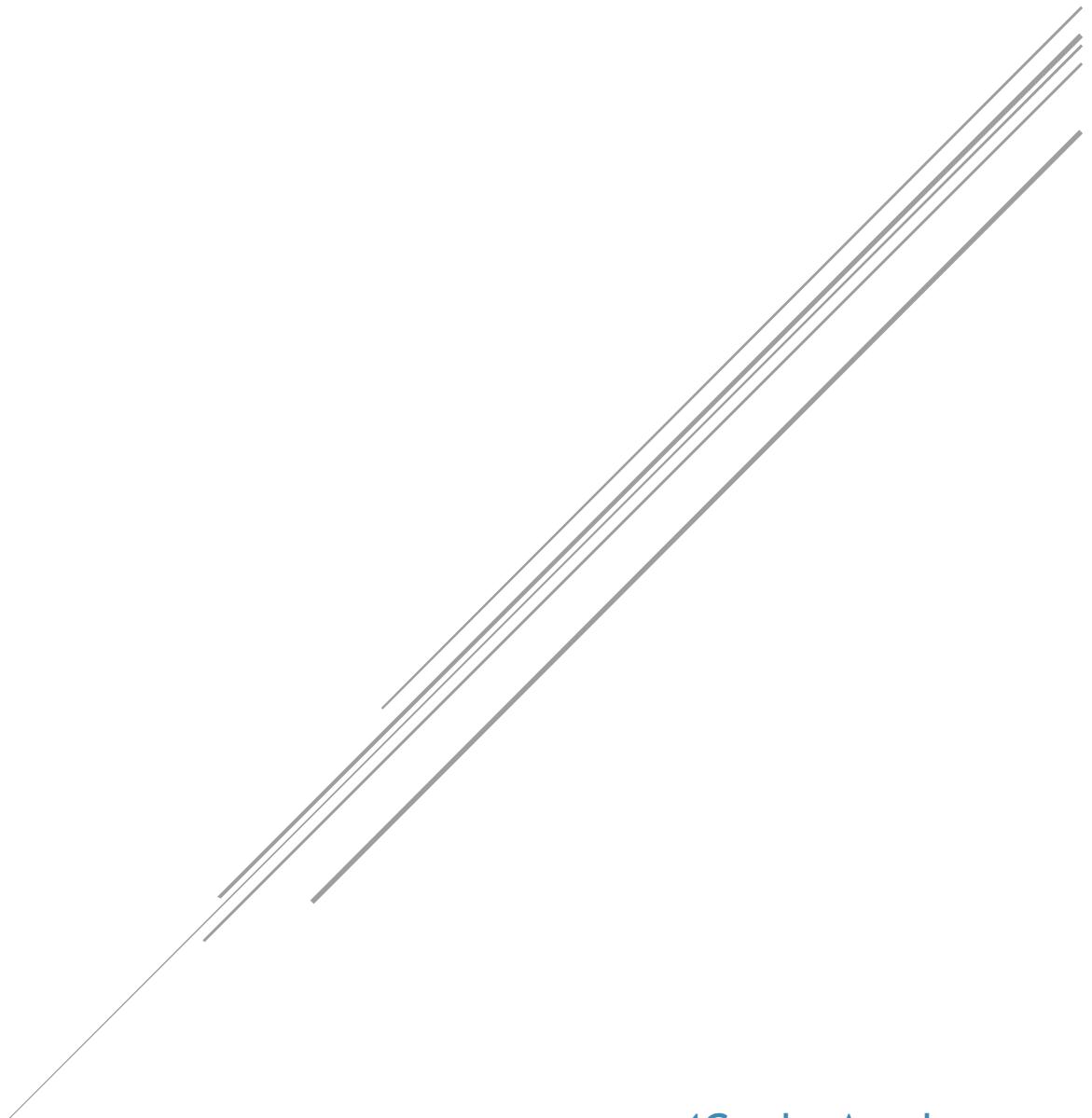


ANÁLISIS FORENSE DE INTRUSIÓN EN EL SERVIDOR DE LEX ABOGADOS & ASOCIADOS

Proyecto Final: Fase 1



4Geeks Academy
Kevin Pitti

Indice

1. Introducción.....	3
2. Fase 1: Reconocimiento y Recolección de Evidencias.....	4
2.1 Información Principal del Sistema.....	4
2.2 Revisión de Logs del Sistema.....	5
2.2.1 Registro SSH (Acceso no autorizado)	7
2.2.2 Registros de MARIADB.....	8
2.2.3 Registros del Servicio FTP (VSFTPD).....	8
2.2.4 Revisión de los Logs de Apache2.....	9
2.2.5 Registros de Autenticación.....	10
2.2.6 Creación de Usuarios.....	10
2.2.7 Conexión y Desconexión del USB.....	11
2.2.8 NetworkManager.....	11
2.2.9 Registros del Kernel.....	12
2.2.10 Registro del Servicio Cron.....	12
3. Revisión de Usuarios, Grupos y Permisos en el Sistema.....	14
3.1 Usuarios del Sistema.....	14
3.2 Grupos del Sistema.....	16
4. Revisión de Carpetas, Permisos y Configuraciones.....	17
4.1 Permisos de Archivos y Directorios Críticos.....	18
4.2 Configuración de wp-config.php y xmlrpc.php.....	19
4.3 Archivo Apache2.conf.....	20
4.4 Archivo vsftpd.conf.....	21
4.5 Archivo sshd_config.....	22
5. Revisión de Datos Comprometidos.....	23
5.1 Credenciales expuestas en la web.....	23
5.2 Revisión del archivo /root/.mysql_history.....	24
5.3 Usuarios en MySQL.....	26

5.4 Bases de Datos en el Sistema.....	27
5.5 Privilegios de los Usuarios.....	28
5.6 Análisis de la Base de Datos de WordPress.....	30
5.7 Posible información comprometida.....	31
6. Análisis de Procesos en Ejecución Inusuales.....	32
6.1 Revisión de Procesos Activos.....	32
6.2 Revisión de Inicios de Sesión y Eventos del Sistema.....	33
6.3 Revisión de Servicios Activos.....	34
7. Historial de Comandos.....	35
7.1 Revisión del historial de debian.....	35
7.2 Revisión del historial de root.....	37
8. Detección de Rootkits o Malware.....	38
8.1 CHKRootKit.....	38
8.2 Conclusiones del Análisis CHKRootkit	42
8.3 RKHunter.....	43
8.4 Conclusiones del Análisis RKHunter.....	47
9. Mitigación de Vulnerabilidades y Recomendaciones.....	48
9.1 Actualización de paquetes	48
9.2 Deshabilitar el acceso SSH root:	49
9.3 Configuración de VSFTPD Actualización de paquetes	51
9.4 Eliminación de Usuarios Maliciosos y Cambio de Contraseñas Débiles.....	53
9.5Configuración Firewall y puertos.....	58
9.6 Cambio de Permisos en Carpetas y Archivos Sensibles.....	61
9.7 Desactivación de la Listabilidad de Directorios.....	63
10. Conclusión.....	65

1. Introducción

El presente informe detalla un análisis forense realizado sobre una intrusión en un servidor Debian perteneciente a la firma de abogados LEX Abogados & Asociados. El objetivo principal es identificar vulnerabilidades, actividades sospechosas y compromisos de seguridad, con el fin de proteger tanto la información confidencial de sus clientes como la infraestructura tecnológica de la firma. A través de un proceso exhaustivo que abarcó desde el reconocimiento inicial hasta la revisión de logs del sistema, la configuración de los servicios y la detección de malware, se identificaron puntos críticos que permitieron el acceso no autorizado al servidor. Este documento también proporciona un conjunto de recomendaciones prácticas para mitigar las vulnerabilidades y reforzar la seguridad del servidor.

Fase 1:

2. Reconocimiento y recolección de evidencias

2.1 Información Principal del Sistema

- **IP:** 192.168.1.117
- **Versión del Kernel:** 5.10.0-8-amd64 (Debian 10).
- **Distribución:** Debian 10 ("buster").
- **Servicios Corriendo:**
 - SSHD VProtocol 2(para conexiones SSH)
 - Apache2 V2.4.62(servidor web)
 - VSFTPD V3.0.3 (servicio FTP)

2.2 Revisión de Logs del Sistema

La revisión de los logs del sistema es un paso fundamental para identificar actividades sospechosas y posibles vulnerabilidades explotadas durante la intrusión. En este análisis, se examinaron los registros de servicios clave como **SSH**, **FTP**, **Apache2**, **MySQL**, y otros componentes críticos del sistema. Al dirigirse a la carpeta /var/log y examinar su contenido se aprecia un archivo Readme.

```
root@debian:/var/log# ls -l
total 1040
-rw-r--r-- 1 root      root          0 Jun  4 21:36 alternatives.log
-rw-r--r-- 1 root      root 48068 Sep 30 2024 alternatives.log.1
drwxr-x--- 2 root      adm   4096 Jun 13 16:44 apache2
drwxr-xr-x  2 root      root   4096 Jun  4 21:36 apt
-rw-r----- 1 root      root  7974 Jun 13 17:32 boot.log
-rw-r----- 1 root      root  8496 Jun 13 16:44 boot.log.1
-rw-r----- 1 root      root 78904 Jun  4 21:36 boot.log.2
-rw-r----- 1 root      utmp   0 Jun  4 21:36 btmp
-rw-r----- 1 root      utmp  2688 Oct  8 2024 btmp.1
drwxr-xr-x  2 root      root   4096 Jun 13 16:44 cups
-rw-r----- 1 root      root   0 Jun  4 21:36 dpkg.log
-rw-r----- 1 root      root 765626 Oct  8 2024 dpkg.log.1
-rw-r----- 1 root      root   0 Jul 31 2024 faillog
-rw-r----- 1 root      root  5602 Sep 30 2024 fontconfig.log
drwxr-xr-x  3 root      root   4096 Jul 31 2024 installer
drwxr-sr-x+ 3 root     systemd-journal 4096 Jul 31 2024 journal
-rw-r----- 1 root      utmp   0 Jul 31 2024 lastlog
drwxr-xr-x  2 root      root  4096 Jun 13 17:32 lightdm
drwxr----- 2 root      root  4096 Jul 31 2024 private
lrwxrwxrwx  1 root      root    39 Jul 31 2024 README -> ../../usr/share/doc/systemd/README.logs
drwxr-xr-x  3 root      root  4096 Sep 30 2024 runit
drwxr----- 2 speech-dispatcher root  4096 Nov 25 2022 speech-dispatcher
-rw-r----- 1 root      utmp  27648 Jun 13 17:59 wtmp
-rw-r----- 1 root      root 25221 Jun 13 18:56 Xorg.0.log
-rw-r----- 1 root      root 24807 Jun 13 17:11 Xorg.0.log.old
```

Al leer este archivo Readme de la carpeta se confirma que el sistema trabaja con SystemD por lo que se usa el comando Journalctl para ingresar a los registros del servidor.

```
debian@debian:/var/log$ cat readme
cat: readme: No such file or directory
debian@debian:/var/log$ cat README
You are looking for the traditional text log files in /var/log, and they are
gone?
```

Here's an explanation on what's going on:

You are running a systemd-based OS where traditional syslog has been replaced with the Journal. The journal stores the same (and more) information as classic syslog. To make use of the journal and access the collected log data simply invoke "journalctl", which will output the logs in the identical text-based format the syslog files in /var/log used to be. For further details, please refer to `journalctl(1)`.

Alternatively, consider installing one of the traditional syslog implementations available for your distribution, which will generate the classic log files for you. Syslog implementations such as `syslog-ng` or `rsyslog` may be installed side-by-side with the journal and will continue to function the way they always did.

Thank you!

Further reading:

Se revisaron los registros del sistema para identificar acciones sospechosas. Se utilizó el comando `'journalctl'` para revisar eventos relacionados con accesos no autorizados, creación de usuarios, manipulación de servicios, etc.

2.1.1. Registro SSH (Acceso no autorizado)

Se realizó una búsqueda de registros en el servicio SSH utilizando el comando `sudo journalctl -u ssh.service`. Se identificó un acceso remoto no autorizado realizado con el usuario root desde la IP **192.168.0.134**, a través del puerto **45623**, el **08 de octubre de 2024 a las 17:40:59**. Este acceso es un claro indicio de una intrusión en el sistema.

```
Oct 08 16:14:16 debian sshd[5341]: Server listening on :: port 22.
Oct 08 16:14:16 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
-- Boot 342683d8f35244b08c4f3863f2978eca --
Oct 08 16:43:18 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Oct 08 16:43:18 debian sshd[543]: Server listening on 0.0.0.0 port 22.
Oct 08 16:43:18 debian sshd[543]: Server listening on :: port 22.
Oct 08 16:43:18 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
-- Boot d28e179bf5884b25bf94452c79fd0afa --
Oct 08 16:48:02 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Oct 08 16:48:02 debian sshd[555]: Server listening on 0.0.0.0 port 22.
Oct 08 16:48:02 debian sshd[555]: Server listening on :: port 22.
Oct 08 16:48:02 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
-- Boot af0a79f76920440c8e08594d6547449b --
Oct 08 17:28:37 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Oct 08 17:28:38 debian sshd[550]: Server listening on 0.0.0.0 port 22.
Oct 08 17:28:38 debian sshd[550]: Server listening on :: port 22.
Oct 08 17:28:38 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Oct 08 17:40:59 debian sshd[1650]: Accepted password for root from 192.168.0.134 port 45623 ssh2
Oct 08 17:40:59 debian sshd[1650]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Oct 08 17:40:59 debian sshd[1650]: pam_env(sshd:session): deprecated reading of user environment enabled
-- Boot ce6fc011548648ffac3a7cc24f234df2 --
Jun 04 21:36:03 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jun 04 21:36:03 debian sshd[589]: Server listening on 0.0.0.0 port 22.
Jun 04 21:36:03 debian sshd[589]: Server listening on :: port 22.
Jun 04 21:36:03 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
-- Boot 8fea5f7ff59e45e0a747e2708b479c41 --
Jun 13 16:44:36 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jun 13 16:44:36 debian sshd[574]: Server listening on 0.0.0.0 port 22.
Jun 13 16:44:36 debian sshd[574]: Server listening on :: port 22.
Jun 13 16:44:36 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

Inmediatamente se procede a **desactivar** este servicio SSH y otros servicios como el FTP, Mariadb y Apache mientras se siguen revisando los demás registros.

```
debian@debian:~$ sudo systemctl stop ssh.service
[sudo] password for debian:
Sorry, try again.
[sudo] password for debian:
debian@debian:~$ sudo systemctl stop sshd.service
```

2.1.2. Registros de MARIADB

Con el comando `journalctl -u mariadb` Los registros de **MariaDB** no muestran actividad sospechosa desde minutos antes de la intrusión en el servicio SSH, lo que indica que la base de datos no recopiló información de fue comprometida durante el ataque en este registro.

```
○ debian@debian:/etc/NetworkManager
File Edit View Search Terminal Help
GNU nano 7.2                                     /home/debian/Desktop/mariadb.txt
Oct 08 17:28:38 debian mariadb[637]: 2024-10-08 17:28:38 0 [Warning] You need to use --log-bin to make --expire-logs-days or --binlog-
Oct 08 17:28:38 debian mariadb[637]: 2024-10-08 17:28:38 0 [Note] Server socket created on IP: '127.0.0.1'.
Oct 08 17:28:39 debian mariadb[637]: 2024-10-08 17:28:39 0 [Note] InnoDB: Buffer pool(s) load completed at 241008 17:28:39
Oct 08 17:28:39 debian mariadb[637]: 2024-10-08 17:28:39 0 [Note] /usr/sbin/mariadb: ready for connections.
Oct 08 17:28:39 debian mariadb[637]: Version: '10.11.6-MariaDB-0+deb12u1' socket: '/run/mysqld/mysql.sock' port: 3306 Debian 12
Oct 08 17:28:39 debian systemd[1]: Started mariadb.service - MariaDB 10.11.6 database server.
Oct 08 17:28:39 debian /etc/mysql/debian-start[672]: Upgrading MySQL tables if necessary.
Oct 08 17:28:39 debian /etc/mysql/debian-start[685]: Checking for insecure root accounts.
Oct 08 17:28:39 debian /etc/mysql/debian-start[689]: Triggering myisam-recover for all MyISAM tables and aria-recover for all Aria table
-- Boot ce6fc011548648ffac3a7cc24f234df2 --
Jun 04 21:36:03 debian systemd[1]: Starting mariadb.service - MariaDB 10.11.6 database server...
Jun 04 21:36:04 debian mariadb[676]: 2025-06-04 21:36:04 0 [Note] Starting MariaDB 10.11.6-MariaDB-0+deb12u1 source revision as proce
Jun 04 21:36:04 debian mariadb[676]: 2025-06-04 21:36:04 0 [Note] InnoDB: Compressed tables use zlib 1.2.13
Jun 04 21:36:04 debian mariadb[676]: 2025-06-04 21:36:04 0 [Note] InnoDB: Number of transaction pools: 1
Jun 04 21:36:04 debian mariadb[676]: 2025-06-04 21:36:04 0 [Note] InnoDB: Using crc32 + pclmulqdq instructions
```

2.1.3. Registros del Servicio FTP (VSFTPD)

Se revisaron los logs del servicio **VSFTPD** pero no se encontraron registros sospechosos relacionados con la intrusión. Este servicio parece no haber sido afectado directamente por el ataque.

```
-- Boot 342683d8f35244b08c4f3863f2978eca --
Oct 08 16:43:18 debian systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Oct 08 16:43:18 debian systemd[1]: Started vsftpd.service - vsftpd FTP server.
-- Boot d28e179bf5884b25bf94452c79fd0afa --
Oct 08 16:48:02 debian systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Oct 08 16:48:02 debian systemd[1]: Started vsftpd.service - vsftpd FTP server.
-- Boot af0a79f76920440c8e08594d6547449b --
Oct 08 17:28:37 debian systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Oct 08 17:28:37 debian systemd[1]: Started vsftpd.service - vsftpd FTP server.
-- Boot ce6fc011548648ffac3a7cc24f234df2 --
Jun 04 21:36:03 debian systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Jun 04 21:36:03 debian systemd[1]: Started vsftpd.service - vsftpd FTP server.
-- Boot 8fea5f7ff59e45e0a747e2708b479c41 --
Jun 13 16:44:36 debian systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Jun 13 16:44:36 debian systemd[1]: Started vsftpd.service - vsftpd FTP server.
```

2.1.4. Revisión de los Logs de Apache2

En los registros de journal con el comando `journalctl -u apache2`, tanto como en los archivos `access.log` y `error.log`, no se encontraron eventos anómalos relacionados con la intrusión.

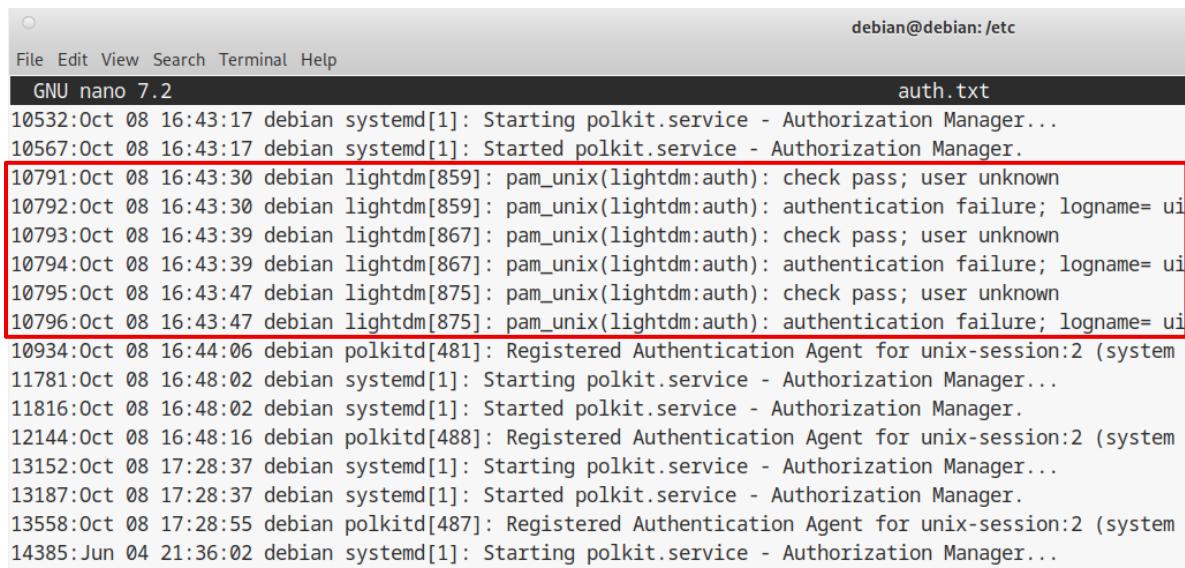
```
GNU nano 7.2                                         apache.txt
Oct 08 16:43:18 debian apachectl[579]: AH00558: apache2: Could not reliably determine the server's
Oct 08 16:43:18 debian systemd[1]: Started apache2.service - The Apache HTTP Server.
-- Boot d28e179bf5884b25bf94452c79fd0afa --
Oct 08 16:48:02 debian systemd[1]: Starting apache2.service - The Apache HTTP Server...
Oct 08 16:48:03 debian systemd[1]: Started apache2.service - The Apache HTTP Server.
-- Boot af0a79f76920440c8e08594d6547449b --
Oct 08 17:28:37 debian systemd[1]: Starting apache2.service - The Apache HTTP Server...
Oct 08 17:28:38 debian apachectl[578]: AH00557: apache2: apr_sockaddr_info_get() failed for debian
Oct 08 17:28:38 debian apachectl[578]: AH00558: apache2: Could not reliably determine the server's
Oct 08 17:28:38 debian systemd[1]: Started apache2.service - The Apache HTTP Server.
-- Boot ce6fc011548648ffac3a7cc24f234df2 --
Jun 04 21:36:03 debian systemd[1]: Starting apache2.service - The Apache HTTP Server...
Jun 04 21:36:03 debian systemd[1]: Started apache2.service - The Apache HTTP Server.
Jun 05 00:00:09 debian systemd[1]: Reloading apache2.service - The Apache HTTP Server...
Jun 05 00:00:09 debian systemd[1]: Reloaded apache2.service - The Apache HTTP Server.
```

```
154:[127.0.0.1 - - [08/Oct/2024:16:49:48 -0400] "GET /wp-includes/js/thickbox/loadingAnimation.gif HTTP/1.1" 200 15525 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
155:[127.0.0.1 - - [08/Oct/2024:16:49:48 -0400] "POST /wp-admin/admin-ajax.php HTTP/1.1" 200 636 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
156:[127.0.0.1 - - [08/Oct/2024:16:49:48 -0400] "GET /wp-admin/images/spinner.gif HTTP/1.1" 200 3941 "http://localhost/wp-admin/load-styles.php?c=0&dir=ltr&load=%5Bchunk_0%5D=dashicons,admin-bar,site-health,common,forms,admin-menu,dashboard,list-tables,edit,revisions,media,themes,about,nav-menus,wp-poi&load=%5Bchunk_1%5D=nter,wIDGETS,site-icon,l10n,buttons,wp-auth-check&ver=6.6.2" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
157:[127.0.0.1 - - [08/Oct/2024:16:49:48 -0400] "GET /wp-admin/admin-ajax.php?action=dashboard-widgets&widget=dashboard_primary&pagenow=dashboard HTTP/1.1" 200 618 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
158:[::1 - - [08/Oct/2024:16:49:52 -0400] "OPTIONS * HTTP/1.0" 200 126 "--" "Apache/2.4.62 (Debian) (internal dummy connection)"
159:[::1 - - [08/Oct/2024:16:49:53 -0400] "OPTIONS * HTTP/1.0" 200 126 "--" "Apache/2.4.62 (Debian) (internal dummy connection)"
160:[::1 - - [08/Oct/2024:16:49:54 -0400] "OPTIONS * HTTP/1.0" 200 126 "--" "Apache/2.4.62 (Debian) (internal dummy connection)"
161:[127.0.0.1 - - [08/Oct/2024:16:50:47 -0400] "POST /wp-admin/admin-ajax.php HTTP/1.1" 200 592 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
162:[127.0.0.1 - - [08/Oct/2024:16:52:48 -0400] "POST /wp-admin/admin-ajax.php HTTP/1.1" 200 592 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
163:[127.0.0.1 - - [08/Oct/2024:16:54:48 -0400] "POST /wp-admin/admin-ajax.php HTTP/1.1" 200 592 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
164:[127.0.0.1 - - [08/Oct/2024:16:56:48 -0400] "POST /wp-admin/admin-ajax.php HTTP/1.1" 200 592 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
165:[127.0.0.1 - - [08/Oct/2024:16:58:48 -0400] "POST /wp-admin/admin-ajax.php HTTP/1.1" 200 592 "http://localhost/wp-admin/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"

[ kali@kali ]-[ /mnt/forense/var/log/apache2 ]
$ grep -in "Oct" error.log
24:[Tue Oct 08 16:24:31.046216 2024] [mpm_prefork:notice] [pid 3188:tid 3188] AH00170: caught SIGWINCH, shutting down gracefully
25:[Tue Oct 08 16:24:31.238481 2024] [mpm_prefork:notice] [pid 5990:tid 5990] AH00163: Apache/2.4.62 (Debian) configured -- resuming normal operations
26:[Tue Oct 08 16:24:31.238544 2024] [core:notice] [pid 5990:tid 5990] AH00094: Command line: '/usr/sbin/apache2'
27:[Tue Oct 08 16:43:19.045745 2024] [mpm_prefork:notice] [pid 620:tid 620] AH00163: Apache/2.4.62 (Debian) configured -- resuming normal operations
28:[Tue Oct 08 16:43:19.046757 2024] [core:notice] [pid 620:tid 620] AH00094: Command line: '/usr/sbin/apache2'
29:[Tue Oct 08 16:48:03.446108 2024] [mpm_prefork:notice] [pid 622:tid 622] AH00163: Apache/2.4.62 (Debian) configured -- resuming normal operations
30:[Tue Oct 08 16:48:03.446734 2024] [core:notice] [pid 622:tid 622] AH00094: Command line: '/usr/sbin/apache2'
31:[Tue Oct 08 17:28:38.662828 2024] [mpm_prefork:notice] [pid 648:tid 648] AH00163: Apache/2.4.62 (Debian) configured -- resuming normal operations
32:[Tue Oct 08 17:28:38.663646 2024] [core:notice] [pid 648:tid 648] AH00094: Command line: '/usr/sbin/apache2'
```

2.1.5. Registros de Autenticación

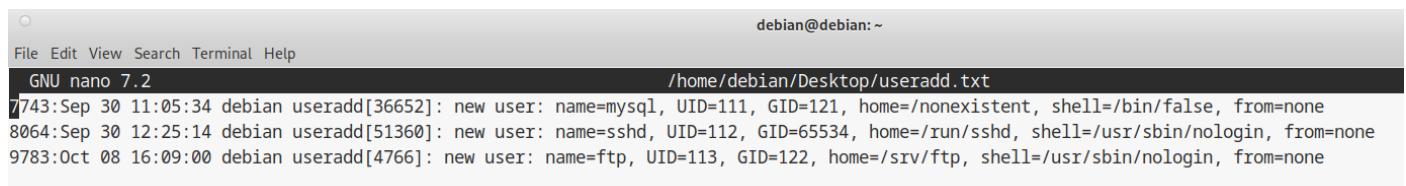
Con el comando `journalctl | grep -i "auth"`, se evidenció que, aunque hubo varios intentos fallidos de autenticación antes de la intrusión, no se encontraron registros de nuevos intentos de login después de la intrusión.



```
File Edit View Search Terminal Help
GNU nano 7.2                                     auth.txt
10532:Oct 08 16:43:17 debian systemd[1]: Starting polkit.service - Authorization Manager...
10567:Oct 08 16:43:17 debian systemd[1]: Started polkit.service - Authorization Manager.
10791:Oct 08 16:43:30 debian lightdm[859]: pam_unix(lightdm:auth): check pass; user unknown
10792:Oct 08 16:43:30 debian lightdm[859]: pam_unix(lightdm:auth): authentication failure; logname= ui
10793:Oct 08 16:43:39 debian lightdm[867]: pam_unix(lightdm:auth): check pass; user unknown
10794:Oct 08 16:43:39 debian lightdm[867]: pam_unix(lightdm:auth): authentication failure; logname= ui
10795:Oct 08 16:43:47 debian lightdm[875]: pam_unix(lightdm:auth): check pass; user unknown
10796:Oct 08 16:43:47 debian lightdm[875]: pam_unix(lightdm:auth): authentication failure; logname= ui
10934:Oct 08 16:44:06 debian polkitd[481]: Registered Authentication Agent for unix-session:2 (system
11781:Oct 08 16:48:02 debian systemd[1]: Starting polkit.service - Authorization Manager...
11816:Oct 08 16:48:02 debian systemd[1]: Started polkit.service - Authorization Manager.
12144:Oct 08 16:48:16 debian polkitd[488]: Registered Authentication Agent for unix-session:2 (system
13152:Oct 08 17:28:37 debian systemd[1]: Starting polkit.service - Authorization Manager...
13187:Oct 08 17:28:37 debian systemd[1]: Started polkit.service - Authorization Manager.
13558:Oct 08 17:28:55 debian polkitd[487]: Registered Authentication Agent for unix-session:2 (system
14385:Jun 04 21:36:02 debian systemd[1]: Starting polkit.service - Authorization Manager...
```

2.1.6. Creación de Usuarios

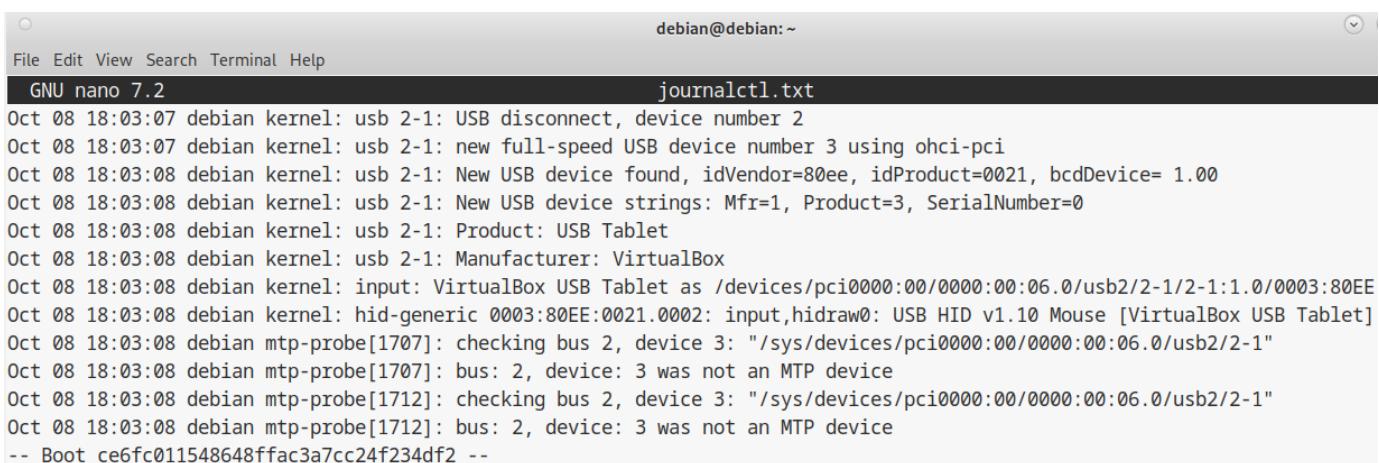
Utilizando el comando `journalctl | grep -in "useradd"`, se identificaron tres usuarios creados en el sistema, los cuales parecen ser usuarios predeterminados (como mysql, sshd y ftp). Es necesario verificar si estos usuarios son legítimos y si su creación fue autorizada. Si alguno de estos usuarios no es necesario, debe ser eliminado o deshabilitado. Con los patrones "usermod" y "passwd" no se encontraron en los registros.



```
File Edit View Search Terminal Help
GNU nano 7.2                                     /home/debian/Desktop/useradd.txt
7743:Sep 30 11:05:34 debian useradd[36652]: new user: name=mysql, UID=111, GID=121, home=/nonexistent, shell=/bin/false, from=none
8064:Sep 30 12:25:14 debian useradd[51360]: new user: name=sshd, UID=112, GID=65534, home=/run/sshd, shell=/usr/sbin/nologin, from=none
9783:Oct 08 16:09:00 debian useradd[4766]: new user: name=ftp, UID=113, GID=122, home=/srv/ftp, shell=/usr/sbin/nologin, from=none
```

2.1.7. Conexión y Desconexión del USB

A las **18:03:07** se **desconectó** un dispositivo USB y, justo un segundo después, a las **18:03:08**, se **conectó** un mouse USB VirtualBox. Este dispositivo **no** tiene la capacidad de transferir archivos multimedia (no es un dispositivo MTP). De igual en tal caso verificar si se captó por vigilancia a una persona usando el servidor para que sea interrogada lo antes posible.

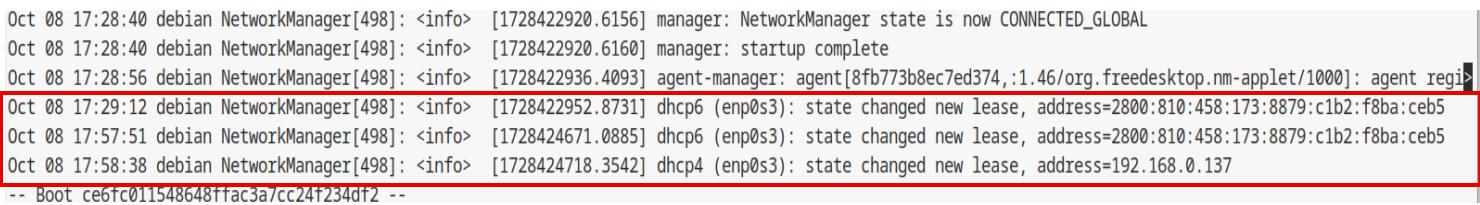


The screenshot shows a terminal window titled "journalctl.txt" being viewed in the "GNU nano 7.2" editor. The terminal window has a standard top bar with "File Edit View Search Terminal Help". The main area displays a log of kernel messages from October 8, 2018, at 18:03:07. The log entries describe the connection and disconnection of a USB device, specifically a VirtualBox USB Tablet, and the subsequent detection by the kernel's hid-generic and mtp-probe modules. The log ends with the boot identifier "ce6fc011548648ffac3a7cc24f234df2".

```
File Edit View Search Terminal Help
GNU nano 7.2 journalctl.txt
Oct 08 18:03:07 debian kernel: usb 2-1: USB disconnect, device number 2
Oct 08 18:03:07 debian kernel: usb 2-1: new full-speed USB device number 3 using ohci-pci
Oct 08 18:03:08 debian kernel: usb 2-1: New USB device found, idVendor=80ee, idProduct=0021, bcdDevice= 1.00
Oct 08 18:03:08 debian kernel: usb 2-1: New USB device strings: Mfr=1, Product=3, SerialNumber=0
Oct 08 18:03:08 debian kernel: usb 2-1: Product: USB Tablet
Oct 08 18:03:08 debian kernel: usb 2-1: Manufacturer: VirtualBox
Oct 08 18:03:08 debian kernel: input: VirtualBox USB Tablet as /devices/pci0000:00/0000:00:06.0/usb2/2-1/2-1:1.0/0003:80EE
Oct 08 18:03:08 debian kernel: hid-generic 0003:80EE:0021.0002: input,hidraw0: USB HID v1.10 Mouse [VirtualBox USB Tablet]
Oct 08 18:03:08 debian mtp-probe[1707]: checking bus 2, device 3: "/sys/devices/pci0000:00/0000:00:06.0/usb2/2-1"
Oct 08 18:03:08 debian mtp-probe[1707]: bus: 2, device: 3 was not an MTP device
Oct 08 18:03:08 debian mtp-probe[1712]: checking bus 2, device 3: "/sys/devices/pci0000:00/0000:00:06.0/usb2/2-1"
Oct 08 18:03:08 debian mtp-probe[1712]: bus: 2, device: 3 was not an MTP device
-- Boot ce6fc011548648ffac3a7cc24f234df2 --
```

2.1.8. NetworkManager

Tras la intrusión, se detectó un cambio en la dirección IP del servidor, lo cual indica que el sistema utiliza **DHCP** para asignar automáticamente direcciones IP. Esto sugiere que el servidor obtuvo una nueva IP desde el router después de la intrusión, y no un cambio a una IP estática configurada manualmente, aún así puede haber posibilidad de que esto haya sido forzado por el atacante. La IPv4 del servidor fue cambiada a **192.168.0.137** y la IPv6 se actualizó a la siguiente: **2800:810:173:8879:c1b2:f8ba:ceb5**



The screenshot shows a terminal window displaying log messages from the NetworkManager daemon. The log entries are timestamped from October 8, 2018, at 17:28:40 to 17:58:38. They show the manager starting up, becoming connected, and managing network leases. A red box highlights several entries from 17:29:12 to 17:58:38, which describe the state changes of dhcpc6 and dhcpc4 interfaces (enp0s3) and their corresponding IPv6 and IPv4 addresses. The last entry in the highlighted block shows the server's IPv4 address changing back to 192.168.0.137.

```
Oct 08 17:28:40 debian NetworkManager[498]: <info> [1728422920.6156] manager: NetworkManager state is now CONNECTED_GLOBAL
Oct 08 17:28:40 debian NetworkManager[498]: <info> [1728422920.6160] manager: startup complete
Oct 08 17:28:56 debian NetworkManager[498]: <info> [1728422936.4093] agent-manager: agent[8fb773b8ec7ed374,:1.46/org/freedesktop.nm-applet/1000]: agent registered
Oct 08 17:29:12 debian NetworkManager[498]: <info> [1728422952.8731] dhcpc6 (enp0s3): state changed new lease, address=2800:810:458:173:8879:c1b2:f8ba:ceb5
Oct 08 17:57:51 debian NetworkManager[498]: <info> [1728424671.0885] dhcpc6 (enp0s3): state changed new lease, address=2800:810:458:173:8879:c1b2:f8ba:ceb5
Oct 08 17:58:38 debian NetworkManager[498]: <info> [1728424718.3542] dhcpc4 (enp0s3): state changed new lease, address=192.168.0.137
-- Boot ce6fc011548648ffac3a7cc24f234df2 --
```

2.1.9. Registros del Kernel

No se registraron eventos inusuales en el **kernel** durante el día de la intrusión. Sin embargo, se observaron algunos errores menores relacionados con la memoria RAM, los cuales no representan un riesgo inmediato.

```
Jun 24 06:26:06 debian kernel: cryptd: max_cpu_qlen set to 1000
Jun 24 06:26:06 debian kernel: AVX version of gcm_enc/dec engaged.
Jun 24 06:26:06 debian kernel: AES CTR mode by8 optimization enabled
Jun 24 06:26:06 debian kernel: Adding 998396k swap on /dev/sda5. Priority:-2 extents:1 across:998396k FS
Jun 24 06:26:06 debian kernel: snd_intel8x0 0000:00:05.0: allow list rate for 1028:0177 is 48000
Jun 24 06:26:07 debian kernel: NET: Registered PF_QIPCRTR protocol family
Jun 24 06:26:07 debian kernel: e1000: enp0s3 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX
Jun 24 06:26:07 debian kernel: IPv6: ADDRCONF(NETDEV_CHANGE): enp0s3: link becomes ready
Jun 24 06:50:19 debian kernel: [drm] vmwgfx: mob memory overflow. Consider increasing guest RAM and graphicsMemory.
Jun 24 06:50:19 debian kernel: [drm:vmw_host_printf [vmwgfx]] *ERROR* Failed to send host log message.
Jun 24 06:50:19 debian kernel: [drm] vmwgfx: increasing guest mob limits to 32768 kB.
Jun 24 08:54:10 debian kernel: e1000: enp0s3 NIC Link is Down
Jun 24 08:54:16 debian kernel: e1000: enp0s3 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX
lines 554-583/583 (END)
```

2.1.10. Registro del Servicio Cron

Se realizó la búsqueda de registros de cron con el comando journald -u cron. Los logs mostraron que los archivos ejecutados por cron son propios del sistema y no presentan anomalías, lo que indica que no hubo tareas programadas maliciosas relacionadas con la intrusión.

```
File Edit View Search Terminal Help
GNU nano 7.2                                     cron.txt
-- Boot af0a79f76920440c8e08594d6547449b --
Oct 08 17:28:37 debian systemd[1]: Started cron.service - Regular background program processing daemon.
Oct 08 17:28:37 debian cron[484]: (CRON) INFO (pidfile fd = 3)
Oct 08 17:28:37 debian cron[484]: (CRON) INFO (Running @reboot jobs)
Oct 08 17:30:01 debian CRON[1500]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Oct 08 17:30:01 debian CRON[1501]: (root) CMD ([ -x /etc/init.d/anacron ] && if [ ! -d /run/systemd/system ]; then /usr/sbin/invocation-rc.d anacron start >/dev/null)
Oct 08 17:30:01 debian CRON[1500]: pam_unix(cron:session): session closed for user root
Oct 08 17:39:01 debian CRON[1574]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Oct 08 17:39:01 debian CRON[1574]: pam_unix(cron:session): session closed for user root
-- Boot ce6fc011548648ffac3a7cc24f234df2 --
Jun 04 21:36:02 debian systemd[1]: Started cron.service - Regular background program processing daemon.
Jun 04 21:36:02 debian cron[466]: (CRON) INFO (pidfile fd = 3)
Jun 04 21:36:02 debian cron[466]: (CRON) INFO (Running @reboot jobs)
Jun 04 21:39:01 debian CRON[956]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Jun 04 21:39:01 debian CRON[957]: (root) CMD ([ -x /usr/lib/php/sessionclean ] && if [ ! -d /run/systemd/system ]; then /usr/lib/php/sessionclean; fi)
Jun 04 21:39:01 debian CRON[956]: pam_unix(cron:session): session closed for user root
Jun 04 22:09:01 debian CRON[2916]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Jun 04 22:09:01 debian CRON[2916]: pam_unix(cron:session): session closed for user root
Jun 04 22:17:01 debian CRON[2996]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Jun 04 22:17:01 debian CRON[2997]: (root) CMD (cd / & run-parts --report /etc/cron.hourly)
Jun 04 22:17:01 debian CRON[2996]: pam_unix(cron:session): session closed for user root
Jun 04 22:30:01 debian CRON[3005]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Jun 04 22:30:01 debian CRON[3006]: (root) CMD ([ -x /etc/init.d/anacron ] && if [ ! -d /run/systemd/system ]; then /usr/sbin/invocation-rc.d anacron start >/dev/null)
Jun 04 22:30:01 debian CRON[3005]: pam_unix(cron:session): session closed for user root
Jun 04 22:39:01 debian CRON[3247]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Jun 04 22:39:01 debian CRON[3248]: (root) CMD ([ -x /usr/lib/php/sessionclean ] && if [ ! -d /run/systemd/system ]; then /usr/lib/php/sessionclean; fi)
Jun 04 22:39:01 debian CRON[3247]: pam_unix(cron:session): session closed for user root
```

```
debian@debian:/etc$ ls /etc/cron
cron.d/      cron.daily/   cron.hourly/  cron.monthly/ crontab      cron.weekly/  cron.yearly/
```

```
○                                            debian@debian:/etc/cron.weekly
File Edit View Search Terminal Help
GNU nano 7.2                                         0anacron
#!/bin/sh
#
# anacron's cron script
#
# This script updates anacron time stamps. It is called through run-parts
# either by anacron itself or by cron.
#
# The script is called "0anacron" to assure that it will be executed
# _before_ all other scripts.

test -x /usr/sbin/anacron || exit 0
anacron -u cron.weekly
```

```
○                                            debian@debian:/etc/cron.weekly
File Edit View Search Terminal Help
GNU nano 7.2                                         man-db *
export PATH="$PATH:/usr/local/sbin:/usr/sbin:/sbin"

iosched_idle=
# Don't try to change I/O priority in a vserver or OpenVZ.
if ! grep -Eq '(envID|VxID):.*[1-9]' /proc/self/status && \
{ [ ! -d /proc/vz ] || [ -d /proc/bc ]; }; then
    iosched_idle='--iosched idle'
fi

if ! [ -d /var/cache/man ]; then
    # Recover from deletion, per FHS.
    install -d -o man -g man -m 0755 /var/cache/man
fi

# regenerate man database
if [ -x /usr/bin/man-db ]; then
    # --pidfile /dev/null so it always starts; mandb isn't really a daemon,
    # but we want to start it like one.
    # shellcheck disable=SC2086
    start-stop-daemon --start --pidfile /dev/null \
                      --startas /usr/bin/man-db --oknodo --chuid man \
                      $iosched_idle \
                      -- --quiet
fi

exit 0
```

3. Revisión de Usuarios, Grupos y Permisos en el Sistema

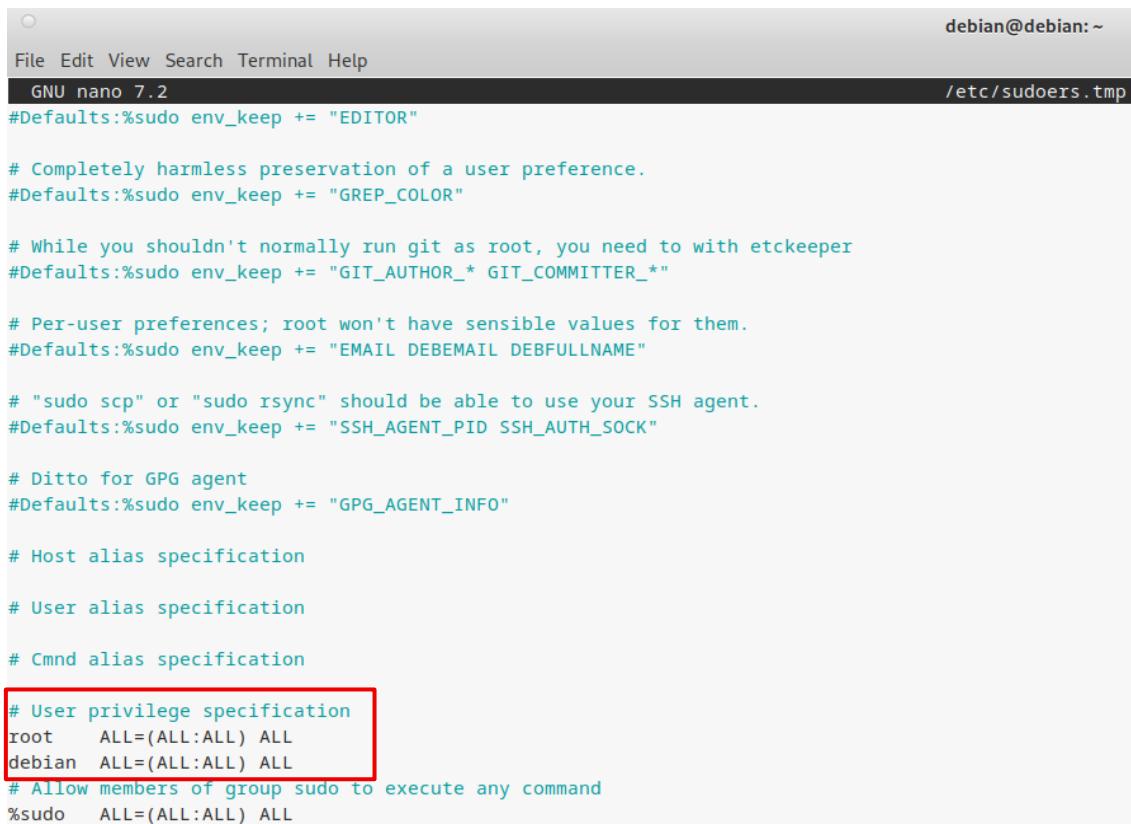
Se realizó una revisión de los usuarios, sus grupos y los permisos de archivos importantes en el servidor para identificar posibles configuraciones inseguras. A continuación, se detallan los hallazgos y las recomendaciones basadas en estos resultados:

3.1. Usuarios del Sistema:

root: Usuario con acceso completo al sistema. Este usuario tiene privilegios elevados y debe ser protegido para evitar accesos no autorizados.

debian: Este usuario no está directamente en el grupo sudo, pero la configuración en el archivo `sudoers.tmp` le otorga acceso completo a los comandos de administrador. La línea `debian ALL=(ALL:ALL) ALL` en el archivo de configuración de sudo permite a este usuario ejecutar cualquier comando con privilegios elevados.

Recomendación: Es importante revisar si este usuario necesita estos privilegios. Si no es necesario, debería limitarse el acceso a privilegios elevados o eliminarlo de la configuración de sudoers.



```
File Edit View Search Terminal Help
GNU nano 7.2                               debian@debian: ~
/etc/sudoers.tmp

#Defaults:%sudo env_keep += "EDITOR"

# Completely harmless preservation of a user preference.
#Defaults:%sudo env_keep += "GREP_COLOR"

# While you shouldn't normally run git as root, you need to with etckeeper
#Defaults:%sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER_"

# Per-user preferences; root won't have sensible values for them.
#Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your SSH agent.
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification

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

Otros: Usuarios como www-data (para el servidor web), mysql (para la base de datos), y ftp están configurados sin acceso interactivo (/usr/sbin/nologin), lo que es adecuado para servicios que no requieren acceso directo al sistema.

```
debian@debian:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:101:110:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:102:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:103:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:104:112:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:x:105:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
pulse:x:106:114:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:x:107:117::/var/lib/saned:/usr/sbin/nologin
lightdm:x:108:118:Light Display Manager:/var/lib/lightdm:/bin/false
polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin
rtkit:x:109:119:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:110:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
debian:x:1000:1000:4geeks,,,:/home/debian:/bin/bash
mysql:x:111:121:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
ftp:x:113:122:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
debian@debian:~$ █
```

3.2. Grupos Del Sistema:

sudo: Aunque el usuario debian no es miembro explícito de este grupo, tiene acceso completo a sudo debido a la configuración en el archivo sudoers. Este acceso debe ser restringido a usuarios que realmente lo necesiten.

www-data: Este grupo es utilizado por el servidor web para acceder a archivos relacionados con el sitio web. Los archivos dentro de /var/www/html tienen permisos de escritura, lo que permite a este grupo modificar el contenido del servidor web.

mysql: Este grupo tiene acceso a los archivos de la base de datos. Los permisos de este grupo deben ser cuidadosamente gestionados para evitar accesos no autorizados a datos sensibles.

```
debian@debian:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:debian
floppy:x:25:debian
tape:x:26:
sudo:x:27:
audio:x:29:pulse,debian
dip:x:30:debian
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
shadow:x:42:
utmp:x:43:
video:x:44:debian
sasl:x:45:
plugdev:x:46:debian
staff:x:50:
games:x:60:
users:x:100:debian
nogroup:x:65534:
systemd-journal:x:999:
systemd-network:x:998:
crontab:x:101:
input:x:102:
sgx:x:103:
kvm:x:104:
render:x:105:
netdev:x:106:debian
systemd-timesync:x:997:
messagebus:x:107:
_ssh:x:108:
ssl-cert:x:109:
avahi-autoipd:x:110:
bluetooth:x:111:debian
avahi:x:112:
lpadmin:x:113:debian
pulse:x:114:
pulse-access:x:115:
scanner:x:116:saned,debian
saned:x:117:
lightdm:x:118:
polkitd:x:996:
rtkit:x:119:
colord:x:120:
debian:x:1000:
mysql:x:121:
ftp:x:122:
```

- **En Conclusión**

Usuarios con shell /bin/bash: El usuario root y debian tienen acceso completo al sistema. Es importante asegurar que estos usuarios tengan contraseñas fuertes, y en el caso de debian, limitar su acceso si no es necesario.

Usuarios con shell /usr/sbin/nologin o /bin/false: Estos usuarios no tienen acceso interactivo, lo que es adecuado para usuarios del sistema como www-data, mysql, ftp, y otros que solo requieren permisos de servicio sin acceso a la línea de comandos.

Usuario	Shell	Grupos	Descripción
root	/bin/bash	root	Usuario administrador con acceso completo al sistema.
debian	/bin/bash	sudo, debian	Usuario estándar, necesita tener una contraseña fuerte para mayor seguridad.
daemon	/usr/sbin/nologin	daemon	Usuario de sistema, no tiene acceso interactivo.
www-data	/usr/sbin/nologin	www-data	Usuario de servidor web, no tiene acceso interactivo.
_apt	/bin/false	_apt	Usuario para gestionar paquetes, sin acceso interactivo.
ftp	/usr/sbin/nologin	ftp	Usuario de servicio FTP, sin acceso interactivo.
polkitd	/usr/sbin/nologin	polkitd	Usuario de servicio de política, sin acceso interactivo.
pulse	/usr/sbin/nologin	pulse, debian	Usuario de servicio de audio, sin acceso interactivo.
mysql	/bin/false	mysql	Usuario de base de datos MySQL, sin acceso interactivo.
saned	/usr/sbin/nologin	saned	Usuario de servicio para escáneres, sin acceso interactivo.

4. Revisión de Carpetas, Permisos y Configuraciones

Durante la revisión del sistema, se encontró que varios archivos y carpetas importantes del servidor tienen configuraciones de seguridad que podrían poner en riesgo la protección de la información. Específicamente, se encontraron dos problemas principales relacionados con los permisos de acceso a los archivos del servidor web y directorios listables.

4.1. Permisos de la carpeta /var/www/html:

La carpeta donde se almacenan los archivos del sitio web, llamada /var/www/html, tiene permisos demasiado amplios. Esto significa que cualquier usuario en el servidor puede modificar, borrar o agregar archivos en esta carpeta, lo cual no es seguro.

Recomendación: Se debe restringir el acceso a esta carpeta para que solo las personas o procesos que necesiten modificar los archivos del sitio web puedan hacerlo. Para ello, los permisos deben cambiarse a 755, lo que permite que solo el dueño de los archivos pueda modificarlos, mientras que otros usuarios solo podrán verlos o ejecutarlos.

```
debian@debian:~$ ls -l /var/www/html/
total 248
-rwxrwxrwx 1 www-data www-data 10701 Sep 30 2024 index.html
-rwxrwxrwx 1 www-data www-data    405 Feb  6 2020 index.php
-rwxrwxrwx 1 www-data www-data 19903 Jun 13 22:26 license.txt
-rwxrwxrwx 1 www-data www-data   7425 Jun 13 22:26 readme.html
-rwxrwxrwx 1 www-data www-data  7387 Feb 13 2024 wp-activate.php
drwxrwxrwx 9 www-data www-data  4096 Sep 10 2024 wp-admin
-rwxrwxrwx 1 www-data www-data    351 Feb  6 2020 wp-blog-header.php
-rwxrwxrwx 1 www-data www-data  2323 Jun 14 2023 wp-comments-post.php
-rwxrwxrwx 1 www-data www-data  3017 Sep 30 2024 wp-config.php
-rwxrwxrwx 1 www-data www-data  3336 Jun 13 22:26 wp-config-sample.php
drwxrwxrwx 6 www-data www-data  4096 Jun 20 19:48 wp-content
-rwxrwxrwx 1 www-data www-data  5617 Jun 13 22:26 wp-cron.php
drwxrwxrwx 30 www-data www-data 12288 Jun 13 22:26 wp-includes
-rwxrwxrwx 1 www-data www-data  2502 Nov 26 2022 wp-links-opml.php
-rwxrwxrwx 1 www-data www-data 3937 Mar 11 2024 wp-load.php
-rwxrwxrwx 1 www-data www-data 51414 Jun 13 22:26 wp-login.php
-rwxrwxrwx 1 www-data www-data  8727 Jun 13 22:26 wp-mail.php
-rwxrwxrwx 1 www-data www-data 30081 Jun 13 22:26 wp-settings.php
-rwxrwxrwx 1 www-data www-data 34516 Jun 13 22:26 wp-signup.php
-rwxrwxrwx 1 www-data www-data  5102 Jun 13 22:26 wp-trackback.php
-rwxrwxrwx 1 www-data www-data  3205 Jun 13 22:26 xmlrpc.php
debian@debian:~$
```

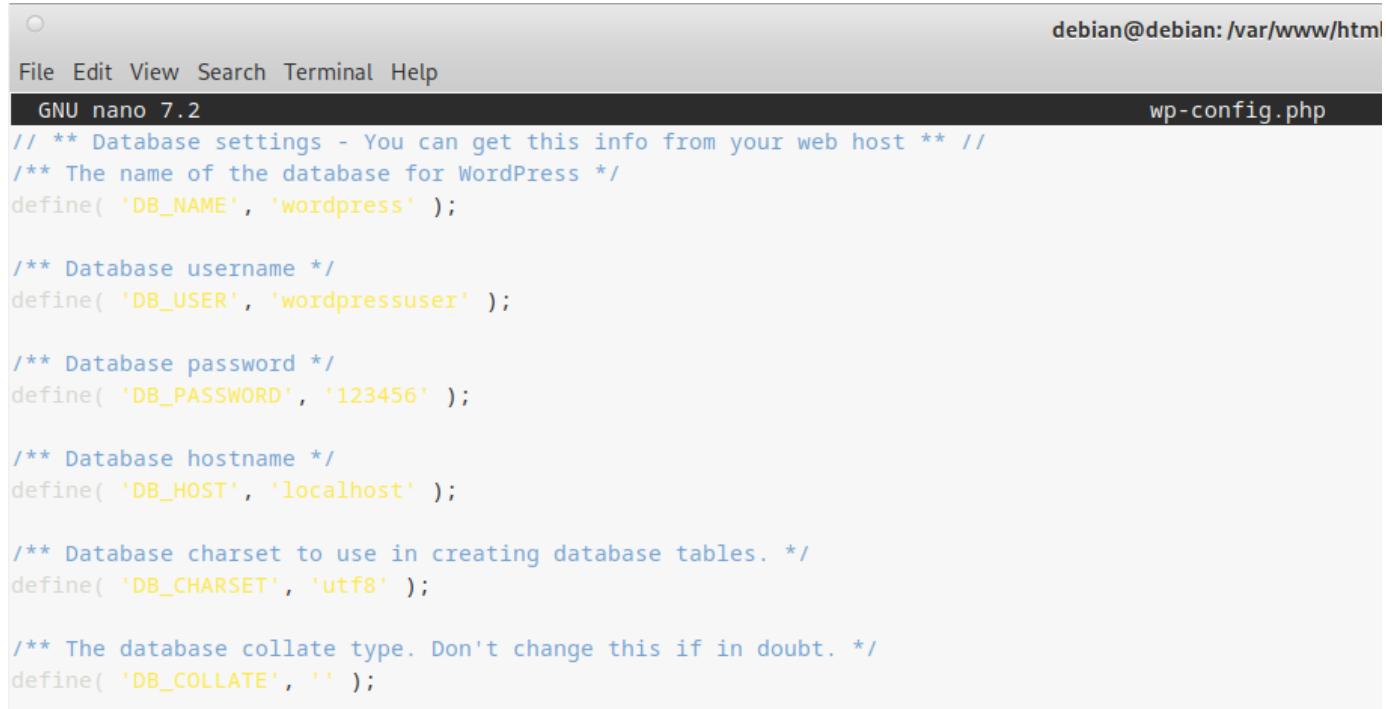
4.2. Archivo wp-config.php:

El archivo wp-config.php contiene información muy sensible, como el nombre de usuario y la contraseña de la base de datos del sitio web. Actualmente, este archivo tiene permisos que admiten a cualquier usuario del servidor acceder a estas credenciales, lo que es un grave problema de seguridad.

Possible acción del atacante: El intruso pudo haber robado estas credenciales para acceder a la web y robar más datos.

Recomendación: Es importante cambiar las credenciales nuevamente colocando contraseñas más fuertes, ademas este archivo debe ser protegido cambiando sus permisos a 600, lo que significa que solo el dueño del archivo podrá verlo o modificarlo. De esta manera, se asegura que la información sensible no esté accesible para personas no autorizadas.

```
debian@debian:~$ ls -l /var/www/html/wp-config.php
-rwxrwxrwx 1 www-data www-data 3017 Sep 30 2024 /var/www/html/wp-config.php
```



The screenshot shows a terminal window with the command 'ls -l /var/www/html/wp-config.php' run, displaying the file's permissions as rwxrwxrwx. Below this, the file 'wp-config.php' is open in the 'nano' text editor. The code within the file is as follows:

```
// ** 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', '' );
```

4.3. Archivo Apache2.conf

Al revisar el archivo apache2.conf, se identificaron varias configuraciones de directorios que permiten el listado de archivos, lo cual representa un riesgo de seguridad. A continuación, se detallan los directorios afectados:

Directarios Listables:

- / (Raíz del sistema):
- /usr/share/:
- /var/www/:

Conclusión:

La configuración actual de Apache permite el listado de directorios en estas tres rutas, lo que representa un riesgo de seguridad. Se debe deshabilitar esta opción cambiando Options Indexes por Options FollowSymLinks en los bloques correspondientes de configuración para proteger el servidor web.

```
GNU nano 7.2                                         apache2.conf *
# the latter may be used for local directories served by the web server. If
# your system is serving content from a sub-directory in /srv you must allow
# access here, or in any related virtual host.
<Directory />
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>

<Directory /usr/share>
    AllowOverride None
    Options Indexes FollowSymLinks
    Require all granted
</Directory>

<Directory /var/www/>
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>
```

4.4. Archivo vsftpd.conf:

Se encontraron las siguientes falencias de seguridad en la configuración de vsftpd.conf:

```
GNU nano 7.2                                     /etc/vsftpd.conf
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
```

Acceso anónimo habilitado:

El acceso anónimo está permitido (anonymous_enable=YES), lo que permite que usuarios no autenticados accedan al FTP.

Recomendación: Deshabilitar el acceso anónimo cambiando a anonymous_enable=NO.

Permisos de escritura habilitados:

La opción write_enable=YES está activada, permitiendo que los usuarios suban archivos.

Recomendación: Deshabilitar la escritura si no es necesaria, cambiando a write_enable=NO.

Con estos ajustes, el servidor FTP será más seguro al limitar el acceso no autorizado y el control de archivos.

4.5. Archivo sshd_config

Se encontraron las siguientes falencias de seguridad en la configuración de sshd_config:

```
GNU nano 7.2                                     /etc/ssh/sshd_config *

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no
```

Acceso remoto de root habilitado:

La opción PermitRootLogin yes está habilitada, lo que permite que el usuario root acceda al servidor de forma remota a través de SSH. Esto representa un riesgo de seguridad ya que un atacante puede intentar obtener acceso al sistema utilizando la cuenta de root.

Recomendación: Deshabilitar el acceso remoto para root cambiando la opción a PermitRootLogin no.

Autenticación de contraseñas en texto claro permitida:

La opción PasswordAuthentication yes está habilitada, lo que permite que los usuarios se autentiquen utilizando contraseñas en texto claro. Esto puede ser riesgoso si las contraseñas no están cifradas.

Recomendación: Deshabilitar la autenticación por contraseña y forzar el uso de claves públicas para la autenticación. Cambiar la opción a PasswordAuthentication no.

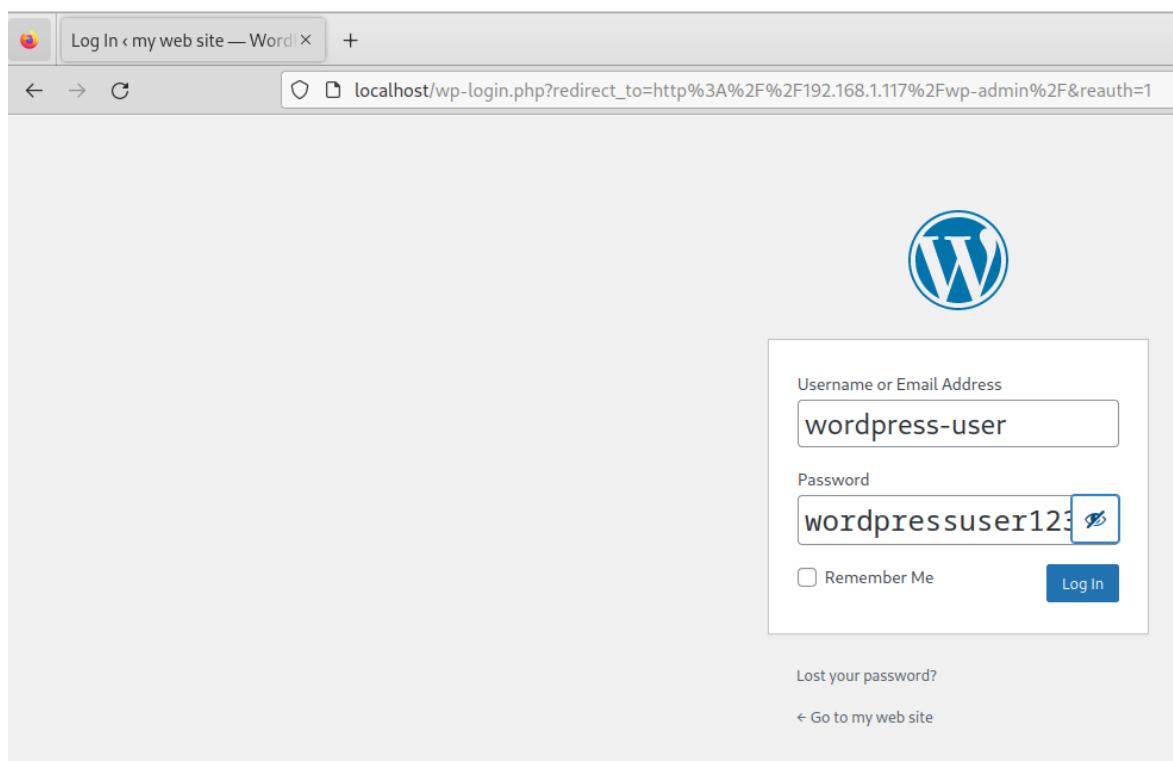
5. Revisión de Datos Comprometidos

5.1. Credenciales expuestas en la web:

Durante la revisión de la seguridad del sistema, se detectó que las credenciales de acceso de un usuario en WordPress estaban expuestas en el formulario de inicio de sesión. Las credenciales de usuario `wordpress-user` con la contraseña `wordpressuser123` fueron visibles en el sistema, lo que aumenta aún más la posibilidad de que estas credenciales hayan sido comprometidas por el atacante.

Posibles acciones del atacante:

- Acceso no autorizado: Las credenciales comprometidas pudieron ser fácilmente utilizadas por el atacante para acceder al panel de administración de WordPress y realizar modificaciones maliciosas.
- Robo de información sensible: El atacante pudo obtener esta información confidencial almacenada en el sistema de WordPress, como tambien datos de usuarios o configuraciones del sitio.



5.2. Revisión del archivo /root/.mysql_history:

El archivo /root/.mysql_history registra los comandos ejecutados en MySQL. Al revisar este archivo, encontramos varios comandos que podrían indicar que el atacante pudo haber hecho cambios importantes en el sistema de bases de datos.

Comando utilizado: sudo cat /root/.mysql_history

```
debian@debian:$ sudo cat /root/.mysql_history
_Hist0rY_V2_
CREATE\040DATABASE\040wordpress\040DEFAULT\040CHARACTER\040SET\040utf8\040COLLATE\040utf8_unicode_ci;
CREATE\040USER\040'wordpressuser'@\040localhost'\040IDENTIFIED\040BY\040'123456';
GRANT\040ALL\040PRIVILEGES\040ON\040wordpress.*\040TO\040'wordpress'@\040localhost';\040
GRANT\040ALL\040PRIVILEGES\040ON\040wordpress.*\040TO\040'wordpressuser'@\040localhost';
FLUSH\040PRIVILEGES;
FLUSH\040PRIVILEGES;
EXIT;
CREATE\040USER\040'user'@\040localhost'\040IDENTIFIED\040BY\040'password';
GRANT\040ALL\040PRIVILEGES\040ON\040*.*\040TO\040'user'@\040localhost'\040WITH\040GRANT\040OPTION;
FLUSH\040PRIVILEGES;
EXIT;
```

Acciones encontradas en el archivo:

- **Creación de la base de datos wordpress:** Se creó una base de datos para instalar o modificar WordPress en el servidor. Si esta acción no fue hecha por la compañía entonces el atacante pudo haber sido el autor de dicha creación.

Comando detectado: CREATE DATABASE wordpress DEFAULT CHARACTER SET utf8 COLLATE utf8_unicode_ci;

- **Creación del usuario wordpressuser:** Se creó un usuario llamado wordpressuser con una contraseña débil 123456 y se le dio privilegios completos sobre la base de datos de WordPress. Esto le permite acceder a toda la información almacenada en WordPress.

Comando detectado: CREATE USER 'wordpressuser'@'localhost' IDENTIFIED BY '123456';

GRANT ALL PRIVILEGES ON wordpress.* TO 'wordpressuser'@'localhost';

- **Creación del usuario user:** También se creó otro usuario llamado user sin contraseña y con privilegios completos sobre todas las bases de datos. Este usuario podría haber sido creado por el atacante para dar acceso adicional y total a la base de datos.

Comando detectado: CREATE USER 'user'@'localhost' IDENTIFIED BY 'password';

GRANT ALL PRIVILEGES ON *.* TO 'user'@'localhost' WITH GRANT OPTION;

- **Possible acción del atacante:**

El atacante pudo haber creado el usuario user para tener control total sobre la información del sistema y WordPress, lo que le permitiría robar o modificar datos sensibles.

Es importante verificar si estos usuarios y bases de datos son parte del entorno de trabajo normal de la compañía para descartar si estas acciones fueron hechas con fines maliciosos y tomar medidas. Aún así hay varias falencias de seguridad como contraseñas débiles y excesos de privilegios que hay que mitigar.

5.3. Usuarios en MySQL:

Se verificaron los usuarios registrados en MySQL y se identificaron los siguientes:

- **mariadb.sys**: Un usuario interno utilizado por MariaDB.
- **mysql**: Usuario del sistema de bases de datos.
- **root**: Usuario administrador con acceso completo al sistema.
- **user**: Posible Usuario creado por el atacante.
- **wordpressuser**: Usuario asociado con la base de datos wordpress, con credenciales débiles.

Possible acción del atacante:

Como en lo anteriormente dicho, el atacante pudo haber creado el usuario user sin contraseña el cual les otorgó privilegios completos sobre la base de datos en general. Esto le habría permitido tener acceso completo a la base de datos y realizar cualquier tipo de operación.

Comando utilizado: sudo mysql -e "SELECT user, host FROM mysql.user;"

```
debian@debian:/$ sudo mysql -e "SELECT user, host FROM mysql.user;"  
+-----+-----+  
| User      | Host    |  
+-----+-----+  
| mariadb.sys | localhost |  
| mysql       | localhost |  
| root        | localhost |  
| user        | localhost |  
| wordpressuser | localhost |  
+-----+-----+
```

5.4. Bases de Datos en el Sistema:

Se revisaron las bases de datos en el sistema y se identificaron las siguientes:

- **information_schema**: Base de datos del sistema de MySQL que almacena metadatos.
- **mysql**: Base de datos del sistema de MySQL que maneja los usuarios y privilegios.
- **performance_schema**: Base de datos que almacena estadísticas de rendimiento.
- **sys**: Base de datos del sistema utilizada para diagnóstico y administración.
- **wordpress**: Base de datos utilizada por el sistema de WordPress.

Recordemos que el archivo **wp-config.php** fue comprometido, por lo que posiblemente se tienen todas las credenciales de la base de datos wordpress.

Comando utilizado: sudo mysql -e "SHOW DATABASES;"

```
debian@debian:/ $ sudo mysql -e "SHOW DATABASES;"  
+-----+  
| Database      |  
+-----+  
| information_schema |  
| mysql          |  
| performance_schema |  
| sys            |  
| wordpress      |  
+-----+
```

5.5. Privilegios de los Usuarios:

Se verificaron los privilegios asignados a varios usuarios de MySQL y se encontraron los siguientes:

- **mariadb.sys:** Este usuario tiene privilegios limitados sobre las bases de datos de sistema.
- **mysql:** Este usuario tiene privilegios completos sobre la base de datos mysql (GRANT ALL PRIVILEGES ON *.* mysql @ localhost).
- **root:** Este usuario tiene privilegios completos sobre todas las bases de datos (GRANT ALL PRIVILEGES ON *.*).
- **user:** Este usuario tiene privilegios elevados sobre todas las bases de datos (GRANT ALL PRIVILEGES ON *.*).
- **wordpressuser:** Este usuario tiene privilegios completos sobre la base de datos wordpress (GRANT ALL PRIVILEGES ON wordpress.*).

Possible acción del atacante:

El atacante pudo haber otorgado privilegios completos al usuario user, lo que le habría permitido manipular cualquier base de datos, crear nuevos usuarios, y alterar configuraciones de seguridad. Esto representa un grave riesgo de seguridad, ya que le otorgó un control total sobre el sistema.

Comando utilizado: sudo mysql -e "SHOW GRANTS FOR 'usuario'@'localhost';"

```
debian@debian:/$ sudo mysql -e "SHOW GRANTS FOR 'mariadb.sys'@'localhost';"
+-----+
| Grants for mariadb.sys@localhost
+-----+
| GRANT USAGE ON *.* TO `mariadb.sys`@`localhost`
| GRANT SELECT, DELETE ON `mysql`.`global_priv` TO `mariadb.sys`@`localhost`
+-----+
debian@debian:/$ sudo mysql -e "SHOW GRANTS FOR 'mysql'@'localhost';"
+-----+
| Grants for mysql@localhost
+-----+
| GRANT ALL PRIVILEGES ON *.* TO `mysql`@`localhost` IDENTIFIED VIA mysql_native_password USING 'invalid' OR unix_socket WITH GRANT OPTION
| GRANT PROXY ON ''@''%'' TO `mysql`@`localhost` WITH GRANT OPTION
+-----+
debian@debian:/$ sudo mysql -e "SHOW GRANTS FOR 'root'@'localhost';"
+-----+
| Grants for root@localhost
+-----+
| GRANT ALL PRIVILEGES ON *.* TO `root`@`localhost` IDENTIFIED VIA mysql_native_password USING '*6BB4837EB74329105EE4568D
DA7DC67ED2CA2AD9' OR unix_socket WITH GRANT OPTION
| GRANT PROXY ON ''@''%'' TO `root`@`localhost` WITH GRANT OPTION
+-----+
+-----+
debian@debian:/$ sudo mysql -e "SHOW GRANTS FOR 'user'@'localhost';"
+-----+
| Grants for user@localhost
+-----+
| GRANT ALL PRIVILEGES ON *.* TO `user`@`localhost` IDENTIFIED BY PASSWORD '*2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19' WITH GRANT OPTION
+-----+
debian@debian:/$ sudo mysql -e "SHOW GRANTS FOR 'wordpressuser'@'localhost';"
+-----+
| Grants for wordpressuser@localhost
+-----+
| GRANT USAGE ON *.* TO `wordpressuser`@`localhost` IDENTIFIED BY PASSWORD '*6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9'
| GRANT ALL PRIVILEGES ON `wordpress`.* TO `wordpressuser`@`localhost`
+-----+
```

5.6. Análisis de la Base de Datos de WordPress:

Durante el análisis de la base de datos de WordPress, se encontraron varias tablas relevantes que contienen información crucial sobre los usuarios y el contenido del sitio. Se revisó la tabla wp_users, que almacena los datos de los usuarios registrados en WordPress. En ella se encontró lo siguiente:

```
MariaDB [wordpress]> SHOW TABLES;
+-----+
| Tables_in_wordpress |
+-----+
| wp_commentmeta      |
| wp_comments          |
| wp_links             |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_termmeta           |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----+
12 rows in set (0.000 sec)

MariaDB [wordpress]> SELECT ID, user_login, user_email, user_pass FROM wp_users;
+-----+-----+-----+
| ID | user_login      | user_email           | user_pass          |
+-----+-----+-----+
| 1  | wordpress-user | rosinnicuentas@gmail.com | $wp$2y$10$SngfA0.aOrie2lg.CQJn9u1H83V2.IQ.pxbXy.rsxQEfr5.sM7muW |
+-----+-----+-----+
1 row in set (0.001 sec)
```

- Usuario ID 1: Corresponde al usuario administrador con el nombre wordpress-user.
- Correo electrónico: rosinnicuentas@gmail.com.
- Contraseña: Encriptada usando bcrypt con el hash:
\$wp\$2y\$10\$SngfA0.aOrie2lg.CQJn9u1H83V2.IQ.pxbXy.rsxQEfr5.sM77muW

5.7. Posible información comprometida:

Correo electrónico: El atacante pudo haber obtenido el correo del administrador.

Contraseña encriptada: Aunque encriptada, la contraseña podría haber sido descifrada si el atacante usó métodos de fuerza bruta. De igual manera ya la contraseña pudo filtrarse sin cifrado por las credenciales expuestas en la página de login de wordpress.

Conclusión:

El atacante pudo haber obtenido el correo electrónico y la contraseña encriptada del administrador, lo que representa un riesgo para el sistema. Se recomienda cambiar inmediatamente las contraseñas y usar otras con mayor seguridad.

6. Análisis de Procesos en Ejecución Inusuales

6.1. Revisión de Procesos Activos:

Se utilizó el comando top para ver los procesos que están en ejecución en el sistema. Esto nos da una visión general de qué programas están usando los recursos del sistema en tiempo real.

En los procesos revisados, no se detectaron procesos sospechosos o desconocidos. Todos los procesos son comunes y relacionados con el funcionamiento del sistema. Tampoco se nota una sobrecarga en el uso de memoria o CPU por lo que se descartan ciertos tipos de malwares.

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1480	debian	20	0	730636	17056	5956	S	7.3	0.8	4:16.65	speech-dispatch
1462	debian	20	0	108936	12080	6776	S	2.7	0.6	1:12.35	sd_espeak-ng
1036	debian	9	-11	1703280	35208	25900	S	2.3	1.7	3:57.61	pulseaudio
593	root	20	0	512668	140348	73400	S	1.3	7.0	1:58.33	Xorg
1566	debian	20	0	626568	51032	36052	S	1.0	2.5	0:45.69	mate-terminal
1224	debian	20	0	390108	72588	33252	S	0.7	3.6	1:09.72	orca
1145	debian	20	0	735888	49032	31436	S	0.3	2.4	0:16.43	marco
1170	debian	20	0	552396	48740	33528	S	0.3	2.4	0:05.15	mate-panel
1240	debian	20	0	496976	34460	23060	S	0.3	1.7	0:01.01	wnck-applet
2741	root	20	0	0	0	0	I	0.3	0.0	0:11.12	kworker/0:3-events
6690	debian	20	0	11624	5400	3256	R	0.3	0.3	0:01.42	top
1	root	20	0	102348	12508	9196	S	0.0	0.6	0:02.27	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.02	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par_gp
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	slub_flushwq
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns
8	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/0:0H-events_highpri
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_percpu_wq
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_kthread
12	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_rude_kthread
13	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_trace_kthread
14	root	20	0	0	0	0	S	0.0	0.0	0:00.22	ksoftirqd/0
15	root	20	0	0	0	0	I	0.0	0.0	0:00.65	rcu_preempt
16	root	rt	0	0	0	0	S	0.0	0.0	0:00.20	migration/0
18	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cpuhp/0
19	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cpuhp/1
20	root	rt	0	0	0	0	S	0.0	0.0	0:00.74	migration/1
21	root	20	0	0	0	0	S	0.0	0.0	0:00.10	ksoftirqd/1
26	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kdevtmpfs

6.2. Revisión de Inicios de Sesión y Eventos del Sistema:

Se revisaron los registros de inicio de sesión con el comando last. Este comando muestra los accesos al sistema y los eventos importantes como reinicios.

El atacante accedió al sistema a través de SSH a las 17:40:59 del 08 de octubre de 2024. Sin embargo, en los registros de last, no se observa actividad sospechosa después de esa hora. No se detectaron otros inicios de sesión anómalos ni eventos inusuales.

```
debian@debian:~$ last
 debian  tty7      :0          Sun Jun 29 21:21    gone - no logout
 reboot  system boot 6.1.0-25-amd64   Sun Jun 29 21:20    still running
 debian  tty7      :0          Wed Jun 25 16:30 - crash (4+04:50)
 reboot  system boot 6.1.0-25-amd64   Wed Jun 25 16:24    still running
 debian  tty7      :0          Tue Jun 24 06:50 - crash (1+09:33)
 reboot  system boot 6.1.0-25-amd64   Tue Jun 24 06:26    still running
 debian  tty7      :0          Mon Jun 23 15:14 - crash (15:11)
 reboot  system boot 6.1.0-25-amd64   Mon Jun 23 14:27    still running
 debian  tty7      :0          Sun Jun 22 20:01 - crash (18:25)
 reboot  system boot 6.1.0-25-amd64   Sun Jun 22 19:58    still running
 debian  tty7      :0          Fri Jun 20 19:48 - crash (2+00:09)
 reboot  system boot 6.1.0-25-amd64   Fri Jun 20 19:48    still running
 debian  tty7      :0          Wed Jun 18 20:21 - crash (1+23:26)
 reboot  system boot 6.1.0-25-amd64   Wed Jun 18 20:20    still running
 debian  tty7      :0          Mon Jun 16 15:27 - crash (2+04:52)
 reboot  system boot 6.1.0-25-amd64   Mon Jun 16 15:27    still running
 debian  tty7      :0          Sun Jun 15 18:30 - crash (20:56)
 reboot  system boot 6.1.0-25-amd64   Sun Jun 15 17:13    still running
 debian  tty7      :0          Fri Jun 13 22:21 - crash (1+18:51)
 reboot  system boot 6.1.0-25-amd64   Fri Jun 13 22:21    still running
 debian  tty7      :0          Fri Jun 13 22:18 - crash (00:02)
 reboot  system boot 6.1.0-25-amd64   Fri Jun 13 22:11    still running
 debian  tty7      :0          Fri Jun 13 17:59 - crash (04:11)
 reboot  system boot 6.1.0-25-amd64   Fri Jun 13 17:32    still running
 debian  tty7      :0          Fri Jun 13 17:11 - crash (00:20)
 reboot  system boot 6.1.0-25-amd64   Fri Jun 13 16:44    still running
 debian  tty7      :0          Wed Jun  4 21:39 - crash (8+19:04)
 reboot  system boot 6.1.0-25-amd64   Wed Jun  4 21:35    still running
 debian  tty7      :0          Tue Oct  8 17:28 - crash (239+04:07)
 reboot  system boot 6.1.0-25-amd64   Tue Oct  8 17:28    still running
 debian  tty7      :0          Tue Oct  8 16:48 - crash (00:40)
 reboot  system boot 6.1.0-25-amd64   Tue Oct  8 16:48    still running
 debian  tty7      :0          Tue Oct  8 16:44 - crash (00:03)
 reboot  system boot 6.1.0-25-amd64   Tue Oct  8 16:43    still running
 debian  tty7      :0          Mon Sep 30 15:13 - crash (8+01:29)
 reboot  system boot 6.1.0-25-amd64   Mon Sep 30 15:09    still running
 debian  tty7      :0          Mon Sep 30 09:49 - 12:27 (02:38)
 reboot  system boot 6.1.0-23-amd64   Mon Sep 30 09:48 - 12:28 (02:39)
 debian  tty7      :0          Sat Sep 28 16:40 - crash (1+17:08)
 reboot  system boot 6.1.0-23-amd64   Sat Sep 28 16:39 - 12:28 (1+19:48)
 debian  tty7      :0          Wed Jul 31 16:45 - 18:18 (01:33)
 reboot  system boot 6.1.0-23-amd64   Wed Jul 31 16:45 - 18:19 (01:34)
 debian  tty7      :0          Wed Jul 31 16:04 - 16:44 (00:39)
 reboot  system boot 6.1.0-23-amd64   Wed Jul 31 16:04 - 16:44 (00:40)
 debian  tty7      :0          Wed Jul 31 15:57 - 15:59 (00:01)
 reboot  system boot 6.1.0-23-amd64   Wed Jul 31 15:56 - 15:59 (00:02)

wtmp begins Wed Jul 31 15:56:58 2024
```

6.3. Revisión de Servicios Activos:

Se utilizaron comandos para revisar los servicios que están corriendo en el sistema. No se encontraron servicios desconocidos ni sospechosos que puedan estar relacionados con la intrusión.

UNIT	LOAD	ACTIVE	SUB	DESCRIPTION
accounts-daemon.service	loaded	active	running	Accounts Service
alsa-restore.service	loaded	active	exited	Save/Restore Sound Card State
apparmor.service	loaded	active	exited	Load AppArmor profiles
avahi-daemon.service	loaded	active	running	Avahi mDNS/DNS-SD Stack
console-setup.service	loaded	active	exited	Set console font and keymap
cron.service	loaded	active	running	Regular background program processing daemon
cups-browsed.service	loaded	active	running	Make remote CUPS printers available locally
cups.service	loaded	active	running	CUPS Scheduler
dbus.service	loaded	active	running	D-Bus System Message Bus
getty@tty1.service	loaded	active	running	Getty on tty1
ifupdown-pre.service	loaded	active	exited	Helper to synchronize boot up for ifupdown
keyboard-setup.service	loaded	active	exited	Set the console keyboard layout
kmod-static-nodes.service	loaded	active	exited	Create List of Static Device Nodes
lightdm.service	loaded	active	running	Light Display Manager
ModemManager.service	loaded	active	running	Modem Manager
networking.service	loaded	active	exited	Raise network interfaces
NetworkManager-wait-online.service	loaded	active	exited	Network Manager Wait Online
NetworkManager.service	loaded	active	running	Network Manager
plymouth-quit-wait.service	loaded	active	exited	Hold until boot process finishes up
plymouth-read-write.service	loaded	active	exited	Tell Plymouth To Write Out Runtime Data
plymouth-start.service	loaded	active	exited	Show Plymouth Boot Screen
polkit.service	loaded	active	running	Authorization Manager
rtkit-daemon.service	loaded	active	running	RealtimeKit Scheduling Policy Service
systemd-binfmt.service	loaded	active	exited	Set Up Additional Binary Formats
systemd-journal-flush.service	loaded	active	exited	Flush Journal to Persistent Storage
systemd-journald.service	loaded	active	running	Journal Service
systemd-logind.service	loaded	active	running	User Login Management
systemd-modules-load.service	loaded	active	exited	Load Kernel Modules
systemd-random-seed.service	loaded	active	exited	Load/Save Random Seed
systemd-remount-fs.service	loaded	active	exited	Remount Root and Kernel File Systems
systemd-sysctl.service	loaded	active	exited	Apply Kernel Variables
systemd-sysusers.service	loaded	active	exited	Create System Users
systemd-timesyncd.service	loaded	active	running	Network Time Synchronization
systemd-tmpfiles-setup-dev.service	loaded	active	exited	Create Static Device Nodes in /dev
systemd-tmpfiles-setup.service	loaded	active	exited	Create System Files and Directories
systemd-udev-trigger.service	loaded	active	exited	Coldplug All udev Devices
systemd-udevd.service	loaded	active	running	Rule-based Manager for Device Events and Files
systemd-update-utmp.service	loaded	active	exited	Record System Boot/Shutdown in UTMP
systemd-user-sessions.service	loaded	active	exited	Permit User Sessions
udisks2.service	loaded	active	running	Disk Manager
upower.service	loaded	active	running	Daemon for power management
user-runtime-dir@1000.service	loaded	active	exited	User Runtime Directory /run/user/1000
user@1000.service	loaded	active	running	User Manager for UID 1000
wpa_supplicant.service	loaded	active	running	WPA supplicant

7. Historial de Comandos

7.1. Revisión del historial de debian:

Se revisó el archivo de historial de comandos de debian. En las primeras entradas, parece que los comandos corresponden a una instalación inicial del sistema, incluyendo la configuración de servicios y la instalación de paquetes.

Comando utilizado:

```
sudo cat /home/debian/.bash_history
```

```
debian@debian:~$ sudo cat /home/debian/.bash_history
sudo systemctl stop speech-dispatcher
sudo usermod -aG root debian
pwd
sudo usermod -aG sudo debian
whoami
sudo visudo
su
sudo rmmod speakup
sudo rmmod speakup
sudo rmmod speakup_soft
sudo apt-get remove speakup
sudo apt-get remove speakup_soft
sudo ls /etc
sudo ls /etc/modprobe.d/
sudo nano /etc/modprobe.d/blacklist-speakup.conf
sudo nano /etc/default/grub
sudo update-grub
sudo reboot
dpkg -l | grep -i speech
sudo apt-get remove speech
dpkg -l | grep -i voice
dpkg -l | grep -i espeak
sudo apt-get remove espeak
sudo apt-get remove espeakup
sudo apt-get remove libespeak
sudo nano /etc/modprobe.d/blacklist-speakup.conf
dpkg -l | grep -i festival
dpkg -l | grep -i espeakup
sudo apt-get remove espeakup
sudo systemctl disable espeakup
sv-inst
sudo systemd-sysv-install disable espeakup
sudo /lib/systemd/systemd-sysv-install disable espeakup
sudo service espeakup stop
sudo systemctl status espeakup
sudo apt-get install git
git --version
pwd
ls
sudo apt update && sudo apt upgrade -y
sudo apt install apache2 -y
sudo systemctl enable apache2
sudo systemctl start apache2
sudo systemctl status apache2
sudo apt install mysql-server php php-mysqli -y
```

```
sudo apt install mariadb-server -y
sudo systemctl start mariadb
sudo apt install mariadb-server
sudo systemctl start mariadb-server
sudo systemctl start mariadb
sudo systemctl enable mariadb
sudo mysql_secure_installation
sudo mysql -u root -p
cd /tmp
curl -O https://wordpress.org/latest.tar.gz
sudo apt install curl
curl -O https://wordpress.org/latest.tar.gz
tar xzvf latest.tar.gz
sudo cp -a /tmp/wordpress/. /var/www/html/
sudo chown -R www-data:www-data /var/www/html/
sudo chmod -R 755 /var/www/html/
cd /var/www/html/
sudo mv wp-config-sample.php wp-config.php
sudo nano wp-config.php
ip a
sudo systemctl restart apache2
sudo systemctl status apache2
sudo apt install php libapache2-mod-php php-mysqli php-gd php-xml php-mbstring php-curl -y
cd ..
sudo nano /etc/apache2/sites-available/000-default.conf
sudo systemctl restart apache2
sudo nano /var/www/html/info.php
ls /var/www/html
sudo apt install openssh-server -y
sudo systemctl start ssh
sudo systemctl enable ssh
sudo systemctl status ssh
sudo systemctl start apache2
```

Comandos encontrados:

Comandos típicos como systemctl, apt-get, y nano se utilizaron para configurar servicios como Apache, MariaDB, y otros paquetes del sistema.

Los comandos de instalación de WordPress también son evidentes, como curl para descargar archivos de WordPress y la configuración de la base de datos.

Tambien se encontraron comandos de modificación de permisos como chmod -R 755 /var/www/html/.

7.2. Revisión del historial de root:

Se revisó el historial de comandos del usuario root. Sin embargo, no se encontraron registros previos a la intrusión; el historial de root parece estar vacío o no contener información relevante antes de los comandos ejecutados tras la intrusión. Esto podría indicar que el atacante borró el historial después realizar sus acciones.

Comando utilizado:

`sudo cat /root/.bash_history`

```
debian@debian:~$ sudo cat /root/.bash_history
sudo visudo
sudo systemctl stop speech-dispatcher
sudo systemctl disable speech-dispatcher
systemctl list-units --type=service
systemctl status apache2
systemctl stop apache2
systemctl status apache2
systemctl status apache2
systemctl stop vsftpd
systemctl status vsftpd
ifconfig
systemctl list-units --type=service --state=active | wc -l
systemctl list-units --type=service --state=active
clear
journalctl | grep -in "root"
journalctl | grep -in "root" > /home/debian/Desktop/root.txt
nano /home/debian/Desktop/root.txt
journalctl | grep -in "useradd" > /home/debian/Desktop/useradd.tx
```

Possible acción del atacante:

La ausencia de registros en el historial de root podría ser una señal de que el atacante borró o alteró el historial de comandos para ocultar sus acciones. Este comportamiento es común para intentar encubrir actividades maliciosas.

8. Detección de Rootkits o Malware

8.1. CHKRootkit

Con la herramienta CHKRootkit se realizaron varias comprobaciones de seguridad en el sistema, específicamente en la presencia de posibles rootkits y actividades sospechosas en el tráfico de red. Los resultados más relevantes fueron son los siguientes:

```
Checking `w'...                                not infected
Checking `write'...                             not infected
Checking `aliens'...                            started
Searching for suspicious files in /dev...      not found
Searching for known suspicious directories...   not found
Searching for known suspicious files...         not found
Searching for sniffer's logs...                 not found
Searching for HiDrootkit rootkit...             not found
Searching for t0rn rootkit...                   not found
Searching for t0rn v8 (or variation)...         not found
Searching for Lion rootkit...                   not found
Searching for RSHA rootkit...                  not found
Searching for RH-Sharpe rootkit...              not found
Searching for Ambient (ark) rootkit...          not found
Searching for suspicious files and dirs...     WARNING

WARNING: The following suspicious files and directories were found:
/usr/lib/libreoffice/share/.registry

Searching for zero-size shell history files...  not found
Searching for hardlinked shell history files... not found
Checking `aliens'...                            finished
Checking `asp'...                               not infected
Checking `bindshell'...                          not found
Checking `lkm'...                               started
Searching for Adore LKM...                     not tested
Searching for sebek LKM (Adore based)...       not tested
Searching for knark LKM rootkit...              not found
Searching for for hidden processes with chkproc... not found
Searching for for hidden directories using chkdirs... not found
Checking `lkm'...                               finished
Checking `rexedcs'...                           not found
Checking `sniffer'...                           WARNING

WARNING: Output from ifpromisc:
lo: not promisc and no packet sniffer sockets
enp0s3: PACKET SNIFFER(/usr/sbin/NetworkManager[467])
```

- **LibreOffice:** Se verificó el directorio .registry de LibreOffice y se confirmó que los archivos son legítimos, por lo que no hay ningún problema con la instalación de LibreOffice. Además, se realizó una reinstalación del programa para asegurar que todo esté en orden.
- **Comandos utilizados:** sudo rm -fr /usr/lib/libreoffice/share/.registry
sudo apt-get install --reinstall libreoffice

```
debian@debian:~$ sudo ls -l /usr/lib/libreoffice/share/.registry
[sudo] password for debian:
total 3380
-rw-r--r-- 1 root root 13613 Mar 18 13:53 base.xcd
-rw-r--r-- 1 root root 220624 Mar 18 13:53 calc.xcd
-rw-r--r-- 1 root root 67698 Mar 18 13:53 draw.xcd
-rw-r--r-- 1 root root 90749 Mar 18 13:53 graphicfilter.xcd
-rw-r--r-- 1 root root 296347 Mar 18 13:53 impress.xcd
-rw-r--r-- 1 root root 568 Mar 18 13:53 Langpack-en-US.xcd
-rw-r--r-- 1 root root 1692 Mar 18 13:53 lingucomponent.xcd
-rw-r--r-- 1 root root 2197121 Mar 18 13:53 main.xcd
-rw-r--r-- 1 root root 24042 Mar 18 13:53 math.xcd
-rw-r--r-- 1 root root 715 Mar 18 13:53 ogltrans.xcd
-rw-r--r-- 1 root root 9288 Mar 18 13:53 pdfimport.xcd
-rw-r--r-- 1 root root 1646 Mar 18 13:53 postgresql.xcd
-rw-r--r-- 1 root root 584 Mar 18 13:53 pyuno.xcd
-rw-r--r-- 1 root root 36537 Mar 18 13:53 reportbuilder.xcd
drwxr-xr-x 2 root root 4096 Jul 2 02:08 res
-rw-r--r-- 1 root root 440672 Mar 18 13:53 writer.xcd
-rw-r--r-- 1 root root 18364 Mar 18 13:53 xsltfilter.xcd
```

```
debian@debian:~$ sudo rm -fr /usr/lib/libreoffice/share/.registry/
debian@debian:~$ sudo apt-get install --reinstall libreoffice
```

- **NetworkManager:** El proceso CHKRootkit reportó que NetworkManager estaba utilizando un sniffer de red. Para confirmar este comportamiento, se verificó si la interfaz enp0s3 estaba en modo promiscuo.

- **Comando utilizado:** ip addr show

```
debian@debian:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1a:22:20 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.117/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
        valid_lft 56905sec preferred_lft 56905sec
    inet6 fe80::a00:27ff:fea:2220/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

La interfaz enp0s3 está configurada correctamente con la dirección IP 192.168.1.117, y no se observó ningún indicio de que estuviera en modo promiscuo, lo que significa que no estaba capturando todo el tráfico de la red, como lo haría un sniffer.

Tambien se verificaron las conexiones activas en el sistema, para asegurarse de que no hubiera puertos o servicios sospechosos escuchando tráfico de red sin autorización.

- **Comando utilizado:** sudo netstat -tulnp

```
debian@debian:~$ sudo netstat -tulnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp      0      0 127.0.0.1:631           0.0.0.0:*            LISTEN    286465/cupsd
tcp      0      0 127.0.0.1:25            0.0.0.0:*            LISTEN    10851/exim4
tcp6     0      0 ::1:25                 ::*:*                LISTEN    10851/exim4
tcp6     0      0 ::1:631                ::*:*                LISTEN    286465/cupsd
udp      0      0 0.0.0.0:44230          0.0.0.0:*            LISTEN    437/avahi-daemon: r
udp      0      0 0.0.0.0:5353           0.0.0.0:*            LISTEN    437/avahi-daemon: r
udp6     0      0 ::::49330              ::*:*                LISTEN    437/avahi-daemon: r
udp6     0      0 ::::5353              ::*:*                LISTEN    437/avahi-daemon: r
```

Se encontraron puertos en escucha (LISTEN) para servicios comunes como **cupsd** (para impresión), **exim4** (servidor de correo), y **avahi-daemon** (para servicios de red). Ningún puerto o servicio relacionado con un sniffer malicioso fue encontrado.

Luego se inspeccionaron los procesos activos utilizando las interfaces de red para confirmar que no había procesos maliciosos.

- **Comando utilizado:** sudo lsof -i -n

```
debian@debian:~$ sudo lsof -i -n
COMMAND   PID   USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
avahi-dae 437   avahi  12u   IPv4  14653      0t0  UDP *:mdns
avahi-dae 437   avahi  13u   IPv6  14654      0t0  UDP *:mdns
avahi-dae 437   avahi  14u   IPv4  14655      0t0  UDP *:44230
avahi-dae 437   avahi  15u   IPv6  14656      0t0  UDP *:49330
NetworkMa 467   root   26u   IPv4  15921      0t0  UDP 192.168.1.117:bootpc->192.168.1.1:bootps
exim4    10851 Debian-exim  4u   IPv4  55181      0t0  TCP 127.0.0.1:smtp (LISTEN)
exim4    10851 Debian-exim  5u   IPv6  55182      0t0  TCP [::1]:smtp (LISTEN)
firefox-e 147813 debian  60u   IPv4  900625     0t0  TCP 192.168.1.117:53902->192.178.50.42:https (ESTABLISHED)
firefox-e 147813 debian  123u  IPv4  897753     0t0  TCP 192.168.1.117:50786->34.107.243.93:https (ESTABLISHED)
firefox-e 147813 debian  518u  IPv4  930479     0t0  TCP 192.168.1.117:59072->192.178.50.67:https (ESTABLISHED)
gvfsd-smb 277066 debian  9u   IPv4  641192     0t0  TCP 192.168.1.117:43152->192.168.1.1:netbios-ssn (ESTABLISHED)
cupsd    286465   root   6u   IPv6  832731     0t0  TCP [::1]:ipp (LISTEN)
cupsd    286465   root   7u   IPv4  832732     0t0  TCP 127.0.0.1:ipp (LISTEN)
```

Los procesos avahi-daemon (mDNS), NetworkManager, y firefox están utilizando la red, pero estos son procesos legítimos y no muestran signos de actividad anómala.

Por último se revisó el archivo de configuración de NetworkManager para asegurarse de que no estuviera realizando actividades de sniffer sin autorización.

- **Comando utilizado:** cat /etc/NetworkManager/NetworkManager.conf

```
debian@debian:~$ cat /etc/NetworkManager/NetworkManager.conf
[main]
plugins=ifupdown,keyfile

[ifupdown]
managed=false
```

La configuración encontrada es estándar y muestra que NetworkManager está gestionando la red de forma adecuada, sin interferencias en las configuraciones de ifupdown.

8.2. Conclusiones del Análisis CHKRootkit:

LibreOffice:

- El directorio .registry en LibreOffice contiene archivos legítimos relacionados con la configuración de los componentes de la suite ofimática. No se encontró ninguna amenaza en este directorio, y la reinstalación de LibreOffice confirmó que la instalación es segura.

NetworkManager:

- El proceso NetworkManager está funcionando correctamente y no está ejecutando ningún sniffer malicioso.
- Aunque CHKRootkit reportó que el servicio podría estar actuando como un sniffer, el análisis confirmó que no está en modo promiscuo ni realizando actividades no autorizadas.
- NetworkManager está configurado correctamente para gestionar las conexiones de red sin realizar actividades sospechosas.

Estado General del Sistema:

- No se encontraron rootkits, malware, ni configuraciones sospechosas en los servicios de red o en los directorios de configuración.
- El sistema está funcionando como se espera, y no se observan signos de compromisos de seguridad.

8.3. RKHunter

El objetivo del análisis realizado con la herramienta RKHunter fue verificar la presencia de rootkits y configuraciones sospechosas en el sistema dando como resultado del análisis los siguientes detalles:

- **Comandos Modificados (lwp-request):**

```
[23:02:45] /usr/bin/gawk [ OK ]
[23:02:45] /usr/bin/lwp-request [ Warning ]
[23:02:45] Warning: The command '/usr/bin/lwp-request' has been replaced by a script: /usr/bin/lwp-request: Perl script text executable
[23:02:46] /usr/bin/mail.mailutils [ OK ]
```

Vemos que el archivo **lwp-request** es parte del paquete libwww-perl, lo que significa que probablemente es completamente legítimo. El sistema lo utiliza para realizar solicitudes web desde la línea de comandos.

Comando utilizado: dpkg -S /usr/bin/lwp-request.

```
debian@debian:~$ dpkg -S /usr/bin/lwp-request
libwww-perl: /usr/bin/lwp-request
```

El archivo **lwp-request** es legítimo y no ha sido alterado ni comprometido. El archivo coincide con la versión oficial del paquete libwww-perl en los repositorios de Debian, lo que confirma que no ha sido modificado maliciosamente. Para verificar esto, se utilizó el siguiente proceso:

- Se descargó y extrajo el paquete oficial de libwww-perl desde el repositorio de Debian. **Comando utilizado:** dpkg-deb -x libwww-perl_6.68-1_all.deb /tmp/libwww-perl

```
root@debian:/home/debian/Desktop# dpkg-deb -x libwww-perl_6.68-1_all.deb /tmp/libwww-perl
```

- Se calculó el hash SHA256 tanto del archivo presente en el sistema como del archivo extraído del paquete oficial. **Comando utilizado:** sha256sum /usr/bin/lwp-request | sha256sum /tmp/libwww-perl/usr/bin/lwp-request

```
debian@debian:~$ sha256sum /usr/bin/lwp-request  
86c1db75d5ee27ecb7aa184ed6770625ccbc6dd9456c1b36ef4ea2dd5bf53707  /usr/bin/lwp-request
```

- Los hashes coinciden, confirmando que el archivo lwp-request es el mismo que el archivo original proporcionado por los repositorios oficiales.

```
root@debian:/home/debian/Desktop# sha256sum /tmp/libwww-perl/usr/bin/lwp-request  
86c1db75d5ee27ecb7aa184ed6770625ccbc6dd9456c1b36ef4ea2dd5bf53707  /tmp/libwww-perl/usr/bin/lwp-request
```

En conclusión: el archivo lwp-request es seguro y puede permanecer en el sistema sin preocupaciones adicionales.

- **Segmentos de Memoria Compartida:**

RKhunter revisó los segmentos de memoria compartida y encontró varios procesos como mate-panel, firefox-esr, y mate-terminal utilizando más memoria de la permitida (1MB), lo cual generó una advertencia. Sin embargo, estos procesos son comunes en entornos de escritorio y no presentan indicios claros de un rootkit.

En conclusión: Los procesos que utilizan más memoria de la permitida no indican un problema de seguridad.

```
[05:21:32]
[05:21:32] Info: Starting test name 'ipc_shared_mem'
[05:21:32] Info: The minimum shared memory segment size to be checked (in bytes): 1048576 (1.0MB)
[05:21:33] Checking for suspicious (large) shared memory segments [ Warning ]
[05:21:33] Warning: The following suspicious (large) shared memory segments have been found:
[05:21:33]     Process: /usr/bin/mate-panel    PID: 1170    Owner: debian    Size: 4.0MB (configured size allowed: 1.0MB)
[05:21:33]     Process: /usr/lib/firefox-esr/firefox-esr    PID: 147813    Owner: debian    Size: 5.2MB (configured size allowed: 1.0MB)
[05:21:33]     Process: /usr/lib/firefox-esr/firefox-esr    PID: 147813    Owner: debian    Size: 5.2MB (configured size allowed: 1.0MB)
[05:21:33]     Process: /usr/lib/mate-panel/wnck-applet    PID: 1240    Owner: debian    Size: 64MB (configured size allowed: 1.0MB)
[05:21:33]     Process: /usr/bin/caja    PID: 1210    Owner: debian    Size: 64MB (configured size allowed: 1.0MB)
[05:21:34]     Process: /usr/bin/mate-terminal    PID: 1566    Owner: debian    Size: 4.0MB (configured size allowed: 1.0MB)
[05:21:34]     Process: /usr/bin/mate-screensaver    PID: 1226    Owner: debian    Size: 64MB (configured size allowed: 1.0MB)
[05:21:34]
```

- **Configuración de SSH:**

Se encontró una advertencia entre las configuraciones de SSH y las de RKhunter:

En la configuración de SSH (archivo /etc/ssh/sshd_config), la opción PermitRootLogin está configurada en yes, lo que permite el acceso remoto al usuario root.

Sin embargo, en RKhunter recomienda colocar esta opción ALLOW_SSH_ROOT_USER en no, para prohibir dicho acceso.

En conclusión: El análisis ha mostrado que el sistema permite actualmente el acceso remoto de root a través de SSH, lo que es un riesgo de seguridad. Se recomienda urgentemente deshabilitar esta opción, en el archivo de configuración de SSH, para garantizar la seguridad del sistema.

```
[05:23:00]
[05:23:00] Info: Starting test name 'system_configs_ssh'
[05:23:00]   Checking for an SSH configuration file      [ Found ]
[05:23:00] Info: Found an SSH configuration file: /etc/ssh/sshd_config
[05:23:01] Info: Rkhunter option ALLOW_SSH_ROOT_USER set to 'no'.
[05:23:01] Info: Rkhunter option ALLOW_SSH_PROT_V1 set to '2'.
[05:23:01]   Checking if SSH root access is allowed      [ Warning ]
[05:23:01] Warning: The SSH and rkhunter configuration options should be the same:
[05:23:01]       SSH configuration option 'PermitRootLogin': yes
[05:23:01]       Rkhunter configuration option 'ALLOW_SSH_ROOT_USER': no
[05:23:01]   Checking if SSH protocol v1 is allowed      [ Not set ]
[05:23:01]   Checking for other suspicious configuration settings [ None found ]
[05:23:01]
```

8.4. Conclusiones del Análisis RKhUNTER:

Comandos Modificados(lwp-request):

- Se detectó que el comando /usr/bin/lwp-request había sido reemplazado por un script Perl. RKhunter generó una advertencia, pero este cambio es legítimo ya que lwp-request forma parte del paquete libwww-perl, utilizado para realizar solicitudes web desde la línea de comandos.
- El reemplazo del comando es legítimo, y no se encontró ningún indicio de alteración maliciosa. No es necesario tomar ninguna acción adicional.

Segmentos de Memoria Compartida:

- No se trata de un riesgo de seguridad, ya que estos son procesos comunes de un entorno de escritorio. No es necesario tomar ninguna medida, pero se debe estar atento a otros procesos que puedan utilizar una cantidad inusual de memoria.

Configuración de SSH:

- PermitRootLogin en SSH estaba configurado en yes, permitiendo el acceso remoto de root.
- ALLOW_SSH_ROOT_USER en RKhunter estaba configurado en no, lo que prohíbe dicho acceso.
- Es recomendable deshabilitar el acceso remoto como root en SSH para mejorar la seguridad. Esto se puede hacer modificando el archivo /etc/ssh/sshd_config y configurando PermitRootLogin no.

9. Mitigación de Vulnerabilidades y Recomendaciones

9.1. Actualización de paquetes

La actualización de paquetes garantiza que el sistema esté utilizando las versiones más recientes y seguras de los paquetes, minimizando el riesgo de vulnerabilidades y errores de seguridad. Hay que asegurarse de realizar actualizaciones periódicas para mantener el sistema protegido y funcionando de manera óptima.

Para asegurarse de que todos los paquetes del sistema estén actualizados, se ejecutó el siguiente comando para actualizar la lista de paquetes disponibles y actualizar los paquetes instalados a sus últimas versiones:

sudo apt update & sudo apt upgrade

```
debian@debian:~$ sudo apt update
Get:1 http://security.debian.org/debian-security bookworm-security InRelease [48.0 kB]
Hit:2 http://deb.debian.org/debian bookworm InRelease
Get:3 http://deb.debian.org/debian bookworm-updates InRelease [55.4 kB]
Get:4 http://security.debian.org/debian-security bookworm-security/main Sources [142 kB]
Get:5 http://security.debian.org/debian-security bookworm-security/main amd64 Packages [271 kB]
Get:6 http://security.debian.org/debian-security bookworm-security/main Translation-en [162 kB]
Fetched 678 kB in 3s (224 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
216 packages can be upgraded. Run 'apt list --upgradable' to see them.
debian@debian:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
```

9.2. Deshabilitar el acceso SSH root:

Se realizaron una serie de configuraciones en el archivo sshd_config con el objetivo de fortalecer la seguridad del servicio SSH. Estas configuraciones incluyeron el cambio del puerto SSH predeterminado, la desactivación del acceso remoto para el usuario root, la limitación de intentos de autenticación y sesiones simultáneas, así como la implementación de autenticación basada en claves públicas. Además, se deshabilitaron opciones como el reenvío de X11, puertos TCP y el reenvío de agentes SSH, todo con el fin de reducir la superficie de ataque y mejorar la protección del sistema. Estas medidas contribuyen a un entorno más seguro y controlado para las conexiones SSH.

```
Port 2200
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

Authentication:

```
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
MaxAuthTries 3
MaxSessions 2
```

```
PubkeyAuthentication yes
```

```
GNU nano 7.2                                     /etc/ssh/sshd_config *

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
KbdInteractiveAuthentication no
#AllowAgentForwarding yes
AllowTcpForwarding no
#GatewayPorts no
X11Forwarding no
#X11DisplayOffset 10
#X11UseLocalhost yes
```

- **Resumen de las Configuraciones Realizadas:**

Configuración	Valor Configurado	Qué Hace
Puerto SSH	Port 2200	Cambia el puerto predeterminado de SSH (22) a 2200 para reducir los ataques automatizados.
Permitir acceso como root	PermitRootLogin no	Deshabilita el acceso remoto para el usuario root, aumentando la seguridad.
Configuración de autenticación	PasswordAuthentication no	Deshabilita la autenticación por contraseña, obligando el uso de claves públicas para mayor seguridad.
Configuración de autenticación de clave pública	PubkeyAuthentication yes	Habilita la autenticación mediante claves públicas, lo que es más seguro que usar contraseñas.
Intentos de autenticación permitidos	MaxAuthTries 3	Limita el número de intentos fallidos de autenticación a 3, lo que ayuda a prevenir ataques de fuerza bruta.
Número máximo de sesiones por usuario	MaxSessions 2	Limita a 2 el número de sesiones SSH simultáneas por usuario para evitar abuso de recursos.
Reenvío de X11	X11Forwarding no	Impide la ejecución de aplicaciones gráficas de forma remota a través de SSH.

9.3. Configuración de VSFTPD

Se hicieron varios cambios de configuración en VSFTPD para asegurar que el servidor FTP sea más seguro y proteger los datos que se transfieren. Los cambios incluyen desde la modificación del puerto de acceso hasta la implementación de conexiones cifradas para proteger los archivos. Estos ajustes limitan el acceso no autorizado, controlan mejor los permisos de los usuarios y aseguran que las transferencias de archivos sean más seguras.

```
GNU nano 7.2                                     /etc/vsftpd.conf *
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=NO
#
# You may restrict local users to their home directories. See the FAQ for
# the possible risks in this before using chroot_local_user or
# chroot_list_enable below.
chroot_local_user=YES

# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
listen_port=2100

# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=YES

#
# Activate logging of uploads/downloads.
xferlog_enable=YES
"
```

- **Resumen de las Configuraciones Realizadas:**

Configuración	Valor Configurado	Qué Hace
Desactivar acceso anónimo	anonymous_enable=NO	Evita que personas sin cuenta accedan al servidor FTP.
Permitir acceso solo a usuarios locales	local_enable=YES	Solo los usuarios con cuentas en el sistema pueden acceder al servidor FTP.
Deshabilitar escritura de archivos	write_enable=NO	Los usuarios locales no pueden subir archivos al servidor, solo pueden descargarlos.
Restringir a los usuarios a su carpeta	chroot_local_user=YES	Limita a cada usuario a solo ver y acceder a su propia carpeta, sin poder ver otras áreas.
Cambiar puerto de acceso	listen_port=2100	Cambia el puerto predeterminado (21) a 2100 para dificultar ataques automáticos que buscan el puerto común.
Activar conexiones seguras (SSL/TLS)	ssl_enable=YES	Encripta las conexiones, protegiendo los datos que se transfieren entre el servidor y el usuario.
Activar registros de transferencia de archivos	xferlog_enable=YES	Guarda un registro de los archivos que se suben y bajan del servidor, útil para monitorear el uso.

9.4. Eliminación de Usuarios Maliciosos y Cambio de Contraseñas

Débiles:

- **Cambio de Contraseña de root (del sistema):**

Se cambió la contraseña del usuario root del sistema para asegurar la integridad del servidor y evitar el acceso no autorizado.

Comando utilizado: sudo passwd root

- **Cambio de Contraseña de debian (del sistema):**

Se cambió la contraseña del usuario debian para asegurar que no estuviera utilizando una contraseña débil.

Comando utilizado: sudo passwd debian

```
root@debian:/etc/apache2# sudo passwd debian
New password:
Retype new password:
passwd: password updated successfully
root@debian:/etc/apache2# passwd root
New password:
Retype new password:
passwd: password updated successfully
root@debian:/etc/apache2# █
```

- **Eliminación de la Cuenta user (de MariaDB):**

La cuenta user en MariaDB, que fue identificada como comprometida, fue eliminada para evitar accesos no autorizados.

Comando utilizado:

```
DROP USER 'user'@'localhost';
```

```
FLUSH PRIVILEGES;
```

```
MariaDB [(none)]> DROP USER 'user'@'localhost';
Query OK, 0 rows affected (0.033 sec)
```

```
MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.012 sec)
```

```
root@debian:/etc/apache2# sudo mysql -e "SELECT user, host FROM mysql.user"
+-----+-----+
| User      | Host     |
+-----+-----+
| mariadb.sys | localhost |
| mysql      | localhost |
| root       | localhost |
| wordpressuser | localhost |
+-----+-----+
```

- Cambio de Contraseña de wordpressuser (de MySQL):

Se actualizó la contraseña del usuario wordpressuser en MySQL a una más segura, ya que la contraseña anterior (123456) era débil y comprometida.

También se actualizó la contraseña en el archivo wp-config.php para que coincidiera con la nueva contraseña de MySQL.

Comando utilizado:

```
SET PASSWORD FOR 'wordpressuser'@'localhost' =
PASSWORD('NuevaContraseñaSegura!');
```

```
FLUSH PRIVILEGES;
```

```
MariaDB [(none)]> SET PASSWORD FOR 'wordpressuser'@'localhost' = PASSWORD('WordPrE$$@20250704');
Query OK, 0 rows affected (0.005 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.003 sec)
```

```
GNU nano 7.2                                     /var/www/html/wp-config.php *
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

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

/** Database password */
define( 'DB_PASSWORD', 'WordPrE$$@20250704' );

/** 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', '' );
```

- **Cambio de Contraseña de wordpress-user (de WordPress):**

Se cambió la contraseña del usuario wordpress-user en la base de datos de WordPress, aplicando una contraseña más fuerte y única.

Comando utilizado:

```
UPDATE wp_users SET user_pass = MD5('NuevaContraseñaSegura!') WHERE user_login = 'wordpress-user';
```

```
Database changed
MariaDB [wordpress]> UPDATE wp_users SET user_pass = MD5('20252520$WpUser.') WHERE user_login = 'wordpress-user';
Query OK, 1 row affected (0.016 sec)
Rows matched: 1  Changed: 1  Warnings: 0
```

- **Recomendaciones de Seguridad:**

- Usar contraseñas fuertes: Asegurarse de que todas las contraseñas sean largas, únicas y combinadas con letras, números y caracteres especiales.
- Revisar contraseñas regularmente: Hacer auditorías para asegurarse de que las contraseñas no sean débiles o se hayan filtrado.
- Eliminar cuentas no necesarias: Si hay cuentas sin uso o comprometidas, eliminarlas de inmediato.
- Activar autenticación en dos pasos (2FA): Siempre que sea posible, usar 2FA para añadir una capa extra de seguridad.
- Monitorear el sistema: Usar herramientas para monitorear el acceso y detectar actividades sospechosas en tiempo real.

9.5. Configuración Firewall y puertos

A continuación las configuraciones realizadas en el firewall del servidor utilizando iptables, con el objetivo de abrir solo los puertos esenciales para los servicios necesarios (HTTP, SSH, FTP) y configurar el firewall con reglas que protegen el servidor contra ataques externos, como los de fuerza bruta en servicios críticos.

```
root@debian:/home/debian# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source          destination
ACCEPT     tcp  --  anywhere        anywhere         tcp dpt:2100
ACCEPT     tcp  --  anywhere        anywhere         tcp dpt:2200
ACCEPT     tcp  --  192.168.0.0/24  anywhere         tcp dpt:2200
REJECT     tcp  --  anywhere        anywhere         tcp dpt:2200 reject-with icmp-port-unreachable
REJECT     tcp  --  anywhere        anywhere         tcp dpt:2200 state NEW recent: SET name: DEFAULT side: source mask: 255.255.255.255
REJECT     tcp  --  anywhere        anywhere         tcp dpt:2200 state NEW recent: UPDATE seconds: 600 hit_count: 6 name: DEFAULT side: source mask:
255.255.255.255 reject-with icmp-port-unreachable
REJECT     all   --  192.168.0.134   anywhere         reject-with icmp-port-unreachable
ACCEPT     tcp  --  anywhere        anywhere         tcp dpt:http
ACCEPT     tcp  --  anywhere        anywhere         tcp dpt:2100 state NEW recent: SET name: DEFAULT side: source mask: 255.255.255.255
REJECT     tcp  --  anywhere        anywhere         tcp dpt:2100 state NEW recent: UPDATE seconds: 600 hit_count: 6 name: DEFAULT side: source mask:
255.255.255.255 reject-with icmp-port-unreachable
```

- **Se permitió el tráfico en los puertos esenciales:**

- **HTTP (puerto 80):**

```
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

- **SSH (puerto 2200):**

```
sudo iptables -A INPUT -p tcp --dport 2200 -j ACCEPT
```

- **FTP (puerto 2100):**

```
sudo iptables -A INPUT -p tcp --dport 2100 -j ACCEPT
```

```
root@debian:/home/debian# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
root@debian:/home/debian# iptables -A INPUT -p tcp --dport 2100 -j ACCEPT
root@debian:/home/debian# iptables -A INPUT -p tcp --dport 2200 -j ACCEPT
```

- **Se limitó el acceso FTP (puerto 2100)** a un máximo de 5 intentos por IP en 10 minutos, bloqueando la IP temporalmente tras exceder este límite:

```
root@debian:/home/debian# iptables -A INPUT -p tcp --dport 2100 -i eth0 -m state --state NEW -m recent --name vsftpd --set  
root@debian:/home/debian# iptables -A INPUT -p tcp --dport 2100 -i eth0 -m state --state NEW -m recent --name vsftpd --update --seconds 600 --hitcount 6 -j REJECT
```

- sudo iptables -A INPUT -p tcp --dport 2100 -i eth0 -m state --state NEW -m recent --name vsftpd --set
 - sudo iptables -A INPUT -p tcp --dport 2100 -i eth0 -m state --state NEW -m recent --name vsftpd --update --seconds 600 --hitcount 6 -j REJECT

- **Se limitó el acceso SSH (puerto 2200)** a un máximo de 5 intentos por IP en 10 minutos, bloqueando la IP temporalmente tras exceder este límite:

```
root@debian:/home/debian# iptables -A INPUT -p tcp --dport 2200 -i eth0 -m state --state NEW -m recent --name vsftpd --set  
root@debian:/home/debian# iptables -A INPUT -p tcp --dport 2200 -i eth0 -m state --state NEW -m recent --name vsftpd --update --seconds 600 --hitcount 6 -j REJECT
```

- **LIMITAR CONEXIONES SSH EN LA RED LOCAL (192.168.0.0/24):** Se está permitiendo acceso SSH solo desde la red local (192.168.0.0/255) y se rechazan todas las conexiones SSH no provenientes de la red local.

```
root@debian:/home/debian# iptables -A INPUT -p tcp --dport 2200 -s 192.168.0.0/24 -j ACCEPT  
root@debian:/home/debian# iptables -A INPUT -p tcp --dport 2200 -j REJECT
```

- sudo iptables -A INPUT -p tcp --dport 2200 -s 192.168.0.0/24 -j ACCEPT
- sudo iptables -A INPUT -p tcp --dport 2200 -j REJECT

- **SE BLOQUEÓ EL TRÁFICO PROVENIENTE DE LA IP ATACANTE 192.168.0.134:**

Por último se bloqueó la dirección IP del Atacante por la cual ingresó por SSH como root.

```
root@debian:/home/debian# iptables -A INPUT -s 192.168.0.134 -j REJECT
```

- sudo iptables -A INPUT -s 192.168.0.134 -j REJECT

9.6. Cambio de Permisos en Carpetas y Archivos Sensibles:

Se ajustaron los permisos de las carpetas y archivos importantes de **WordPress** para mejorar la seguridad:

```
root@debian:/var/www# ls -l
total 4
drwxrwxrwx 5 www-data www-data 4096 Jul  4 02:39 html
root@debian:/var/www# chmod 755 html/
root@debian:/var/www# ls -l
total 4
drwxr-xr-x 5 www-data www-data 4096 Jul  4 02:39 html
```

- **Carpetas:**

- Se cambiaron los permisos de **/var/www/html** y sus subdirectorios (**wp-admin**, **wp-content**, **wp-includes**) a **755**, permitiendo que solo el propietario (www-data) pueda **modificar** los archivos, mientras que otros usuarios solo puedan **leer** y **ejecutar**.

Comando utilizado: chmod 755 /var/www/html

- **Archivos:**

- Los archivos en **/var/www/html** fueron configurados con **644**, lo que permite que el **propietario** lea y escriba, mientras que **otros usuarios** solo pueden **leer** los archivos.

Comando utilizado en la carpeta **/var/www/html**: chmod 644 *

- **wp-config.php** y **xmlrpc.php** se configuraron con **600**, permitiendo que **solo el propietario** pueda **leer y escribir** en estos archivos sensibles.

Comando utilizado: chmod 600 /var/www/html/wp-config.php

chmod 600 /var/www/html/xmlrpc.php

```
root@debian:/var/www/html# chmod 644 *
root@debian:/var/www/html# chmod 600 wp-config.php
root@debian:/var/www/html# chmod 755 wp-admin/ wp-content/ wp-includes/
root@debian:/var/www/html# chmod 600 xmlrpc.php
root@debian:/var/www/html# ls -l
total 248
-rw-r--r-- 1 www-data www-data 10701 Sep 30 2024 index.html
-rw-r--r-- 1 www-data www-data 405 Feb 6 2020 index.php
-rw-r--r-- 1 www-data www-data 19903 Jun 13 22:26 license.txt
-rw-r--r-- 1 www-data www-data 7425 Jun 13 22:26 readme.html
-rw-r--r-- 1 www-data www-data 7387 Feb 13 2024 wp-activate.php
drwxr-xr-x 9 www-data www-data 4096 Sep 10 2024 wp-admin
-rw-r--r-- 1 www-data www-data 351 Feb 6 2020 wp-blog-header.php
-rw-r--r-- 1 www-data www-data 2323 Jun 14 2023 wp-comments-post.php
-rw----- 1 www-data www-data 3029 Jul 4 02:39 wp-config.php
-rw-r--r-- 1 www-data www-data 3336 Jun 13 22:26 wp-config-sample.php
drwxr-xr-x 6 www-data www-data 4096 Jul 2 06:28 wp-content
-rw-r--r-- 1 www-data www-data 5617 Jun 13 22:26 wp-cron.php
drwxr-xr-x 30 www-data www-data 12288 Jun 13 22:26 wp-includes
-rw-r--r-- 1 www-data www-data 2502 Nov 26 2022 wp-links-opml.php
-rw-r--r-- 1 www-data www-data 3937 Mar 11 2024 wp-load.php
-rw-r--r-- 1 www-data www-data 51414 Jun 13 22:26 wp-login.php
-rw-r--r-- 1 www-data www-data 8727 Jun 13 22:26 wp-mail.php
-rw-r--r-- 1 www-data www-data 30081 Jun 13 22:26 wp-settings.php
-rw-r--r-- 1 www-data www-data 34516 Jun 13 22:26 wp-signup.php
-rw-r--r-- 1 www-data www-data 5102 Jun 13 22:26 wp-trackback.php
-rw----- 1 www-data www-data 3205 Jun 13 22:26 xmlrpc.php
```

Estos cambios aseguran que solo los usuarios autorizados puedan modificar o acceder a los archivos y directorios críticos de WordPress, protegiendo así los datos sensibles como las credenciales de la base de datos y configuraciones importantes. Este enfoque de seguridad reduce el riesgo de modificaciones no autorizadas, ejecución de scripts maliciosos y accesos no deseados, mejorando la seguridad general del servidor.

9.7. Desactivación de la Listabilidad de Directorios:

Index of /wp-content/uploads

Name	Last modified	Size	Description
Parent Directory		-	
2024/	2024-10-08 16:49	-	
2025/	2025-07-02 06:28	-	

Apache/2.4.62 (Debian) Server at 192.168.1.117 Port 80

Se modificó la configuración de Apache para evitar que los directorios sean listados y proteger así el servidor web de exposiciones innecesarias.

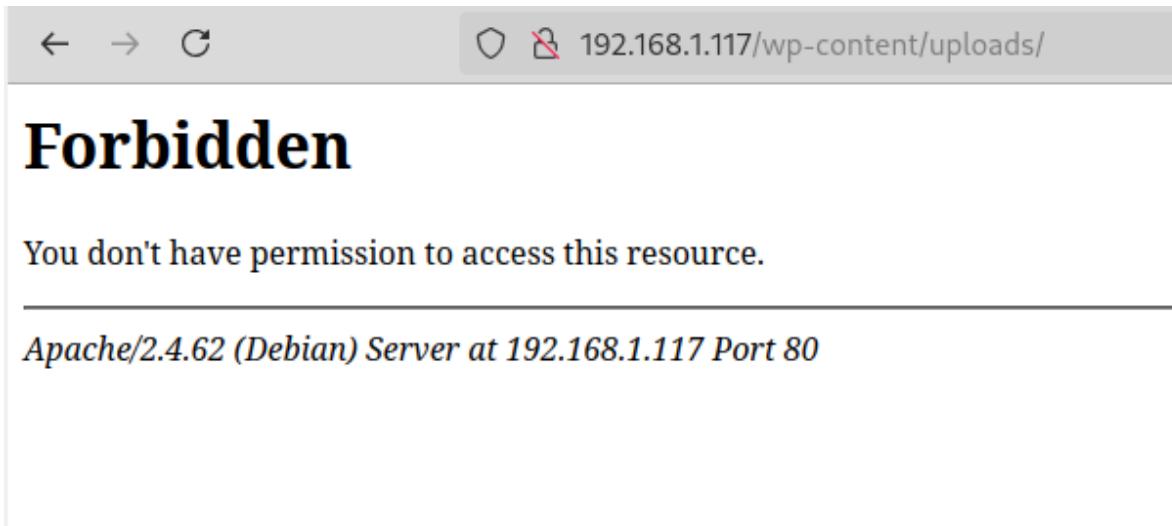
Esto fue logrado eliminando la opción **Indexes** en las directivas de configuración de los directorios /, /usr/share y /var/www/ en el archivo **apache2.conf**.

```
GNU nano 7.2                                         /etc/apache2/apache2.conf
# access here, or in any related virtual host.
<Directory />
    Options FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>

<Directory /usr/share>
    AllowOverride None
    Options FollowSymLinks
    Require all granted
</Directory>

<Directory /var/www/>
    Options FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>
```

Se realizaron las verificaciones necesarias para confirmar que los directorios ahora no son listables.



Estas modificaciones mejoran la seguridad del servidor, evitando que usuarios no autorizados puedan acceder a la estructura de archivos del servidor web.

10. Conclusión

El análisis del servidor Debian de LEX Abogados & Asociados ha revelado diversas vulnerabilidades de seguridad que facilitaron la intrusión, incluyendo configuraciones incorrectas en servicios críticos como SSH, FTP y Apache, así como el uso de contraseñas débiles y la exposición de credenciales sensibles. Tras la detección de la intrusión, se implementaron medidas correctivas, tales como el cambio de contraseñas comprometidas, la eliminación de usuarios maliciosos y la reconfiguración de permisos en archivos y directorios sensibles.

Adicionalmente, se recomendó a LEX Abogados & Asociados la actualización continua de los paquetes del sistema, el fortalecimiento de las contraseñas, y la implementación de autenticación multifactor en servicios clave. Con estas acciones, se busca reducir al mínimo el riesgo de futuras intrusiones, asegurando la integridad y confidencialidad de los datos almacenados en el servidor y protegiendo los activos digitales de la empresa.