

Informe de Análisis de Puertos Abiertos y Vulnerabilidades en Debian

1. Introducción

Este informe documenta los resultados obtenidos tras realizar un escaneo de puertos y vulnerabilidades en un servidor Debian utilizando la herramienta **Nmap**. Se identificaron servicios activos, versiones de software y posibles vulnerabilidades asociadas. Además, se incluyen recomendaciones básicas para mitigar riesgos.

2. Metodología

Se utilizó **Kali Linux** para ejecutar los escaneos sobre la máquina Debian con la dirección IP **192.168.1.10**. Se ejecutaron los siguientes comandos:

- **Escaneo de puertos abiertos y detección de servicios:**
`nmap -sV 192.168.1.10`
- **Búsqueda de vulnerabilidades en los servicios detectados:**
`nmap -sV --script=vuln 192.168.1.10`
- **Análisis específico de WordPress:**
`wpscan --url http://192.168.1.10/wordpress/ --enumerate vp`

3. Resultados Obtenidos



3.1 Puertos Abiertos

Puerto	Estado	Servicio	Versión
		o	
80	Abierto	HTTP	Apache 2.4.62 (Debian)

Los puertos **22 (SSH)** y **443 (HTTPS)** aparecen **cerrados** en el escaneo.

3.2 Vulnerabilidades Identificadas

Tras buscar en bases de datos de vulnerabilidades (NVD, CVE Details, Exploit-DB), se identificaron las siguientes vulnerabilidades en **Apache 2.4.62**:

CVE	Severidad	Descripción
CVE-2024-40898	 ALTA (7.5)	Vulnerabilidad SSRF en Apache HTTP Server con <code>mod_rewrite</code> , permite filtrar hashes NTLM a servidores maliciosos. Mitigación: Actualizar a 2.4.62 (ya aplicada).
CVE-2024-40725	 MEDIA (5.3)	Divulgación de código fuente en ciertas configuraciones, afectando archivos PHP. Mitigación: Actualizar a 2.4.62 (ya aplicada).

3.3 Análisis de WordPress

El escaneo con **WPScan** no detectó la versión exacta de WordPress ni plugins vulnerables. Sin embargo, se observó la presencia de un blog en la ruta:

`http://192.168.1.10/wordpress/`

Adicionalmente, se realizaron pruebas de enumeración con **Nmap** y **cURL** sin obtener información sensible.9

4. Recomendaciones

1. **Mantener Apache actualizado:** Se confirmó que la versión 2.4.62 ya mitiga las vulnerabilidades detectadas.
2. **Restringir acceso al panel de WordPress:** Implementar reglas en el `.htaccess` para limitar accesos a `wp-login.php` y `wp-admin`.
3. **Activar seguridad en WordPress:**
 - Instalar plugins de seguridad como **Wordfence**.
 - Deshabilitar el listado de directorios en Apache.
4. **Monitorear el tráfico HTTP:** Configurar herramientas como **Fail2Ban** para bloquear IPs sospechosas.

5. Conclusiones

El servidor Debian tiene expuesto solo el puerto **80 (HTTP)**, con Apache 2.4.62. Las vulnerabilidades identificadas en versiones anteriores de Apache ya han sido solucionadas. Se recomienda reforzar la seguridad en WordPress y monitorear el tráfico HTTP para evitar posibles ataques.