NMAP en Kali Linux

Contexto:

El escenario se encuentra compuesto por un Cliente Windows 10 y un agente de amenaza Kali Linux.

Vamos a ejecutar los comandos básicos de nmap para escanear los puertos de Windows 10 (en este caso el Fiewall de Windows se encuentra deshabilitado).

1. Descargamos una máquina virtual preparada para Virtual Box.

2. Validamos la versión de Nmap instalado

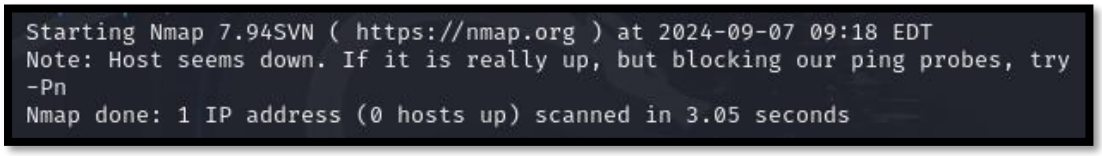
Comando: nmap -V

Resultado:

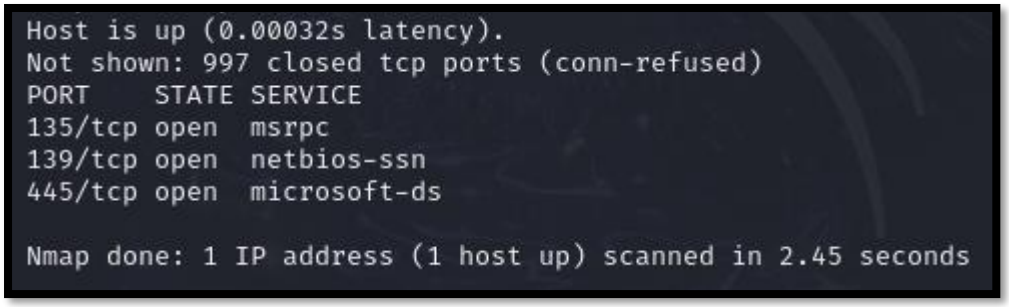

3. Utilizamos el comando básico

Comando: nmap <IP>

Resultado: El host parece estar apagado. Recomienda utilizar "-Pn"



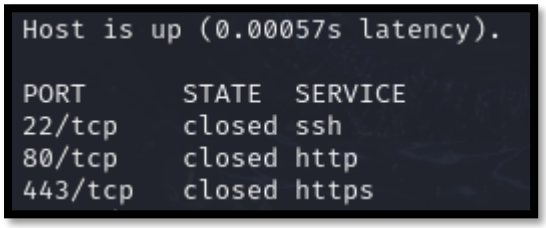

Análisis: Esto pasa porque Windows tiene el Firewall activo y Nmap intenta realizar un ping y lo bloquea.




Conclusión: Al utilizar "nmap -Pn <IP>" nos muestra los puertos, estado y servicios activos.

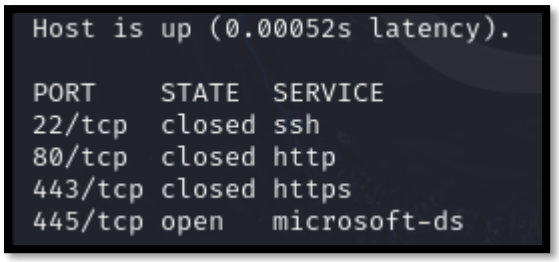
4. Escaneo de puertos específicos

Comando: nmap -p 22,80,443 <IP>




Conclusión: Aquí deshabilitamos el Firewall de Windows para visualizar los puertos especificados.

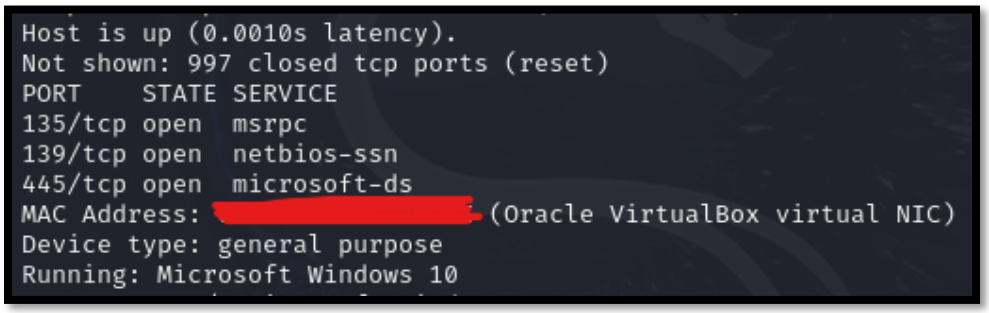
Comando: nmap -p 22,80,443,445 <IP>




Conclusión: Aquí agregamos el puerto 445 para visualizar el estado “open”.

5. Detección de Sistema Operativo

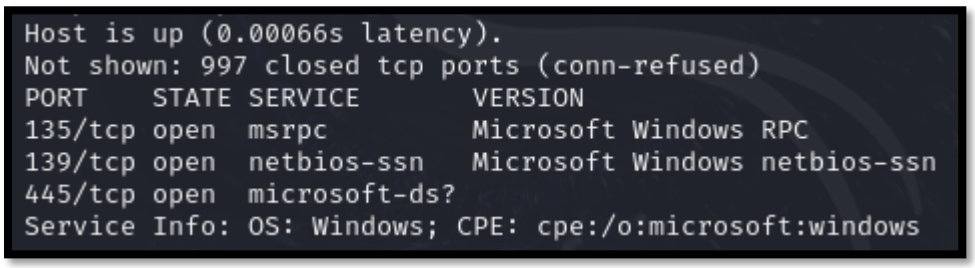
Comando: sudo nmap -O <IP>




Conclusión: Al ejecutar el comando también se visualiza los puertos, MAC Address y el SO. que se encuentra iniciado en el Cliente.

6. Detección de versión de servicios

Comando: nmap -sV <IP>




Conclusión: Agregamos “-sV” para visualizar la versión de los servicios. Esto implica más información para el agente de amenaza.