Escanear puertos con nmap

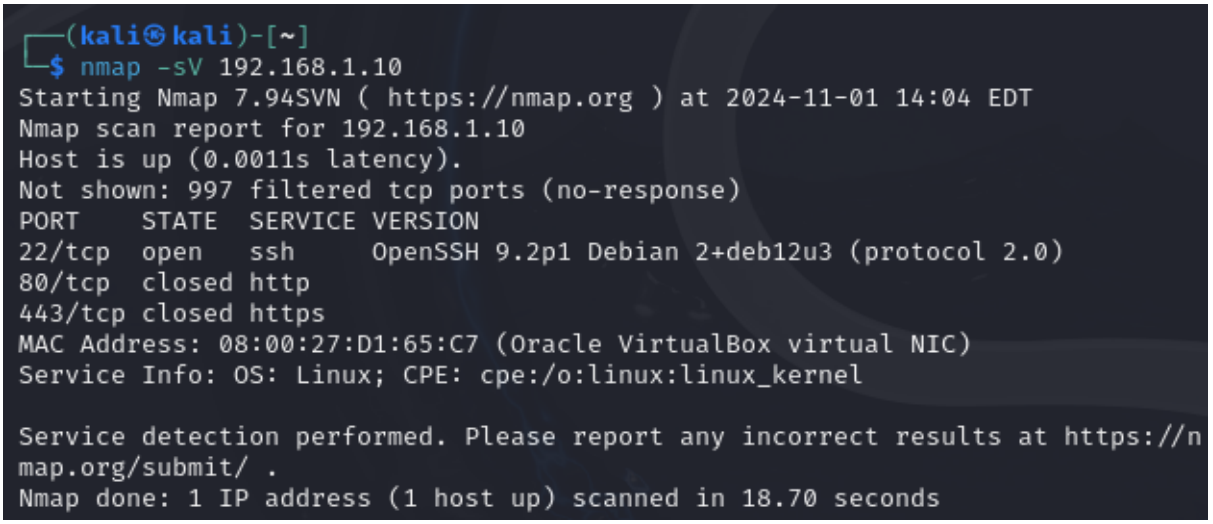
En esta práctica realizaremos un escaner de puertos desde nuestra máquina Kali a la máquina Debian.

Los resultados obtenidos del escaner son:

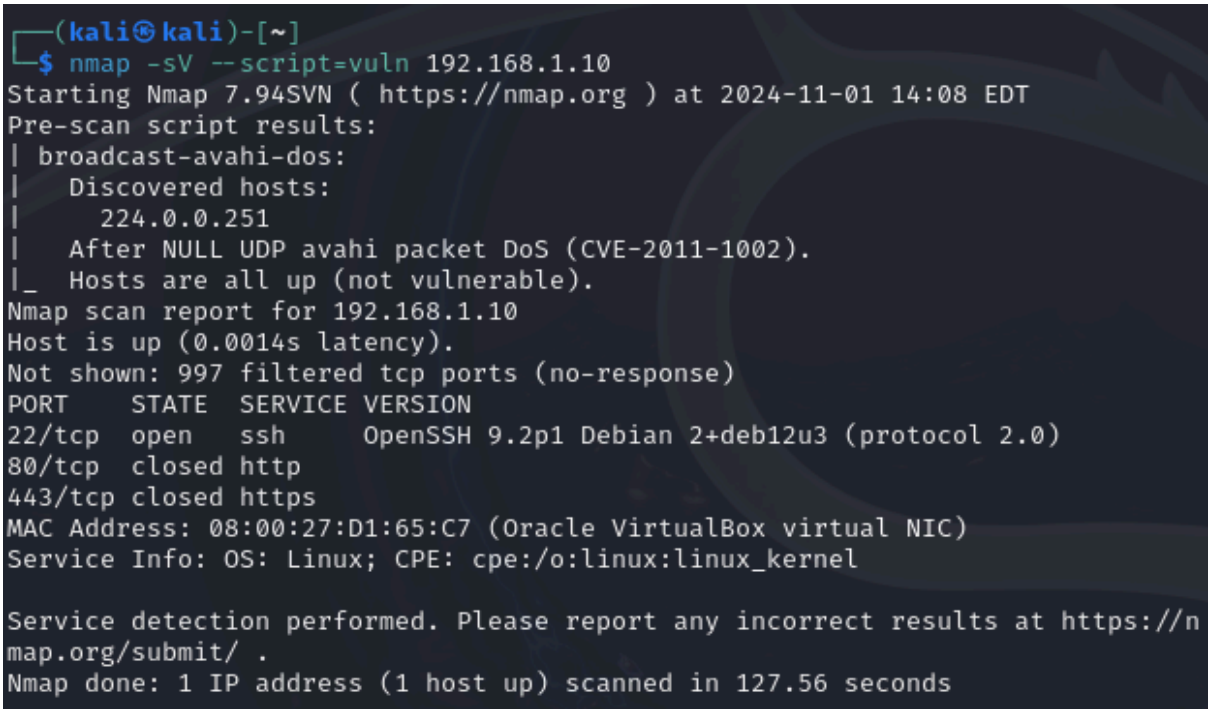
Puerto	Servicio	Versión	Vulnerabilidad	Descripción	Referencia
22	ssh	OpenSSH 9.2p1	CVE-2024-6387	Administración de algunas señales de forma insegura **Solución:** Actualizar a la versión 9.8	https://www.cvedetails.com/cve/CVE-2024-6387/
80	http	N/A (puerto cerrado)	N/A (puerto cerrado)	N/A (puerto cerrado)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



- Escaneo detallado y búsqueda de vulnerabilidades:



En esta imagen podemos observar dos aspectos relevantes:

1. Hay 997 puertos filtrados en la máquina Debian. La mayoria de puertos estan 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