Informe Análisis forense

Informe de Incidente de Seguridad

Fecha del informe: 25/04/2025

Cliente: 4Geeks

Responsable del informe: Víctor Ruiz Sánchez y Valentina Cassioli

---

1. Resumen del Incidente

Se detectó actividad sospechosa en los servidores de una máquina con sistema operativo Debian, lo que generó la sospecha de un posible compromiso de seguridad. Este informe presenta los hallazgos del análisis forense realizado sobre los servicios SSH, Apache y vsftpd. La investigacion se centrò en analizar logs de sistema, las configuraciones de los servicios y eventos criticos para entender las acciones del posible ataque.

---

2. Descripción del Entorno Afectado

- **Sistema Operativo:** Linux Debian 6.1.0-25-amd64
- **IP del sistema:** 10.0.2.10
- **Servicios en ejecución:** vsftpd 3.0.3, OpenSSH 9.2p1, Apache httpd 2.4.62, MariaDB
- **Fecha estimada de compromiso:** 08-10-2024

---

3. Análisis Forense Realizado

Se ejecutaron las siguientes actividades para identificar el vector de ataque :

- **Inspección de logs del sistema**

SERVICIO SSH

- Actividad anómala registrada en los logs de sistema en fecha :

```
Oct 08 17:40:59 debian sshd[1650]: Accepted password for root from 192.168.
Oct 08 17:40:59 debian sshd[1650]: pam_unix(sshd:session): session opened
```

Antes de esta fecha no se detectaron autenticaciones de una IP especifica, por lo tanto a seguir hemos revisado la configuracion del servidor SSH para ver si se hicieron combios sospechosos

Revisión de accesos SSH:

Se analizaron los registros en `/var/log/auth.log`, identificando conexiones sospechosas desde la IP interna 192.168.0.134 con privilegios elevados.

- Se revisa `/etc/ssh/sshd_config` :

```
debian@debian:~$ grep -Ei 'permitrootlogin|passwordauthentication' /etc/ssh/ssh
d_config
PermitRootLogin yes
PasswordAuthentication yes
# PasswordAuthentication.  Depending on your PAM configuration,
# the setting of "PermitRootLogin prohibit-password".
# PAM authentication, then enable this but set PasswordAuthentication
```

> 💡 Esta configuración del servidor SSH es insegura debido a que permite el acceso directo como root y la autenticación mediante contraseña, lo cual expone al sistema a posibles ataques de fuerza bruta.

HALLAZGOS PRINCIPALES:

1. Acceso exitoso como *root* desde 192.163.0.134.
2. Fallos de autenticación con usuarios inexistentes.
3. Reinicios del servicio que coinciden con cambios sospechosos.

SERVICIO APACHE

Se destacan actividades relevantes, acceso a recursos, instalación de WordPress y eventos del sistema web.

Primeros eventos detectados:

1. 30 de septiembre de 2024, con accesos HTTP al sitio por parte de `127.0.0.1` (localhost).
2. No se encontraron entradas anteriores a esta fecha, por lo que **se asume que Apache fue instalado o activado el 30/09/2024**.

HALLAZGOS:

1. Accessos anómalos, al panel de administración de Wordpress.
2. Posibles escaneos de directorio /wp-admin. y /wp.login.php
3. No hay evidencias claras de explotacion directa de Apache

OBSERVACIONES:

Reinicios frecuentes del servicio Apache. Probablemente relacionados con:

- Cambios en configuraciones
- Activación/desactivación de módulos o sitios
- Pruebas de entorno de desarrollo
- No se detectaron accesos externos pero IPs internas accediendo a wp-admin
- Se usa Apache en modo `prefork` y `event`, lo que indica experimentación o cambio de configuraciones en tiempo real

SERVICIO MARIADB

HALLAZGOS:

1. Varias recuperaciones y crash recoveries detectadas
2. Reinicios no justificado del servidor de base de datos

---

6. Medidas Preventivas Recomendadas

- Implementación de autenticación por clave pública en SSH
- Uso de firewall (ej. UFW) con reglas restrictivas
- Actualizaciones automáticas y revisión periódica de paquetes (por ejemplo, usando Cron)
- Eliminar acceso anonimo para FTP

---

7. Conclusión

Tras el análisis forense realizado sobre los servicios SSH, Apache y vsftpd en el entorno Debian afectado, **no se han identificado pruebas concluyentes de un ataque externo exitoso ni de una explotación activa de vulnerabilidades**. Los indicios detectados —como accesos SSH como root, reinicios frecuentes de servicios, y actividad interna en Apache y MariaDB— apuntan más a **una mala configuración o pruebas internas realizadas por parte del administrador del sistema**, que a un compromiso externo o malicioso.

En concreto:

- El acceso como root mediante contraseña desde una IP interna sugiere un entorno de pruebas sin políticas aplicadas, más que un ataque real.
- Los eventos en Apache y MariaDB coinciden con instalaciones recientes, pruebas locales y reinicios no maliciosos.
- No se encontraron payloads sospechosos, backdoors ni tráfico anómalo hacia el exterior que indique una exfiltración o presencia persistente de un

atacante.

Por tanto, **el incidente parece derivar de prácticas inseguras de administración del sistema**, como permitir acceso root directo, contraseñas débiles o nula segmentación de red, más que de una intrusión externa.

Se recomienda aplicar las medidas preventivas detalladas en la sección anterior para minimizar el riesgo de futuros incidentes y reforzar la postura de seguridad del entorno.