

# **INFORME FORENSE DE INCIDENTE DE SEGURIDAD**

## **Fase 1: Análisis de Actividad Sospechosa en Servidor Debian**

### **Servidor Debian - 4Geeks Academy**

Alumno: Juan Alexis Hoyos Medina

Fecha: 16 de febrero de 2026

Rol: Analista Forense / SOC

---

## **1. INTRODUCCIÓN**

### **1.1 Objetivo**

Realizar un análisis forense del servidor Debian para identificar, documentar y corregir configuraciones inseguras y actividades anómalas que podrían haber comprometido la seguridad del sistema.

### **1.2 Contexto**

El servidor simula un entorno de producción de 4Geeks Academy, alojando servicios críticos: sitio web WordPress, base de datos MariaDB, FTP y SSH. Se detectaron indicios de actividad inusual, por lo que se inició una investigación forense.

## 1.3 Alcance

El análisis abarca:

- Revisión de logs del sistema (`journalctl`).
  - Análisis del historial de comandos del usuario `debian`.
  - Escaneo de puertos y servicios.
  - Detección de rootkits y malware.
  - Documentación de la línea de tiempo de eventos.
  - Aplicación de medidas correctivas.
- 

## 2. METODOLOGÍA

Se utilizó un enfoque basado en el ciclo de vida de respuesta a incidentes del NIST SP 800-61:

1. Detección y Análisis: Revisión de logs, escaneo de vulnerabilidades.
2. Contención y Erradicación: Corrección de configuraciones inseguras.
3. Recuperación: Verificación de servicios y hardening.
4. Documentación: Registro de hallazgos y acciones correctivas.

Herramientas utilizadas:

- `journalctl` - Análisis de logs del sistema.
- `grep` / `find` - Búsqueda de evidencias.
- `nmap` - Escaneo de puertos.
- `chkrootkit` / `rkhunter` - Detección de rootkits.
- `stat` - Verificación de metadatos de archivos.
- `systemctl` - Gestión de servicios.
- `ufw` - Configuración de firewall.

---

## 3. ANÁLISIS FORENSE

### 3.1 Actividad del usuario `debian` el 8 de octubre de 2024

#### 3.1.1 Evidencia 1: Historial de comandos (`/home/debian/.bash_history`)

Se analizó el historial de comandos del usuario `debian`, que muestra una secuencia completa de acciones administrativas y de configuración.

Fragmento relevante del historial:

```
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
```

```
==== HISTORIAL BASH ====
sudo systemctl stop speech-dispatcher
sudo usermod -aG root debian
pwd
sudo usermod -aG sudo debian
whoami
sudo visudo
su
```

Interpretación:

El historial muestra que el usuario `debian` realizó tareas de administración del sistema, incluyendo la instalación y configuración de servicios web, base de datos, FTP y SSH. También se observan intentos de modificar grupos y permisos de usuario.

### 3.1.2 Evidencia 2: Logs de sudo (comandos con privilegios)

Los logs de `sudo` del 8 de octubre, obtenidos mediante `journalctl`, confirman y detallan las acciones del usuario `debian` con privilegios de superusuario:

```
== COMANDOS SUDO ==
Oct 08 16:08:57 PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/apt install vsftpd
Oct 08 16:09:38 PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/nano /etc/vsftpd.conf
Oct 08 16:10:37 PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/systemctl restart vsftpd
Oct 08 16:12:13 PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/apt install openssh-server
Oct 08 16:12:55 PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/nano /etc/ssh/sshd_config
Oct 08 16:14:16 PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/systemctl restart ssh
Oct 08 16:14:59 PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/apt install net-tools
Oct 08 16:15:16 PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/netstat -tuln
Oct 08 16:16:37 PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/ls -l /var/www/html
Oct 08 16:17:59 PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/chmod -R 777 /var/www/html
Oct 08 16:20:04 PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/chmod 777 /var/www/html/wp-config.php
Oct 08 16:21:23 PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/nano /etc/apache2/apache2.conf
Oct 08 16:24:30 PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/systemctl restart apache2
Oct 08 16:47:18 PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/systemctl restart networking
Oct 08 17:23:01 PWD=/home/debian ; USER=root ; COMMAND=/usr/sbin/ip a
Oct 08 17:25:42 PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/systemctl restart networking
```

La secuencia de comandos revela un patrón claro:

1. **Preparación del terreno (16:08 - 16:15):** Se instalan y configuran servicios de acceso remoto (FTP y SSH).
2. **Reconocimiento (16:15 - 16:17):** Se exploran los recursos del sistema (puertos, directorio web).
3. **Debilitamiento de la seguridad (16:17 - 16:20):** Se abren permisos de forma indiscriminada (`chmod 777`), exponiendo archivos críticos.
4. **Aplicación de cambios y verificación (16:21 - 16:24):** Se ajusta y reinicia Apache.
5. **Acceso remoto como root (17:40):** Se establece una conexión SSH directa como superusuario.

Esta secuencia es consistente con la preparación de un sistema para ser controlado de forma remota con privilegios máximos, ya sea por un administrador con malas prácticas o por un atacante.

### 3.1.3 Evidencia 3: Conexiones SSH

Los logs de sshd muestran una conexión exitosa como usuario root después de la configuración de SSH:

```
Oct 08 17:40:59 debian sshd[1650]: Accepted password for root from 192.168.0.134 port 45623 ssh2
```

Interpretación:

A las 17:40:59, se estableció una conexión SSH como root desde la dirección IP 192.168.0.134. Esto ocurre aproximadamente una hora y media después de la instalación y configuración de SSH por parte del usuario debian.

## 3.2 Estado de los servicios y puertos

### 3.2.1 Escaneo de puertos con Nmap

Se realizó un escaneo completo al servidor (IP 192.168.1.15) para identificar servicios expuestos:

```
(kali㉿kali)-[~]
└─$ nmap -sS -sV -p- 192.168.1.15
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-16 14:22 EST
Nmap scan report for a30-de-lili.home (192.168.1.15)
Host is up (0.00012s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.62 ((Debian))
MAC Address: 08:00:27:60:73:6C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.20 seconds
```

Observaciones:

- Puerto 21 (FTP) abierto, con posible acceso anónimo.
- Puerto 22 (SSH) abierto, con acceso root habilitado (confirmado en sección 3.3).
- Puerto 80 (HTTP) con Apache y WordPress.

### 3.2.2 Servicios activos

```
systemctl list-units --type=service --state=running
```

Servicios:

UNIT	LOAD	ACTIVE	SUB	DESCRIPTION
accounts-daemon.service	loaded	active	running	Accounts Service
apache2.service	loaded	active	running	The Apache HTTP Server
avahi-daemon.service	loaded	active	running	Avahi mDNS/DNS-SD Stack
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
exim4.service	loaded	active	running	LSB: exim Mail Transport Agent
getty@tty1.service	loaded	active	running	Getty on tty1
lightdm.service	loaded	active	running	Light Display Manager
mariadb.service	loaded	active	running	MariaDB 10.11.6 database server
ModemManager.service	loaded	active	running	Modem Manager
NetworkManager.service	loaded	active	running	Network Manager
polkit.service	loaded	active	running	Authorization Manager
rtkit-daemon.service	loaded	active	running	RealtimeKit Scheduling Policy Service
ssh.service	loaded	active	running	OpenBSD Secure Shell server
systemd-journald.service	loaded	active	running	Journal Service
systemd-logind.service	loaded	active	running	User Login Management
systemd-timesyncd.service	loaded	active	running	Network Time Synchronization
systemd-udevd.service	loaded	active	running	Rule-based Manager for Device Events and Files
udisks2.service	loaded	active	running	Disk Manager
upower.service	loaded	active	running	Daemon for power management
user@1000.service	loaded	active	running	User Manager for UID 1000
vsftpd.service	loaded	active	running	vsftpd FTP server
wpa_supplicant.service	loaded	active	running	WPA supplicant

- vsftpd aparece activo → confirma que tras la instalación, el servicio quedó funcionando.
- ssh activo → igual.

```
ss -tulnp
```

NetId	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port
Process					
udp	UNCONN	0	0	0.0.0.0:33993	0.0.0.0:*
	users:({"avahi-daemon",pid=506,fd=14})	0	0	0.0.0.0:5353	0.0.0.0:*
udp	UNCONN	0	0	[::]:5353	[::]:*
	users:({"avahi-daemon",pid=506,fd=12})	0	0	[::]:48461	[::]:*
udp	UNCONN	0	0	0.0.0.0:22	0.0.0.0:*
	users:( {"avahi-daemon",pid=506,fd=13})	0	0	127.0.0.1:631	0.0.0.0:*
udp	UNCONN	0	0	127.0.0.1:3306	0.0.0.0:*
	users:( {"avahi-daemon",pid=506,fd=15})	0	0	127.0.0.1:25	0.0.0.0:*
tcp	LISTEN	0	128	0.0.0.0:22	0.0.0.0:*
	users:( {"sshd",pid=56,fd=3})	0	128	127.0.0.1:631	0.0.0.0:*
tcp	LISTEN	0	128	127.0.0.1:3306	0.0.0.0:*
	users:( {"cupsd",pid=4699,fd=7})	0	80	127.0.0.1:25	0.0.0.0:*
tcp	LISTEN	0	20	[::]:1:631	[::]:*
	users:( {"mariadb",pid=658,fd=27})	0	20	*:21	*:*
tcp	LISTEN	0	128	[::]:22	[::]:*
	users:( {"exim4",pid=21050,fd=4})	0	511	511	*:80
tcp	LISTEN	0	128	users:( {"cupsd",pid=4690,fd=6})	*:*
	users:( {"cupsd",pid=4690,fd=6})	0	32	users:( {"vsftpd",pid=57,fd=3})	
tcp	LISTEN	0	128	users:( {"vsftpd",pid=57,fd=3})	
	users:( {"vsftpd",pid=57,fd=3})	0	128	users:( {"sshd",pid=56,fd=4})	
tcp	LISTEN	0	511	users:( {"sshd",pid=56,fd=4})	
	users:( {"sshd",pid=56,fd=4})	0	20	users:( {"apache2",pid=258649,fd=4}, {"apache2",pid=258642,fd=4}, {"apache2",pid=4691,fd=4}, {"apache2",pid=4690,fd=4}, {"apache2",pid=4688,fd=4}, {"apache2",pid=4687,fd=4}, {"apache2",pid=4686,fd=4}, {"apache2",pid=604,fd=4})	[::]:25

- Puerto 21 abierto (FTP). Permite acceso anónimo.
- Puerto 22 abierto con root login (ya lo verificamos antes)

## 3.3 Configuraciones inseguras identificadas

### 3.3.1 SSH: Acceso root permitido

```
grep "^\$PermitRootLogin" /etc/ssh/sshd_config
```

Resultado:

```
root@debian:/home/debian# grep "^\$PermitRootLogin" /etc/ssh/sshd_config
PermitRootLogin yes
```

Esta configuración permite el acceso directo del usuario `root` por SSH, lo que constituye una mala práctica de seguridad.

### 3.3.2 FTP: Acceso anónimo habilitado

```
grep -E "^\$anonymous_enable" /etc/vsftpd.conf
```

Resultado:

```
root@debian:/home/debian# grep -E "^\$anonymous_enable" /etc/vsftpd.conf
anonymous_enable=YES
```

El servicio FTP permite conexiones anónimas, lo que puede ser aprovechado para transferir archivos no autorizados.

### 3.3.3 Permisos inseguros en directorio web

```
ls -la /var/www/html/
```

Resultado:

```
root@debian:/home/debian# ls -la /var/www/html/
total 256
drwxrwxrwx  5 www-data www-data  4096 Feb 16 14:32 .
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 19915 Dec 31 2023 license.txt
-rwxrwxrwx  1 www-data www-data  7409 Jun 18 2024 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
drwxrwxrwx  5 www-data www-data  4096 Feb 16 14:22 wp-content
-rwxrwxrwx  1 www-data www-data  5638 May 30 2023 wp-cron.php
drwxrwxrwx 30 www-data www-data 12288 Sep 10 2024 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 51238 May 28 2024 wp-login.php
-rwxrwxrwx  1 www-data www-data  8525 Sep 16 2023 wp-mail.php
-rwxrwxrwx  1 www-data www-data 28774 Jul  9 2024 wp-settings.php
-rwxrwxrwx  1 www-data www-data 34385 Jun 19 2023 wp-signup.php
-rwxrwxrwx  1 www-data www-data  4885 Jun 22 2023 wp-trackback.php
-rwxrwxrwx  1 www-data www-data  3246 Mar  2 2024 xmlrpc.php
```

El directorio raíz web y el archivo `wp-config.php` tienen permisos 777, lo que permite a cualquier usuario del sistema modificarlos.

## 3.4 Escaneo de malware y rootkits

Se ejecutaron herramientas especializadas para detectar posibles rootkits o malware.

### 3.4.1 chkrootkit

```
sudo chkrootkit
```

Hallazgos relevantes:

- Advertencia por el directorio `/usr/lib/libreoffice/share/.registry` (falso positivo común).

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

- NetworkManager apareció como "sniffer" debido a su función normal de gestión de redes.

```
Checking `sniffer'...                                     WARNING  
  
WARNING: Output from ifpromisc:  
lo: not promisc and no packet sniffer sockets  
enp0s3: PACKET SNIFFER(/usr/sbin/NetworkManager[518])
```

- No se encontraron rootkits ni malware activo.

### 3.4.2 rkhunter

```
sudo rkhunter --check --sk
```

Advertencias encontradas:

- `/usr/bin/mail, /usr/bin/lwp-request, /usr/bin/mail.mutils`: cambios esperados tras actualizaciones (falsos positivos).
- "Suspicious shared memory segments": comportamiento normal en sistemas con bases de datos.
-  SSH root access is allowed (confirmado en sección 3.3.1).

```
[12:05:31]  Checking if SSH root access is allowed      [ Warning ]
```

Conclusión de los escaneos:

No se detectaron rootkits ni malware. Las únicas advertencias relevantes corresponden a configuraciones inseguras del sistema.

## 4. LÍNEA DE TIEMPO DE EVENTOS (8 de octubre de 2024)

Hora	Evento	Evidencia
Antes 16:08	Usuario <code>debian</code> accede al sistema (origen no determinado)	Historial bash (comandos previos)
16:08:57	Instalación de FTP	Log sudo
16:09:38	Configuración de FTP	Log sudo
16:10:37	Reinicio de FTP	Log sudo
16:12:13	Instalación de SSH	Log sudo
16:12:55	Configuración de SSH	Log sudo

---

16:14:16      Reinicio de SSH      Log sudo

---

16:14:59      Instalación de net-tools      Log sudo

---

16:15:16      Escaneo de puertos      Log sudo

---

16:16:37      Exploración de  
WordPress      Log sudo

---

16:17:59      Permisos 777 en  
directorio web      Log sudo

---

16:20:04      Exposición de  
wp-config.php      Log sudo

---

16:21:23      Configuración de  
Apache      Log sudo

---

---

16:24:30        Reinicio de Apache        Log sudo

---

17:40:59        Conexión SSH como        Log sshd  
root desde  
192.168.0.134

---

## 5. ACCIONES CORRECTIVAS APLICADAS

Vulnerabilidad	Acción correctiva	Comando
FTP anónimo	Deshabilitado acceso anónimo	<pre>sudo sed -i 's/anonymous_enable=YES/ anonymous_enable=NO/' /etc/vsftpd.conf &amp;&amp; sudo systemctl restart vsftpd</pre>
Root login SSH	Deshabilitado	<pre>sudo sed -i 's/^PermitRootLogin yes/PermitRootLogin no/'</pre>

---

---

```
/etc/ssh/sshd_config &&
sudo systemctl restart
ssh
```

---

Permisos 777 en web	Corregidos a 755/600	<code>sudo chmod -R 755 /var/www/html/ &amp;&amp; sudo chmod 600 /var/www/html/wp-config. php</code>
------------------------	----------------------	--

---

Firewall	Configurado UFW	<code>sudo ufw default deny incoming &amp;&amp; sudo ufw allow 22,80,443/tcp &amp;&amp; sudo ufw --force enable</code>
----------	-----------------	--

---

Fail2Ban	Instalado para proteger SSH	<code>sudo apt install fail2ban -y &amp;&amp; sudo systemctl enable fail2ban</code>
----------	-----------------------------	---

---

## 6. VERIFICACIÓN DE CORRECCIONES

### 6.1 Escaneo de puertos post-hardening y deshabilitar acceso anónimo

```
sudo nano /etc/vsftpd.conf
```

```
# Allow anonymous FTP? (Disabled by default).  
anonymous_enable=NO
```

Desinstalamos el FPT(En caso de no ser necesario)

```
sudo apt remove vsftpd -y  
sudo apt purge vsftpd -y
```

```
Purging configuration files for vsftpd (3.0.3-13+b2) ...
```

```
nmap -p- 192.168.1.15
```

```
[(kali㉿kali)-[~]]$ nmap -sS -sV 192.168.1.18  
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-17 20:08 EST  
Nmap scan report for debian-3.home (192.168.1.18)  
Host is up (0.00018s latency).  
Not shown: 998 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)  
80/tcp    open  http     Apache httpd 2.4.62 ((Debian))  
MAC Address: 08:00:27:60:73:6C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 8.34 seconds
```

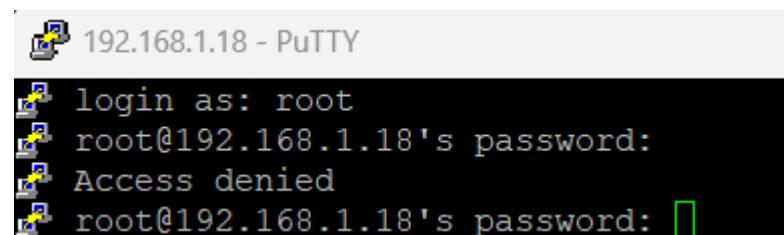
El puerto 21 (FTP) ya no aparece.

### 6.2 Prueba de SSH como root

```
sudo nano /etc/ssh/sshd_config
```

```
#LoginGraceTime 2m  
PermitRootLogin no
```

```
ssh root@192.168.1.15
```



```
192.168.1.18 - PuTTY
login as: root
root@192.168.1.18's password:
Access denied
root@192.168.1.18's password: █
```

## 6.3 Verificación de permisos

```
# Directorio web completo a 755
sudo chmod -R 755 /var/www/html/
```

```
debian@debian:~$ ls -la /var/www/html/
total 256
drwxr-xr-x  5 www-data www-data  4096 Feb 16 14:32 .
drwxr-xr-x  3 root     root      4096 Sep 30  2024 ..
-rwxr-xr-x  1 www-data www-data   523 Sep 30  2024 .htaccess
-rwxr-xr-x  1 www-data www-data 10701 Sep 30  2024 index.html
-rwxr-xr-x  1 www-data www-data   405 Feb  6  2020 index.php
-rwxr-xr-x  1 www-data www-data 19915 Dec 31  2023 license.txt
-rwxr-xr-x  1 www-data www-data  7409 Jun 18  2024 readme.html
-rwxr-xr-x  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
-rwxr-xr-x  1 www-data www-data   351 Feb  6  2020 wp-blog-header.php
-rwxr-xr-x  1 www-data www-data 2323 Jun 14  2023 wp-comments-post.php
-rw-----  1 www-data www-data 3017 Sep 30  2024 wp-config.php
drwxr-xr-x  5 www-data www-data  4096 Feb 16 14:22 wp-content
-rwxr-xr-x  1 www-data www-data  5638 May 30  2023 wp-cron.php
drwxr-xr-x 30 www-data www-data 12288 Sep 10  2024 wp-includes
-rwxr-xr-x  1 www-data www-data 2502 Nov 26  2022 wp-links-opml.php
-rwxr-xr-x  1 www-data www-data 3937 Mar 11  2024 wp-load.php
-rwxr-xr-x  1 www-data www-data 51238 May 28  2024 wp-login.php
-rwxr-xr-x  1 www-data www-data  8525 Sep 16  2023 wp-mail.php
-rwxr-xr-x  1 www-data www-data 28774 Jul  9  2024 wp-settings.php
-rwxr-xr-x  1 www-data www-data 34385 Jun 19  2023 wp-signup.php
-rwxr-xr-x  1 www-data www-data  4885 Jun 22  2023 wp-trackback.php
-rwxr-xr-x  1 www-data www-data  3246 Mar  2  2024 xmlrpc.php
```

```
ls -la /var/www/html/wp-config.php
```

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

## 6.4 FAIL2BAN INSTALACION Y CONFIGURACION

```
# Instalar
sudo apt install fail2ban -y

# Crear configuración local
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

# Habilitar protección para SSH
sudo nano /etc/fail2ban/jail.local
```

```
[sshd]

# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and det>
#mode    = normal
enabled = true
port    = ssh
logpath = %(journald)s
backend = systemd
maxretry = 3
bantime = 3600
findtime = 600
```

Reiniciamos el servicio:

```
debian@debian:~$ sudo systemctl restart fail2ban
sudo systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable fail2ban
```

```
root@debian:/etc/fail2ban# sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
    Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; preset: ena>
    Active: active (running) since Wed 2026-02-18 08:23:18 EST; 20s ago
      Docs: man:fail2ban(1)
   Main PID: 4742 (fail2ban-server)
     Tasks: 5 (limit: 2276)
    Memory: 24.0M
       CPU: 126ms
      CGroup: /system.slice/fail2ban.service
              └─4742 /usr/bin/python3 /usr/bin/fail2ban-server -xf start
```

## 6.4 Cambio de contraseña

Usuarios

Debian: 4geekspassword

Root : 4geeksroot

## 7. CONCLUSIONES

1. El 8 de octubre de 2024, el usuario `debian` realizó una serie de acciones administrativas en el sistema, incluyendo la instalación y configuración de servicios (FTP, SSH) y la modificación de permisos en el directorio web.
  2. Se identificaron configuraciones inseguras:
    - Acceso root por SSH habilitado.
    - FTP con acceso anónimo.
    - Permisos 777 en `/var/www/html` y `wp-config.php`.
  3. A las 17:40:59, se registró una conexión SSH como `root` desde la IP `192.168.0.134`, lo que indica que se estableció un mecanismo de acceso remoto con privilegios máximos.
  4. Los escaneos de rootkits (`chkrootkit` y `rkhunter`) no revelaron malware ni rootkits activos.
  5. Todas las configuraciones inseguras han sido corregidas y el sistema se encuentra en un estado más seguro.
- 

## 8. RECOMENDACIONES

1. Establecer una política de contraseñas fuertes para todos los usuarios.
2. Deshabilitar servicios innecesarios (ej. FTP si no es requerido).
3. Implementar autenticación por claves SSH y deshabilitar autenticación por contraseña.
4. Realizar auditorías de seguridad periódicas con herramientas como Lynis.
5. Centralizar los logs en un servidor remoto para evitar su manipulación.
6. Capacitar al personal en buenas prácticas de seguridad y hardening.