

Paso 1: Escaneo con Nmap

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ nmap 192.168.0.101  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-27 23:22 EDT  
Nmap scan report for 192.168.0.101  
Host is up (0.00017s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
80/tcp    open  http  
MAC Address: 08:00:27:D1:65:C7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

Paso 2: Enumerar puertos y Verificar servicios

```
(kali@kali)-[~]  
$ nmap -sV 192.168.0.101  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-27 23:23 EDT  
Nmap scan report for 192.168.0.101  
Host is up (0.00017s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
80/tcp    open  http      Apache httpd 2.4.62 ((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 7.00 seconds
```

```
(kali@kali)-[~]  
$ nmap -sV --script=vuln 192.168.0.101  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-27 23:24 EDT  
Nmap scan report for 192.168.0.101  
Host is up (0.00036s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
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)  
_vulners:  
  cpe:/a:apache:http_server:2.4.62:  
    95499236-C9FE-56A6-9D7D-E943A248633A 10.0 https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A248633A *EXPLOIT*  
    2C119FFA-ECE0-5E14-A4A4-354A2C38071A 10.0 https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A *EXPLOIT*  
    A5425A79-9D81-513A-9CC5-549D6321897C 9.8 https://vulners.com/githubexploit/A5425A79-9D81-513A-9CC5-549D6321897C *EXPLOIT*  
  CVE-2025-23048 9.1 https://vulners.com/cve/CVE-2025-23048  
  CVE-2025-53020 7.5 https://vulners.com/cve/CVE-2025-53020  
  CVE-2025-49630 7.5 https://vulners.com/cve/CVE-2025-49630  
  CVE-2024-47252 7.5 https://vulners.com/cve/CVE-2024-47252  
  CVE-2024-43394 7.5 https://vulners.com/cve/CVE-2024-43394  
  CVE-2024-43204 7.5 https://vulners.com/cve/CVE-2024-43204  
  CVE-2024-42516 7.5 https://vulners.com/cve/CVE-2024-42516  
  CVE-2025-49812 7.4 https://vulners.com/cve/CVE-2025-49812  
  CVE-2025-54090 6.3 https://vulners.com/cve/CVE-2025-54090  
_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 38.67 seconds
```

Puerto	Servicio	Versión	Vulnerabilidad	Descripción	Referencia
80	HTTP	Apache 2.4.63	CVE-2025-53020	Vulnerabilidad de liberación tardía de memoria tras el tiempo de vida útil efectivo en el servidor Apache HTTP. Este problema afecta al servidor Apache HTTP desde la versión 2.4.17 hasta la 2.4.63.	https://nvd.nist.gov/vuln/detail/CVE-2025-53020
443	HTTPS	OpenSsl 3.5.0	CVE-2020-36168	Se detectó un problema en Veritas Resiliency Platform 3.4 y 3.5. Utiliza OpenSSL en sistemas Windows al usar el complemento Host administrado. Al iniciar, carga la biblioteca OpenSSL. Esta biblioteca podría intentar cargar el archivo de configuración	https://nvd.nist.gov/vuln/detail/CVE-2020-36168

				openssl.cnf, que no existe. De forma predetermin ada, en Windows...	
--	--	--	--	---	--