Reporte de Vulnerabilidades

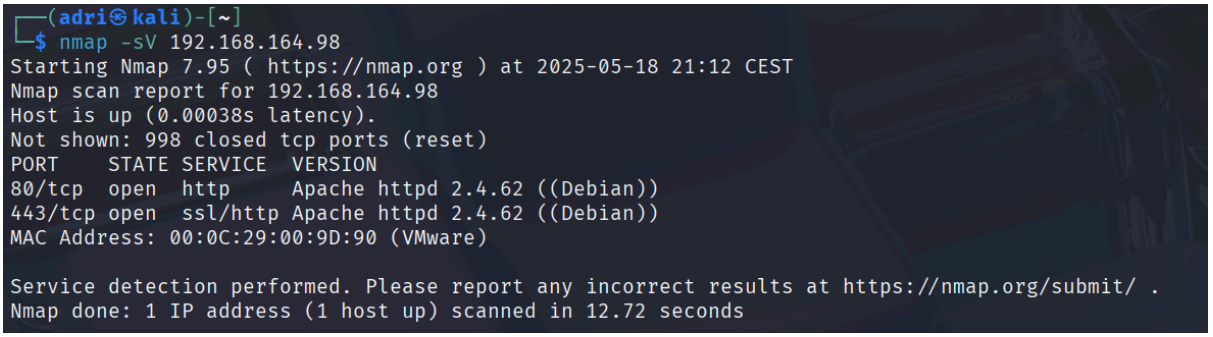
Fecha: 18/05/2025
Atacante: 192.168.164.133 (*Máquina Virtual Kali Linux*)
Defensor: 192.168.164.98 (*Máquina Virtual Debian 12*)

Introducción

En esta tarea se nos pide realizar un escaneo profundo a nuestro objetivo usando la herramienta ***nmap***, para luego comparar y analizar las vulnerabilidades resultantes con distintas fuentes de bases de datos públicas de vulnerabilidades como **NVD** (National Vulnerability Database), **CVE Details** y **Vulners**.
Para ello damos uso de otra máquina virtual, *Kali Linux*, que será la máquina desde la que lanzaremos los escáneres.

Hallazgos Detectados

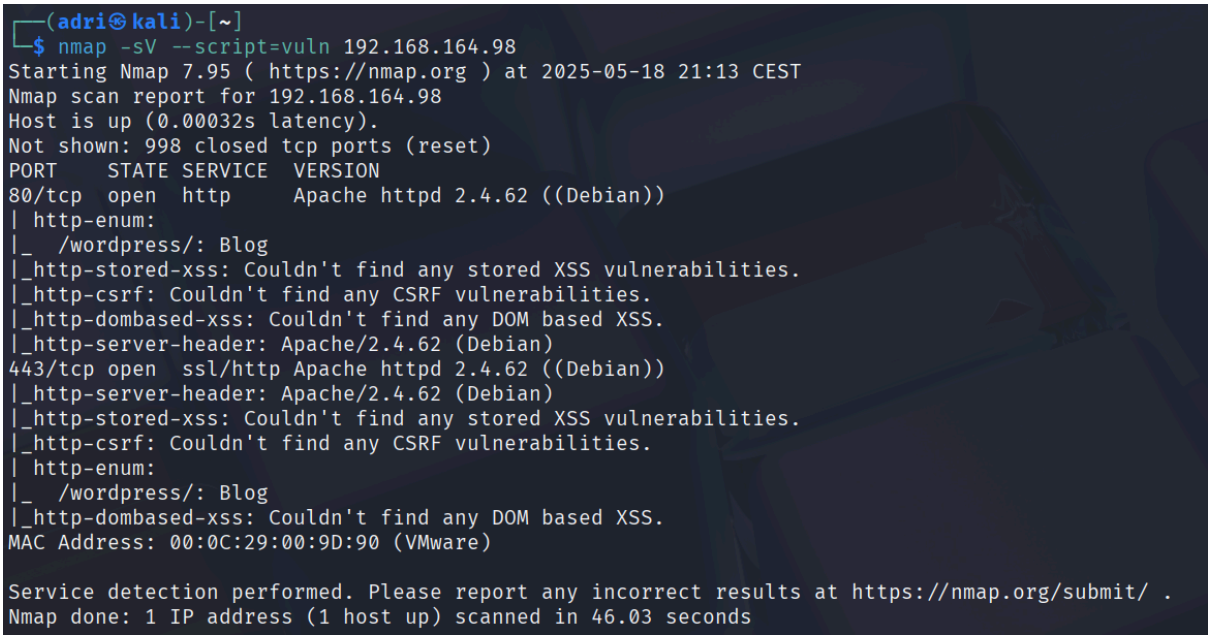
Empezamos el escaneo de vulnerabilidades usando el comando ***nmap -sV <IP_Defensor>*** para saber así que puertos están abiertos y la versión de los servicios que operan en ellos.



Como se ve en la captura de pantalla, la máquina defensora tiene únicamente 2 puertos abiertos; el 80 y el 443. A continuación una cuadrícula con una mejor interpretación de los resultados:

Puerto	Servicio	Versión	Detalles
80/tcp	*HTTP*	*Apache 2.4.62 (Debian)*	*WordPress detectado (/wordpress)*
443/tcp	*HTTPS*	*Apache 2.4.62 (Debian)*	*WordPress detectado (/wordpress)*

Una vez sabiendo que puertos hay y los servicios que tienen, es hora de pasar a la **identificación de vulnerabilidades**. Para ellos usamos el comando ***nmap -sV –script=vuln <IP_Defensor>***, que se encarga de ejecutar scripts de detección de vulnerabilidades que Nmap ya tiene incorporados para encontrar posibles vulnerabilidades de nuestros puertos. Estos son los resultados:



1. **Apache 2.4.62**
   Actualmente Apache cuenta ya con una versión más moderna (Apache 2.4.63). A pesar de no ser una diferencia muy grande entre versiones, puede ser que se haya encontrado una o más vulnerabilidades en la versión 2.4.62 (la que tenemos actualmente).

2. **WordPress Expuesto**
   Hay que tener en cuenta que la gran mayoría de vulnerabilidades en WordPress provienen de plugins desactualizados/obsoletos. Es por esto mismo que mantenerlos *up to date* es vital en WordPress. Un ejemplo de lo dicho es la siguiente vulnerabilidad encontrada recientemente en ***National Vulnerability Database (NVD)***.
   Esta trata sobre el plugin **NinjaForms** para **versiones anteriores a la 3.10.1**. Explicado de forma rápida; es una falla que permite al administrador inyectar código malicioso (Cross Site Scripting XSS) en los ajustes del plugin, incluso cuando WordPress les bloquea hacerlo normalmente. Como consecuencias, el administrador puede robar cookies (información sensible del usuario) y/ redirigirlo a enlaces maliciosos para sacar aún más beneficio.

Conclusión

Basándonos en los resultados del **nmap**, nos damos cuenta de que, a priori, **no existe una vulnerabilidad crítica evidente**. De hecho, según el comando nmap con ***–script=vuln***, nuestra máquina no cuenta con ninguna vulnerabilidad.
Sin embargo, es cierto que tenemos potenciales amenazas como una versión menos de la actual, y con la exposición de WordPress.
En conclusión, manteniendo tanto Apache como los plugins de WordPress actualizados, no debería haber ninguna preocupación.