INFORME FINAL DE PENTESTING

Proyecto: Auditoría de Seguridad "The Lovers" (Entorno Dockerizado)

1. Introducción y Alcance

1.1 Objetivo

El objetivo de esta auditoría ha sido evaluar la postura de seguridad de un entorno simulado compuesto por servicios vulnerables y aplicaciones web (DVWA), identificar vectores de ataque y demostrar el impacto mediante la explotación controlada, finalizando con una propuesta de remediación.

1.2 Alcance (Scope)

Debido a restricciones de arquitectura de hardware (Apple Silicon M1/ARM64), el entorno se ha simulado mediante contenedores Docker nativos:

- **Activo 1 (Reconocimiento):** Contenedor Debian con servicios expuestos (FTP, HTTP). IP: 172.17.0.2
- **Activo 2 (Explotación):** Aplicación Web DVWA. IP: 127.0.0.1

1.3 Metodología

Se ha seguido una metodología estándar de pruebas de penetración:

1. **Reconocimiento:** Identificación de activos y servicios (Nmap).
2. **Enumeración:** Búsqueda de versiones y archivos sensibles (Nikto, Gobuster).
3. **Explotación:** Uso de Metasploit y scripts manuales para obtener acceso.
4. **Post-Explotación:** Escalada de privilegios a root.

2. Resumen de Vulnerabilidades Detectadas

ID	Vulnerabilidad	Severidad	Estado
VULN-01	Inyección de Comandos (RCE) en DVWA	**Crítica**	Explotada
VULN-02	Escalada de Privilegios Local (SUID)	**Crítica**	Explotada
VULN-03	Divulgación de Información (phpinfo/robots)	Media	Detectada
VULN-04	Transmisión de credenciales en texto plano (FTP)	Media	Detectada

3. Análisis Detallado y Evidencias (Flags)

VULN-01: Remote Command Execution (RCE)

- **Descripción:** La aplicación web DVWA, en su módulo de "Command Injection", no sanitiza correctamente los datos introducidos por el usuario, permitiendo concatenar comandos del sistema operativo.
- **Descubrimiento:** Durante la navegación manual y pruebas de inyección básica.
- **Explotación:** Se utilizó un payload de Python inyectado manualmente para establecer una *Reverse Shell* hacia la máquina atacante, debido a la obsolescencia del módulo automático de Metasploit.
- **Evidencia (Flag):** Acceso obtenido como usuario www-data.

VULN-02: Escalada de Privilegios (SUID Misconfiguration)

- **Descripción:** El binario /usr/bin/find tenía activado el bit **SUID**. Esto permite a cualquier usuario ejecutar el comando con los permisos del propietario del archivo (root).
- **Descubrimiento:** Enumeración de permisos locales con el comando find
- **Explotación:** Ejecución del comando /usr/bin/find . -exec /bin/sh -p \; -quit.
- **Evidencia (Flag):** Cambio de identidad de www-data a root.

VULN-03: Divulgación de Información Sensible

- **Descripción:** El servidor web expone archivos de configuración y depuración que revelan información crítica sobre la infraestructura.
- **Archivos afectados:**
  - /phpinfo.php: Revela versión de PHP, módulos activos y rutas del sistema.
  - /robots.txt: Revela rutas ocultas como /admin o /passwords.
- **Evidencia:**

4. Propuesta de Prevención

Estas medidas buscan evitar que estas vulnerabilidades vuelvan a introducirse en el ciclo de desarrollo o despliegue.

1. **Ciclo de Desarrollo Seguro (SDLC):**
   - Implementar análisis estático de código (SAST) para detectar funciones peligrosas como exec() o shell_exec() en el código PHP antes de que llegue a producción.
   - Validación estricta de *inputs*:
   - Privilegios:

- El usuario del servidor web (www-data) debe tener permisos de solo lectura en el código web y solo escritura en directorios temporales específicos.

5. Propuesta de Mitigación (Corrección Inmediata)

Acciones tácticas para solucionar los problemas encontrados en el sistema actual.

Para VULN-01 (Command Injection):

- **Acción:** Modificar el código fuente de DVWA (o la aplicación real) para eliminar la llamada a shell_exec y utilizar librerías de red nativas de PHP para realizar el ping.
- **WAF:** Implementar un Web Application Firewall (como ModSecurity) con reglas para bloquear caracteres de concatenación como ;, |, && en las peticiones HTTP.

Para VULN-02 (Escalada SUID):

- **Acción Inmediata:** Retirar el permiso SUID del binario afectado.
  Bash

  chmod u-s /usr/bin/find
- **Auditoría:** Ejecutar un script para localizar otros binarios peligrosos (vim, nmap, awk, bash) que puedan tener SUID y corregirlos.

Para VULN-03 (Info Disclosure):

- **Acción:** Eliminar inmediatamente los archivos phpinfo.php y install.php del directorio público.
- **Configuración:** Editar php.ini para establecer expose_php = Off y configurar Apache (ServerTokens Prod) para no revelar versiones.

Para VULN-04 (FTP):

- **Acción:** Detener y deshabilitar el servicio vsftpd.
- **Sustitución:** Implementar acceso exclusivamente mediante SFTP (SSH) utilizando autenticación por clave pública/privada en lugar de contraseñas.

6. Conclusión

La auditoría ha revelado fallos críticos que permiten el compromiso total del servidor. La combinación de una vulnerabilidad web (RCE) con una mala configuración del sistema operativo (SUID) permitió convertirse en administrador (root)

La implementación de las medidas de mitigación descritas en este informe reducirá drásticamente la superficie de ataque y el riesgo asociado.