NMAP es la abreviatura de Network Mapper siendo así una herramienta gratuita ya que es de código abierto para la exploración de vulnerabilidades y la detección de redes

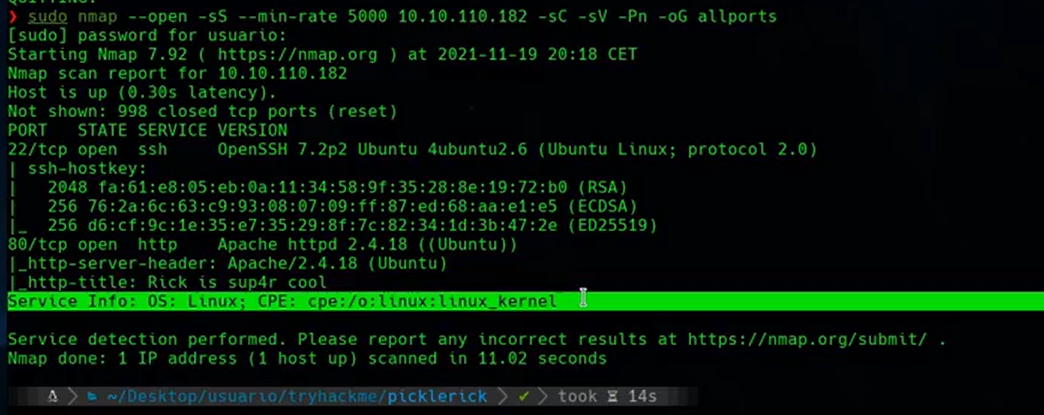
Los administradores de red utilizan nmap para identificar que dispositivos se están ejecutando en sus sistemas, descubrir hosts y los servicios que ofrecen también encontrar puertos abiertos y detectar riesgos de seguridad, también se puede utilizar para monitorear hosts individuales, así como redes extensas que abarcan cientos de miles de dispositivos

Aunque ha aumentado a lo largo de los años y es extremadamente flexible, en el fondo es una herramienta de escaneo de puertos que recopila información enviando paquetes sin procesar a los puertos del sistema. Escucha y determina si los puertos están abiertos o cerrados

Usa distintos protocolos como TCP, UDP, SCTP o ICMP para saber que puertos hay abiertos o cerrados

Podemos usar zenmap que es lo mismo que nmap pero representado de forma grafica en vez de terminal, para mi me gusta mas en terminal pero eso según gustos

Ejemplo de nmap



sudo nmap –open -sS –min-rate 5000 10.10.110.182 -sC -sV -oG allports

--open: sirve para identificar que solo muestre los puertos abiertos

-sS: Analisis TCP SYN

--min-rate 5000: Enviar paquetes no mas lentos que 5000 paquetes por segundo

10.10.110.182: IP de la máquina, en mi caso es la ip de una máquina de tryhackme

-sC: Analisis por los script por defecto

-sV: Detecta que versión del servicio activo

-oG allports: la salida la guarda en un archivo grepeable, en este caso es allports