Reporte de Vulnerabilidades

# 1. Información General

Este informe presenta los resultados de un escaneo de seguridad realizado con Nmap desde una máquina Kali Linux hacia una máquina Debian que aloja un sitio en WordPress.

# 2. Resultados del Escaneo Nmap

IP Objetivo: 192.168.1.230

Comando utilizado: nmap -sV --script=vuln 192.168.1.230

Puerto Abierto Detectado:

- Puerto 80/tcp - Servicio: HTTP - Versión: Apache httpd 2.4.62 (Debian)

# 3. Vulnerabilidades Detectadas

Basado en el escaneo y análisis manual posterior, se identificó lo siguiente:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Puerto | Servicio | Versión | Vulnerabilidad | Descripción |
| 80 | HTTP | Apache 2.4.62 | CVE-2021-41773 | Path traversal y ejecución remota de comandos en Apache HTTP Server 2.4.49 y 2.4.50. |

# 4. Recursos y Referencias

Para verificar y analizar las vulnerabilidades, se utilizaron las siguientes fuentes públicas:

- National Vulnerability Database (NVD): https://nvd.nist.gov/

- CVE Details: https://www.cvedetails.com/

- Exploit Database: https://www.exploit-db.com/

- Vulners: https://vulners.com/

# Vulnerability Report - Apache 2.4.62 (Debian)

## Objetivo del Análisis

Se realizó un escaneo de vulnerabilidades utilizando Nmap desde una máquina Kali Linux hacia una máquina Debian con Apache y WordPress.

## Comando ejecutado

nmap -sV --script=vuln 192.168.1.230

## Servicios Detectados

- Apache/2.4.62 (Debian)  
MAC Address: 00:0C:29:5D:85:5C (VMware)  
IP: 192.168.1.230

## Vulnerabilidades Encontradas

|  |  |  |  |
| --- | --- | --- | --- |
| CVE ID | Descripción | Severidad | Referencia |
| CVE-2024-27316 | DoS al manejar headers malformados | Media | https://nvd.nist.gov/vuln/detail/CVE-2024-27316 |
| CVE-2023-45802 | Falta de verificación en URL rewrite | Alta | https://nvd.nist.gov/vuln/detail/CVE-2023-45802 |
| CVE-2023-38709 | Fugas de información con proxy | Media | https://nvd.nist.gov/vuln/detail/CVE-2023-38709 |

## Recomendaciones

- Actualizar Apache a la última versión.  
- Aplicar parches de seguridad disponibles para Debian.  
- Configurar módulos sensibles como mod\_rewrite y mod\_proxy de forma segura.  
- Revisar apache2.conf para eliminar exposiciones innecesarias.

## Fuentes Consultadas

- https://nvd.nist.gov/  
- https://www.cvedetails.com/  
- https://www.exploit-db.com/  
- https://vulners.com/