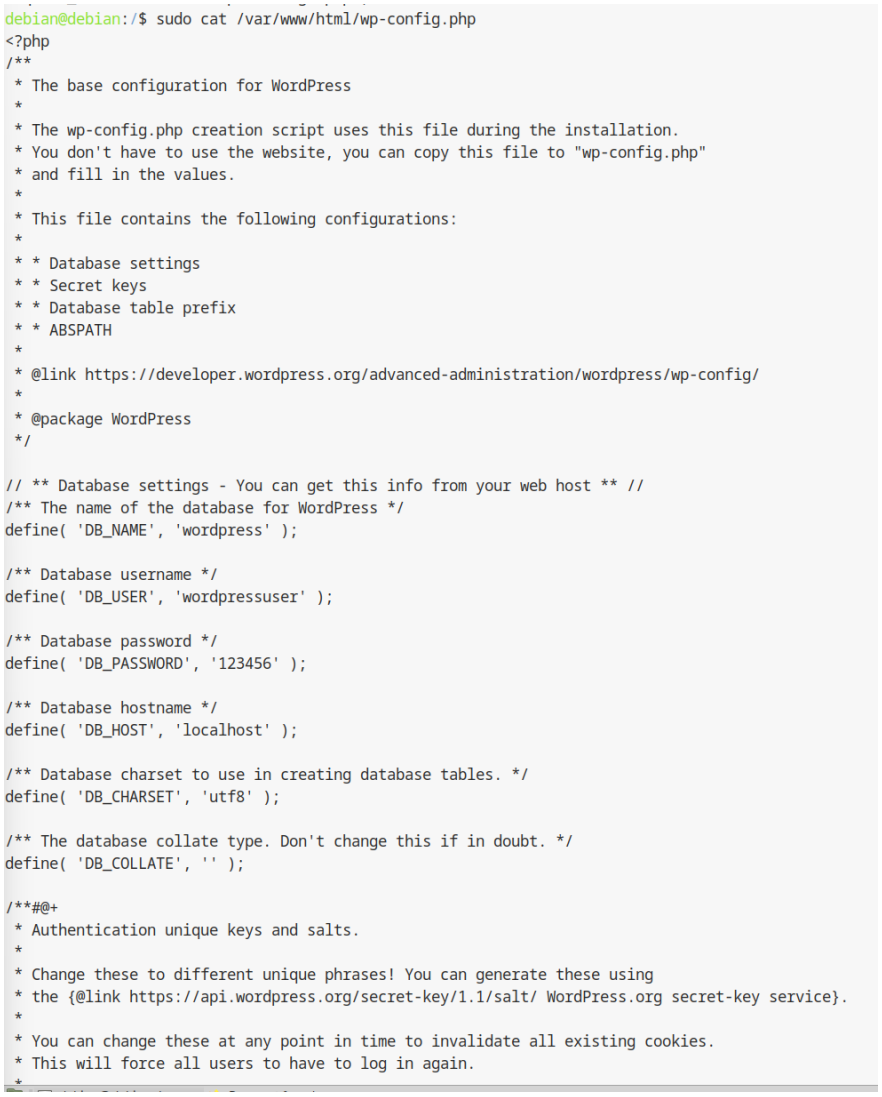
- **Archivos logs:**
  - `/var/log/vsftpd.log`: Este archivo no mostró actividad inusual, lo que indica que el servicio FTP no fue explotado durante el período analizado. Sin embargo, su revisión detallada resalta la necesidad de mantener configuraciones seguras en servicios que puedan ser vulnerables a ataques si no son adecuadamente monitorizados.

```
debian@debian:/var/log$ sudo cat vsftpd.log
[sudo] password for debian:
Sun Dec 15 15:43:28 2024 [pid 7362] CONNECT: Client "::ffff:192.168.1.124"
Sun Dec 15 15:43:28 2024 [pid 7365] CONNECT: Client "::ffff:192.168.1.124"
Sun Dec 15 15:43:28 2024 [pid 7367] CONNECT: Client "::ffff:192.168.1.124"
Sun Dec 15 15:43:28 2024 [pid 7370] CONNECT: Client "::ffff:192.168.1.124"
Sun Dec 15 15:43:28 2024 [pid 7373] CONNECT: Client "::ffff:192.168.1.124"
Sun Dec 15 15:43:28 2024 [pid 7377] CONNECT: Client "::ffff:192.168.1.124"
Sun Dec 15 15:43:28 2024 [pid 7380] CONNECT: Client "::ffff:192.168.1.124"
Sun Dec 15 15:43:28 2024 [pid 7382] CONNECT: Client "::ffff:192.168.1.124"
Sun Dec 15 15:43:33 2024 [pid 7389] CONNECT: Client "::ffff:192.168.1.124"
Sun Dec 15 15:43:33 2024 [pid 7391] CONNECT: Client "::ffff:192.168.1.124"
Sun Dec 15 15:43:38 2024 [pid 7393] CONNECT: Client "::ffff:192.168.1.124"
Sun Dec 15 15:43:43 2024 [pid 7399] CONNECT: Client "::ffff:192.168.1.124"
Sun Dec 15 15:44:32 2024 [pid 7447] CONNECT: Client "::ffff:192.168.1.124"
Sun Dec 15 15:44:32 2024 [pid 7449] CONNECT: Client "::ffff:192.168.1.124"
Sun Dec 15 15:44:37 2024 [pid 7448] [${jndi:ldap://log4shell-ftp-fGZnb9FafpXcY2QzlqMD${lower:ten}.w.nessus.org/ne
OGIN: Client "::ffff:192.168.1.124"
Sun Dec 15 15:44:43 2024 [pid 7448] [ftp] OK LOGIN: Client "::ffff:192.168.1.124", anon password "ftp"
Sun Dec 15 15:45:07 2024 [pid 7455] CONNECT: Client "::ffff:192.168.1.124"
Sun Dec 15 15:45:30 2024 [pid 7461] CONNECT: Client "::ffff:192.168.1.124"
Sun Dec 15 15:45:35 2024 [pid 7463] CONNECT: Client "::ffff:192.168.1.124"
```

- `/var/log/apache2/access.log`: Este log registró un alto volumen de peticiones concentradas en intervalos de tiempo muy cortos. Este patrón de actividad sugiere un análisis de pentesting dirigido al servicio Apache, posiblemente con el objetivo de identificar configuraciones inseguras o puntos de entrada explotables. Esta evidencia enfatiza la importancia de aplicar mecanismos de detección temprana.

```
debian@debian:/var/log$ sudo zgrep -i "08/Oct/2024" apache2/access.log.5.gz
127.0.0.1 - - [08/Oct/2024:16:49:46 -0400] "POST /wp-cron.php HTTP/1.1" 200 259 "-" "WordPress/6.6.2; http://localhost"
127.0.0.1 - - [08/Oct/2024:16:49:46 -0400] "GET / HTTP/1.1" 200 3343 "-" "WordPress/6.6.2; http://localhost"
127.0.0.1 - - [08/Oct/2024:16:49:46 -0400] "GET / HTTP/1.1" 200 3343 "-" "WordPress/6.6.2; http://localhost"
127.0.0.1 - - [08/Oct/2024:16:49:46 -0400] "GET / HTTP/1.1" 200 3343 "-" "WordPress/6.6.2; http://localhost"
127.0.0.1 - - [08/Oct/2024:16:49:46 -0400] "POST /wp-cron.php?doing_wp_cron=1728420586.2589499950408935546875 HTTP/1.1" 200 259 "-" "WordPress/6.6.2; http://localhost"
127.0.0.1 - - [08/Oct/2024:16:49:45 -0400] "GET /wp-admin/ HTTP/1.1" 200 17535 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Oct/2024:16:49:46 -0400] "GET /wp-includes/js/thickbox/thickbox.css?ver=6.6.2 HTTP/1.1" 200 1274 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linux
 x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Oct/2024:16:49:46 -0400] "GET /wp-includes/css/editor.min.css?ver=6.6.2 HTTP/1.1" 200 6183 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linux x86_6
4; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Oct/2024:16:49:46 -0400] "GET /wp-admin/js/common.min.js?ver=6.6.2 HTTP/1.1" 200 7675 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linux x86_64; rv
:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Oct/2024:16:49:46 -0400] "GET /wp-includes/js/dist/i18n.min.js?ver=5e580eb46a90c2b997e6 HTTP/1.1" 200 4011 "http://localhost/wp-admin/" "Mozilla/5.0 (
X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Oct/2024:16:49:46 -0400] "GET /wp-includes/js/hoverintent-js.min.js?ver=2.2.1 HTTP/1.1" 200 1060 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linux
 x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Oct/2024:16:49:46 -0400] "GET /wp-includes/js/admin-bar.min.js?ver=6.6.2 HTTP/1.1" 200 1700 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linux x86_
64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Oct/2024:16:49:46 -0400] "GET /wp-includes/js/clipboard.min.js?ver=2.0.11 HTTP/1.1" 200 3494 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linux x86
_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Oct/2024:16:49:46 -0400] "GET /wp-includes/js/underscore.min.js?ver=1.13.4 HTTP/1.1" 200 7655 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linux x8
6_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Oct/2024:16:49:46 -0400] "GET /wp-includes/js/dist/dom-ready.min.js?ver=f77871ff7694fffea381 HTTP/1.1" 200 662 "http://localhost/wp-admin/" "Mozilla/5
.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Oct/2024:16:49:46 -0400] "GET /wp-includes/js/dist/url.min.js?ver=36ae0e4dd9043bb8749b HTTP/1.1" 200 4080 "http://localhost/wp-admin/" "Mozilla/5.0 (X
11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Oct/2024:16:49:46 -0400] "GET /wp-includes/js/wp-util.min.js?ver=6.6.2 HTTP/1.1" 200 1098 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linux x86_64
; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Oct/2024:16:49:47 -0400] "GET /wp-includes/js/api-request.min.js?ver=6.6.2 HTTP/1.1" 200 933 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linux x86
_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Oct/2024:16:49:47 -0400] "GET /wp-includes/js/dist/a11y.min.js?ver=d90eebea464f6c09bfd5 HTTP/1.1" 200 1293 "http://localhost/wp-admin/" "Mozilla/5.0 (
X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Oct/2024:16:49:47 -0400] "GET /wp-includes/js/wp-ajax-response.min.js?ver=6.6.2 HTTP/1.1" 200 1434 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Lin
ux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Oct/2024:16:49:47 -0400] "GET /wp-admin/js/site-health.min.js?ver=6.6.2 HTTP/1.1" 200 2541 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linux x86_6
4; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Oct/2024:16:49:47 -0400] "GET /wp-includes/js/wp-lists.min.js?ver=6.6.2 HTTP/1.1" 200 2878 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linux x86_6
4; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Oct/2024:16:49:47 -0400] "GET /wp-includes/js/jquery/jquery.color.min.js?ver=2.2.0 HTTP/1.1" 200 3248 "http://localhost/wp-admin/" "Mozilla/5.0 (X11;
Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Oct/2024:16:49:47 -0400] "GET /wp-includes/js/quicktags.min.js?ver=6.6.2 HTTP/1.1" 200 3853 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linux x86_
64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Oct/2024:16:49:47 -0400] "GET /wp-includes/js/jquery/jquery.query.js?ver=2.2.3 HTTP/1.1" 200 1970 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linu
x x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Oct/2024:16:49:47 -0400] "GET /wp-admin/js/postbox.min.js?ver=6.6.2 HTTP/1.1" 200 2565 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linux x86_64; r
v:109.0) Gecko/20100101 Firefox/115.0"
```

- **Configuraciones inseguras:**
  - `wp-config.php`: Este archivo contiene credenciales predeterminadas (“wordpressuser” y “123456”), una práctica extremadamente riesgosa que facilita el acceso no autorizado a la base de datos. Esto podría permitir a los atacantes ejecutar consultas no autorizadas, alterar información sensible o comprometer funcionalidades críticas del sistema.



```
debian@debian:/$ sudo cat /var/www/html/wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the installation.
 * You don't have to use the website, you can copy this file to "wp-config.php"
 * and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * Database settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://developer.wordpress.org/advanced-administration/wordpress/wp-config/
 *
 * @package WordPress
 */

// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'wordpressuser' );

/** Database password */
define( 'DB_PASSWORD', '123456' );

/** Database hostname */
define( 'DB_HOST', 'localhost' );

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The database collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

/**#@+
 * Authentication unique keys and salts.
 *
 * Change these to different unique phrases! You can generate these using
 * the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}.
 *
 * You can change these at any point in time to invalidate all existing cookies.
 * This will force all users to have to log in again.
 *
```

- `apache2.conf`: Presenta configuraciones excesivamente permisivas que otorgan acceso irrestricto a todo el sistema de archivos. Este nivel de acceso aumenta considerablemente el riesgo de explotación, especialmente si un atacante puede acceder a directorios sensibles o modificar configuraciones claves. Las prácticas de endurecimiento de configuraciones serían cruciales para mitigar estas vulnerabilidades.

```
debian@debian:/$ sudo cat /var/www/html/wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the installation.
 * You don't have to use the website, you can copy this file to "wp-config.php"
 * and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * Database settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://developer.wordpress.org/advanced-administration/wordpress/wp-config/
 *
 * @package WordPress
 */

// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'wordpressuser' );

/** Database password */
define( 'DB_PASSWORD', '123456' );

/** Database hostname */
define( 'DB_HOST', 'localhost' );

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The database collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

/**#@+
 * Authentication unique keys and salts.
 *
 * Change these to different unique phrases! You can generate these using
 * the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}.
 *
 * You can change these at any point in time to invalidate all existing cookies.
 * This will force all users to have to log in again.
 *
```

Estas evidencias subrayan las debilidades significativas presentes en el sistema, tanto en su configuración como en la gestión de credenciales y servicios, que pudieron haber facilitado no solo el compromiso inicial, sino también movimientos laterales dentro de la infraestructura comprometida. La combinación de configuraciones inseguras y registros que indican actividades sospechosas refuerza la necesidad de un enfoque proactivo en seguridad para mitigar estos riesgos.

2. Análisis de Actividades Sospechosas

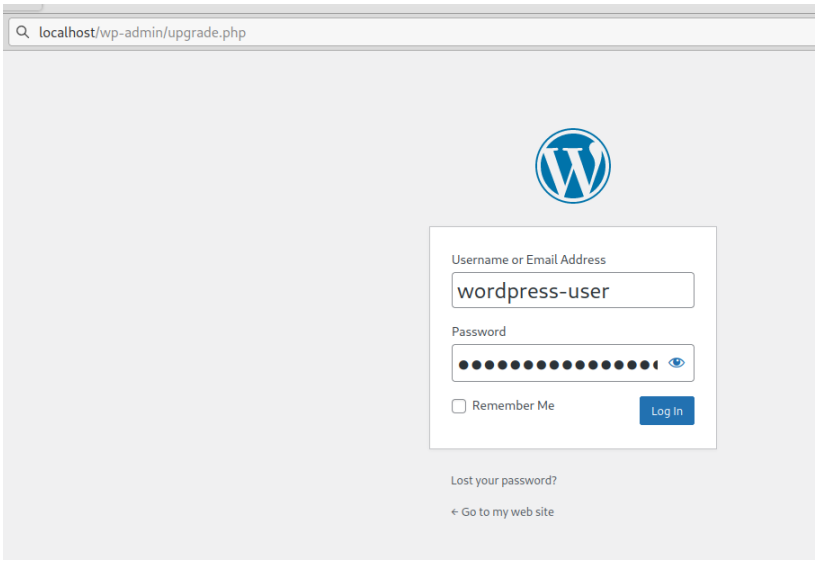
2.1 Ataques de Pentesting

El servicio Apache evidenció un uso intensivo que sugiere un ataque metódico dirigido a mapear las vulnerabilidades existentes en el sistema. Esta actividad es típica en las fases iniciales de un ataque, donde los atacantes emplean herramientas automatizadas para identificar configuraciones inadecuadas y puntos de entrada. La alta concentración de peticiones observadas en los registros refuerza la hipótesis de un intento sistemático por comprometer el servidor.

Uno de los hallazgos más alarmantes fue el acceso repetido a la ruta `localhost/wp-admin`. En esta ubicación, las credenciales del sistema estaban precargadas, una configuración que no solo reduce significativamente los controles de seguridad, sino que también permite a un atacante obtener acceso inmediato sin necesidad de autenticar sus credenciales. Este tipo de

configuración no solo compromete la seguridad del sistema, sino que también facilita la manipulación de información crítica y el escalamiento de privilegios dentro del entorno.

Además, las pruebas sugieren que los atacantes aprovecharon la falta de protecciones adicionales, como un sistema de autenticación de dos factores o restricciones de acceso por dirección IP. Esto indica una falla en las políticas de seguridad básicas y la ausencia de medidas de defensa en profundidad, aumentando exponencialmente el riesgo de compromisos más serios. La ruta `localhost/wp-admin` se convirtió en el eje central de las actividades de reconocimiento y explotación detectadas.



La evidencia recolectada a través de los registros sugiere que esta etapa de pentesting fue clave para que el atacante pudiera evaluar y aprovechar las configuraciones más vulnerables del servidor, reafirmando la importancia de reforzar este tipo de puntos críticos en los entornos productivos.

2.2 Manipulación de Archivos

Se detectaron cambios recientes en configuraciones clave utilizando el comando `find / -type f -newermt \"2024-10-08\"`, el cual permite listar archivos modificados en una fecha específica y analizar su contenido en busca de alteraciones sospechosas. Entre estos cambios, destaca la alteración del archivo `/var/www/html/wp-admin/options.php`, un componente esencial en la configuración del sistema. Este archivo regula múltiples parámetros críticos, y su modificación podría indicar la inserción de código malicioso diseñado para facilitar el acceso no autorizado a otras áreas del sistema, ya sea mediante la apertura de backdoors o la eliminación de restricciones de seguridad previamente establecidas.

```
/var/www/html/wp-admin/includes/class-wp-site-health-auto-updates.php
/var/www/html/wp-admin/includes/class-wp-ms-sites-list-table.php
/var/www/html/wp-admin/includes/translation-install.php
/var/www/html/wp-admin/includes/class-core-upgrader.php
/var/www/html/wp-admin/includes/class-wp-posts-list-table.php
/var/www/html/wp-admin/includes/class-theme-upgrader.php
/var/www/html/wp-admin/includes/post.php
/var/www/html/wp-admin/includes/class-custom-image-header.php
/var/www/html/wp-admin/includes/class-wp-themes-list-table.php
/var/www/html/wp-admin/includes/class-plugin-upgrader.php
/var/www/html/wp-admin/includes/admin-filters.php
/var/www/html/wp-admin/includes/class-wp-debug-data.php
/var/www/html/wp-admin/includes/class-plugin-installer-skin.php
/var/www/html/wp-admin/includes/credits.php
/var/www/html/wp-admin/edit-form-advanced.php
/var/www/html/wp-admin/widgets-form-blocks.php
/var/www/html/wp-admin/install.php
/var/www/html/wp-admin/load-scripts.php
/var/www/html/wp-admin/about.php
/var/www/html/wp-admin/edit-tags.php
/var/www/html/wp-admin/maint/repair.php
/var/www/html/wp-admin/options-general.php
/var/www/html/wp-admin/options-discussion.php
/var/www/html/wp-admin/menu.php
/var/www/html/wp-admin/themes.php
/var/www/html/wp-admin/edit-tag-form.php
/var/www/html/wp-admin/load-styles.php
/var/www/html/wp-admin/options.php
/var/www/html/wp-admin/images/about-release-badge.svg
/var/www/html/wp-admin/user-edit.php
/var/www/html/wp-config-sample.php
/var/www/html/readme.html
/var/www/html/wp-cron.php
/var/www/html/wp-content/themes/twentytwentyfive/theme.json
/var/www/html/wp-content/themes/twentytwentyfive/patterns/services-team-photos.php
/var/www/html/wp-content/themes/twentytwentyfive/patterns/template-search-photo-blog.php
/var/www/html/wp-content/themes/twentytwentyfive/patterns/cta-book-locations.php
/var/www/html/wp-content/themes/twentytwentyfive/patterns/more-posts.php
/var/www/html/wp-content/themes/twentytwentyfive/patterns/footer-social.php
/var/www/html/wp-content/themes/twentytwentyfive/patterns/template-single-left-aligned-content.php
/var/www/html/wp-content/themes/twentytwentyfive/patterns/template-archive-photo-blog.php
/var/www/html/wp-content/themes/twentytwentyfive/patterns/vertical-header.php
/var/www/html/wp-content/themes/twentytwentyfive/patterns/hidden-search.php
/var/www/html/wp-content/themes/twentytwentyfive/patterns/footer-newsletter.php
/var/www/html/wp-content/themes/twentytwentyfive/patterns/hidden-404.php
/var/www/html/wp-content/themes/twentytwentyfive/patterns/pricing-3-col.php
/var/www/html/wp-content/themes/twentytwentyfive/patterns/header.php
/var/www/html/wp-content/themes/twentytwentyfive/patterns/banner-cover-big-heading.php
/var/www/html/wp-content/themes/twentytwentyfive/patterns/template-query-loop-vertical-header-blog.php
```

Adicionalmente, el análisis profundo de los directorios sugiere que múltiples configuraciones relacionadas con la gestión de usuarios y permisos han sido manipuladas. Por ejemplo, se detectaron inconsistencias en las políticas de permisos de acceso, lo cual podría permitir a usuarios no autorizados interactuar con archivos y configuraciones sensibles. Este tipo de actividad incrementa significativamente el riesgo de explotación futura, ya que reduce la efectividad de las barreras de seguridad implementadas inicialmente.

La revisión también reveló patrones anómalos en archivos secundarios que interactúan con `options.php`, lo que sugiere que las modificaciones podrían haber sido parte de una estrategia más amplia para comprometer el sistema. Estas acciones no solo afectan la integridad del entorno actual, sino que también facilitan el establecimiento de persistencia, permitiendo que el atacante mantenga control a largo plazo sobre el sistema sin ser detectado fácilmente. En conjunto, estas evidencias subrayan la necesidad de una auditoría exhaustiva para identificar todos los cambios realizados y restaurar configuraciones seguras en cada componente afectado.

2.3 Explotación de Vulnerabilidades

El acceso no autorizado fue facilitado por una serie de configuraciones deficientes que comprometieron la seguridad del sistema. Entre las principales se encuentran la carga de credenciales predeterminadas, las cuales son ampliamente conocidas y explotables, y la ausencia de reglas de acceso restrictivas, que permitieron el libre acceso a recursos críticos. Estas debilidades no solo abrieron la puerta a la posibilidad de inyección de código PHP malicioso, sino que también permitieron el establecimiento de puertas traseras que otorgaron a los atacantes una persistencia prolongada en el sistema. Esto incluye la capacidad de ejecutar comandos arbitrarios que podrían haber modificado, eliminado o accedido a datos sensibles sin restricciones.

La evidencia recopilada durante el análisis sugiere que los atacantes identificaron y aprovecharon principalmente los servicios expuestos, como el servidor web y las configuraciones no protegidas, para explotar estas debilidades. Al comprometer

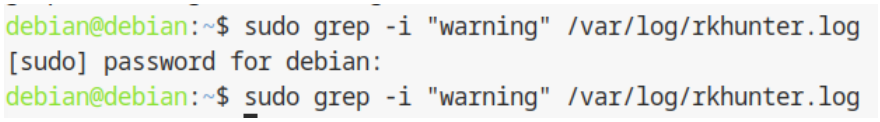
componentes clave del sistema, lograron establecer un punto de entrada que les permitió un control persistente, incrementando su capacidad para moverse lateralmente dentro de la infraestructura. Este tipo de ataque pone en evidencia la importancia de adoptar medidas de seguridad proactivas, como la actualización constante de credenciales y la implementación de políticas estrictas de control de acceso, para prevenir escenarios similares en el futuro.

---

3. Resultados de Herramientas Forenses

3.1 Análisis con Rootkit Hunter (rkhunter)

Se utilizó la herramienta Rootkit Hunter (rkhunter) para realizar un escaneo exhaustivo en busca de rootkits, puertas traseras o exploits que pudieran estar activos en el sistema. Tras un análisis detallado, no se encontraron evidencias de actividades maliciosas activas que comprometieran el sistema de manera directa. Sin embargo, la falta de hallazgos no excluye la posibilidad de actividades pasadas no detectadas por esta herramienta, lo que subraya la importancia de utilizar métodos complementarios.



3.2 Revisión de Logs del Sistema

Se procedió a un análisis profundo de varios logs clave del sistema para identificar patrones sospechosos o evidencias de actividades no autorizadas:

- **dpkg.log:** Este archivo contiene registros detallados de las instalaciones realizadas en el sistema. Durante el análisis, se confirmó que las entradas estaban relacionadas con las herramientas necesarias para el entorno de análisis y no presentaban indicios de actividad sospechosa o instalaciones maliciosas.

```
debian@debian:~$ sudo grep "install" /var/log/dpkg.log
2024-12-13 20:57:23 install fonts-lato:all <none> 2.0-2.1
2024-12-13 20:57:23 status half-installed fonts-lato:all 2.0-2.1
2024-12-13 20:57:23 install binutils-common:amd64 <none> 2.40-2
2024-12-13 20:57:23 status half-installed binutils-common:amd64 2.40-2
2024-12-13 20:57:24 install libbinutils:amd64 <none> 2.40-2
2024-12-13 20:57:24 status half-installed libbinutils:amd64 2.40-2
2024-12-13 20:57:24 install libctf-nobfd0:amd64 <none> 2.40-2
2024-12-13 20:57:24 status half-installed libctf-nobfd0:amd64 2.40-2
2024-12-13 20:57:24 install libctf0:amd64 <none> 2.40-2
2024-12-13 20:57:24 status half-installed libctf0:amd64 2.40-2
2024-12-13 20:57:24 install libgprofng0:amd64 <none> 2.40-2
2024-12-13 20:57:24 status half-installed libgprofng0:amd64 2.40-2
2024-12-13 20:57:24 install binutils-x86-64-linux-gnu:amd64 <none> 2.40-2
2024-12-13 20:57:24 status half-installed binutils-x86-64-linux-gnu:amd64 2.40-2
2024-12-13 20:57:24 install binutils:amd64 <none> 2.40-2
2024-12-13 20:57:24 status half-installed binutils:amd64 2.40-2
2024-12-13 20:57:24 install rkhunter:all <none> 1.4.6-11
2024-12-13 20:57:24 status half-installed rkhunter:all 1.4.6-11
2024-12-13 20:57:24 install exim4-config:all <none> 4.96-15+deb12u5
2024-12-13 20:57:24 status half-installed exim4-config:all 4.96-15+deb12u5
2024-12-13 20:57:25 install exim4-base:amd64 <none> 4.96-15+deb12u5
2024-12-13 20:57:25 status half-installed exim4-base:amd64 4.96-15+deb12u5
2024-12-13 20:57:25 install libunbound8:amd64 <none> 1.17.1-2+deb12u2
2024-12-13 20:57:25 status half-installed libunbound8:amd64 1.17.1-2+deb12u2
2024-12-13 20:57:25 install libgnutls-dane0:amd64 <none> 3.7.9-2+deb12u3
2024-12-13 20:57:25 status half-installed libgnutls-dane0:amd64 3.7.9-2+deb12u3
2024-12-13 20:57:25 install exim4-daemon-light:amd64 <none> 4.96-15+deb12u5
2024-12-13 20:57:25 status half-installed exim4-daemon-light:amd64 4.96-15+deb12u5
2024-12-13 20:57:25 install liblockfile1:amd64 <none> 1.17-1+b1
2024-12-13 20:57:25 status half-installed liblockfile1:amd64 1.17-1+b1
2024-12-13 20:57:25 install bsd-mailx:amd64 <none> 8.1.2-0.20220412cvs-1
2024-12-13 20:57:25 status half-installed bsd-mailx:amd64 8.1.2-0.20220412cvs-1
2024-12-13 20:57:25 install libjs-jquery:all <none> 3.6.1+dfsg+~3.5.14-1
2024-12-13 20:57:25 status half-installed libjs-jquery:all 3.6.1+dfsg+~3.5.14-1
2024-12-13 20:57:25 install rubygems-integration:all <none> 1.18
2024-12-13 20:57:25 status half-installed rubygems-integration:all 1.18
2024-12-13 20:57:25 install ruby3.1:amd64 <none> 3.1.2-7+deb12u1
2024-12-13 20:57:25 status half-installed ruby3.1:amd64 3.1.2-7+deb12u1
2024-12-13 20:57:25 install ruby-rubygems:all <none> 3.3.15-2
2024-12-13 20:57:25 status half-installed ruby-rubygems:all 3.3.15-2
2024-12-13 20:57:25 install ruby:amd64 <none> 1:3.1
2024-12-13 20:57:25 status half-installed ruby:amd64 1:3.1
2024-12-13 20:57:25 install rake:all <none> 13.0.6-3
2024-12-13 20:57:25 status half-installed rake:all 13.0.6-3
2024-12-13 20:57:26 install ruby-net-telnet:all <none> 0.2.0-1
2024-12-13 20:57:26 status half-installed ruby-net-telnet:all 0.2.0-1
2024-12-13 20:57:26 install ruby-webrick:all <none> 1.8.1-1
2024-12-13 20:57:26 status half-installed ruby-webrick:all 1.8.1-1
```

- **faillog:** Este log se utiliza para registrar intentos fallidos de acceso al sistema. Tras revisar su contenido, se verificó que el archivo se encontraba vacío, lo que indica que no hubo intentos fallidos de inicio de sesión durante el período analizado. Aunque esto podría ser un indicador positivo, también es posible que los atacantes hayan utilizado técnicas para evitar dejar rastros en este archivo.

```
-rw-r--r--   1 root              root                0 Jul 31 12:14 faillog
```

- **boot.log:** Este log documenta los eventos ocurridos durante el proceso de arranque del sistema. Los registros analizados muestran un arranque limpio y sin irregularidades, con todos los servicios esenciales iniciados correctamente. Los detalles del proceso de arranque no muestran eventos sospechosos, lo que refuerza la idea de que los atacantes no alteraron este aspecto del sistema.

```
debian@debian:/var/log$ sudo cat boot.log
------------ Tue Dec 17 19:44:54 EST 2024 ------------
/dev/sda1: recovering journal
/dev/sda1: Clearing orphaned inode 786817 (uid=0, gid=0, mode=0100666, size=0)
/dev/sda1: Clearing orphaned inode 786814 (uid=1000, gid=1000, mode=0100600, size=0)
/dev/sda1: Clearing orphaned inode 786813 (uid=1000, gid=1000, mode=0100600, size=0)
/dev/sda1: Clearing orphaned inode 786807 (uid=1000, gid=1000, mode=0100600, size=65536)
/dev/sda1: Clearing orphaned inode 1184119 (uid=1000, gid=1000, mode=0100644, size=32768)
/dev/sda1: Clearing orphaned inode 1182107 (uid=1000, gid=1000, mode=0100600, size=560)
/dev/sda1: Clearing orphaned inode 786810 (uid=1000, gid=1000, mode=0100600, size=0)
/dev/sda1: Clearing orphaned inode 786806 (uid=1000, gid=1000, mode=0100600, size=65536)
/dev/sda1: Clearing orphaned inode 1179706 (uid=1000, gid=1000, mode=0100644, size=7459)
/dev/sda1: Clearing orphaned inode 1182104 (uid=1000, gid=1000, mode=0100644, size=7459)
/dev/sda1: Clearing orphaned inode 786800 (uid=111, gid=121, mode=0100660, size=0)
/dev/sda1: Clearing orphaned inode 786799 (uid=111, gid=121, mode=0100660, size=0)
/dev/sda1: Clearing orphaned inode 786790 (uid=111, gid=121, mode=0100660, size=0)
/dev/sda1: Clearing orphaned inode 786789 (uid=111, gid=121, mode=0100660, size=0)
/dev/sda1: clean, 193361/1925120 files, 1741832/7688960 blocks
[  OK  ] Finished systemd-tmpfiles-setup.service - Create System Files and Directories.
         Starting systemd-update-utmp.service - Record System Boot/Shutdown in UTMP...
[  OK  ] Finished systemd-update-utmp.service - Record System Boot/Shutdown in UTMP.
[  OK  ] Started systemd-udevd.service - Rule-based Manager for Device Events and Files.
         Starting plymouth-start.service - Show Plymouth Boot Screen...
[  OK  ] Finished apparmor.service - Load AppArmor profiles.
         Starting networking.service - Raise network interfaces...
[  OK  ] Started plymouth-start.service - Show Plymouth Boot Screen.
[  OK  ] Started systemd-ask-password-plymouth.path - Forward Password Requests to Plymouth Directory Watch.
[  OK  ] Reached target cryptsetup.target - Local Encrypted Volumes.
[  OK  ] Found device dev-disk-by\x2duuid-a16246c5\x2d44fe\x2d4bf1\x2d99e3\x2db05e4df433ca.device - VBOX_HARDDISK 5.
         Activating swap dev-disk-by\x2duuid-a16246c5\x2d44fe\x2d4bf1\x2d99…433ca.swap - /dev/disk/by-uuid/a16246c5-44fe-4bf1-99e3-b05e4df433ca...
[  OK  ] Activated swap dev-disk-by\x2duuid-a16246c5\x2d44fe\x2d4bf1\x2d99e…df433ca.swap - /dev/disk/by-uuid/a16246c5-44fe-4bf1-99e3-b05e4df433ca.
[  OK  ] Finished networking.service - Raise network interfaces.
[  OK  ] Reached target swap.target - Swaps.
         Starting modprobe@dm_mod.service - Load Kernel Module dm_mod...
         Starting modprobe@efi_pstore.service - Load Kernel Module efi_pstore...
         Starting modprobe@loop.service - Load Kernel Module loop...
         Starting systemd-timesyncd.service - Network Time Synchronization...
[  OK  ] Finished modprobe@dm_mod.service - Load Kernel Module dm_mod.
[  OK  ] Finished modprobe@efi_pstore.service - Load Kernel Module efi_pstore.
[  OK  ] Finished modprobe@loop.service - Load Kernel Module loop.
         Mounting proc-sys-fs-binfmt_misc.mount - Arbitrary Executable File Formats File System...
[  OK  ] Mounted proc-sys-fs-binfmt_misc.mount - Arbitrary Executable File Formats File System.
[  OK  ] Finished systemd-binfmt.service - Set Up Additional Binary Formats.
[  OK  ] Started systemd-timesyncd.service - Network Time Synchronization.
[  OK  ] Reached target sysinit.target - System Initialization.
[  OK  ] Started cups.path - CUPS Scheduler.
[  OK  ] Started anacron.timer - Trigger anacron every hour.
[  OK  ] Started apt-daily.timer - Daily apt download activities.
[  OK  ] Started apt-daily-upgrade.timer - Daily apt upgrade and clean activities.
```

En conjunto, los resultados de estas revisiones indican que, si bien no se detectaron actividades maliciosas directas en estos logs, la configuración general del sistema y otras evidencias externas continúan sugiriendo una posible actividad malintencionada en etapas previas.

---

4. Conclusiones

4.1 Principales Vulnerabilidades

El análisis realizado identificó varias vulnerabilidades que fueron clave para comprometer el sistema. Entre las más críticas destacan:

- **Credenciales predeterminadas visibles en `wp-config.php`:** Este archivo contiene información de autenticación crucial, como el usuario y contraseña de la base de datos. Estas credenciales, al estar configuradas con valores por defecto y sin medidas de protección adecuadas, facilitaron el acceso no autorizado al sistema.
- **Configuraciones abiertas en `apache2.conf`:** Las configuraciones permisivas en este archivo permitieron acceso irrestricto a ciertas áreas del sistema, aumentando el riesgo de explotación de vulnerabilidades conocidas en Apache.

Estas debilidades evidencian una falta de medidas de seguridad básicas que habrían podido prevenir la explotación inicial del sistema.

4.2 Actividades Maliciosas Probables

Con base en las evidencias recolectadas, se concluye que el atacante pudo haber realizado las siguientes actividades maliciosas:

- **Creación de puertas traseras a través de archivos PHP:** Modificaciones sospechosas en archivos como `wp-admin/options.php` indican que se pudo haber inyectado código malicioso, permitiendo acceso remoto persistente al sistema.
- **Manipulación de configuraciones para acceder a datos sensibles y bases de datos:** Con las credenciales expuestas, el atacante pudo haber obtenido acceso directo a la base de datos, lo que incluye la posibilidad de extraer información confidencial o realizar cambios en los registros.
- **Ejecución de comandos maliciosos:** Las configuraciones permisivas en Apache facilitaron el uso de scripts automatizados para escanear y comprometer otros componentes del sistema.

Estas actividades muestran un patrón de comportamiento que apunta a un atacante con intenciones de explorar y explotar múltiples vectores de ataque disponibles.

4.3 Limitaciones del Análisis

A pesar de los esfuerzos realizados, el análisis presentó algunas limitaciones importantes:

- **Falta de claridad en el vector inicial de ataque:** Aunque se identificaron múltiples vulnerabilidades, no se pudo determinar con exactitud cuál fue el punto de entrada utilizado por el atacante para comprometer el sistema.
- **Actividad limitada en servicios FTP y SSH:** Aunque estos servicios presentaban configuraciones vulnerables, no se encontraron evidencias concluyentes de explotación significativa. Esto podría indicar que el atacante centró sus esfuerzos en otros vectores, como Apache y WordPress.
- **Dependencia en configuraciones actuales:** Dado que el sistema ya había sido manipulado para fines del análisis, algunos registros pudieron haber sido alterados o incompletos, lo que limita la reconstrucción completa de las acciones del atacante.

Estas limitaciones subrayan la importancia de implementar monitoreo continuo y medidas proactivas para identificar y mitigar actividades maliciosas antes de que se conviertan en compromisos graves del sistema.