# INFORME DE INCIDENTE DE SEGURIDAD

## 1. Introducción

Este informe documenta el análisis forense de un incidente de seguridad detectado en el sistema, detallando los hallazgos, las técnicas utilizadas para la investigación, y las medidas correctivas y preventivas implementadas para mitigar futuros riesgos.

## 2. Resumen del Incidente

- **Fecha del incidente:** 08/10/2024
- **Sistema afectado:** Servidor web y base de datos
- **Vectores de ataque:** Acceso no autorizado vía SSH, explotación de vulnerabilidad en Apache, uso de credenciales débiles en MySQL.
- **Impacto:** Posible exfiltración de datos, alteración de archivos críticos y compromiso de usuarios.

---

## 3. Análisis Forense del Incidente

### 3.1. Detección del Incidente

**Métodos de detección:**

- Análisis de logs del sistema (/var/log/auth.log, /var/log/apache2/access.log).
- Identificación de conexiones sospechosas en /var/log/secure.
- Uso de herramientas forenses (rkhunter, chkrootkit, ps aux).

**Hallazgos iniciales:**

- Conexión sospechosa desde la IP **192.168.0.134** con credenciales root.

- Creación de un usuario no autorizado (hacker) en el sistema.
- Modificación de archivos en /var/www/html/uploads.
- Ejecución de procesos desconocidos con privilegios elevados.

### 3.2. Análisis de Evidencia Digital

**Evidencia recolectada:**

- Logs de acceso y errores en Apache y MySQL.
- Dumps de memoria y procesos (volatility, gcore).
- Registros de comandos ejecutados en ~/.bash_history.

**Herramientas utilizadas:**

- Wireshark: Captura de tráfico sospechoso.
- Volatility: Análisis de memoria.
- Autopsy: Inspección de archivos alterados.
- grep y awk: Filtrado de logs para correlación de eventos.

**Hallazgos clave:**

- Usuario hacker ejecutó wget para descargar un script malicioso.
- Script alojado en /tmp/backdoor.sh, que establecía una reverse shell.
- Uso de MySQL para extraer datos con SELECT * FROM users.

---

## 4. Medidas Correctivas Implementadas

1. **Erradicación de la amenaza:**
    - Eliminación del usuario hacker con userdel -r hacker.
    - Eliminación de scripts maliciosos (rm -rf /tmp/backdoor.sh).

    - Deshabilitación de accesos sospechosos con iptables -A INPUT -s 192.168.0.134 -j DROP.
2. **Reconfiguración de Servicios:**
    - Restricción del acceso SSH (PermitRootLogin no, AllowUsers admin).
    - Aplicación de parches de seguridad en Apache y MySQL (apt update && apt upgrade).
    - Modificación de contraseñas de todos los usuarios afectados (passwd --expire user).

---

## 5. Medidas Preventivas Implementadas

1. **Fortalecimiento de Seguridad en SSH:**
    - Implementación de autenticación por clave pública.
    - Restricción de acceso mediante fail2ban.
2. **Seguridad en la Base de Datos:**
    - Habilitación de validación de contraseñas en MySQL.
    - Configuración de auditoría de accesos (log_bin_trust_function_creators = OFF).
3. **Monitoreo y Respuesta a Incidentes:**
    - Implementación de OSSEC para detección de intrusos.
    - Configuración de auditd para registrar modificaciones en archivos críticos.

---

## 6. Conclusión y Recomendaciones

- Se identificó y erradicó la amenaza sin pérdida confirmada de datos sensibles.
- Se mejoraron las políticas de acceso y seguridad en SSH, Apache y MySQL.
- Se recomienda la ejecución periódica de auditorías de seguridad y la capacitación del equipo en respuesta a incidentes.

Con estas acciones, se ha reducido significativamente la exposición del sistema a futuros ataques y se ha fortalecido la seguridad general de la infraestructura.