

Escanear puertos con nmap

En esta práctica realizaremos un escaner de puertos desde nuestra máquina Kali a la máquina Debian.

Los resultados obtenidos del escaner son:

Puerto	Servicio	Versión	Vulnerabilidad	Descripción	Referencia
22	ssh	OpenSSH 9.2p1	CVE-2024-6387	Administración de algunas señales de forma insegura Solución: Actualizar a la versión 9.8	https://www.cvedetails.com/cve/CVE-2024-6387/
80	http	N/A (puerto cerrado)	N/A (puerto cerrado)	N/A (puerto cerrado)	N/A (puerto cerrado)
443	https	N/A (puerto cerrado)	N/A (puerto cerrado)	N/A (puerto cerrado)	N/A (puerto cerrado)

Adjuntamos como evidencia los resultados de los escaneos realizados desde Kali a Debian utilizando NMAP:

- Escaneo de puertos y servicios:

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-01 14:04 EDT
Nmap scan report for 192.168.1.10
Host is up (0.0011s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE  SERVICE VERSION
22/tcp    open   ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
80/tcp    closed http
443/tcp   closed https
MAC Address: 08:00:27:D1:65:C7 (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/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.70 seconds
```

- Escaneo detallado y búsqueda de vulnerabilidades:

```
(kali@kali)-[~]
$ nmap -sV --script=vuln 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-01 14:08 EDT
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).
Nmap scan report for 192.168.1.10
Host is up (0.0014s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
80/tcp    closed http
443/tcp   closed https
MAC Address: 08:00:27:D1:65:C7 (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/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 127.56 seconds
```

En esta imagen podemos observar dos aspectos relevantes:

1. Hay 997 puertos filtrados en la máquina Debian. La mayoría de puertos están bloqueados gracias a las configuraciones previas que se han realizado en el firewall de iptables de Debian.
2. Vulnerabilidad de Avahi (CVE-2011-1002): Nmap probó una vulnerabilidad DoS en el servicio Avahi, pero se puede ver que Debian no es vulnerable a este ataque