INFORME Y ANÁLISIS FORENSE

-Servidor clave de una empresa de informatica (invento)

- Objetivo atacado: Servidor Clave de la empresa de informatica (192.168.1.153)
- Incidente: Irrupción en el servidor, cambio de privilegios y eliminación de logs.
- Agente: Aaron Jorge Climent
- Fecha: 10 enero 2026

ÍNDICE

1. Introducción

Este informe técnico describe las actividades realizadas en el análisis forense, las acciones de contención y las medidas de recuperación en un activo crítico de la infraestructura tecnológica de una empresa de informática. El servidor identificado como clave, fue comprometido, comprometiendo la confidencialidad de los datos y la disponibilidad de servicios administrativos.

El principal objetivo de esta intervención fue:

1. Determinar el vector de intrusión: cómo el atacante logró vulnerar la seguridad del hospital.
2. Contener y erradicar los accesos no autorizados, asegurando la integridad de la red sanitaria.
3. Restaurar la operatividad del sistema con medidas de endurecimiento que cumplan con los estándares del SGSI.

Se documentan las evidencias técnicas, acciones correctivas y el estado final del sistema.

2. Identificación del servidor

2.1. Metodología de Acceso y Autenticación

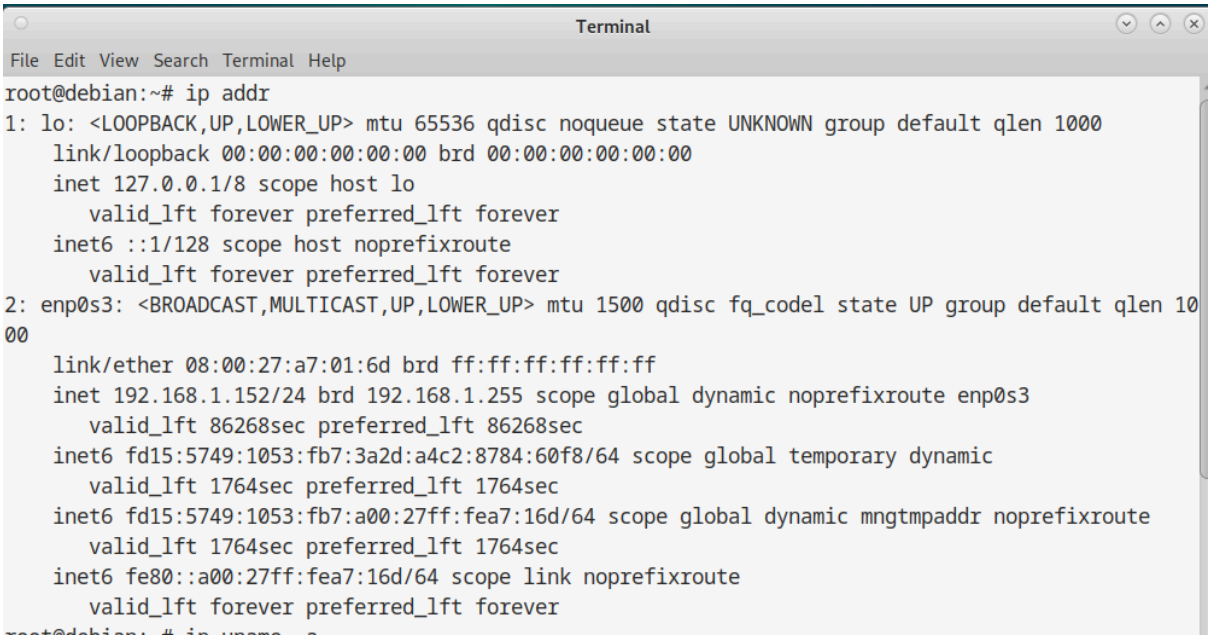
Se inició el proceso mediante acceso físico o consola del activo. Dado que no hubo credenciales proporcionadas por la administración, se empleó una auditoría de caja gris realizando pruebas con diccionarios de credenciales comunes.

Se logró ingresar con éxito en la consola del sistema usando el usuario “Debian” y la contraseña “123456”. Este hallazgo revela una política de contraseñas débil y predecible.

2.2 Información del sistema

Tras obtener acceso, se identificó el sistema operativo y la dirección IP mediante comandos nativos:
-Comando: ***ip addr***

Resultado:



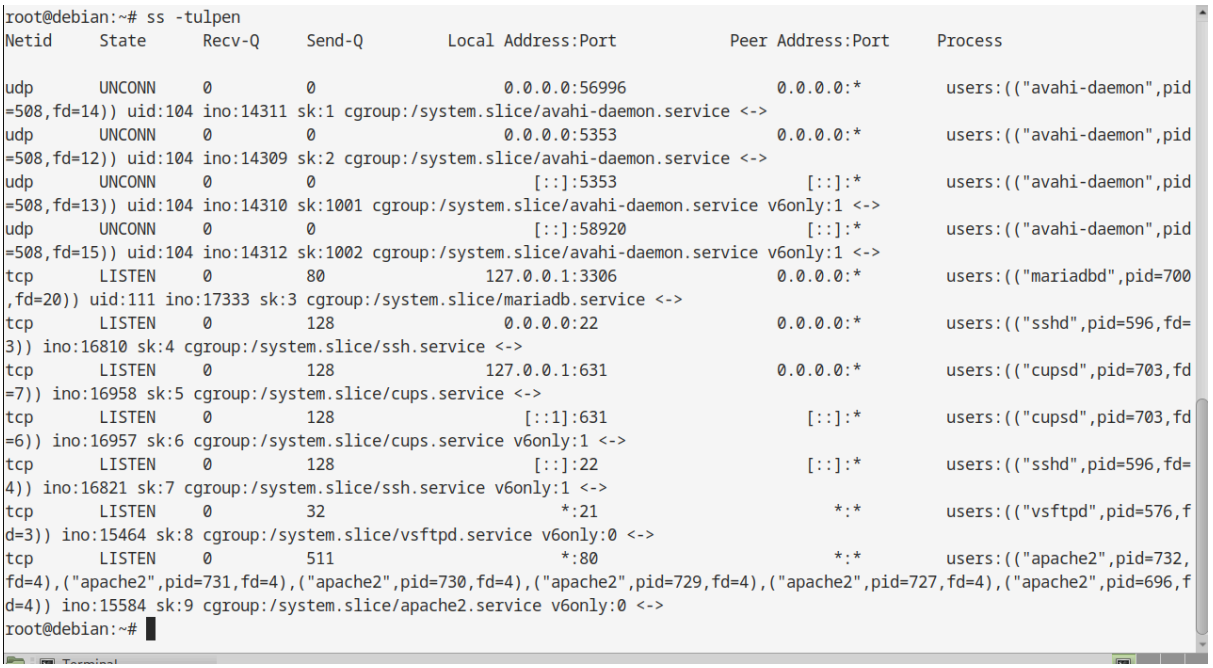
-IP: 192.168.1.152

2.3 Información de puertos

Se realizó un recorrido de puertos abiertos para identificar servicios expuestos:

-Comando: ***ss -tulpen***

Resultado:



-Puertos importantes detectados:

-Puerto 21 (vsftpd): Puerto en escucha expuesto publicamente → **CRITICO**

-Puerto 80 (apache2): Servidor web accesible de forma publica → **CRITICO**

-Puerto 22 (sshd): Permite el acceso remoto al servidor → **CRITICO**

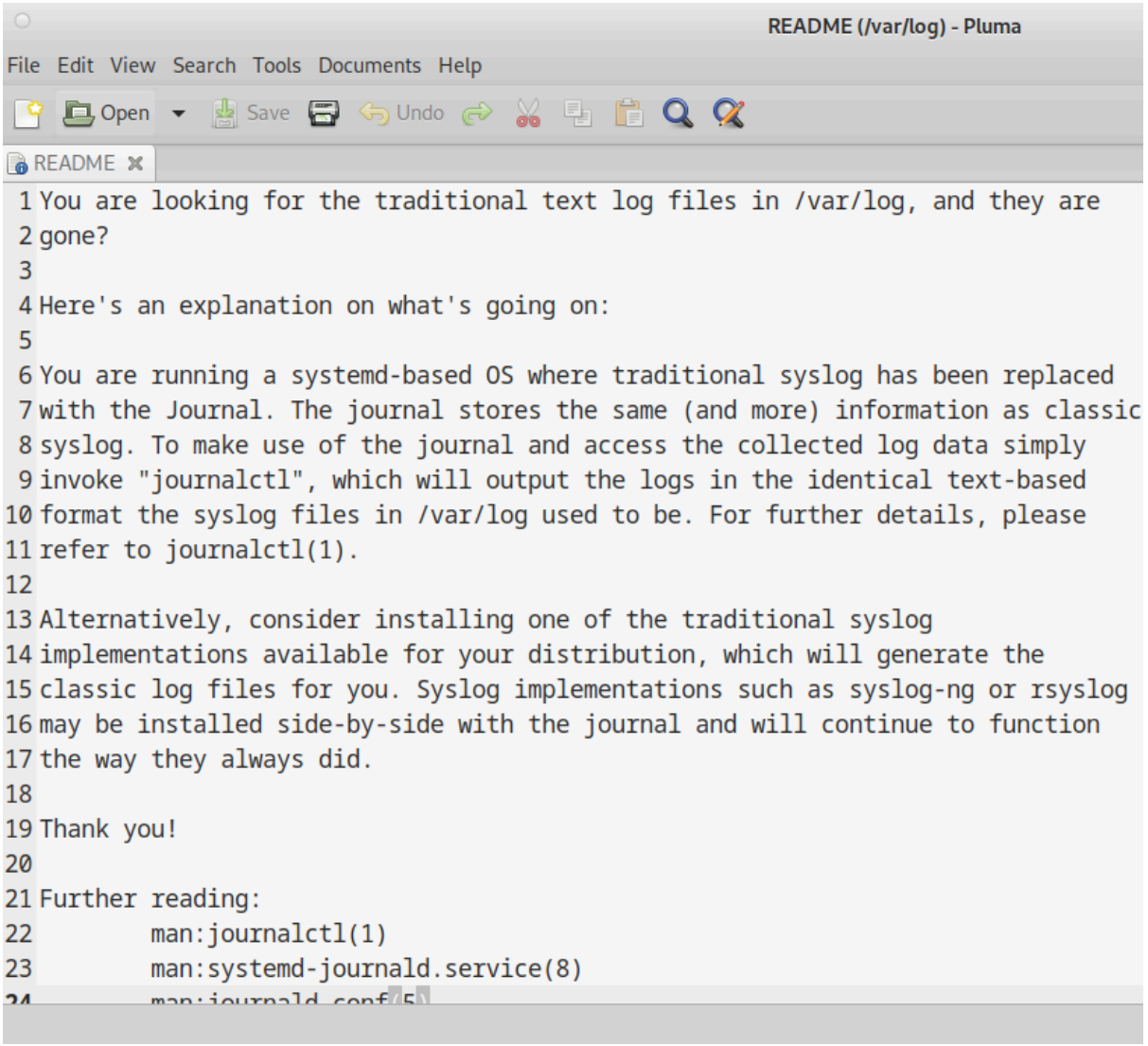
3. Analisis Forense

3.1 Incidente con los logs

Se verificó que los archivos `/var/log/auth.log` y `/var/log/syslog` estaban ausentes, no por técnicas antiforense sino por la estructura de log del sistema basada en systemd-journald. Los registros se almacenan en formato binario, requiriendo "`journalctl`" para su consulta.

-Comando: ***cat /var/log/README***

Resultado:



3.2 Lectura de Logs

Como paso extra, para no tener que usar el comando “journalctl” para leer los logs o analizarlos cada vez que se necesite, lo que hice fue pasarlos a un documento .txt con el siguiente comando.

-Comando: journalctl > /var/log/logs.txt

Resultado:

```
root@debian:~# journalctl > /var/log/logs.txt
root@debian:~#
```

-Ahora los logs del sistema que estaban administrados hasta la fecha en el journal se copiaron al txt para su revisión.

3.3 Analisis de los Logs

Se analizó el acceso SSH para detectar acciones sospechosas o intrusiones, con el comando:

-Comando: grep -i “accepted” /var/log/logs.txt

Resultado

```
root@debian:~# grep -i "accepted" /var/log/logs.txt
Oct 08 17:40:59 debian sshd[1650]: Accepted password for root from 192.168.0.134 port 45623 ssh2
```

-Se identificó un acceso exitoso el 8 de octubre de 2024 a las 17:40:59, desde IP 192.168.0.134, con el usuario root.
La ausencia de intentos fallidos indica que la credencial probablemente ya era conocida o comprometida anteriormente.

4. Analisis del sistema

El análisis del historial del usuario root reveló actividades posteriores al compromiso:

- Uso de visudo para manipular privilegios.
- Detención y deshabilitación del servicio speech-dispatcher.
- Mapeo de servicios con systemctl.
- Archivo /root/.bash_history: evidencia de estas acciones.

```
root@debian:~# cat /root/.bash_history
sudo visudo
sudo systemctl stop speech-dispatcher
sudo systemctl disable speech-dispatcher
systemctl list-units --type=service
```

4.1 Permisos Inseguros en Web

Se detectó que la carpeta raíz del servidor web (/var/www/html) tenía permisos peligrosos: 777. Esto permitía la lectura y modificación de archivos sensibles, incluyendo wp-config.php.

```
root@debian:~# ls -l /var/www/html
total 252
-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 Jan  9 12:45 license.txt
-rwxrwxrwx  1 www-data www-data  7425 Jan  9 12:45 readme.html
-rwxrwxrwx  1 www-data www-data  7349 Jan  9 12:45 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  3339 Jan  9 12:45 wp-config-sample.php
drwxrwxrwx  6 www-data www-data  4096 Jan  9 12:45 wp-content
-rwxrwxrwx  1 www-data www-data  5617 Jan  9 12:45 wp-cron.php
drwxrwxrwx 31 www-data www-data 16384 Jan  9 12:45 wp-includes
-rwxrwxrwx  1 www-data www-data  2493 Jan  9 12:45 wp-links-opml.php
-rwxrwxrwx  1 www-data www-data  3937 Mar 11  2024 wp-load.php
-rwxrwxrwx  1 www-data www-data 51437 Jan  9 12:45 wp-login.php
-rwxrwxrwx  1 www-data www-data  8727 Jan  9 12:45 wp-mail.php
-rwxrwxrwx  1 www-data www-data 31055 Jan  9 12:45 wp-settings.php
-rwxrwxrwx  1 www-data www-data 34516 Jan  9 12:45 wp-signup.php
-rwxrwxrwx  1 www-data www-data  5214 Jan  9 12:45 wp-trackback.php
-rwxrwxrwx  1 www-data www-data  3205 Jan  9 12:45 xmlrpc.php
root@debian:~#
```

4.2 Claves predeterminadas

El archivo wp-config.php fue revisado y contenía credenciales débiles (DB_PASSWORD: '123456'). Como los permisos permitían la lectura mundial, el atacante pudo acceder a la base de datos y comprometer datos sensibles.

```
 * @package WordPress
 */

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

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

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

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

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

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

4.3 Configuración SSH Insegura
Se detectó que la configuración permitía el acceso directo con root:

-Comando: sshd -T | grep -i permitrootlogin

Resultado:

```
root@debian:/# sshd -T | grep -i permitrootlogin
permitrootlogin yes
```

-La configuración “PermitRootLogin” estaba en “yes”. Esto habilita los ataques de fuerza bruta y permite total acceso.

5. Contención y mitigación
Tras verificar las alteraciones, se implementaron las siguientes medidas:

5.1 Fortalecimiento del SSH
Se modificó la configuración para impedir el inicio de sesión directo con root:

-Comando: sudo nano /etc/ssh/sshd_config

```
root@debian:/# sudo nano /etc/ssh/sshd_config
```

-Accion: se cambio desde dentro del archivo la configuración del PermitRootLogin a “no”

Resultado:

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

5.2 Cambio de Credenciales en la Base de Datos
Se cambio la contraseña del usuario wordpressuser con una clave más robusta: “Str0ngVe_ryP4ssword”

-Comando:

- sudo mysql
- ALTER USER ‘wp_user’@’localhost’ IDENTIFIED BY ‘Str0ngVe_ryP4ssword’ ; FLUSH PRIVILEGES; EXIT;

Resultado:

```
root@debian:/# sudo mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.6-MariaDB-0+deb12u1 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> ALTER USER 'wp_user'@'localhost' IDENTIFIED BY 'Str0ngVe_ryP4ssw0rd'; FLUSH PRIVILEGES; EXIT;
```

5.3 Corrección de Permisos en Webroot

Se restauraron permisos seguros en /var/www/html y sus archivos:

-Comando:

- sudo chown root:www-data /var/www/html/wp-config.php
- sudo chmod 640 /var/www/html/wp-config.php

```
root@debian:/# sudo chown root:www-data /var/www/html/wp-config.php
```

```
root@debian:/# sudo chmod 640 /var/www/html/wp-config.php
```

Después se uso comandos para buscar los archivos a los que se les cambio el permiso.

-Comando:

- sudo find /var/www/html -type f -exec chmod 640 {} \ ;
- sudo find /var/www/html -type f -exec chmod 750 {} \ ;

```
root@debian:/# sudo find /var/www/html -type f -exec chmod 640 {} \;
```

```
root@debian:/# sudo find /var/www/html -type f -exec chmod 750 {} \;
```

Resultado:

```
root@debian:/# ls -la /var/www/html
total 264
drwxrwxrwx  5 www-data www-data  4096 Jan 14 12:10 .
drwxr-xr-x  3 root     root      4096 Sep 30  2024 ..
-rwxr-x---  1 www-data www-data   523 Sep 30  2024 .htaccess
-rwxr-x---  1 www-data www-data 10701 Sep 30  2024 index.html
-rwxr-x---  1 www-data www-data   405 Feb  6  2020 index.php
-rwxr-x---  1 www-data www-data 19903 Jan  9 12:45 license.txt
-rwxr-x---  1 www-data www-data  7425 Jan  9 12:45 readme.html
-rwxr-x---  1 www-data www-data  7349 Jan  9 12:45 wp-activate.php
drwxrwxrwx  9 www-data www-data  4096 Sep 10  2024 wp-admin
-rwxr-x---  1 www-data www-data   351 Feb  6  2020 wp-blog-header.php
-rwxr-x---  1 www-data www-data  2323 Jun 14  2023 wp-comments-post.php
-rwxr-x---  1 root     www-data  3017 Sep 30  2024 wp-config.php
-rwxr-x---  1 www-data www-data  3339 Jan  9 12:45 wp-config-sample.php
drwxrwxrwx  6 www-data www-data  4096 Jan  9 12:45 wp-content
-rwxr-x---  1 www-data www-data  5617 Jan  9 12:45 wp-cron.php
drwxrwxrwx 31 www-data www-data 16384 Jan  9 12:45 wp-includes
-rwxr-x---  1 www-data www-data  2493 Jan  9 12:45 wp-links-opml.php
-rwxr-x---  1 www-data www-data  3937 Mar 11  2024 wp-load.php
-rwxr-x---  1 www-data www-data 51437 Jan  9 12:45 wp-login.php
-rwxr-x---  1 www-data www-data  8727 Jan  9 12:45 wp-mail.php
-rwxr-x---  1 www-data www-data 31055 Jan  9 12:45 wp-settings.php
-rwxr-x---  1 www-data www-data 34516 Jan  9 12:45 wp-signup.php
-rwxr-x---  1 www-data www-data  5214 Jan  9 12:45 wp-trackback.php
-rwxr-x---  1 www-data www-data  3205 Jan  9 12:45 xmlrpc.php
```

Como se puede ver se aplicaron los cambios de privilegios, aplicando la norma del minimo privilegio.

6 Resumen y Recomendaciones

6.1 Resumen

Se ha confirmado que el sistema fue completamente comprometido el 8 de octubre de 2024. El origen del ataque se debió a la combinación de tres vulnerabilidades críticas: la habilitación de listados de directorios (Indexes), permisos excesivos (777) en el servidor web y la utilización de una contraseña débil (123456). Gracias a estas fallas, el atacante consiguió las credenciales de la base de datos a partir del archivo wp-config.php y las empleó para acceder directamente en modo root a través de SSH el mismo día, a las 17:40:59. La investigación aclara que no hubo borrado de logs; en su lugar, el atacante accedió al journal binario del sistema, demostrando que la auditoría sólo detectó su actividad mediante el acceso a estos registros.

6.2 Recomendaciones

-Usar contraseñas robustas
-Usar el principio del minimo privilegio
-Llevar un registro de quien accede al servidor.
-No habilitar el acceso remoto
-Proteger los archivos con contenido sensible