Karolina Gucko 20/10/2024

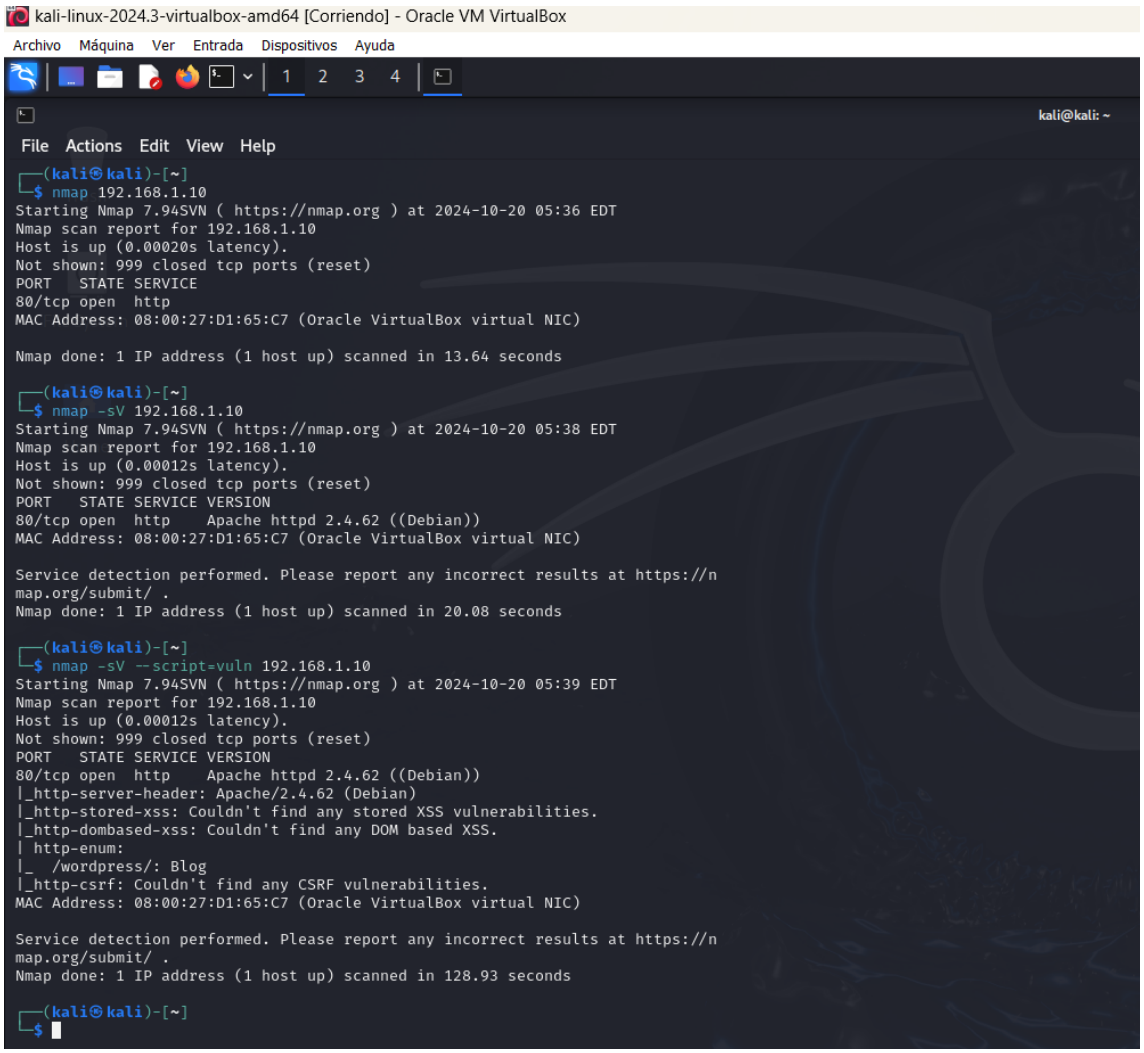
Informe de vulnerabilidades asociadas con servicios detectados usando Nmap

Introducción: Este informe documenta las vulnerabilidades asociadas con los servicios detectados en un sistema objetivo (máquina Debian) mediante el uso de Nmap. El escaneo se llevó a cabo desde una máquina Kali, identificando los hosts activos, los puertos abiertos, los servicios en ejecución, y sus versiones. Posteriormente, se investigaron las vulnerabilidades públicas asociadas.

Comandos Nmap utilizados:

nmap <IP_debian>
nmap -sV <IP_debian>
nmap -sV --script=vuln <IP_debian>

Resultados del escaneo: Se detectaron los siguientes puertos, servicios y versiones en la máquina objetivo: **Puerto: 80, Servicio: http, Versión: Apache httpd 2.4.62 (Debian)**



Estado de vulnerabilidades para Apache HTTP Server 2.4.62

Apache HTTP Server 2.4.62 no tiene vulnerabilidades listadas en las bases de datos públicas (p.ej. CVE Details, NVD, Exploit database). Además, en la salida del comando **nmap -sV --script=vuln <IP_debian>** se intentaron encontrar vulnerabilidades asociadas con servicios web, pero sin éxito.

Conclusión

Todas las fuentes públicas revisadas y el comando nmap -sV --script=vuln <IP_debian> coinciden en que Apache HTTP Server 2.4.62 no presenta vulnerabilidades registradas hasta la fecha. Esto sugiere que es una versión segura y actualizada en comparación con versiones anteriores que sí tenían vulnerabilidades.

Es importante seguir las mejores prácticas de seguridad y aplicar actualizaciones cuando sea necesario, incluso si una versión específica no tiene vulnerabilidades conocidas, ya que pueden surgir nuevas vulnerabilidades con el tiempo.