Fase 2 - Detección y corrección de una nueva vulnerabilidad

1. Escaneo y Análisis de Vulnerabilidades

Tras realizar un escaneo del sistema, se identificaron vulnerabilidades críticas en los servicios activos:

OpenSSH (v9.2p1): Se detectó la vulnerabilidad **CVE-2024-6387**, conocida como **"RegreSSHion"**.

Impacto: Crítico, ya que permite la **Ejecución Remota de Código (RCE)**.

VSFTPD (v3.0.3): Se identificó el **CVE-2021-30047**.

Impacto: Alto, permitiendo ataques de **Denegación de Servicio (DoS)**.

2. Explotación Controlada (Ataque de Fuerza Bruta)

Para demostrar la debilidad de las credenciales en el servicio SSH, se ejecutó un ataque controlado desde una máquina **Kali Linux** hacia el servidor **Debian** (IP: `192.168.1.69`) utilizando la herramienta **Hydra**.

Resultado del ataque: Se halló la contraseña de forma rápida debido a su baja complejidad.

Credencial Comprometida: Usuario: `debian` / Contraseña: `123456`.

Impacto: El atacante obtuvo **acceso remoto completo** al sistema sin necesidad de un exploit de código complejo, simplemente aprovechando la debilidad de la política de contraseñas.

---

3. Corrección y Persistencia de Evidencias

Durante el análisis, se descubrió un problema crítico en la gestión de registros: los logs solo se almacenaban en memoria volátil (`journald`). Esto representaba un riesgo forense, ya que un reinicio del servidor borraría cualquier evidencia del ataque.

Solución Implementada: Se instaló el servicio **rsyslog** para asegurar que los eventos se escriban de forma persistente en el disco.

Ruta de Auditoría: Se creó el archivo `/var/log/auth.log`, esencial para el seguimiento de intentos de acceso.

---

4. Monitorización y Defensa Automatizada

Para prevenir futuros ataques de fuerza bruta, se configuró un sistema de defensa activa utilizando **Fail2Ban**:

- **Política `jail.local`:**

  Umbral de Bloqueo: Máximo de **3 intentos fallidos**.

  Tiempo de Baneado: Configurado en 1 minuto para pruebas, con proyección a **Permanente** en producción.

Acción de Defensa: Uso de `iptables-allports` para un bloqueo total de la IP atacante.

> **Efectividad:** El sistema ahora detecta ataques en tiempo real mediante el monitoreo de `auth.log` y detiene la intrusión automáticamente sin intervención humana.

Con estas medidas, no solo se ha corregido la vulnerabilidad de acceso, sino que se ha dotado al sistema de una capacidad de **autodefensa y persistencia forense**.