

Escanear puertos con nmap



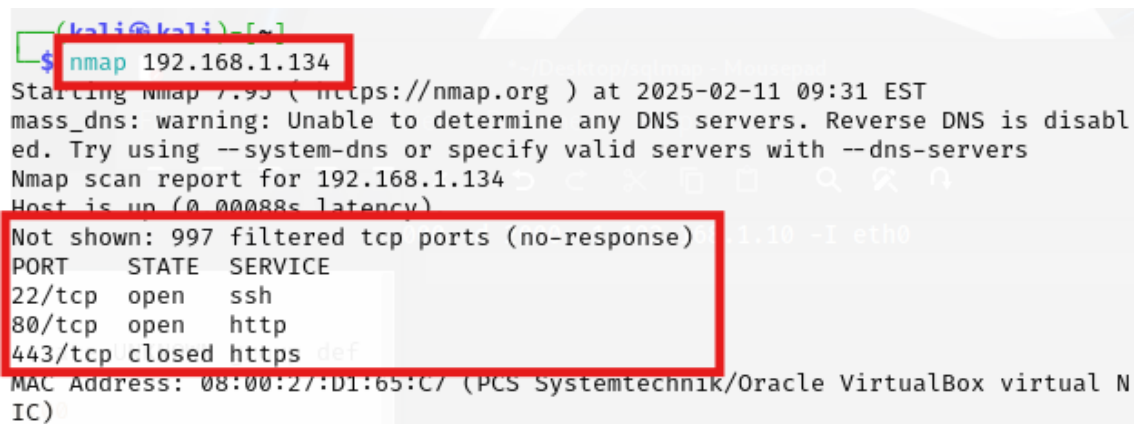
| | |
|---|----------|
| 1. Escaneo con Nmap | 3 |
| a. Escaneo básico | 3 |
| 2. Enumerar puertos y verificar servicios | 3 |
| a. Escaneo de puertos y servicios | 3 |
| b. Escaneo detallado y búsqueda de vulnerabilidades | 4 |
| 3. Documentación de vulnerabilidades | 5 |
| Conclusión | 6 |

1. Escaneo con Nmap

a. Escaneo básico

Usaremos el comando '**nmap**', seguido de la ip del objetivo(máquina debian).

```
$ nmap 192.168.1.134
```



```
(kali@kali)~$ nmap 192.168.1.134
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-11 09:31 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.134
Host is up (0.00088s latency)
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   closed https
MAC Address: 08:00:27:D1:65:C7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

2. Enumerar puertos y verificar servicios

a. Escaneo de puertos y servicios

Usaremos el comando '**nmap**', y esta vez añadimos el flag '**-sV**' para detectar la versión del servicio que usa cada puerto.

```
$ nmap -sV 192.168.1.134
```

```

$ nmap -sV 192.168.1.134
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-11 09:31 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try u
m-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.134
Host is up (0.00069s latency).
Not shown: 997 filtered tcp ports (no response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u4 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.62 ((Debian))
443/tcp   closed https
MAC Address: 08:00:27:D1:65:C7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/s
Nmap done: 1 IP address (1 host up) scanned in 11.23 seconds
  
```

b. Escaneo detallado y búsqueda de vulnerabilidades

Usaremos el comando **'nmap'**, y esta vez añadimos el flag **'--script=vuln'**, el cual ejecuta un script para detectar la vulnerabilidad concreta que encuentre en cada servicio.

```
$ nmap -sV --script=vuln 192.168.1.134
```

```

$ nmap -sV --script=vuln 192.168.1.134
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-11 10:06 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try u
m-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.134
Host is up (0.00086s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u4 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.62 ((Debian))
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Apache/2.4.62 (Debian)
|_http-enum:
|_ /wordpress/: Blog
|_ /wordpress/wp-login.php: Wordpress login page.
443/tcp   closed https
MAC Address: 08:00:27:D1:65:C7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux kernel

Service detection performed. Please report any incorrect results at https://nmap.org/s
Nmap done: 1 IP address (1 host up) scanned in 43.39 seconds
  
```

3. Documentación de vulnerabilidades

| Puerto | Servicio | Versión | Vulnerabilidad | Descripción | Referencia |
|--------|----------|--|----------------------------|--|--------------------------------|
| 22/tcp | ssh | OpenSSH 9.2p1 Debian 2+deb12u4 (protocol 2.0) | CVE-2021-2804 1 | Vulnerabilidad de escalada de privilegios en OpenSSH. | CVE-2021-28041 |
| 80/tcp | http | Apache httpd 2.4.62 ((Debian)) | - | No se encontraron vulnerabilidades específicas. | - |
| - | - | - | - | _http-dombase-d-xss: No se encontraron vulnerabilidades de XSS basadas en DOM. | - |
| - | - | - | - | _http-csrf: No se encontraron vulnerabilidades CSRF. | - |

| | | | | | |
|---|---|---|---|--|---|
| - | - | - | - | _http-stored-xss: No se encontraron vulnerabilidades de XSS almacenadas. | - |
| - | - | - | - | _http-server-header: Apache/2.4.62 (Debian) | - |
| - | - | - | - | _http-enum: Se encontró un blog de Wordpress en /wordpress/ y una página de inicio de sesión en /wordpress/wp-login.php. | - |

Conclusión

El escaneo de la máquina Debian ha identificado dos puertos abiertos: el puerto 22, que está ejecutando **OpenSSH 9.2p1**, y el puerto 80, que corre **Apache HTTPD 2.4.62**. Aunque no se encontraron vulnerabilidades críticas en el servicio HTTP, se detectó una vulnerabilidad de escalada de privilegios en **OpenSSH** ([CVE-2021-28041](#)) que requiere atención.

Además, se observó la presencia de un blog de Wordpress, lo que podría ser un posible vector de ataque si no se gestiona adecuadamente. Es fundamental aplicar las



actualizaciones de seguridad necesarias y mantener un monitoreo constante de las vulnerabilidades para asegurar la protección del sistema.