

Informe de Vulnerabilidades en el Servidor Debian

Fecha: 2025-05-27

1. Introducción

Este informe presenta los resultados del análisis de seguridad realizado sobre un servidor Debian que aloja un sitio web WordPress

2. Detalles del Escaneo

- IP del objetivo: 192.168.1.145
- Puerto abierto: 80/tcp
- Servicio detectado: HTTP
- Versión del servicio: Apache 2.4.62 (Debian)

3. Herramienta Utilizada

Se utilizó Nmap con los scripts de vulnerabilidad (--script=vuln) para detectar posibles fallos de seguridad

4. Resultados del escaneo

- WordPress identificado en /wordpress/
- Página de login detectada en /wordpress/wp-login.php
- No se detectaron vulnerabilidades por los scripts activos (XSS, CSRF, etc.)

5. Análisis de Riesgos

Actualmente, no se detectaron vulnerabilidades críticas. Sin embargo, mantener los servicios actualizados y monitorizados es esencial

CVE-2011-1002 - Avahi NULL UDP DoS				
Descripción: Esta vulnerabilidad permite realizar un ataque de denegación de servicio mediante el envío de paquetes UDP vacíos al puerto Avahi (mDNS)	Servicio objetivo: Avahi daemon	Script de Nmap utilizado: broadcast-avahi-dos	Resultado: No vulnerable	Detalles: El sistema respondió correctamente al paquete de prueba. La vulnerabilidad no se encuentra presente o está mitigada por actualizaciones

6. Recomendaciones

- Mantener Apache y WordPress actualizados.
- Utilizar plugins de seguridad en WordPress como Wordfence.
- Configurar reglas de firewall para limitar el acceso al puerto 80 desde IPs no autorizadas.

7. Conclusión

El sistema analizado no muestra vulnerabilidades conocidas según los scripts de Nmap, pero se recomienda realizar auditorías regulares.

Captura del escaneo:

Archivo Acciones Editar Vista Ayuda

zsh: suspended nmap -sV --script=vuln 192.168.1.145 -oN vulnerabilidades.txt

(anonymousroot@kali)-[~]

\$ nmap -sV --script=vuln 192.168.1.145 -oN vulnerabilidades.txt -v

Starting Nmap 7.95 (<https://nmap.org>) at 2025-05-27 12:01 CEST

NSE: Loaded 151 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 12:01

NSE Timing: About 46.67% done; ETC: 12:02 (0:00:37 remaining)

Completed NSE at 12:02, 34.37s elapsed

Initiating NSE at 12:02

Completed NSE at 12:02, 0.00s elapsed

Pre-scan script results:

| broadcast-avahi-dos:

| | Discovered hosts:

| | 224.0.0.251

| | After NULL UDP avahi packet DoS (CVE-2011-1002).

|_ Hosts are all up (not vulnerable).

Initiating ARP Ping Scan at 12:02

Scanning 192.168.1.145 [1 port]

Completed ARP Ping Scan at 12:02, 0.14s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 12:02

Completed Parallel DNS resolution of 1 host. at 12:02, 0.03s elapsed

Initiating SYN Stealth Scan at 12:02

Scanning magikz-3.home (192.168.1.145) [1000 ports]

Discovered open port 80/tcp on 192.168.1.145

Completed SYN Stealth Scan at 12:02, 0.16s elapsed (1000 total ports)

Initiating Service scan at 12:02

Scanning 1 service on magikz-3.home (192.168.1.145)

Completed Service scan at 12:02, 6.10s elapsed (1 service on 1 host)

NSE: Script scanning 192.168.1.145.

Initiating NSE at 12:02

Completed NSE at 12:02, 22.05s elapsed

Initiating NSE at 12:02

Completed NSE at 12:02, 0.02s elapsed

Nmap scan report for magikz-3.home (192.168.1.145)

Host is up (0.00098s latency).

Not shown: 999 closed tcp ports (reset)

PORT STATE SERVICE

80/tcp open http Apache httpd 2.4.62 ((Debian))

|_http-dombased-xss: Couldn't find any DOM based XSS.

|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

|_http-csrf: Couldn't find any CSRF vulnerabilities.

|_http-server-header: Apache/2.4.62 (Debian)

| http-enum:

| | /wordpress/: Blog

|_ /wordpress/wp-login.php: Wordpress login page.

MAC Address: 00:0C:29:32:4D:1E (VMware)

NSE: Script Post-scanning.

Initiating NSE at 12:02

Completed NSE at 12:02, 0.00s elapsed

Initiating NSE at 12:02

Completed NSE at 12:02, 0.00s elapsed

Read data files from: /usr/share/nmap

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 63.28 seconds

Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.032KB)