

REPORTE DE VULNERABILIDADES CON NMAP

Para este ejercicio se hizo un escaneo de puertos con versiones mediante la herramienta nmap. Se utilizaron dos sistemas operativos Linux diferentes, el primero Debían 12 que se usó como la máquina atacada y Kali linux como la máquina atacante. Ambas máquinas se encuentran virtualizadas con el software Virtualbox instalado en un computador Windows 11.

Antes de usar el comando de Nmap, fue necesario configurar las máquinas para que se conectaran a una red NAT. Se realizó una prueba ping del atacante (Kali Linux) al atacado (Debían 12), con resultado exitoso, encontrando que era posible un escaneo mediante nmap. Por lo cual se ejecutó el primer comando “nmap -sV 10.0.2.4” (Ver imagen 1) el cual permite recolectar información de los puertos abiertos y versiones de los mismos. Se encuentra que el único puerto abierto es el 80 tcp con versión apache httpd 2.4.62, que nos permite alojar servicios web http, este puerto es un objetivo común para los ciberdelincuentes de acuerdo a que el tráfico de este no está cifrado.

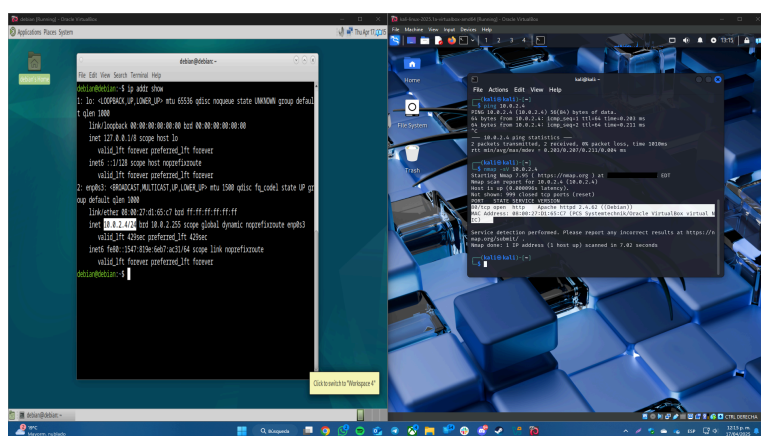


Imagen 1. Escaneo de puerto y versiones con nmap.

El segundo comando que fue ejecutado fue “nmap -sV --script=vuln 10.0.2.4”, este permite ejecutar los scripts de NSE (Nmap Scripting Engine) de la categoría vuln, otorgando vulnerabilidades conocidas para las versiones de los puertos encontrados, para el caso práctico de este ejercicio, no se encontraron vulnerabilidades conocidas para el puerto 80 con la versión de apache httpd 2.4.62 (ver imagen 2).

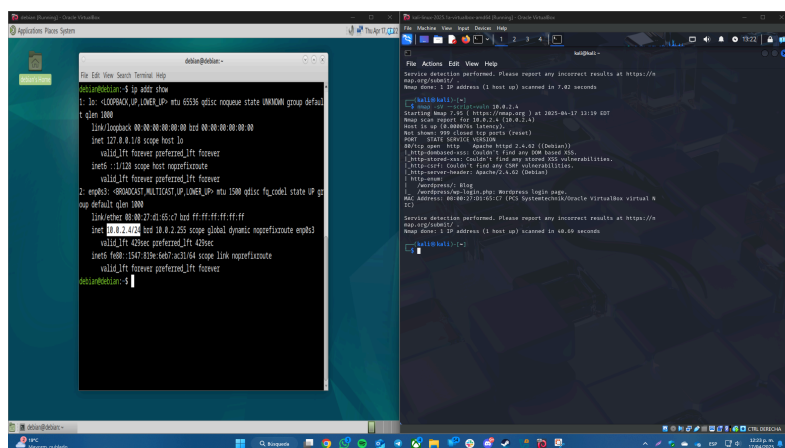


Imagen 2. Ejecución comando nmap con scripts de NSE.

Se consultó en diferentes bases de datos de vulnerabilidades la versión de servicio apache, pero de momento no se han encontrado vulnerabilidades reportadas en las siguientes bases de datos.

- CVE details <https://www.cvedetails.com/>

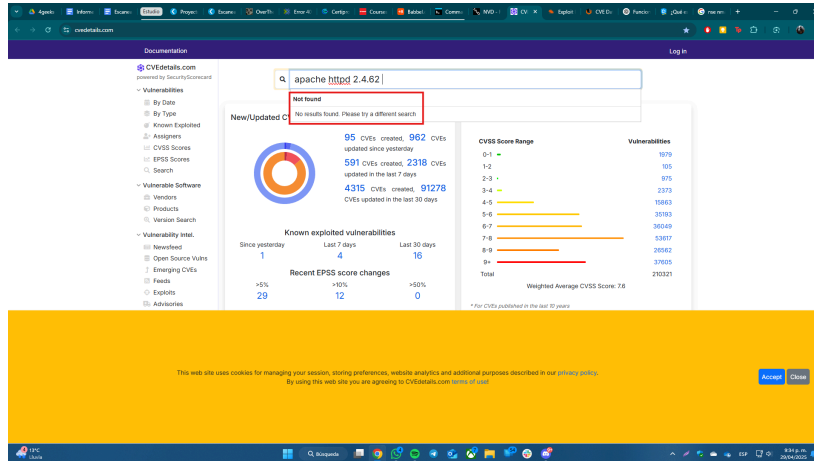


Imagen 3. CVE details

- NIST (National institute of standards and technology) <https://nvd.nist.gov/>

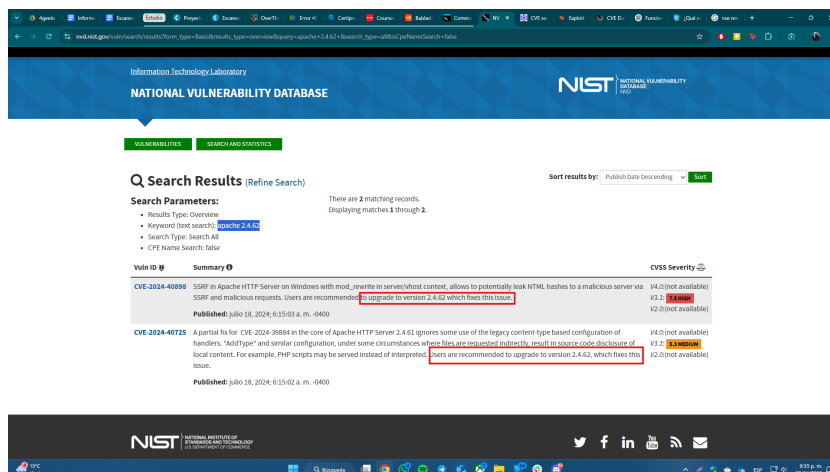


Imagen 4. NIST

- Exploit Database <https://www.exploit-db.com/google-hacking-database>

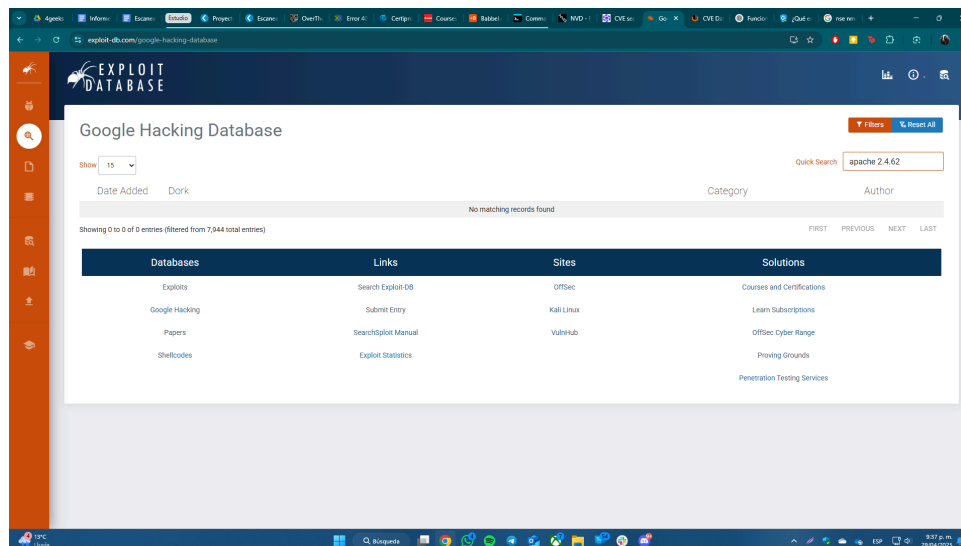


Imagen 5. Exploit database

Conclusión

El puerto 80 se encuentra abierto y ejecuta el servicio Apache httpd versión 2.4.62. Según los resultados obtenidos mediante nmap --script=vuln, no se han identificado vulnerabilidades conocidas asociadas a esta versión en las bases de datos de seguridad consultadas por Nmap.

Esto indica que, al momento del análisis, el servicio web no presenta vulnerabilidades reportadas públicamente que puedan ser explotadas directamente.