INFORME DE ESCANEO DE RED CON NMAP

REALIZADO POR: Pablo García Torres

FECHA: 18 de febrero de 2025

OBJETIVO: Se realizará escaneo de una máquina Debian (IP: 10.0.2.15/24) para identificar puertos abiertos, servicios activos y posibles vulnerabilidades.

INTRODUCCIÓN:

En el presente informe, se va a documentar el escaneo realizado a una máquina Debian, con el objetivo de localizar puertos y servicio abiertos, y posibles vulnerabilidades de seguridad, que podrían exponer la integridad y confidencialidad de los datos de la organización

Par realiza este proceso, hemo utilizado el software “NMAP”, versión 7.95. NMAP es una herramienta de código abierto diseñada para exploración de red y auditoría de seguridad.

METODOLOGÍA UTILIZADA:

☑ Comandos utilizados:

- Nmap -sV 10.0.2.15
- Nmap -sV –script=vuln 10.0.2.15

☑ Tipo de escaneo realizado:

- Detección de versiones de servicios (-sV)
- Detección de vulnerabilidades conocidas en un sistema o red (--scritp=vuln).

RESULTADOS DEL ESCANEO:

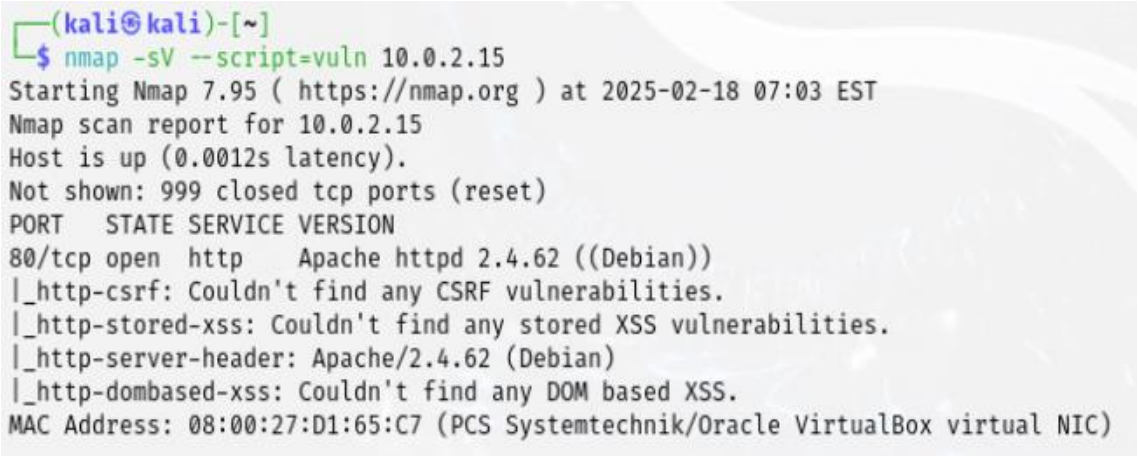
➔ Se realiza el escaneo sobre la IP 10.0.2.15.

➔ Se encuentra abierto el puerto 80/tcp, correspondiente al servidor Apache versión 2.4.62, en el sistema operativo Debian.

ANALISIS DE RESULTADOS:

Tras realizar el escaneo, se localiza abierto el puerto 80 TCP correspondiente con el servicio HTTP, donde se encuentra corriendo el servidor Apache con versión 2.4.62, correspondiente a una máquina Debian.

No se encuentra ninguna vulnerabilidad en el sistema.



CONCLUSIONES:

Tras analizado de los puertos, no se localizan vulnerabilidades activas, pero si se recomienda la eliminación de la cabecera “Server” (http-server-header), puesto no previene los ataques por completo, pero sí puede dificultar el reconocimiento de vulnerabilidades por parte de los atacantes.