Cuanto más se conozca el sistema o la red de destino, más opciones se tendrán. Para buscar vulnerabilidades de manera automática con nmap, se utiliza el siguiente comando:

sudo nmap -A -v -T4 —script=vuln IP/Mask

-A: Identificar el dispositivo y sus versiones

-v: Verbosidad

T4: Escaneo Agresivo

—script=vuln: Es la categoría para identificar vulnerabilidades

No busca vulnerabilidades

nmap no es una herramienta especializada para el análisis de vulnerabilidades, solo se usan los script para detectar p ver si tiene vulnerabilidades 💡

Sintaxis

—script=categoría

Ejemplo

—script=vuln

Vulnerabilidades con NMAP

Nmap además de servirnos para analizar y escanear información, nos ayuda a buscar vulnerabilidades, es decir, que esta herramienta puede emplearse para la fase 1 y 2 del ciclo del pentesting.

Ahora bien, a pesar de no ser una herramienta especializada en el análisis de vulnerabilidades, sí que nos permite obtener información valiosa y de calidad que podemos triangular o falsear con la provista por otras herramientas especializadas.

*Usé mi laboratorio diseñado en el curso de fundamentos de pentesting para ejecutar el análisis de vulnerabilidades, ya que la máquina de metasploitable nos permite ver información útil para el aprendizaje que de otra forma no obtendríamos de máquinas menos vulnerables.*

Nmap as vuln searcher.png