**Informe de Incidente de seguridad**

**Reportado por:**

**Germán Alberto Parra Araque**

**4Geeks Academy**

**Colombia**

**2025**

[**1. Introducción 3**](#_bdhyecksw6l6)

[**2. Detalles del incidente 3**](#_viwhpwg701ft)

[**2.1. Fecha y hora del incidente: 3**](#_awm7b3xgwzup)

[**2.2. Fecha y hora de detección: 3**](#_h86w2p730xrk)

[**2.3. Sistema(s) afectado(s): 3**](#_akqo3eftljv4)

[**2.4. Tipo de incidente: 3**](#_iuxk2nronnwr)

[**2.5. Descripción del incidente: 3**](#_bdjr6yu37wdx)

[**2.6. Usuarios o áreas afectadas: 4**](#_b3zqf8uf0mmk)

[**3. Evidencias Recopiladas 4**](#_t3r0xh1ik0hd)

[**3.1. MySQL 4**](#_bsspn82glrsu)

[**3.2. FTP 7**](#_5kcf2zw7vz54)

[**3.3. SSH 9**](#_9e8g0e3qyxk4)

[**3.4. Escaneo de puertos con nmap 9**](#_a88kyxld3ft4)

[**3.5. Archivo de configuración wp-config.php 10**](#_ywxb5fv4fnn1)

[**3.6. Comandos Ejecutados con Privilegios (sudo) 10**](#_g6loqietxdf1)

[**3.7. Archivo de logs 13**](#_p0aziif1jj36)

[**4. Análisis del Incidente 14**](#_350prvitdl3h)

[**4.1. Vector de ataque 14**](#_gcvzdqp3v40i)

[**4.2. Medidas Tomadas 15**](#_a7x20vwm1k1n)

[**4.3. Gestión de usuarios y contraseñas 15**](#_oqhm0z5rr2cq)

[**4.4. Revisión de configuraciones de seguridad. 15**](#_jxt1ysm3qa28)

[**4.5. Parcheo de vulnerabilidades detectadas. 18**](#_o3wkt582yh0e)

[**4.6. Archivo de configuración wp-config.ph 18**](#_w00k2vbuat2q)

[**5. Recomendaciones 18**](#_82acgjmgxdj0)

[**5.1. Endurecimiento del sistema (Hardening) 18**](#_5mj87gco1l9e)

[**5.2. Gestión de usuarios y privilegios 19**](#_usw58cnfye9u)

[**5.3. Capacitación al personal 19**](#_ahsrsy7sjpxw)

[**5.4. Uso de controles de red y aplicación 19**](#_r6o1ed82ky88)

[**5.5. Segmentación de red 19**](#_myvrcalqr28)

[**5.6. Auditoría interna 20**](#_sk5lyyc5b9xu)

[**6. Conclusiones 20**](#_kv315f7v301m)

## **Introducción**

El día 6 de junio de 2025 a las 18:30 horas, se detectó un incidente de seguridad en un servidor con sistema operativo Debian 12, perteneciente a la infraestructura crítica de la empresa **Banco Teusaquillo**. El incidente fue atribuido al grupo hacktivista autodenominado *“Los Cyber Sayayines”*, quienes lograron comprometer el sistema.

La detección del evento se dio tras observar un comportamiento anómalo en el rendimiento del servidor, acompañado de alertas generadas por la plataforma SIEM (Security Information and Event Management). Ante la sospecha de una intrusión, el servidor fue inmediatamente aislado de la red corporativa para contener el posible impacto.

Dada la criticidad del equipo comprometido en las operaciones del banco, se activó el protocolo de respuesta ante incidentes. El servidor fue entregado al equipo de análisis forense y ciberseguridad, el cual inició la investigación para determinar el alcance del ataque, identificar vectores de compromiso y preservar la evidencia digital.

Este informe documenta los hallazgos principales, las evidencias recopiladas durante el análisis, las medidas de contención implementadas, y una serie de recomendaciones para evitar futuros incidentes similares.

## **Detalles del incidente**

### **Fecha y hora del incidente:**

6 de junio del 2025, 17:30 Hora Colombia(GMT-5).

### **Fecha y hora de detección:**

6 de junio del 2025, 18:30 Hora Colombia(GMT-5).

### **Sistema(s) afectado(s):**

Servidor virtualizado Debían 12.

### **Tipo de incidente:**

Acceso no autorizado y cambio de configuraciones en diferentes servicios.

### **Descripción del incidente:**

El sistema SIEM (Security Information and Event Management) generó alertas relacionadas con el acceso remoto al servidor mediante el usuario root vía SSH desde una dirección IP no reconocida por la red corporativa. A partir del análisis inicial, se identificaron modificaciones en los servicios FTP, HTTP y SSH, orientadas a debilitar la seguridad del sistema y facilitar la instalación de una puerta trasera (backdoor) que permitiera el acceso persistente por parte del atacante.

### **Usuarios o áreas afectadas:**

No se evidenciaron movimientos laterales hacia otros equipos dentro de la red empresarial. Sin embargo, existe una alta probabilidad de que información sensible del área de tecnología (encargada de la administración del servidor comprometido) haya sido accedida o infiltrada durante el ataque.

## **Evidencias Recopiladas**

A continuación se muestran las evidencias recopiladas a través del proceso de análisis realizado sobre el servidor virtualizado Debían 12:

### **MySQL**

Se llevó a cabo una validación sobre la base de datos relacional **MySQL**, accediendo al servicio mediante el usuario **root**. Una vez dentro, se consultó la tabla mysql.user con el fin de identificar las cuentas de usuario existentes y verificar posibles accesos no autorizados o modificaciones anómalas en los privilegios asignados.

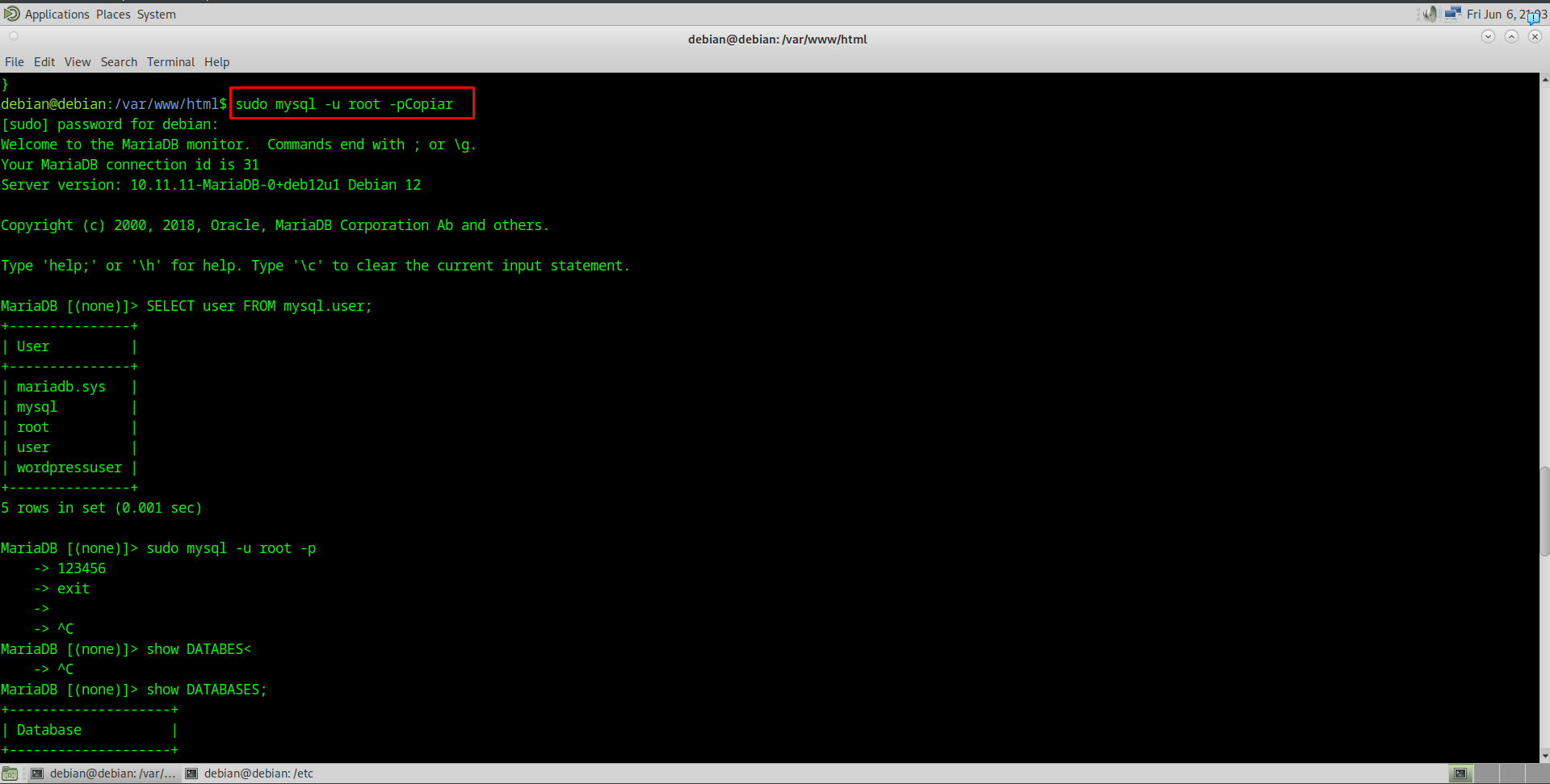


Figura 1. Acceso a MySQL y consulta a tabla de usuarios.

Se accede a la tabla “user” donde se muestran los usuarios:

* root
* user
* wordpressuser



Figura 2. Acceso a tabla “user” de base de datos “mysql”.

Se encuentran los siguientes hashes de contraseña :

* “root” y “wordpressuser”:

\*6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9

* “user”:

\*2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19

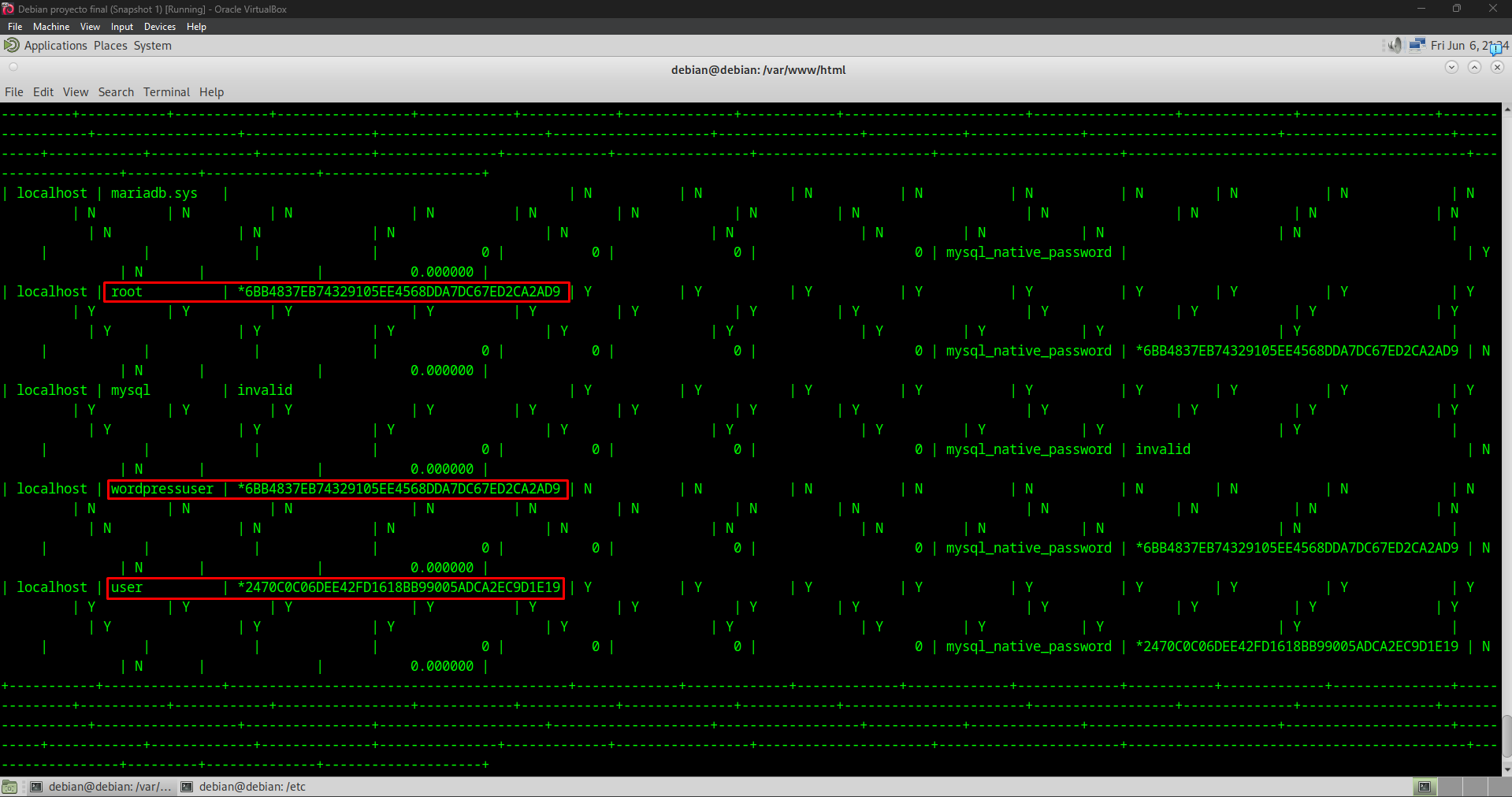


Figura 3. Usuarios con sus respectivos hashes de contraseña.

Se utilizó la plataforma **hashes.com** para realizar el descifrado de hashes encontrados en la base de datos. En este caso, se trataba de hashes en formato **MySQL (double SHA1 hashing)**, lo cual dificulta el uso efectivo de herramientas tradicionales como **John the Ripper** o **Hashcat**, debido a la falta de soporte directo para este tipo específico de hash o a la necesidad de configuraciones avanzadas. La herramienta web permitió identificar contraseñas en texto plano asociadas a usuarios del sistema.

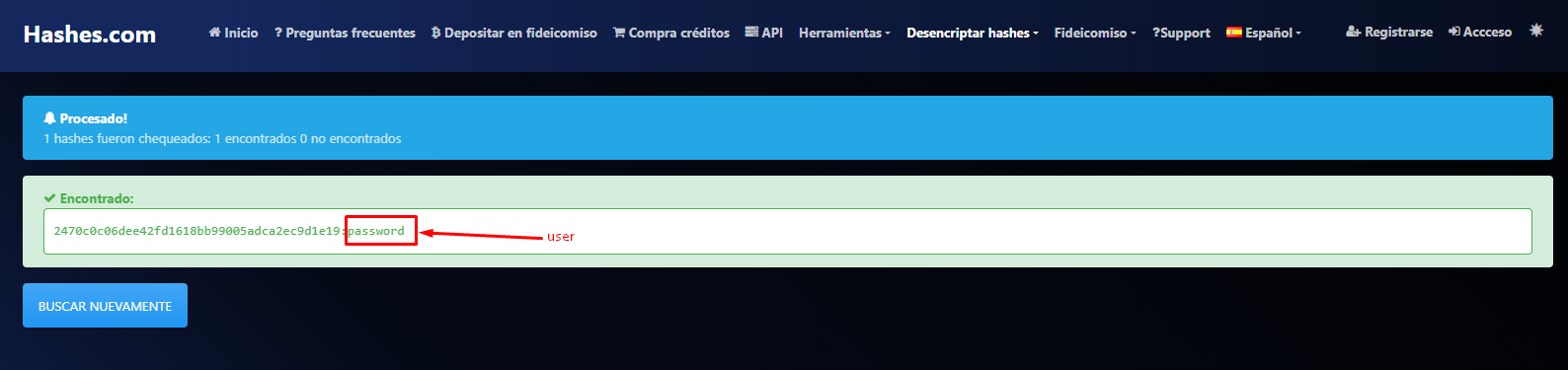


Figura 4. Contraseña “user”.

Se identifica que la contraseña del usuario “user” es “password” y la contraseña de los usuarios “root” y “wordpressuser”

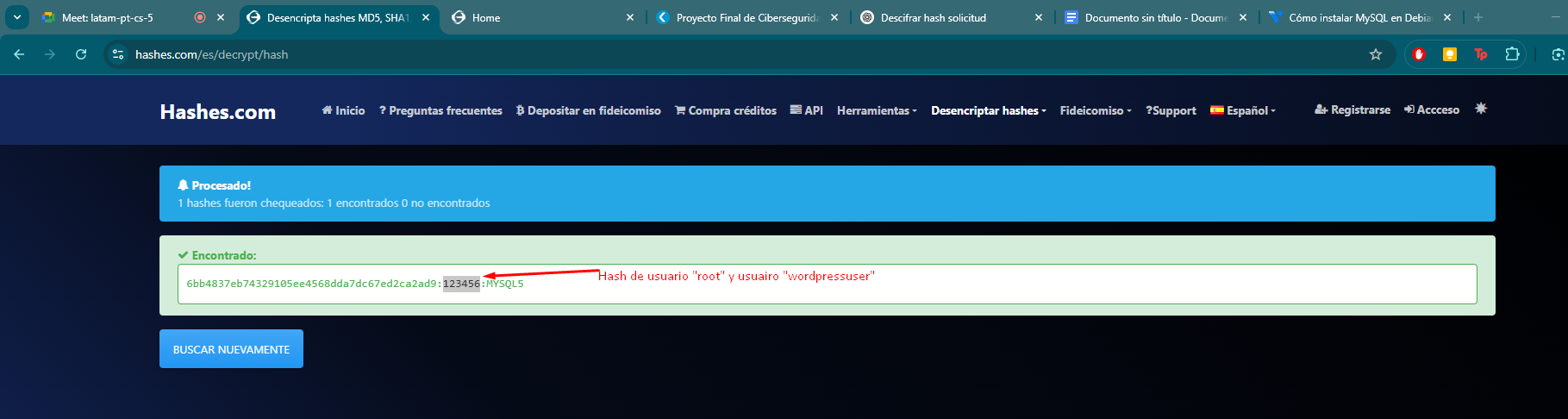


Figura 5. Contraseña “root” y “wordpressuser”.

Se identificó que el sistema utiliza **MariaDB versión 10.1.x** como motor de base de datos. Esta versión es un **fork de MySQL 5.6**, por lo que hereda gran parte de su arquitectura interna, incluyendo el sistema de autenticación predeterminado utilizado en MySQL 5.x.

Este tipo de configuración puede implicar ciertas limitaciones en términos de seguridad, especialmente si no se han aplicado políticas de endurecimiento, como el uso de autenticación reforzada, cifrado de contraseñas o revisión de privilegios asignados a los usuarios.

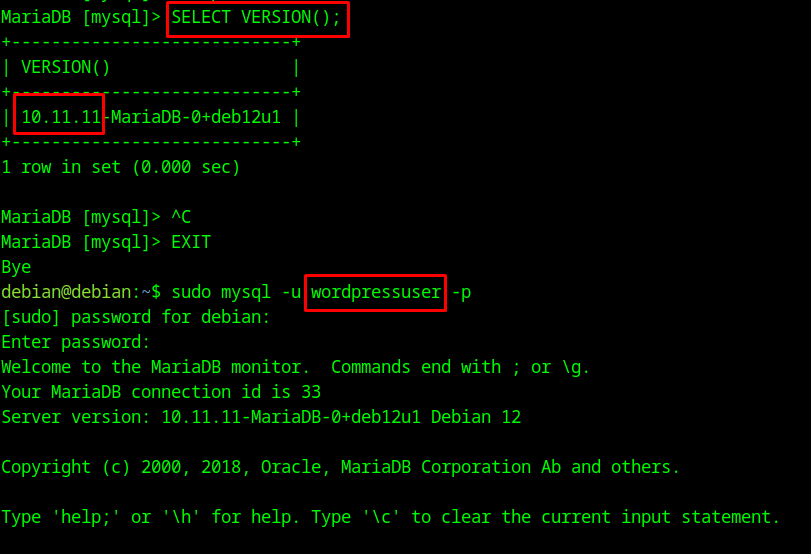


Figura 6. Versión MariaDB.

Se procede a validar el acceso mediante el usuario “user”, se usan las credenciales previamente identificadas.

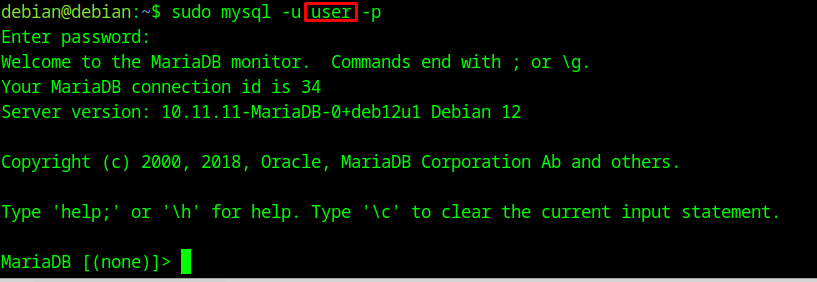


Figura 7. Acceso usuario “user”

Se verifican permisos para usuarios “user” y “wordpressuser”

Comando SHOW GRANTS FOR 'user'@'localhost';

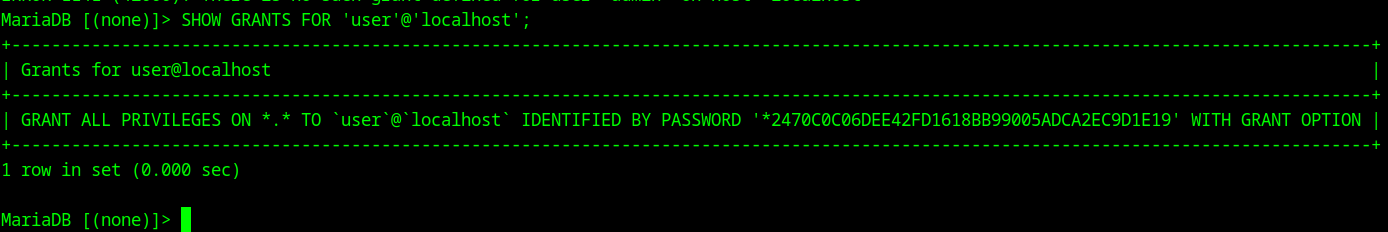


Figura 8. Permisos usuario “user”.

Comando SHOW GRANTS FOR 'wordpressuser'@'localhost';

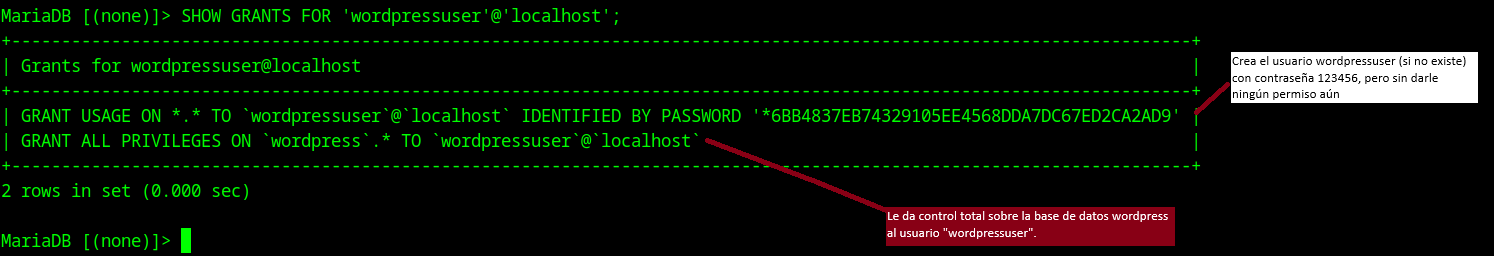


Figura 9. Permisos usuario “wordpressuser”.

### **FTP**

Se verificó que el **servicio FTP** se encuentra activo y en estado de **escucha** en el puerto **21/TCP**, utilizando el servicio **vsftpd**. Esto se evidenció mediante la ejecución del comando:



Figura 10. Validación FTP

El resultado muestra que el servicio está escuchando en todas las interfaces IPv6 (:::21), lo que podría representar un riesgo adicional si no se aplican controles de acceso adecuados.

Se evidencia que el software que se usa es “vsftpd” un servidor de FTP software libre popular en sistemas Linux. Por lo cual se verifica el estado actual del servicio con el siguiente comando

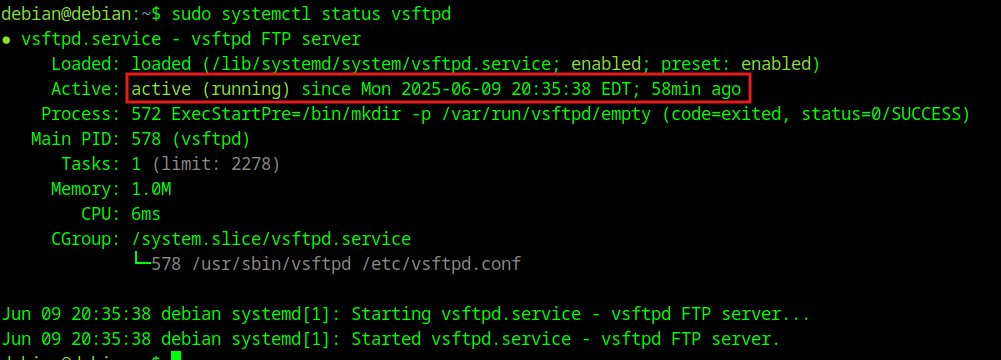


Figura 11. Validación estado servidor vsftpd.

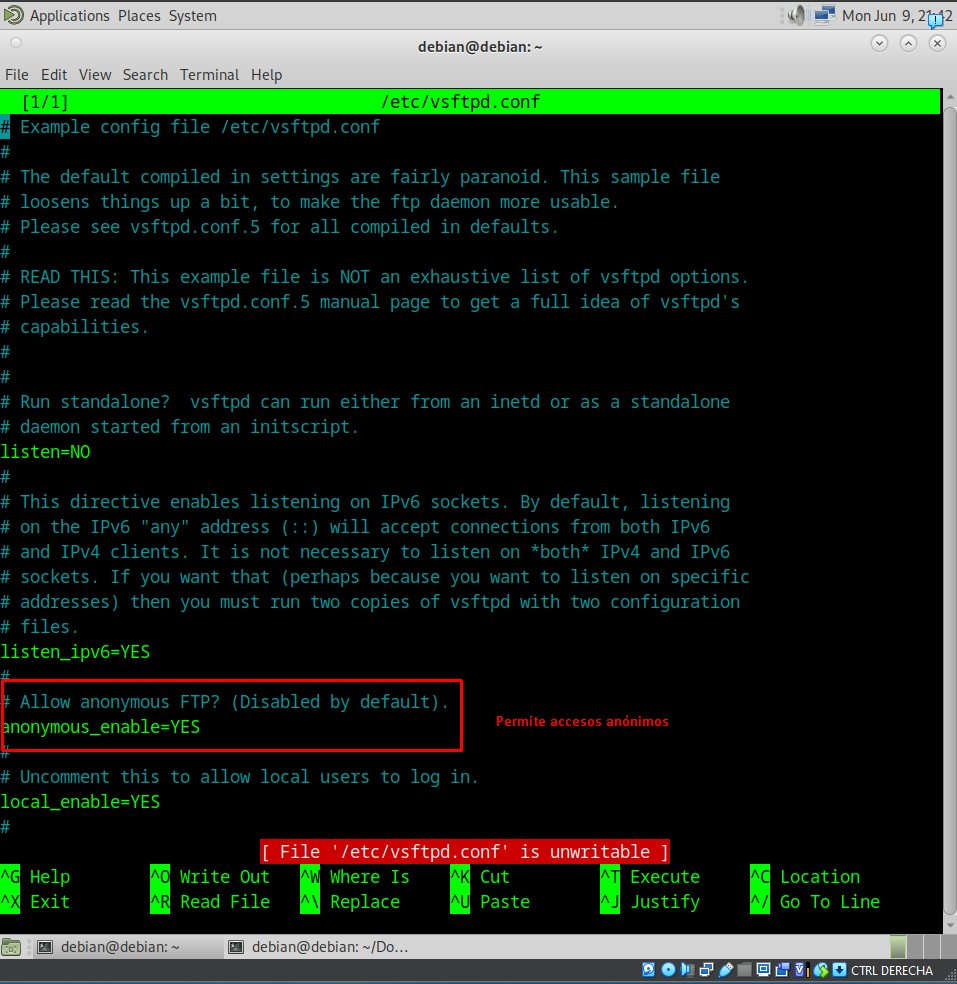
Se procede a verificar el archivo de configuración del servicio vsftpd el cual es “/etc/vsftpd.conf”. Se encuentra una configuración establecida que no es recomendable, la cual permite conexiones anónimas al servicio FTP.

Figura 12. Archivo de configuración FTP.

### **SSH**

Se accede al archivo /etc/ssh/sshd\_config donde se encuentran las configuraciones del servidor ssh.

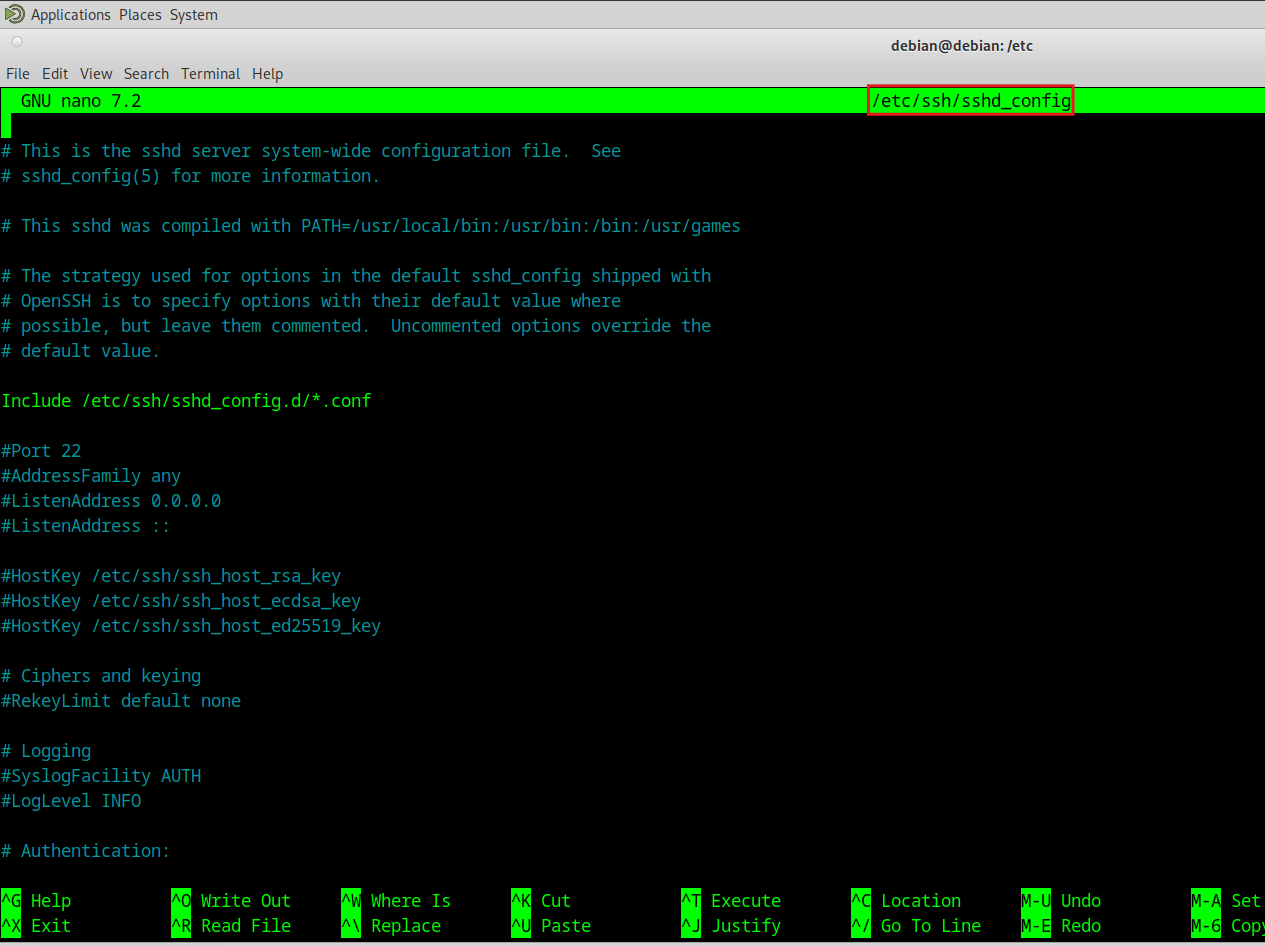


Figura 13.Archivo de configuración sshd\_config.

### **Escaneo de puertos con nmap**

Se utiliza nmap para hacer un escaneo activo sobre la máquina Debian 12. El comando busca escanear los puertos del 1 al 65535.

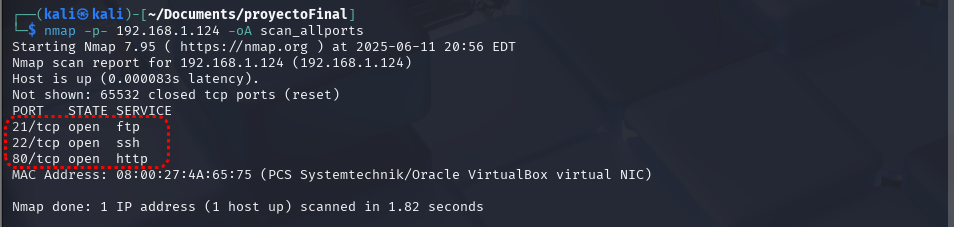


Figura 14. Escaneo de todos los puertos posibles.

Se identifican 3 puertos abiertos con los servicios:

* FTP
* SSH
* HTTP

y se ejecuta el siguiente comando

nmap -p 21,22,80 192.168.1.124 -sV -sC -oA scan\_services

* **-p-**:Se limita escaneo a puertos 21, 22 y 80.
* **-sV:**Se identifican versiones de los servicios que corren en esos puertos.
* **-sC:** Ejecuta el conjunto de scripts NSE “default”, ayudando a
* **-oA scan\_services** : Guarda los resultados en tres formatos (.nmap, .xml, .gnmap) con el prefijo scan\_services.

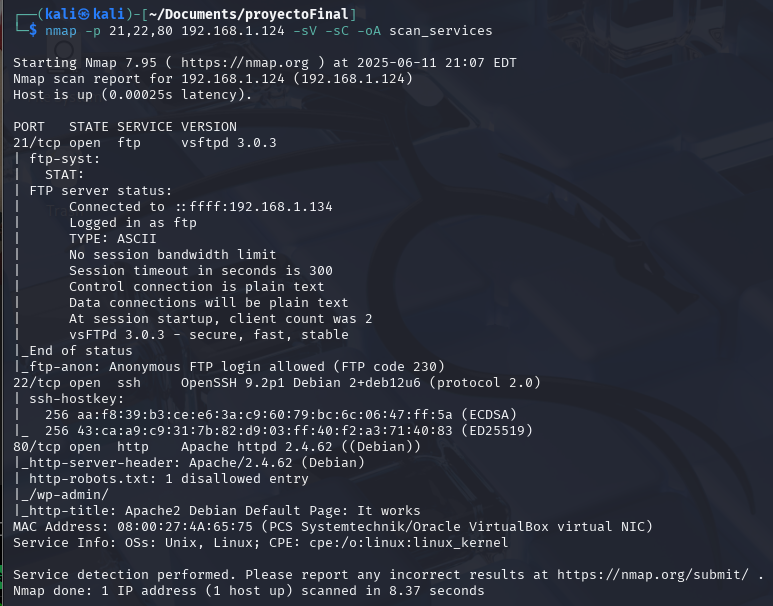


Figura 15. Escaneo puertos 21,22 y 80.

### **Archivo de configuración wp-config.php**

Se identificó que el archivo de configuración principal de WordPress (wp-config.php) tiene permisos **inseguros** (777), permitiendo lectura, escritura y ejecución a cualquier usuario del sistema. Esto representa una **vulnerabilidad crítica**, ya que expone información sensible como las credenciales de base de datos y claves secretas.



Figura 16. Permisos archivo wp-config.php.

### **Comandos Ejecutados con Privilegios (sudo)**

Para identificar actividades sospechosas realizadas con privilegios elevados, se utilizó el siguiente comando:

journalctl | grep "sudo" | grep "COMMAND"

Este comando realiza una búsqueda en los registros del sistema administrados por journalctl, filtrando específicamente:

* Entradas relacionadas con el uso de sudo (es decir, ejecuciones de comandos con privilegios administrativos).
* Líneas que contienen la palabra **"COMMAND"**, lo cual indica el comando exacto que fue ejecutado por el usuario con permisos elevados.

Este procedimiento permite rastrear las acciones que requieren privilegios administrativos, facilitando la detección de posibles movimientos del atacante, como la instalación de software malicioso, cambios en configuraciones del sistema o creación de cuentas privilegiadas.

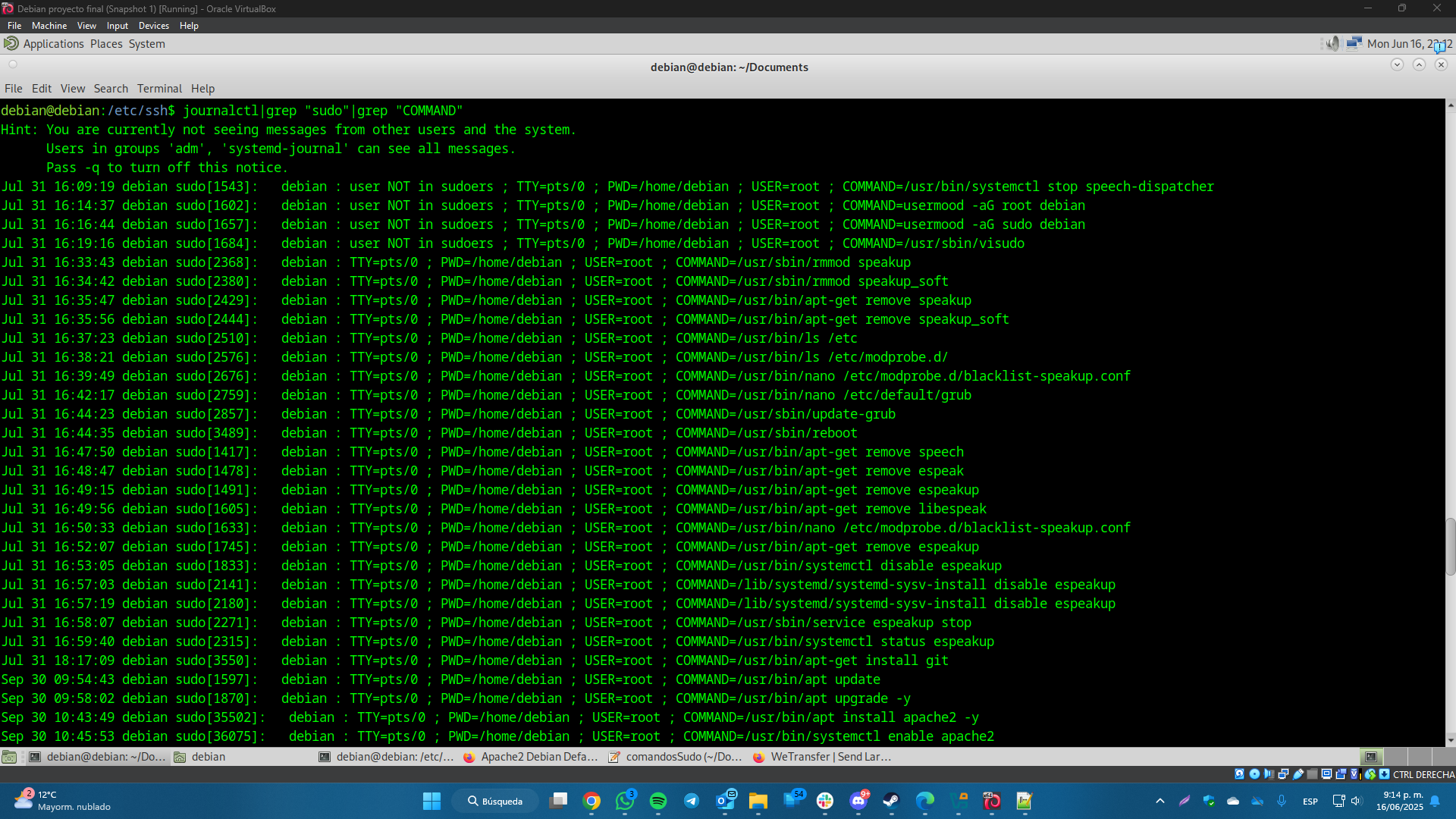


Figura 17. Comandos usados con “sudo”.

**Escalada de privilegios y modificación de sudoers:**

* usermood -aG root debian
* usermood -aG sudo debian
* visudo

**Gestión de servicios y módulos del sistema:**

* systemctl stop speech-dispatcher
* rmmod speakup
* rmmod speakup\_soft
* update-grub
* systemctl reboot
* systemctl restart apache2
* systemctl restart vsftpd
* systemctl restart ssh
* systemctl restart networking

**Edición de archivos críticos:**

* nano /etc/modprobe.d/blacklist-speakup.conf
* nano /etc/default/grub
* nano /etc/apache2/apache2.conf
* nano /etc/apache2/sites-available/000-default.conf
* nano /etc/ssh/sshd\_config
* nano wp-config.php

**Instalación y configuración de servicios:**

* apt install apache2
* apt install mysql-server php php-mysqli
* apt install mariadb-server
* apt install vsftpd
* apt install openssh-server
* systemctl enable apache2
* systemctl start apache2
* systemctl start mariadb
* systemctl enable mariadb
* mysql\_secure\_installation

**Manipulación de archivos web:**

* cp -a /tmp/wordpress/. /var/www/html/
* chown -R www-data:www-data /var/www/html/
* chmod -R 755 /var/www/html/
* chmod -R 777 /var/www/html
* chmod 777 /var/www/html/wp-config.php
* mv wp-config-sample.php wp-config.php

**Comandos de red y monitoreo:**

* netstat -tuln
* netstat -tulpn
* ip a

**Acceso a bases de datos:**

* mysql -u root -p
* mysql -u wordpressuser -p
* mysql -u user -p

**Otras utilidades:**

* apt-get remove speakup
* apt-get remove espeakup
* apt-get remove libespeak
* apt-get install build-essential
* apt-get install linux-headers-6.1.0-25-amd64 dkms
* apt-get install module-assistant
* sh ./VBoxLinuxAdditions.run

### **Archivo de logs**

Se evidencia que el archivo auth.log no se encuentra dentro del directorio esperado

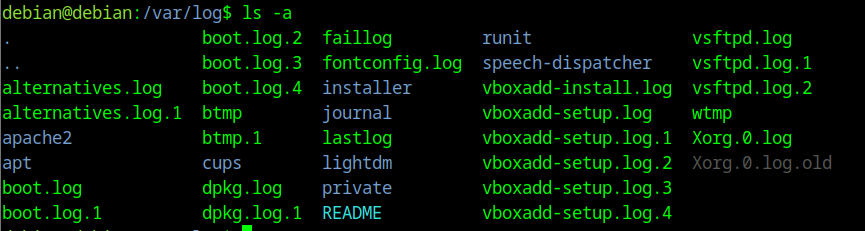


Figura 18. Contenido directorio /var/log.

Se utilizó el siguiente comando para buscarlo de manera recursiva en el sistema de archivos:

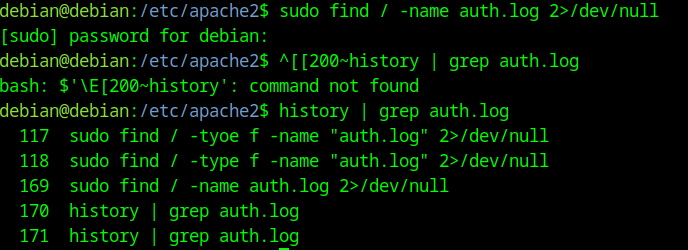


Figura 19. Búsqueda auth.log sin resultados

No se encontró el archivo de registros **auth.log**, el cual normalmente almacena eventos relacionados con la seguridad del sistema. Este archivo es clave para observar:

* Conexiones SSH exitosas y fallidas
* Cambios de sesión
* Uso de privilegios mediante sudo
* Intentos de acceso por usuarios no válidos

## **Análisis del Incidente**

El ataque fue realizado de manera remota, de acuerdo a que el servidor con sistema Debian 12, está recluido en un datacenter con seguridad física, se verificaron registros de video y seguridad y nadie estaba en esa sala en ese momento. Por lo cual es posible que se interactuara con el servidor dentro de la red empresarial o de manera remota.

### **Vector de ataque**

El vector de ataque más probable en este incidente fue el **acceso remoto a través del servicio SSH**, aprovechando una de las siguientes condiciones:

* **Credenciales débiles o comprometidas**:  
   El atacante pudo haber realizado un ataque de fuerza bruta o haber obtenido credenciales válidas del usuario root o de otro usuario con privilegios sudo.
* **Servicio SSH expuesto a internet sin restricciones**:  
   Se identificó que el servicio SSH estaba activo y escuchando en todas las interfaces, lo que indica que el servidor era accesible desde redes externas.
* **Configuraciones inseguras en servicios**:  
   El servicio FTP permitía acceso y escritura, y no se encontraron controles como chroot\_local\_user. Esto pudo ser explotado para subir scripts o herramientas maliciosas.

Se muestra los posibles daños realizados por el atacante

* **Modificación permisos /var/www/html y archivo wp-config.php** :  
  Se procedió a dar acceso de permisos totales al directorio “html” con todos sus repositorios de manera recursiva y al archivo “wp-config.php”, permitiendo que cualquier usuario del sistema pueda ejercer cambios sobre los mismos.
* **Creación usuario en MySQL:** También realizó configuraciones sobre MySQL donde se hizo la creación del usuario “user” con todos los permisos habilitados.
* Posibles modificaciones a servicios FTP, SSH y HTTP.
* **Eliminación de logs (auth.log)**:  
   Se detectó la ausencia del archivo auth.log, lo que sugiere una acción deliberada para eliminar evidencia y dificultar la trazabilidad del ataque.
* **Instalación de software y modificación del sistema**:  
   Una vez dentro del sistema, el atacante utilizó privilegios elevados (sudo) para modificar servicios como Apache, MariaDB y vsftpd, posiblemente con el fin de establecer persistencia y crear un entorno de servidor web comprometido.

### 

### **Medidas Tomadas**

Dentro del Banco Teusaquillo, el **primer mecanismo de contención** implementado fue la **desconexión inmediata del servidor afectado de la red empresarial**, con el fin de evitar la propagación del incidente y preservar la integridad de la información.

Una vez aislado el equipo, el **equipo de Ciberseguridad** procedió a ejecutar el protocolo establecido para realizar las **validaciones correspondientes al análisis post-mortem**. Dicho análisis constituye la base del presente informe, en el cual se documentan los hallazgos técnicos, las causas del incidente y las recomendaciones para mitigar futuras amenazas**.**

### **Gestión de usuarios y contraseñas**

Se realiza cambio de contraseña usuario “root” y se solicita cambio de contraseña para los usuarios que existen dentro del sistema.

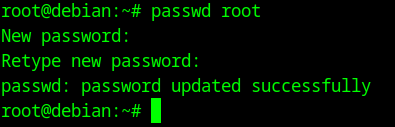


Figura 20. Cambio de contraseña de usuario root.

Asimismo, se audita la base de datos “MySQL”, eliminando el usuario “user” y cambiando las contraseñas de los usuarios “root” y “wordpressuser”.

### **Revisión de configuraciones de seguridad.**

Se hace revisión de los siguientes servicios:

* FTP: El servicio FTP se utiliza para la transferencia de archivos. Se analiza el archivo de configuración (por ejemplo, /etc/vsftpd.conf).

| **Opción** | **Significado** | **Estado en la máquina** | **Sugerencia** |
| --- | --- | --- | --- |
| anonymous\_enable=NO | No permite acceso anónimo (recomendado). | anonymous\_enable=YES | Deshabilitar acceso de manera anónima |
| local\_enable=YES | Permite a los usuarios del sistema iniciar sesión. | local\_enable=YES | Puede estar habilitado si los usuarios que tienen acceso están monitoreados y tienen contraseñas seguras |
| write\_enable=YES | Permite subir o modificar archivos. | write\_enable=YES | Asegurarse que solo usuarios autorizados tengan acceso. Activar “userlist\_enable” |
| chroot\_local\_user=YES | Encierra a los usuarios en su directorio personal (recomendado por seguridad). | No se encontró configuración | Se sugiere habilitar para que los usuarios solo naveguen en su propio directorio. |
| userlist\_enable=YES | Habilita el uso de una lista de control de acceso para usuarios. | No se encontró configuración | Se sugiere configurar y solo permitir usuarios con el privilegio necesario. |
| userlist\_file=/etc/vsftpd.user\_list | Ruta del archivo con los usuarios definidos. | No se encontró configuración | Es la ruta donde está la lista de usuarios con permiso para acceder a FTP. El archivo no debe ser editado por cualquier usuario del sistema. |
| userlist\_deny=NO | Si está en NO, solo los usuarios de la lista pueden acceder. | No se encontró configuración | Dejarlo como está. |
| listen=YES | Habilita la escucha en IPv4. | listen=NO | Validar si es necesaria la conexión a través de ipv4. |
| listen\_ipv6=YES | Habilita la escucha en IPv6. | listen\_ipv6=YES | Validar si es necesaria la conexión a través de ipv6. |
| local\_umask=022 | Define los permisos por defecto para archivos subidos. | No se encontró configuración | Establecer permisos de archivos subidos (644) y para directorios (755) |

Figura 21. Recomendaciones archivo configuración vsftpd.conf.

* SSH: El servicio SSH es utilizado para la administración remota del servidor. Se verifica el archivo de configuración ubicado en /etc/ssh/sshd\_config y se presentan sugerencias que se deben tener en cuenta con el equipo de tecnología.

| **Opción** | **Significado** | **Estado en la máquina** | **Sugerencia** |
| --- | --- | --- | --- |
| PasswordAuthentication | Se usa para habilitar o desactivar el acceso por contraseña | Activo | Deshabilitar y autenticarse por llaves públicas |
| AuthenticationMethods | Permite combinación de métodos de autenticación | No está configurado | Escoger autenticación por llaves públicas |
| PermitRootLogin | Permite acceder mediante al usuario root en una sesión ssh | Está activo | Desactivar de acuerdo a que el primer usuario que se trata de vulnerar es el root, se evitan ataques por fuerza bruta |
| MaxAuthTries | Limita los intentos de autenticación | No está configurado | Se recomienda establecer un valor menor a 4. |
| LoginGraceTime | Limita en segundos el tiempo para establecer la conexión ssh | No está configurado | Se recomienda establecer un plazo de 30 segundos para establecer la conexión |
| AllowUsers | Limita el acceso SSH a usuarios definidos en una lista de acceso | No está configurado | Se recomienda establecer un lista acceso con usuarios |
| Port | Permite escoger en qué puerto se va a prestar el servicio. | No está configurado, queda en el 22 por defecto. | Se recomienda validar con el equipo de tecnología para validar otro puerto, que no sea común |

Figura 22. Recomendaciones archivo configuración ssh\_config.

### **Parcheo de vulnerabilidades detectadas.**

Para asegurar el correcto funcionamiento del sistema Debian, se procede a actualizar e instalar la lista de paquete del sistema, con los siguientes comandos en el orden entregado

* sudo apt-get update
* sudo apt-get upgrade

Se realizó un análisis de las versiones de los servicios expuestos en la máquina Debian con dirección IP 192.168.1.124 a traves de nmap, siendo estos los resultados:

* FTP: Se está usando una versión segura rápida y estable, la versión vsftpd 3.0.3. Se encuentra que se pueden hacer conexiones anónimas, lo cual permite que cualquiera se pueda conectar sin credenciales.
* SSH: La versión es relativamente reciente y carece de vulnerabilidades conocidas. Se muestran huellas de las claves con algoritmos ECDSA y ED25519 (llaves públicas).
* HTTP: Evidencia que no se ha desplegado el sitio web, se encuentra un directorio ”wp\_admin” identificando que hay o hubo un servidor wordpress” y se revela información de la versión Apache.

### 

### **Archivo de configuración wp-config.ph**

Se recomienda aplicar el principio de **mínimo privilegio**, de modo que **solo el usuario root tenga permisos de lectura y escritura**, y que el grupo del servidor web (www-data) tenga únicamente permisos de lectura. Los demás usuarios del sistema no deben tener ningún tipo de acceso al archivo.

## **Recomendaciones**

Con base en los hallazgos obtenidos durante el análisis forense, se proponen las siguientes recomendaciones para mejorar la postura de seguridad del servidor y de la red empresarial del Banco Teusaquillo:

### **Endurecimiento del sistema (Hardening)**

Es prioritario aplicar un proceso de hardening al servidor Debian, dado que muchas de las configuraciones actuales no fueron diseñadas para restringir adecuadamente los accesos remotos. Esto incluye:

* Deshabilitar servicios innecesarios.
* Restringir accesos SSH mediante autenticación por claves y reglas de firewall.
* Fortalecer la configuración de servicios como FTP, SSH y Apache.
* Optar por servicios más seguros como SFTP y HTTPS.
* Si es necesario publicar la página web, es necesario sustituir la página por defecto por un aplicativo web y toca revisar el uso de wordpress

### **Gestión de usuarios y privilegios**

Se debe establecer un plan de mantenimiento y auditoría continua sobre las cuentas de usuario con acceso al servidor. Es fundamental aplicar el principio de menor privilegio, garantizando que cada usuario posea únicamente los permisos necesarios para su función.

### **Capacitación al personal**

Los empleados deben ser considerados la primera línea de defensa. Por ello, se recomienda implementar planes de formación continua en ciberseguridad, orientados a todas las áreas corporativas. Estas capacitaciones deben incluir:

* Reconocimiento de correos de phishing.
* Manejo seguro de contraseñas.
* Reporte de actividades sospechosas.

### **Uso de controles de red y aplicación**

Para mitigar futuros riesgos:

* Implementar un Web Application Firewall (WAF) que proteja las aplicaciones web frente a ataques como XSS, inyecciones y escaneos automatizados.
* Configurar un firewall perimetral y local con políticas estrictas de acceso.

### **Segmentación de red**

Es crucial implementar una segmentación lógica de la red empresarial, de manera que las áreas corporativas del Banco Teusaquillo se encuentren separadas. Solo el área de Tecnología debe tener acceso directo a servidores y recursos críticos, reduciendo así la superficie de ataque.

### **Auditoría interna**

Se recomienda llevar a cabo una auditoría técnica interna, con participación del equipo de tecnología del banco, con el fin de:

* Validar configuraciones actuales.
* Evaluar el cumplimiento de políticas de seguridad.  
  Detectar vulnerabilidades o malas prácticas operativas.
* Monitorear actividades de usuarios privilegiados
* Auditar detalladamente los servicios alojados dentro de la máquina Debian

## **Conclusiones**

El incidente de seguridad ocurrido en el Banco Teusaquillo representó una afectación directa en términos de tiempo, recursos humanos y financieros, los cuales no se encontraban contemplados dentro del presupuesto ni de la planificación operativa establecida. El sistema comprometido logró ser asegurado y aislado exitosamente el día viernes 13 de junio de 2025, tras la activación del plan de respuesta ante incidentes por parte del equipo de ciberseguridad.

Este evento evidencia la necesidad de fortalecer la preparación institucional ante posibles amenazas de seguridad de la información. Es imperativo establecer procesos proactivos de gestión del riesgo, acompañados por planes de contingencia, simulacros, y auditorías periódicas.

Asimismo, se recomienda que la organización adopte un enfoque alineado con los principios de la norma ISO/IEC 27001, la cual proporciona un marco adecuado para implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI), permitiendo una mejor preparación frente a futuras amenazas y vulnerabilidades.

El incidente de seguridad terminó siendo contenido, es primordial seguir las recomendaciones otorgadas.