

# ESCANEO DE PUERTOS CON NMAP DESDE UNA VM KALI A UNA VM DEBIAN

En la siguiente práctica se realiza una búsqueda de puertos abiertos, los servicios que dirigen y las vulnerabilidades de los mismos mediante la herramienta Nmap desde un dispositivo Kali a un dispositivo Debian. Para ello se introducen los siguientes comandos en la terminal de Nmap con dirección IP de la maquina Debian con el fin de extraer dicha información.

- ```
(kali㉿kali)-[~]  
└─$ sudo nmap -sV xxx.xxx.x.xx
```

El siguiente escaneo revela información de los puertos abiertos, el protocolo y el servicio, así como su versión: 80/tcp http Apache httpd 2.4.62 ((Debian))

Por otra parte nos indica la dirección MAC de la terminal, que la misma procede de VirtualBox y el tiempo de latencia.

- ```
(kali㉿kali)-[~]  
└─$ sudo nmap -f -sV --script=vuln xxx.xxx.x.xx
```

Gracias a este script además de la información anterior nos da información alojada en el servidor Apache, en el cual hay una cuenta de Wordpress. (no menciona versión).

PUERTO	SERVICIO	VERSIÓN	CVE	DESCRIPCIÓN	REFERENCIA
80/tcp	HTTP	Apache 2.4.62	No detectadas	No se encontraron vulnerabilidades	<a href="#">NVD Apache 2.4.62</a>

Tras realizar escaneos y consultar las bases de datos pertinentes se puede atestiguar que a fecha de este informe no consta ninguna vulnerabilidad en el servicio Apache, ya que los CVE de las versiones anteriores han sido corregidas en la actual versión Apache 2.4.62.