Análisis forense

Versión	Fecha	Autor	Descripción
v.01	04/06/2025	Luis F. Gómez Guzmán	Análisis forense

Índice

1. Objetivo y alcance 3
2. Herramientas y técnicas utilizadas 3
3. Análisis y resultados 3
Logs 3
SSH 6
Usuarios 6
Usuarios MariaDB (MySQL) 7
Rootkits y malware 8
Wordpress 9
4. Mitigación 10
A. Restricción del tráfico 10
B. Configuración segura de SSH 11
C. Modificación de las credenciales del usuario root 15
D. Administración de servidor 15
E. Actualización del sistema 17
5. Conclusiones de prevención futuras 18

1. Objetivo y alcance

El objetivo de este informe es documentar el análisis forense de la máquina virtual Debian hackeada.

El alcance incluye el análisis de los logs, procesos y archivos; el escaneo de rootkits y malware; la corrección de las configuraciones; la propuesta de hardening y de políticas de seguridad.

2. Herramientas y técnicas utilizadas

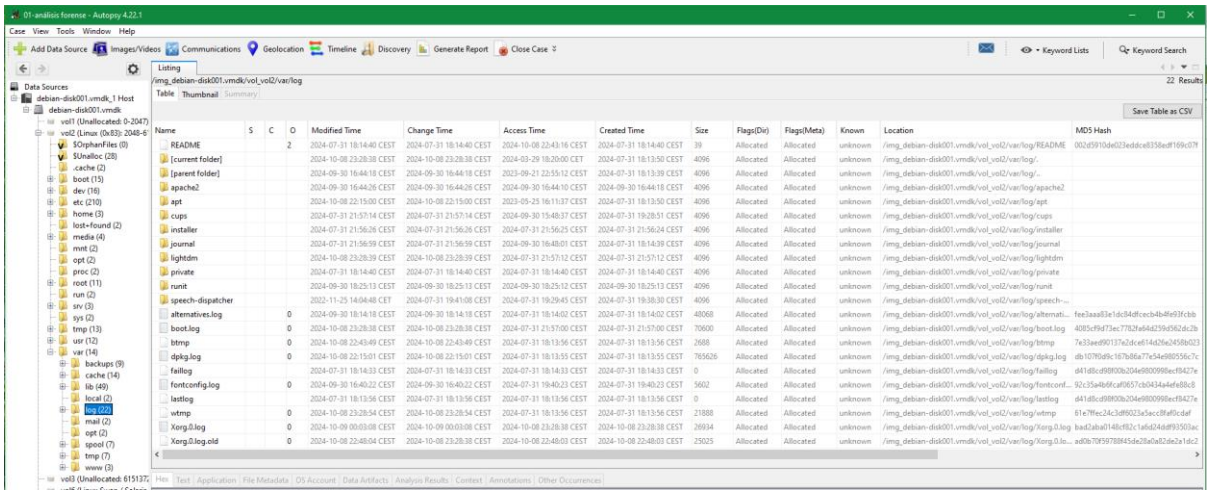
- **Autopsy**
  En el empleo de Autopsy se ha mantenido la cadena de custodia de la imagen (.ova) de la máquina virtual, garantizando así su integridad y autenticidad.

- **Chkrootkit**

- **Rkhunter**

3. Análisis y resultados

<u>Logs</u>



debian@debian: /var/log

Browse and run installed applications

```
debian@debian:/var/log$ ls -al
total 1072
drwxr-xr-x  11 root              root              4096 Jun  2 07:25 .
drwxr-xr-x  12 root              root              4096 Sep 30  2024 ..
-rw-r--r--   1 root              root                 0 May 19 07:00 alternatives.log
-rw-r--r--   1 root              root             48068 Sep 30  2024 alternatives.log.1
drwxr-x---   2 root              adm               4096 Sep 30  2024 apache2
drwxr-xr-x   2 root              root              4096 May 19 07:00 apt
-rw-------   1 root              root             30686 Jun  2 07:25 boot.log
-rw-------   1 root              root             78567 May 19 07:00 boot.log.1
-rw-rw----   1 root              utmp                 0 May 19 07:00 btmp
-rw-rw----   1 root              utmp              2688 Oct  8  2024 btmp.1
drwxr-xr-x   2 root              root              4096 May 19 07:00 cups
-rw-r--r--   1 root              root                 0 May 19 07:00 dpkg.log
-rw-r--r--   1 root              root            765626 Oct  8  2024 dpkg.log.1
-rw-r--r--   1 root              root                 0 Jul 31  2024 faillog
-rw-r--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-rw-r--   1 root              utmp                 0 Jul 31  2024 lastlog
drwx--x--x   2 root              root              4096 Jun  2 07:25 lightdm
drwx------   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
drwx------   2 speech-dispatcher root              4096 Nov 25  2022 speech-dispatcher
-rw-------   1 root              root              1820 May 19 09:04 vsftpd.log
-rw-rw-r--   1 root              utmp             36096 Jun  2 07:26 wtmp
```

debian@debian: /var/log

File Edit View Search Terminal Help

```
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:
        man:journalctl(1)
        man:systemd-journald.service(8)
        man:journald.conf(5)
        https://0pointer.de/blog/projects/the-journal.html
debian@debian:/var/log$
```

debian@debian: /var/log/journal

File Edit View Search Terminal Help

```
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:
        man:journalctl(1)
        man:systemd-journald.service(8)
        man:journald.conf(5)
        https://0pointer.de/blog/projects/the-journal.html
debian@debian:/var/log$ cd journal
debian@debian:/var/log/journal$ ls -al
total 12
drwxr-sr-x+  3 root systemd-journal 4096 Jul 31  2024 .
drwxr-xr-x  11 root root            4096 Jun  2 07:25 ..
drwxr-sr-x+  2 root systemd-journal 4096 May 19 07:00 41b6de202c3f48fdaa490411748aaaff
debian@debian:/var/log/journal$
```

debian@debian: /var/log/journal

File Edit View Search Terminal Help

```
Jul 31 15:56:59 debian kernel:         Rude variant of Tasks RCU enabled.
Jul 31 15:56:59 debian kernel:         Tracing variant of Tasks RCU enabled.
Jul 31 15:56:59 debian kernel: rcu: RCU calculated value of scheduler-enlistment delay is 25 jiffies.
Jul 31 15:56:59 debian kernel: rcu: Adjusting geometry for rcu_fanout_leaf=16, nr_cpu_ids=2
Jul 31 15:56:59 debian kernel: NR_IRQS: 524544, nr_irqs: 440, preallocated irqs: 16
Jul 31 15:56:59 debian kernel: rcu: srcu_init: Setting srcu_struct sizes based on contention.
Jul 31 15:56:59 debian kernel: Console: colour VGA+ 80x25
Jul 31 15:56:59 debian kernel: printk: console [tty0] enabled
Jul 31 15:56:59 debian kernel: ACPI: Core revision 20220331
Jul 31 15:56:59 debian kernel: APIC: Switch to symmetric I/O mode setup
Jul 31 15:56:59 debian kernel: ..TIMER: vector=0x30 apic1=0 pin1=2 apic2=-1 pin2=-1
Jul 31 15:56:59 debian kernel: clocksource: tsc-early: mask: 0xffffffffffffffff max_cycles: 0x29dc05e54fc, max_idle_ns: 440>
Jul 31 15:56:59 debian kernel: Calibrating delay loop (skipped) preset value.. 5808.00 BogoMIPS (lpj=11616000)
Jul 31 15:56:59 debian kernel: Last level iTLB entries: 4KB 64, 2MB 8, 4MB 8
Jul 31 15:56:59 debian kernel: Last level dTLB entries: 4KB 64, 2MB 0, 4MB 0, 1GB 4
Jul 31 15:56:59 debian kernel: Spectre V1 : Mitigation: usercopy/swapgs barriers and __user pointer sanitization
Jul 31 15:56:59 debian kernel: Spectre V2 : Mitigation: Retpolines
Jul 31 15:56:59 debian kernel: Spectre V2 : Spectre v2 / SpectreRSB mitigation: Filling RSB on context switch
Jul 31 15:56:59 debian kernel: Spectre V2 : Spectre v2 / SpectreRSB : Filling RSB on VMEXIT
Jul 31 15:56:59 debian kernel: RETBleed: WARNING: Spectre v2 mitigation leaves CPU vulnerable to RETBleed attacks, data lea>
Jul 31 15:56:59 debian kernel: RETBleed: Vulnerable
Jul 31 15:56:59 debian kernel: Speculative Store Bypass: Vulnerable
Jul 31 15:56:59 debian kernel: MDS: Mitigation: Clear CPU buffers
Jul 31 15:56:59 debian kernel: MMIO Stale Data: Mitigation: Clear CPU buffers
Jul 31 15:56:59 debian kernel: SRBDS: Unknown: Dependent on hypervisor status
Jul 31 15:56:59 debian kernel: x86/fpu: x87 FPU will use FXSAVE
lines 97-122
```

```
debian@debian: /var/log/journal
File  Edit  View  Search  Terminal  Help
Oct 08 16:43:16 debian systemd-modules-load[241]: Inserted module 'lp'
Oct 08 16:43:16 debian systemd-modules-load[241]: Inserted module 'ppdev'
Oct 08 16:43:16 debian systemd-modules-load[241]: Inserted module 'parport_pc'
Oct 08 16:43:16 debian systemd[1]: Finished keyboard-setup.service - Set the console keyboard layout.
Oct 08 16:43:16 debian systemd[1]: Finished systemd-udev-trigger.service - Coldplug All udev Devices.
Oct 08 16:43:16 debian systemd[1]: Starting systemd-sysctl.service - Apply Kernel Variables...
Oct 08 16:43:16 debian systemd[1]: Started systemd-journald.service - Journal Service.
Oct 08 16:43:16 debian systemd[1]: Starting ifupdown-pre.service - Helper to synchronize boot up for ifupdown...
Oct 08 16:43:16 debian systemd[1]: Starting systemd-journal-flush.service - Flush Journal to Persistent Storage...
Oct 08 16:43:16 debian systemd[1]: Finished systemd-sysusers.service - Create System Users.
Oct 08 16:43:16 debian systemd[1]: Starting systemd-tmpfiles-setup-dev.service - Create Static Device Nodes in /dev...
Oct 08 16:43:16 debian systemd-journald[239]: Time spent on flushing to /var/log/journal/41b6de202c3f48fdaa490411748aaaff i>
Oct 08 16:43:16 debian systemd-journald[239]: System Journal (/var/log/journal/41b6de202c3f48fdaa490411748aaaff) is 47.4M, >
Oct 08 16:43:16 debian systemd-journald[239]: Received client request to flush runtime journal.
Oct 08 16:43:16 debian systemd-journald[239]: File /var/log/journal/41b6de202c3f48fdaa490411748aaaff/system.journal corrupt>
Oct 08 16:43:16 debian systemd[1]: Finished systemd-sysctl.service - Apply Kernel Variables.
Oct 08 16:43:16 debian systemd[1]: Finished ifupdown-pre.service - Helper to synchronize boot up for ifupdown.
Oct 08 16:43:16 debian systemd[1]: Finished systemd-tmpfiles-setup-dev.service - Create Static Device Nodes in /dev.
Oct 08 16:43:16 debian systemd[1]: Reached target local-fs-pre.target - Preparation for Local File Systems.
Oct 08 16:43:16 debian systemd[1]: Reached target local-fs.target - Local File Systems.
Oct 08 16:43:16 debian systemd[1]: Starting apparmor.service - Load AppArmor profiles...
Oct 08 16:43:16 debian systemd[1]: Starting console-setup.service - Set console font and keymap...
Oct 08 16:43:16 debian systemd[1]: Starting plymouth-read-write.service - Tell Plymouth To Write Out Runtime Data...
Oct 08 16:43:16 debian systemd[1]: Starting systemd-binfmt.service - Set Up Additional Binary Formats...
Oct 08 16:43:16 debian systemd[1]: systemd-machine-id-commit.service - Commit a transient machine-id on disk was skipped be>
Oct 08 16:43:16 debian systemd[1]: Starting systemd-udevd.service - Rule-based Manager for Device Events and Files...
lines 10404-10429
```

SSH

```
debian@debian: /var/log/journal
File  Edit  View  Search  Terminal  Tabs  Help
debian@debian: /var/log/journal    debian@debian: /var/log/journal
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 e37eaed4bb834946ad5ff13f475457d7 --
May 19 07:00:26 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
May 19 07:00:27 debian sshd[598]: Server listening on 0.0.0.0 port 22.
May 19 07:00:27 debian sshd[598]: Server listening on :: port 22.
May 19 07:00:27 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
May 19 07:04:28 debian sshd[598]: Received signal 15; terminating.
May 19 07:04:28 debian systemd[1]: Stopping ssh.service - OpenBSD Secure Shell server...
May 19 07:04:28 debian systemd[1]: ssh.service: Deactivated successfully.
May 19 07:04:28 debian systemd[1]: Stopped ssh.service - OpenBSD Secure Shell server.
lines 24-48/98 44%
```

```
debian@debian: /
File  Edit  View  Search  Terminal  Help
debian@debian:/$ sudo journalctl -S "2024-10-08" -U "2024-10-09" -u ssh | grep "Accepted password"
Oct 08 17:40:59 debian sshd[1650]: Accepted password for root from 192.168.0.134 port 45623 ssh2
debian@debian:/$
```

Usuarios

```
debian@debian: /
File Edit View Search Terminal Help
debian@debian:/$ cat /etc/passwd |grep "/bin/bash"
root:x:0:0:root:/root:/bin/bash
debian:x:1000:1000:4geeks,,,:/home/debian:/bin/bash
debian@debian:/$ ls -l /etc/passwd
-rw-r--r-- 1 root root 2004 Oct  8  2024 /etc/passwd
debian@debian:/$
```

<u>Usuarios MariaDB (MySQL)</u>

```
debian@debian: /
File Edit View Search Terminal Help
debian@debian:/$ sudo mysql -e "SELECT user, host, password FROM mysql.user;"
[sudo] password for debian:
+--------------+-----------+-------------------------------------------+
| User         | Host      | Password                                  |
+--------------+-----------+-------------------------------------------+
| mariadb.sys  | localhost |                                           |
| root         | localhost | *6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9 |
| mysql        | localhost | invalid                                   |
| wordpressuser | localhost | *6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9 |
| user         | localhost | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 |
+--------------+-----------+-------------------------------------------+
debian@debian:/$
```

```
debian@debian: /
File Edit View Search Terminal Help
debian@debian:/$ sudo mysql -e "SELECT user, host, plugin FROM mysql.user WHERE user='mysql';"
+-------+-----------+-----------------------+
| User  | Host      | plugin                |
+-------+-----------+-----------------------+
| mysql | localhost | mysql_native_password |
+-------+-----------+-----------------------+
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 WIT
H GRANT OPTION |
| GRANT PROXY ON ''@'%' TO 'mysql'@'localhost' WITH GRANT OPTION
              |
+------------------------------------------------------------------------------------------------------------------------------
--------------+
debian@debian:/$ sudo mysql -e "SELECT user, host, authentication_string FROM mysql.user WHERE user='mysql';"
+-------+-----------+-----------------------+
| User  | Host      | authentication_string |
+-------+-----------+-----------------------+
| mysql | localhost | invalid               |
+-------+-----------+-----------------------+
debian@debian:/$
```

```
debian@debian:/$ sudo mysql -e "SELECT user, host FROM mysql.user WHERE user='mysql';"
+-------+-----------+
| User  | Host      |
+-------+-----------+
| mysql | localhost |
+-------+-----------+
debian@debian:/$
```

```
debian@debian: /
File  Edit  View  Search  Terminal  Help
debian@debian:/$ sudo cat /root/.mysql_history
_HiStOrY_V2_
CREATE\040DATABASE\040wordpress\040DEFAULT\040CHARACTER\040SET\040utf8\040COLLATE\040utf8_unicode_ci;
CREATE\040USER\040'wordpressuser'@'localhost'\040IDENTIFIED\040BY\040'123456';
GRANT\040ALL\040PRIVILEGES\040ON\040wordpress.*\040TO\040'wordpress'@'localhost';\040
GRANT\040ALL\040PRIVILEGES\040ON\040wordpress.*\040TO\040'wordpressuser'@'localhost';
FLUSH\040PRIVILIGES;
FLUSH\040PRIVILEGES;
EXIT;
CREATE\040USER\040'user'@'localhost'\040IDENTIFIED\040BY\040'password';
GRANT\040ALL\040PRIVILEGES\040ON\040*.*\040TO\040'user'@'localhost'\040WITH\040GRANT\040OPTION;
FLUSH\040PRIVILEGES;
EXIT;
debian@debian:/$
```

Rootkits y malware

- Chkrootkit

```
Checking `sniffer'...                                    WARNING

WARNING: Output from ifpromisc:
lo: not promisc and no packet sniffer sockets
enp0s3: PACKET SNIFFER(/usr/sbin/NetworkManager[446], /usr/sbin/NetworkManager[446])
```

```
Searching for suspicious files and dirs...                  WARNING

WARNING: The following suspicious files and directories were found:
/usr/lib/ruby/gems/3.1.0/gems/typeprof-0.21.2/vscode/.vscodeignore
/usr/lib/ruby/gems/3.1.0/gems/typeprof-0.21.2/vscode/.gitignore
/usr/lib/ruby/gems/3.1.0/gems/typeprof-0.21.2/vscode/.vscode
/usr/lib/ruby/vendor_ruby/rubygems/ssl_certs/.document
/usr/lib/ruby/vendor_ruby/rubygems/tsort/.document
/usr/lib/ruby/vendor_ruby/rubygems/optparse/.document
/usr/lib/libreoffice/share/.registry
```

- Rkhunter

```
/usr/bin/kmod                                                [ OK ]
/usr/bin/systemd                                             [ OK ]
/usr/bin/systemctl                                           [ OK ]
/usr/bin/gawk                                                [ OK ]
/usr/bin/lwp-request                                         [ Warning ]
/usr/bin/bsd-mailx                                           [ OK ]
/usr/bin/dash                                                [ OK ]
/usr/bin/x86_64-linux-gnu-size                               [ OK ]
/usr/bin/x86_64-linux-gnu-strings                            [ OK ]
```

```
Performing malware checks
  Checking running processes for suspicious files          [ None found ]
  Checking for login backdoors                             [ None found ]
  Checking for sniffer log files                           [ None found ]
  Checking for suspicious directories                      [ None found ]
  Checking for suspicious (large) shared memory segments   [ Warning ]
  Checking for Apache backdoor                             [ Not found ]
```

```
Performing system configuration file checks
  Checking for an SSH configuration file                     [ Found ]
  Checking if SSH root access is allowed                     [ Warning ]
  Checking if SSH protocol v1 is allowed                     [ Not set ]
  Checking for other suspicious configuration settings       [ None found ]
  Checking for a running system logging daemon               [ Found ]
  Checking for a system logging configuration file           [ Found ]
```

```
System checks summary
=====================

File properties checks...
    Files checked: 144
    Suspect files: 1

Rootkit checks...
    Rootkits checked : 497
    Possible rootkits: 4

Applications checks...
    All checks skipped

The system checks took: 3 minutes and 36 seconds

All results have been written to the log file: /var/log/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)

debian@debian:/$
```

Wordpress

```
debian@debian: ~
File  Edit  View  Search  Terminal  Help
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Mon 2025-06-02 07:25:28 EDT; 4h 25min ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 597 (apache2)
      Tasks: 6 (limit: 2284)
     Memory: 24.7M
        CPU: 1.650s
     CGroup: /system.slice/apache2.service
             ├─597 /usr/sbin/apache2 -k start
             ├─654 /usr/sbin/apache2 -k start
             ├─664 /usr/sbin/apache2 -k start
             ├─665 /usr/sbin/apache2 -k start
             ├─669 /usr/sbin/apache2 -k start
             └─671 /usr/sbin/apache2 -k start

Jun 02 07:25:27 debian systemd[1]: Starting apache2.service - The Apache HTTP Server...
Jun 02 07:25:28 debian systemd[1]: Started apache2.service - The Apache HTTP Server.
~
```

```
debian@debian: /
File  Edit  View  Search  Terminal  Help
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 May 19 08:11 license.txt
-rwxrwxrwx  1 www-data www-data  7425 May 19 08:11 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 May 19 08:11 wp-config-sample.php
drwxrwxrwx  6 www-data www-data  4096 May 19 08:12 wp-content
-rwxrwxrwx  1 www-data www-data  5617 May 19 08:11 wp-cron.php
drwxrwxrwx 30 www-data www-data 12288 May 19 08:11 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 May 19 08:11 wp-login.php
-rwxrwxrwx  1 www-data www-data  8727 May 19 08:11 wp-mail.php
-rwxrwxrwx  1 www-data www-data 30081 May 19 08:11 wp-settings.php
-rwxrwxrwx  1 www-data www-data 34516 May 19 08:11 wp-signup.php
-rwxrwxrwx  1 www-data www-data  5102 May 19 08:11 wp-trackback.php
-rwxrwxrwx  1 www-data www-data  3205 May 19 08:11 xmlrpc.php
debian@debian:/$
```

4. Mitigación

A. <u>Restricción del tráfico</u>

Para evitar el acceso como root al servidor a través de SSH, se restringe el tráfico de la IP sospechosa (192.168.0.134) mediante reglas específicas en iptables que impiden su conexión.

```
debian@debian: ~
File  Edit  View  Search  Terminal  Help
debian@debian:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
debian@debian:~$ sudo iptables -A INPUT -s 192.168.0.134 -j DROP
debian@debian:~$ sudo iptables-save
# Generated by iptables-save v1.8.9 (nf_tables) on Mon Jun  2 12:04:26 2025
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -s 192.168.0.134/32 -j DROP
COMMIT
# Completed on Mon Jun  2 12:04:26 2025
debian@debian:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  192.168.0.134        anywhere
```

B. <u>Configuración segura de SSH</u>

Para reforzar la seguridad en SSH, se modifica la configuración del archivo (sudo nano /etc/ssh/sshd_config) con el propósito de desactivar el acceso mediante contraseña y evitar el inicio de sesión como usuario root.

```
debian@debian: /var/www/html
File  Edit  View  Search  Terminal  Help
debian@debian:/var/www/html$ cat /etc/ssh/sshd_config | grep "PermitRootLogin\|PasswordAuthentication"
PermitRootLogin yes
PasswordAuthentication yes
# PasswordAuthentication.  Depending on your PAM configuration,
# the setting of "PermitRootLogin prohibit-password".
# PAM authentication, then enable this but set PasswordAuthentication
debian@debian:/var/www/html$
```

```
debian@debian: /var/www/html
File  Edit  View  Search  Terminal  Help
  GNU nano 7.2                    /etc/ssh/sshd_config *
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

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

^G Help      ^O Write Out   ^W Where Is    ^K Cut       ^T Execute   ^C Location   M-U Undo
^X Exit      ^R Read File   ^\ Replace     ^U Paste     ^J Justify   ^/ Go To Line M-E Redo
```

```
debian@debian: /var/www/html
File  Edit  View  Search  Terminal  Help
  GNU nano 7.2                    /etc/ssh/sshd_config *

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# 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

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes

^G Help      ^O Write Out   ^W Where Is    ^K Cut       ^T Execute   ^C Location   M-U Undo
^X Exit      ^R Read File   ^\ Replace     ^U Paste     ^J Justify   ^/ Go To Line M-E Redo
```

```
debian@debian: /var/www/html
File  Edit  View  Search  Terminal  Help
debian@debian:/var/www/html$ sudo nano /etc/ssh/sshd_config
[sudo] password for debian:
debian@debian:/var/www/html$ cat /etc/ssh/sshd_config | grep "PermitRootLogin\|PasswordAuthentication"
PermitRootLogin no
PasswordAuthentication no
# PasswordAuthentication.  Depending on your PAM configuration,
# the setting of "PermitRootLogin prohibit-password".
# PAM authentication, then enable this but set PasswordAuthentication
debian@debian:/var/www/html$
```

Además, se instala, configura y activa fail2ban:

```
debian@debian: ~
File  Edit  View  Search  Terminal  Help
debian@debian:~$ sudo apt install fail2ban
[sudo] password for debian:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  linux-image-6.1.0-22-amd64
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  python3-pyinotify python3-systemd whois
Suggested packages:
  system-log-daemon monit sqlite3 python-pyinotify-doc
The following NEW packages will be installed:
  fail2ban python3-pyinotify python3-systemd whois
0 upgraded, 4 newly installed, 0 to remove and 213 not upgraded.
Need to get 589 kB of archives.
After this operation, 2,901 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://deb.debian.org/debian bookworm/main amd64 fail2ban all 1.0.2-2 [451 kB]
Get:2 http://deb.debian.org/debian bookworm/main amd64 python3-pyinotify all 0.9.6-2 [27.4 kB]
Get:3 http://deb.debian.org/debian bookworm/main amd64 python3-systemd amd64 235-1+b2 [39.3 kB]
Get:4 http://deb.debian.org/debian bookworm/main amd64 whois amd64 5.5.17 [70.8 kB]
Fetched 589 kB in 0s (1,890 kB/s)
Selecting previously unselected package fail2ban.
(Reading database ... 174549 files and directories currently installed.)
Preparing to unpack .../fail2ban_1.0.2-2_all.deb ...
```

```
debian@debian: ~
File  Edit  View  Search  Terminal  Tabs  Help
debian@debian: ~        debian@debian: ~
  GNU nano 7.2                /etc/fail2ban/jail.local
[sshd]
enabled = true
backend = systemd
logpath = journalctl -u ssh -b

                              [ Read 4 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

```
debian@debian: ~
File  Edit  View  Search  Terminal  Help
debian@debian:~$ sudo nano /etc/fail2ban/jail.local
[sudo] password for debian:
debian@debian:~$ sudo systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /lib/syste
md/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable fail2ban
debian@debian:~$ sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; preset: ena>
     Active: active (running) since Tue 2025-06-03 05:12:42 EDT; 9min ago
       Docs: man:fail2ban(1)
   Main PID: 538 (fail2ban-server)
      Tasks: 5 (limit: 2284)
     Memory: 29.8M
        CPU: 1.269s
     CGroup: /system.slice/fail2ban.service
             └─538 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Jun 03 05:12:42 debian systemd[1]: Started fail2ban.service - Fail2Ban Service.
Jun 03 05:12:43 debian fail2ban-server[538]: 2025-06-03 05:12:43,014 fail2ban.c>
Jun 03 05:12:43 debian fail2ban-server[538]: Server ready
lines 1-14/14 (END)
```

```
debian@debian: ~
File  Edit  View  Search  Terminal  Help
debian@debian:~$ sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; preset: ena>
     Active: active (running) since Tue 2025-06-03 05:12:42 EDT; 9min ago
       Docs: man:fail2ban(1)
   Main PID: 538 (fail2ban-server)
      Tasks: 5 (limit: 2284)
     Memory: 29.8M
        CPU: 1.269s
     CGroup: /system.slice/fail2ban.service
             └─538 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Jun 03 05:12:42 debian systemd[1]: Started fail2ban.service - Fail2Ban Service.
Jun 03 05:12:43 debian fail2ban-server[538]: 2025-06-03 05:12:43,014 fail2ban.c>
Jun 03 05:12:43 debian fail2ban-server[538]: Server ready
lines 1-14/14 (END)
debian@debian:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
debian@debian:~$
```

C. Modificación de las credenciales del usuario root

Se actualiza la contraseña del usuario root debido a su compromiso de seguridad, reemplazando “123456” por una nueva clave más segura (LDeb_3625_).

```
debian@debian: ~
File  Edit  View  Search  Terminal  Help
debian@debian:~$ sudo passwd root
[sudo] password for debian:
New password:
Retype new password:
passwd: password updated successfully
debian@debian:~$
```

D. Administración de servidor

1. wp-config.php

Se ajustan los permisos del archivo wp-config.php que contiene información sensible de la base de datos para aplicar el principio de mínimo privilegio y minimizar el riesgo de modificaciones no autorizadas por parte de cualquier usuario.

Además, se modifican los permisos de la carpeta wp-content/uploads para:

→ Permitir la lectura, escritura y ejecución al propietario, y sólo lectura y ejecución al resto (útil para permitir la subida y acceso a imágenes y archivos en WordPress)

→ Cambiar el propietario de la carpeta (lo cual permite que el servidor web tenga el control de los archivos subidos)

```
debian@debian: /var/www/html
File  Edit  View  Search  Terminal  Help
debian@debian:/var/www/html$ sudo chmod 640 wp-config.php
debian@debian:/var/www/html$ sudo chmod -R 755 wp-content/uploads
debian@debian:/var/www/html$ sudo chown -R www-data:www-data wp-content/uploads
```

```
debian@debian: /var/www/html
File  Edit  View  Search  Terminal  Help
debian@debian:/var/www/html$ ls -al
total 260
drwxrwxrwx  5 www-data www-data  4096 May 19 08:11 .
drwxr-xr-x  3 root     root      4096 Sep 30  2024 ..
-rwxrwxrwx  1 www-data www-data   523 Sep 30  2024 .htaccess
-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 May 19 08:11 license.txt
-rwxrwxrwx  1 www-data www-data  7425 May 19 08:11 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
-rw-r-----  1 www-data www-data  3017 Sep 30  2024 wp-config.php
-rwxrwxrwx  1 www-data www-data  3336 May 19 08:11 wp-config-sample.php
drwxrwxrwx  6 www-data www-data  4096 May 19 08:12 wp-content
-rwxrwxrwx  1 www-data www-data  5617 May 19 08:11 wp-cron.php
drwxrwxrwx 30 www-data www-data 12288 May 19 08:11 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 May 19 08:11 wp-login.php
-rwxrwxrwx  1 www-data www-data  8727 May 19 08:11 wp-mail.php
-rwxrwxrwx  1 www-data www-data 30081 May 19 08:11 wp-settings.php
-rwxrwxrwx  1 www-data www-data 34516 May 19 08:11 wp-signup.php
-rwxrwxrwx  1 www-data www-data  5102 May 19 08:11 wp-trackback.php
-rwxrwxrwx  1 www-data www-data  3205 May 19 08:11 xmlrpc.php
debian@debian:/var/www/html$
```

2. Directorios y archivos

Se ajustan los permisos de los directorios y archivos:

- Los directorios tendrán permisos de lectura, escritura y ejecución para el propietario, y sólo lectura y ejecución para el resto.
- Los archivos tendrán permisos de lectura y escritura para el propietario, pero sólo lectura para el resto.

```
debian@debian: /var/www/html
File  Edit  View  Search  Terminal  Help
debian@debian:/var/www/html$ sudo find . -type d -exec chmod 755 {} \;
debian@debian:/var/www/html$ sudo find . -type f -exec chmod 644 {} \;
debian@debian:/var/www/html$ ls -al
total 260
drwxr-xr-x  5 www-data www-data  4096 May 19 08:11 .
drwxr-xr-x  3 root     root      4096 Sep 30  2024 ..
-rw-r--r--  1 www-data www-data   523 Sep 30  2024 .htaccess
-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 May 19 08:11 license.txt
-rw-r--r--  1 www-data www-data  7425 May 19 08:11 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-r--r--  1 www-data www-data  3017 Sep 30  2024 wp-config.php
-rw-r--r--  1 www-data www-data  3336 May 19 08:11 wp-config-sample.php
drwxr-xr-x  6 www-data www-data  4096 May 19 08:12 wp-content
-rw-r--r--  1 www-data www-data  5617 May 19 08:11 wp-cron.php
drwxr-xr-x 30 www-data www-data 12288 May 19 08:11 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 May 19 08:11 wp-login.php
-rw-r--r--  1 www-data www-data  8727 May 19 08:11 wp-mail.php
-rw-r--r--  1 www-data www-data 30081 May 19 08:11 wp-settings.php
-rw-r--r--  1 www-data www-data 34516 May 19 08:11 wp-signup.php
-rw-r--r--  1 www-data www-data  5102 May 19 08:11 wp-trackback.php
-rw-r--r--  1 www-data www-data  3205 May 19 08:11 xmlrpc.php
debian@debian:/var/www/html$
```

E. Actualización del sistema

Se buscan y actualizan las últimas versiones de los paquetes disponibles y se eliminan los paquetes innecesarios.

```
debian@debian: ~
File  Edit  View  Search  Terminal  Help
Found initrd image: /boot/initrd.img-6.1.0-37-amd64
Found linux image: /boot/vmlinuz-6.1.0-25-amd64
Found initrd image: /boot/initrd.img-6.1.0-25-amd64
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
done
Processing triggers for man-db (2.11.2-2) ...
Processing triggers for libc-bin (2.36-9+deb12u10) ...
debian@debian:~$ sudo apt update && sudo apt upgrade -y && sudo apt autoremove -y
Hit:1 http://deb.debian.org/debian bookworm InRelease
Hit:2 http://deb.debian.org/debian bookworm-updates InRelease
Hit:3 http://security.debian.org/debian-security bookworm-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
debian@debian:~$
```

5. Conclusiones de prevención futuras

- Autenticación multifactor (MFA) para SSH
- Monitorización continua con WAZUH/SIEMs
- Desarrollo e implementación de una Política de contraseña seguras
- Realización de:
    - Auditorías de seguridad con periodicidad
    - Copias de seguridad de las bases de datos y archivos críticos