Informe de pentesting

Jesus Castaño Martínez

# Resumen Ejecutivo

El presente informe detalla los resultados del pentesting realizado sobre la infraestructura de TI del cliente, enfocado en evaluar posibles vulnerabilidades en sus aplicaciones web y redes internas. El objetivo fue identificar brechas de seguridad que podrían ser explotadas por atacantes y ofrecer recomendaciones para mejorar el nivel de seguridad general.

Durante la evaluación, se detectaron un total de **35 vulnerabilidades**, de las cuales **8 fueron clasificadas como críticas**, **18 como altas , 8 como medias y 1 como baja**. Las vulnerabilidades críticas están relacionadas con:

* **Inyección de SQL (SQLi)** en la aplicación web principal, que permite acceso no autorizado a datos confidenciales.
* **Autenticación débil**, que podría permitir a atacantes obtener acceso administrativo con credenciales fácilmente adivinables.

Además, se identificaron problemas de configuración en firewalls y servidores, así como exposición de información sensible mediante métodos de descubrimiento público.

# Alcance y Metodología

* 1. Alcance:  
     El alcance de esta prueba de penetración se define como el conjunto de sistemas, aplicaciones y redes que serán evaluados para identificar vulnerabilidades y debilidades de seguridad. El objetivo es proporcionar una evaluación exhaustiva de la seguridad del entorno objetivo.
     1. Objetivos **:**
        1. **Sistemas a Evaluar:**

- Debian (IP: 192.168.1.40)

- Aplicaciones web alojadas en la máquina, incluyendo:

- Servidor Apache (puerto 80)

- Servidor FTP (puerto 21)

- Servidor SSH (puerto 22)

* + - 1. **Exclusiones:**

- Cualquier sistema fuera de la dirección IP especificada.

- Sistemas de producción que no estén relacionados con la máquina objetivo.

- Redes externas no controladas.

* + - 1. **Duración de la Prueba:**

- La prueba de penetración se llevará a cabo durante un período de 5 días, comenzando el 20 de febrero de 2025 y finalizando el 25 de febrero de 2025

* + - 1. **Métodos Permitidos:**

- Escaneo de red y puertos.

- Enumeración de servicios y aplicaciones.

- Pruebas de explotación de vulnerabilidades identificadas.

- Pruebas de ingeniería social (previa autorización).

* + - 1. **Restricciones:**

- No se permite la denegación de servicio (DoS).

- No se realizarán pruebas que puedan comprometer la integridad de los datos o la disponibilidad de los sistemas.

* + 1. **Metodología:**  
       La metodología utilizada para llevar a cabo la prueba de penetración se basa en un enfoque sistemático y estructurado, siguiendo las mejores prácticas de la industria. A continuación, se describen las fases de la metodología:
       1. **Planificación y Preparación:**

- Definición del alcance y objetivos de la prueba.

- Reunión inicial con el cliente para discutir expectativas y restricciones.

- Obtención de permisos necesarios para realizar la prueba.

* + - 1. **Reconocimiento:**

- Reconocimiento Pasivo: Recolección de información sobre el objetivo sin interactuar directamente con él. Esto incluye la búsqueda de información pública, como registros WHOIS y datos

de DNS.

- Reconocimiento Activo: Uso de herramientas como Nmap para identificar direcciones IP activas, puertos abiertos y servicios en ejecución.

* + - 1. **Enumeración:**

- Identificación de servicios y aplicaciones en ejecución en los puertos abiertos.

- Uso de herramientas como Nikto para detectar vulnerabilidades en aplicaciones web.

- Enumeración de subdominios y directorios utilizando herramientas como Gobuster y Dirb.

* + - 1. **Explotación:**

- Intento de explotación de las vulnerabilidades identificadas en la fase de enumeración.

- Uso de herramientas y scripts para llevar a cabo ataques específicos, como inyección SQL, XSS, y acceso no autorizado a directorios sensibles.

* + - 1. **Post-Explotación:**

- Evaluación del impacto de las vulnerabilidades explotadas.

- Recolección de información adicional que pueda ser útil para el análisis posterior.

- Limpieza de cualquier rastro dejado durante la prueba.

* + - 1. **Informe:**

- Documentación de los hallazgos, incluyendo vulnerabilidades identificadas, pruebas realizadas y recomendaciones para mitigar los riesgos.

- Presentación de un informe final al cliente, que incluye un resumen ejecutivo y detalles técnicos.

* + - 1. **Revisión y Cierre:**

- Reunión final con el cliente para discutir los hallazgos y recomendaciones.

- Proporcionar soporte para la implementación de las recomendaciones, si es necesario.

# Hallazgos Principales

## 3.1. Resumen de Vulnerabilidades

| **Vulnerabilidad** | **Severidad (Baja/Media/Alta/Crítica)** | **Impacto** |
| --- | --- | --- |

## 3.2. Detalles de las Vulnerabilidades

**CVE-1999-0497**

* **Descripción:** El FTP anónimo está activado.
* **Impacto:** Crítica
* **Vector de Ataque:** puerto 21
* **Evidencia:**

Texto

El contenido generado por IA puede ser incorrecto.

* **Riesgo:** Acceso no autorizado. Posibilidad de subir software malintencionado a la máquina y descargar información de la máquina.
* **Recomendación:** Cerrar puerto 21 puesto que el tráfico no está cifrado. En caso de necesitar un servidor ftp, utilizar el protocolo sftp que si tiene el tráfico encriptado.

**Acceso SSH inseguro**

* **Descripción:** Conexión por ssh a la máquina con contraseña débil.
* **Impacto:** Crítica
* **Vector de Ataque:** puerto 22
* **Evidencia:**

Texto

El contenido generado por IA puede ser incorrecto.

Imagen de la pantalla de un celular con texto

El contenido generado por IA puede ser incorrecto.

* **Riesgo:** Acceso no autorizado. Una vez obtenida la contraseña débil mediante fuerza bruta, conectarse a la máquina con usuario root.
* **Recomendación:** Utilizar la política de contraseñas especificada en el SGSI para evitar contraseñas débiles.

**Directorio web listable**

* **Descripción:** Los servidores web pueden configurarse para listar automáticamente el contenido de los directorios que no tienen una página de índice presente. Esto puede ayudar a un atacante permitiéndole identificar rápidamente los recursos en una ruta dada, y proceder directamente a analizar y atacar esos recursos. En particular, aumenta la exposición de archivos sensibles dentro del directorio que no están destinados a ser accesibles a los usuarios, tales como archivos temporales y volcados de memoria.
* **Impacto:** Media
* **Vector de Ataque:** puerto 80
* **Evidencia:**

Tabla

El contenido generado por IA puede ser incorrecto.

* **Riesgo:** Los listados de directorios en sí mismos no constituyen necesariamente una vulnerabilidad de seguridad. En cualquier caso, cualquier recurso sensible dentro de la raíz de la web debería tener un control de acceso adecuado, y no debería ser accesible por una parte no autorizada que conozca o adivine la URL. Incluso cuando los listados de directorios están desactivados, un atacante puede adivinar la ubicación de archivos sensibles utilizando herramientas automatizadas.
* **Recomendación:** Desactivar el listado de directorios**.**

[**CVE-2024-10470**](https://www.cve.org/CVERecord?id=CVE-2024-10470)

* **Descripción:** El sistema de gestión de aprendizaje WPLMS para WordPress, tema de WordPress LMS para WordPress es vulnerable a la lectura y eliminación arbitraria de archivos debido a la insuficiente validación de rutas de archivos y comprobaciones de permisos en las funciones readfile y unlink en todas las versiones hasta, e incluyendo, 4.962. Esto hace posible que atacantes no autenticados eliminen archivos arbitrarios en el servidor, lo que puede llevar fácilmente a la ejecución remota de código cuando se elimina el archivo correcto (como wp-config.php). El tema es vulnerable incluso cuando no está activado.
* **Impacto:** Crítica
* **Vector de Ataque:** Servidor de aplicaciones
* **Evidencia:**

Texto

El contenido generado por IA puede ser incorrecto.

* **Riesgo:** Acceso no autorizado permitiendo que atacantes no autenticados eliminen archivos arbitrarios en el servidor, lo que puede llevar fácilmente a la ejecución remota de código cuando se elimina el archivo correcto (como wp-config.php). El tema es vulnerable incluso cuando no está activado.
* **Recomendación:** Asignar permisos más restrictivos a ficheros de configuración de Wordpress como wp-config.php.

Ejemplo:  chmod 600 wp-config.php

# Conclusiones

Las conclusiones obtenidas del pentesting es que la mayoría de vulnerabilidades de la máquina se resolverían utilizando contraseñas seguras, protocolos seguros o actualizando el software para evitar vulnerabilidades conocidas.

# Anexos

**Anexo 1: Listado Completo de Activos Evaluados**

A continuación, se presenta un listado de los activos evaluados durante la prueba de penetración:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Activo** | **Dirección IP** | **Tipo de Servicio** | **Sistema Operativo** | **Observaciones** |
| 1 | Servidor Web | 192.168.1.38 | Apache 2.4 | Debian | Servidor principal de la aplicación |
| 2 | Base de Datos | 192.168.1.38 | MySQL 8.0 | Debian | Contiene datos sensibles |
|  |  |  |  |  |  |

**Anexo 2: Capturas de Pantalla Adicionales**

Se incluyen a continuación capturas de pantalla relevantes tomadas durante la ejecución de las pruebas:

1. **Escaneo de puertos realizado con Nmap**

Texto

El contenido generado por IA puede ser incorrecto.

1. **Escaneo con gobuster**

Tabla

El contenido generado por IA puede ser incorrecto.

1. **Escaneo de vulnerabilidades con nikto**

Interfaz de usuario gráfica, Texto, Aplicación, Carta, Correo electrónico

El contenido generado por IA puede ser incorrecto.

1. Una vez conectado a la base de datos como root, obtenemos la información de la tabla users de la base de datos de wordpress para obtener el usuario y contraseña

Texto

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.