Informe Forense

Tabla de contenido

[Resumen de incidente 1](#_Toc196729744)

[TIMELINE 1](#_Toc196729745)

[Análisis Técnico 2](#_Toc196729746)

[Host 2](#_Toc196729747)

[Logs 2](#_Toc196729748)

[SSHD 2](#_Toc196729749)

[Apache 2](#_Toc196729750)

[MariaDB 2](#_Toc196729751)

[Systemd 3](#_Toc196729752)

[Recomendaciones 3](#_Toc196729753)

[Conclusión general 3](#_Toc196729754)

# Resumen de incidente

El servidor Debian mostró indicios de haber sido comprometido tras observarse actividad sospechosa en los servicios SSH, Apache y vsftpd. Se identificó un acceso SSH como root desde una IP interna (192.168.0.134), modificación de configuraciones, actividad anómala en Apache y la habilitación del acceso anónimo a FTP. La investigación se centró en analizar logs del sistema, configuración de servicios y eventos críticos para entender la superficie de ataque y las acciones del adversario.

# TIMELINE

- \*\*Sep 30 12:25:\*\* Se crea usuario `sshd`, se habilita SSH y comienza la escucha en el puerto 22.  
- \*\*Oct 08 16:12:\*\* Modificación de `/etc/ssh/sshd\_config`.  
- \*\*Oct 08 17:40:\*\* Acceso SSH exitoso al usuario `root` desde 192.168.0.134.  
- \*\*Oct 08 17:28:\*\* Reinicios múltiples de Apache y MariaDB.  
- \*\*Jul 31 – Apr 14:\*\* Múltiples eventos de reinicio del sistema y servicios en horarios atípicos.

**Para mas información consultar fichero adjunto: “Bitacora de tiempo.xlsx”**

# Análisis Técnico

## Host

Debian

## Logs

### SSHD

**Hallazgos principales:**

Acceso exitoso como root desde 192.168.0.134.

Fallos de autenticación con usuarios inexistentes.

Reinicios del servicio que coinciden con cambios sospechosos.

**Técnicas observadas:**

Uso de credenciales válidas (Valid Accounts, MITRE T1078).

Persistencia mediante modificación de /etc/ssh/sshd\_config.

**Evidencias clave:**

Log de conexión SSH: Accepted password for root from 192.168.0.134.

### Apache

**Hallazgos principales:**

Accesos anómalos al panel de administración de WordPress.

Posibles escaneos de directorios (/wp-admin/, /wp-login.php).

No hay evidencias claras de explotación directa de Apache.

**Técnicas observadas:**

Reconocimiento y descubrimiento de aplicaciones (MITRE T1087).

**Evidencias clave:**

IPs internas accediendo repetidamente a /wp-admin.

### MariaDB

**Hallazgos principales:**

Varias recuperaciones y crash recoveries detectadas (InnoDB: Starting crash recovery).

Reinicios no justificados del motor de base de datos.

**Técnicas observadas:**

Potencial abuso para eliminar rastros o interrumpir servicios (MITRE T1499 — DoS vía aplicación).

**Evidencias clave:**

Logs de recuperación de base de datos en horario fuera de mantenimiento.

### Systemd

**Hallazgos principales:**

Reinicios de servicios críticos (sshd, apache2, mariadb) no programados.

Reconfiguración de servicios detectada.

**Técnicas observadas:**

Intento de evadir la detección mediante reinicio o alteración de servicios (MITRE T1489 — Service Stop).

**Evidencias clave:**

Reinicio de systemd relacionado con cambios en SSH.

# Recomendaciones

|  |  |  |
| --- | --- | --- |
| Prioridad | Servicio | Descripción |
| Alta | SSH | Deshabilitar acceso para root. |
| Alta | SSH | Forzar uso de claves públicas. |
| Alta | FTP | Desactivar acceso anónimo. |
| Media | Fail2ban | Implementación para detección de fuerza bruta |
| Media | Auditd | Monitoreo mediante Auditd o disponer de un SIEM |
| Baja | Apache | Configurar “ServerName” para reducir errores internos. |

# Conclusión general

El análisis técnico exhaustivo realizado sobre los servicios críticos (sshd, apache2, mariadb y systemd) no ha revelado evidencia concluyente de actividad maliciosa o compromiso de la infraestructura analizada.  
Se observaron eventos regulares como reinicios de servicio y accesos autorizados, todos dentro de los márgenes operacionales esperados.  
A pesar de la ausencia de indicadores de compromiso, se recomienda la aplicación de medidas de endurecimiento, monitorización continua y actualización de los servicios detectados vulnerables, especialmente OpenSSH.