

## Informe de vulnerabilidades: Escanéo de servicios con Nmap

En este proyecto se busca recoger las posibles vulnerabilidades percibidas en una máquina que está expuesta a la red publicando una página web de wordpress, para ello se usará la herramienta **nmap**, con objetivo de listar información de interés acerca de los servicios expuestos por dicha máquina.

Primeramente se realiza un escaneo básico de servicios y la versión de estos haciendo uso del comando **sudo nmap -sV 192.168.1.10**, siendo esta la IP del equipo objetivo:

```
(kali@kali)-[~]
$ sudo nmap -sV 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-31 15:48 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00039s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.65 ((Debian))
MAC Address: 08:00:27:D1:65:C7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.52 seconds
```

Inicialmente se puede percibir que el único servicio expuesto por el equipo es el de Apache, presumiblemente el que se está usando para publicar la página de wordpress a la red, en primera instancia se puede observar la versión de Apache que se está usando en el equipo.

Con objetivo de recabar información adicional de las vulnerabilidades presentes en el servicio, se procede a buscar los *exploits* que pueden ser usados en el servicio, para ello se va a hacer uso del comando **searchsploit**, para acceder a la base de datos de vulnerabilidades presente en la máquina Kali que se está usando:

```
(kali@kali)-[~]
$ searchsploit Apache Debian
```

Exploit Title	Path
Apache 1.3.34/1.3.33 (Ubuntu / Debian) - CGI TTY Privilege Escalation	linux/local/3384.c
Apache Tomcat 8/7/6 (Debian-Based Distros) - Local Privilege Escalation	linux/local/40450.txt


```
Shellcodes: No Results
```

Inicialmente no parece haber una vulnerabilidad para la versión del servicio expuesto, sin embargo, para poder ahondar en la búsqueda, se va a correr el comando de **nmap** avanzado, usando en conjunto el script que trae disponible para detectar vulnerabilidades en los servicios encontrados, gracias a esto, es posible que se nos indiquen vulnerabilidades más actuales que las que figuran en *exploit db* haciendo uso del comando **sudo nmap -sV --scrip=vuln 192.168.1.10**:

```
(kali㉿kali)-[~]
$ sudo nmap -sV --script=vuln 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-31 16:00 EDT
Nmap scan report for 192.168.1.10
Host is up (0.0012s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.65 ((Debian))
|_http-server-header: Apache/2.4.65 (Debian)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-enum:
|_ /wordpress/: Blog
|_ /wordpress/wp-login.php: Wordpress login page.
MAC Address: 08:00:27:D1:65:C7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 124.45 seconds
```

De nuevo parece que la versión de Apache que la máquina está usando no se ha asociado a ninguna vulnerabilidad que el comando nos es capaz de listar, por ende se va a pasar a la búsqueda manual, en las páginas web de la [NVD](#), de [Vulners](#) y de [Exploit Database](#) para comprobar si vulnerabilidades han sido detectadas en el pasado muy reciente en el caso de que el script de *nmap* no lo haya detectado:

Identifier	CISA Key Info	Published Date	CNA	Description
CVE-2025-54090		2025-07-23	Apache Software Foundation	A bug in Apache HTTP Server 2.4.64 results in all "RewriteCond expr ..." tests evaluating as "true". Users are recommended to upgrade to version 2.4.65, which fixes the issue.

De todas las búsquedas, primeramente se puede comprobar que la referencia a la versión de apache usada es porque esta versión arregla una seria vulnerabilidad de ejecución remota de código, siendo que la actualización solventa el problema,.

De la misma forma se puede comprobar en el resto de páginas que la versión objetivo ha arreglado múltiples vulnerabilidades en diferentes plataformas como AWS, IBM o Azure, entre otros, por lo que se puede inferir que, actualmente, no se ha encontrado ninguna vulnerabilidad que pueda ser explotada para la versión objetivo.

### Bibliografía de enlaces

- ❖ NVD - 31/10/2025 \_21:10- Búsqueda de CVEs para versión Apache:  
<https://nvd.nist.gov/vuln/search#/nvd/home?keyword=Apache%202.4.65&resultType=records>.
- ❖ Vulners - 31/10/2025 \_21:20: Búsqueda adicional de CVEs para la versión de Apache: <https://vulners.com/search?query=Apache%202.4.65>.