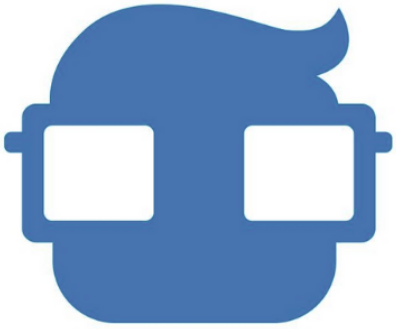
4GEEKS ACADEMY
BOOTCAMP DE CIBERSEGURIDAD



INFORME DE VULNERABILIDADES

HACIENDO USO DE NMAP

NOMBRE DEL ESTUDIANTE: JORGE TERAN

PROYECTO: ESCANEAR PUERTOS CON NMAP

Metodología

Herramienta Utilizada - Nmap

Es una herramienta de código abierto para la exploración de redes y auditoría de seguridad, que permite identificar hosts, servicios, y vulnerabilidades en una red. Con Nmap llevaremos a cabo escaneos en una máquina objetivo (en este caso, una máquina con Debian) desde una máquina con Kali Linux.

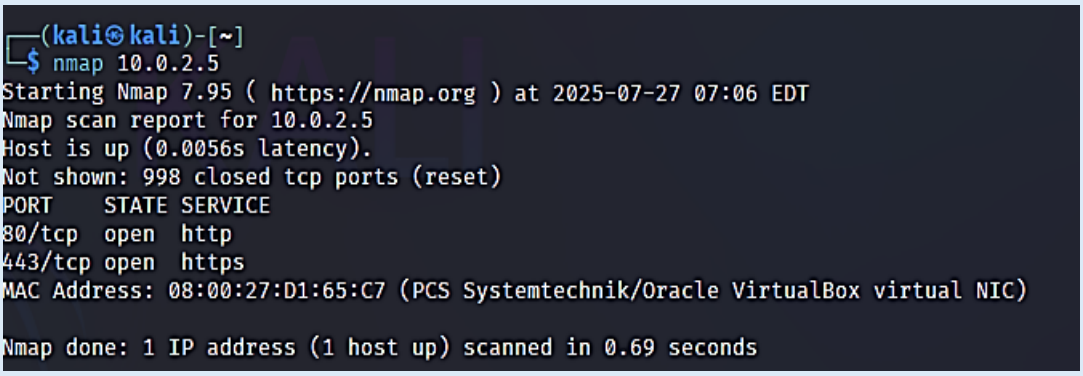
Paso 1: Escaneo básico con Nmap

Para comenzar el análisis, se ejecutó un escaneo básico contra la IP de la máquina objetivo utilizando el siguiente comando:

```
kali@kali:~$ nmap 10.0.2.5
```

Este comando permite detectar puertos abiertos utilizando el escaneo por defecto de Nmap, que analiza los **1.000 puertos TCP más comunes**.

A continuación, se muestra la salida obtenida:



Anexo 1.0

Se puede observar en el Anexo **1.0** que el Fabricante: **PCS Systemtechnik / Oracle VirtualBox virtual NIC**, Dirección MAC: **08:00:27:D1:65:C7**, esto indica que estás escaneando una máquina virtual montada en VirtualBox, asimismo dos puertos abiertos el **80 (HTTP) y 443 (HTTPS)**. Al estar expuestos, estos puertos pueden ser analizados más a fondo para detectar posibles vulnerabilidades.

Paso 2: Enumerar Puertos

Se ejecutó el siguiente comando **(-sV**) permite detectar la versión del servicio que está operando en cada puerto:

```
kali@kali:~$ nmap -Sv 10.0.2.5
```

A continuación, se muestra la salida obtenida:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.0.2.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-27 07:32 EDT
Nmap scan report for 10.0.2.5
Host is up (0.0047s latency).
Not shown: 998 closed tcp ports (reset)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Apache httpd 2.4.62
443/tcp open  ssl/http Apache httpd 2.4.62 ((Debian))
MAC Address: 08:00:27:D1:65:C7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: debian.debian

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
```

Anexo 1.1: Resultado de -sV mostrando Apache

Se observa en el anexo **1.1** que el servicio web corre sobre **Apache 2.4.62**, tanto en **HTTP** como en **HTTPS**. El servicio de **HTTPS** (**443**) está configurado como un alias de Apache con SSL (**ssl/http**), lo cual sugiere que probablemente tiene certificado auto firmado.

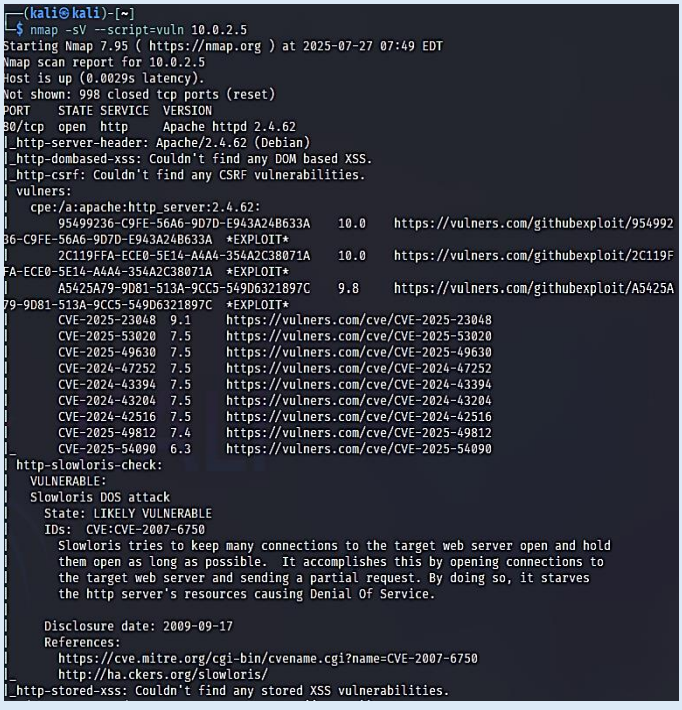
La información extraída es útil para investigar posibles **vulnerabilidades conocidas (CVEs)** en esa versión específica de Apache.

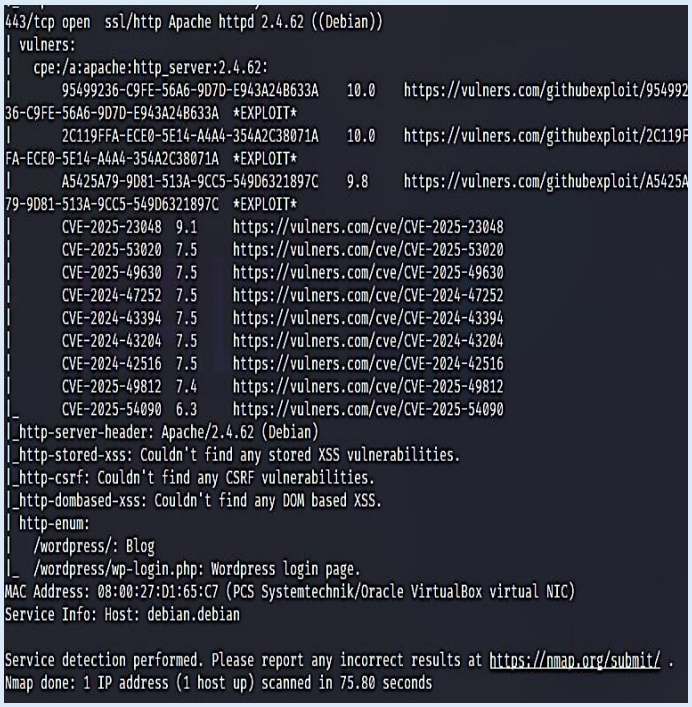
Paso 3: Escaneo Detallado y Búsqueda de Vulnerabilidades

Se ejecutó el siguiente comando **(--script=vuln)** ejecuta scripts de detección de vulnerabilidades que Nmap tiene incorporados:

```
kali@kali:~$ nmap -Sv –script=vuln 10.0.2.5
```

A continuación, se muestra la salida obtenida:





Anexo 1.2: Resultado de -sV –script=vuln

En el **Anexo 1.2** se observa un escaneo con **nmap** usando el script vuln sobre la IP **10.0.2.5**, el cual identificó múltiples vulnerabilidades asociadas con el servidor web **Apache HTTPD 2.4.6** en los puertos **80** y **443**.

A continuación, te presento tabla de las vulnerabilidades encontradas, debido a que ambos puertos (**80 y 443**) están sirviendo el mismo servicio (**Apache HTTP Server 2.4.57**), comparten las **mismas vulnerabilidades**:

Puerto	Servicio	Versión	CVE ID	Enlace	Riesgo
			CVE-2025-23048	**https://vulners.com/cve/CVE-2025-23048**	**9.1 (Alta)**
			CVE-2025-53020	**https://vulners.com/cve/CVE-2025-53020**	**7.5 (Alta)**
			CVE-2025-49630	**https://vulners.com/cve/CVE-2025-49630**	**7.5 (Alta)**
80/tcp	**Apache HTTP**	**2.4.57**	**CVE-2024-47252**	**https://vulners.com/cve/CVE-2024-47252**	**7.5 (Alta)**
			CVE-2024-43394	**https://vulners.com/cve/CVE-2024-43394**	**7.5 (Alta)**
			CVE-2024-43204	**https://vulners.com/cve/CVE-2024-43204**	**7.5 (Alta)**
			CVE-2024-42516	**https://vulners.com/cve/CVE-2024-42516**	**7.5 (Alta)**
			CVE-2025-49812	**https://vulners.com/cve/CVE-2025-49812**	**7.4 (Alta)**
			CVE-2025-23048	**https://vulners.com/cve/CVE-2025-23048**	**9.1 (Alta)**
			CVE-2025-53020	**https://vulners.com/cve/CVE-2025-53020**	**7.5 (Alta)**
			CVE-2025-49630	**https://vulners.com/cve/CVE-2025-49630**	**7.5 (Alta)**
443/tcp	**Apache HTTPS**	**2.4.57**	**CVE-2024-47252**	**https://vulners.com/cve/CVE-2024-47252**	**7.5 (Alta)**
			CVE-2024-43394	**https://vulners.com/cve/CVE-2024-43394**	**7.5 (Alta)**
			CVE-2024-43204	**https://vulners.com/cve/CVE-2024-43204**	**7.5 (Alta)**
			CVE-2024-42516	**https://vulners.com/cve/CVE-2024-42516**	**7.5 (Alta)**
			CVE-2025-49812	**https://vulners.com/cve/CVE-2025-49812**	**7.4 (Alta)**