12/11/25

Laboratorio de Reconocimiento de Red

Redes de computadoras II

Alumno: Jared López Toledo
Profesor: Ing. Carlos Mijangos Jiménez

Índice

Análisis de red con Nmap y Wireshark

Introducción:

En el ámbito de la ciberseguridad, es fundamental comprender tanto las metodologías de ataque como las de defensa. Esta práctica se realiza en un **"sandbox"** (un entorno controlado y seguro) para simular un escenario de auditoría de red sin riesgos, ético y con fines educativos.

El objetivo es utilizar dos técnicas complementarias:

1. **Escaneo Activo:** Se utiliza **Nmap** para enviar paquetes a la red y "preguntar" activamente qué hosts están vivos y qué servicios (puertos) están ejecutando.
2. **Monitoreo Pasivo:** Se utiliza **Wireshark** para "escuchar" (sniffar) pasivamente el tráfico de la red, permitiéndonos analizar la huella que deja nuestro ataque y detectar comportamientos anómalos.

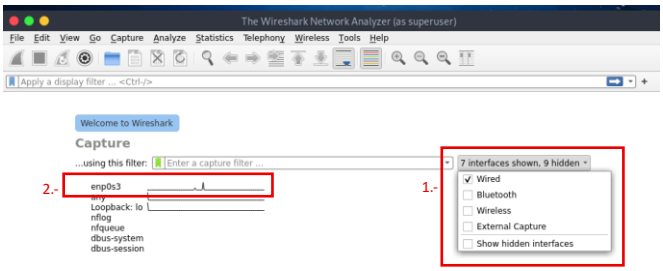
El laboratorio consiste en un hipervisor (VirtualBox), una máquina atacante (ParrotOS) y una máquina víctima (Windows 11) que ejecuta servicios web (XAMPP).

Desarrollo:

Cómo usar WireShark:

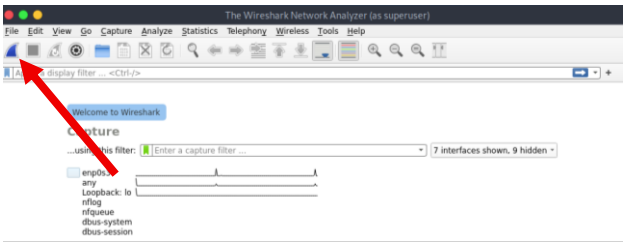
Una vez lanzada nuestra aplicación, para enfocarnos en sniffar la red:

1.- Dejaremos seleccionados solo Wired.
2.- Seleccionamos nuestra interfaz de red, en este caso “enp0s3”.



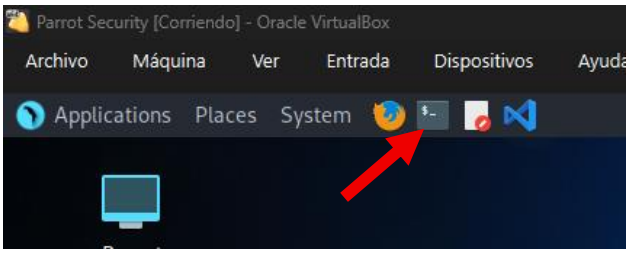
Comenzar la captura de paquetes (***justo antes de lanzar nuestro escaneo con Nmap***):

Para comenzar la captura de paquetes hacemos clic en el botón de aleta de tiburón:



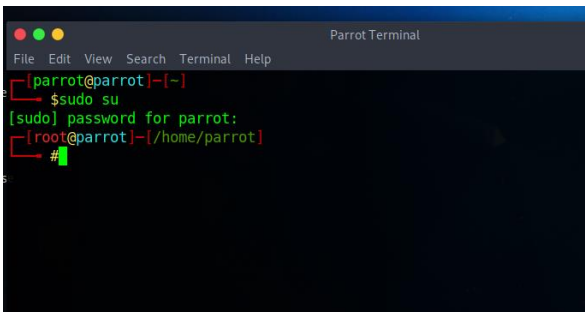
Cómo usar NMAP:

Para usar NMAP vamos a nuestra terminal, que la podemos ubicar en la barra de tareas de la parte superior:



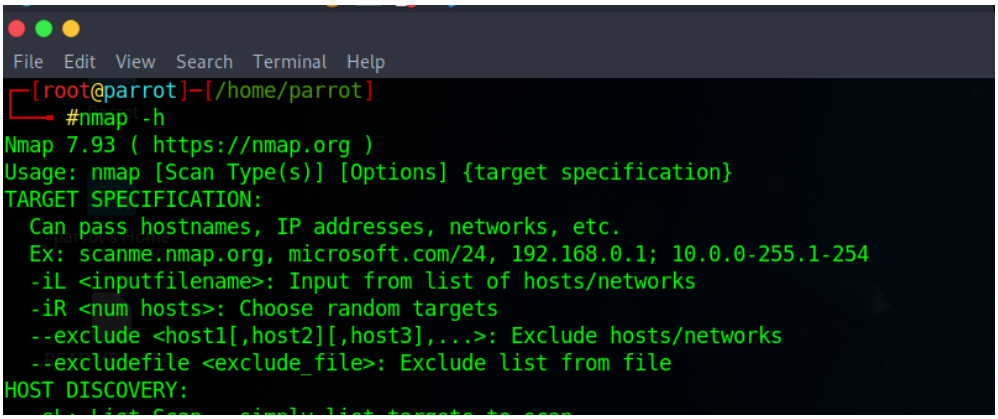
(Barra de tareas del escritorio de ParrotOS, mostrando el icono de la terminal que se utiliza para lanzar los comandos de Nmap).

Ejecutamos el comando "*sudo su*" para ingresar al modo superusuario y a continuación ingresamos nuestra contraseña.



(Es normal que no muestre la contraseña al ingresarla en nuestra terminal)

Para comenzar a usar Nmap, podemos primero ejecuta el comando "*nmap -h*" que nos muestra un resumen de cómo podemos usar la herramienta.



Para escanear una red con Nmap en un rango determinado, puedes utilizar varias sintaxis según el tipo de rango que desees abarcar. Si deseas escanear un rango específico de direcciones IP, como de 192.168.0.1 a 192.168.0.50, puedes usar la siguiente sintaxis:
nmap 192.168.0.1-50

Este comando escaneará todos los hosts dentro del rango especificado y mostrará información sobre los puertos abiertos, cerrados o filtrados en cada dispositivo activo. Para escanear un rango más amplio, como de *186.33.200 a 220* en el tercer octeto y de 80 a 120 en el cuarto octeto, se puede usar:
nmap 186.33.200-220.80-120

Este tipo de escaneo puede tardar considerablemente, especialmente en redes grandes. Alternativamente, si deseas escanear todos los hosts de una subred completa, como una red Clase C con la máscara 255.255.255.0, puedes usar la notación CIDR:
nmap 192.168.0.0/24

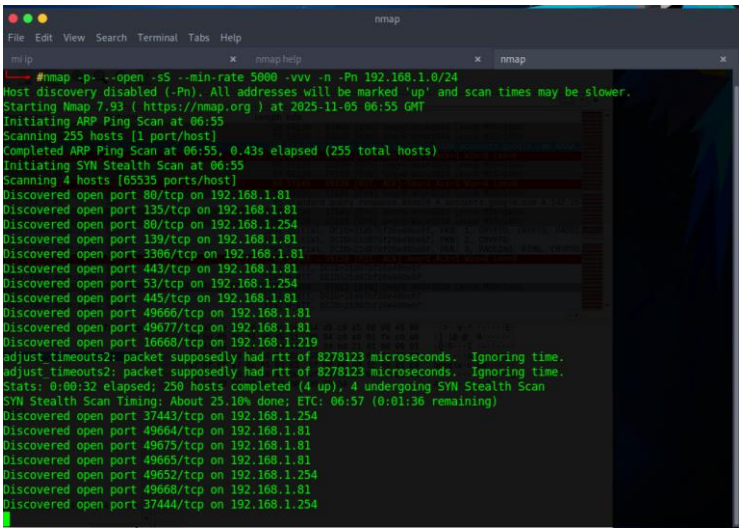
Este comando escanea todas las direcciones IP desde 192.168.0.0 hasta 192.168.0.255. También puedes usar el asterisco como comodín para escanear todo un octeto, por ejemplo: *nmap 192.168.0.**
Aunque esta opción puede generar procesos largos en redes grandes, por lo que se recomienda ajustarla según la capacidad y la ventana de pruebas. Además, puedes combinar rangos y direcciones individuales en un archivo de entrada y usar la opción

-iL para procesarlos línea por línea.

En este caso se utilizará una combinación de flags que me permitirán hacer un escaneo más rápido y agresivo, suponiendo que aún no tenemos un target especifico en la red que estamos analizando.

Comando: *nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 192.168.1.0/24*

Nota: *Para definir nuestro rango de ip's podemos ejecutar "ifconfig" en nuestra terminal de Linux y ver la ip que está asignada a nuestra interfaz de red, por ejemplo: "192.168.**0**.#" ó "192.168.**1**.#"*



Flags individuales:

- -p-: Escanea **todos los puertos** (1-65535)
- --open: Muestra **solo los puertos abiertos**, omite los filtrados/cerrados
- -sS: **TCP SYN scan** - Escaneo sigiloso que no completa la conexión TCP
- --min-rate 5000: Envía **mínimo 5000 paquetes por segundo** (escaneo rápido)
- -vvv: **Triple verbose** - Muestra información muy detallada del progreso
- -n: **Sin resolución DNS** - No resuelve nombres de dominio
- -Pn: **Sin descubrimiento de hosts** - Asume que todos los hosts están activos

Dirección de red:

- 192.168.1.0/24: Escanea toda la red 192.168.1.1 - 192.168.1.254

¿Qué hace todo junto?

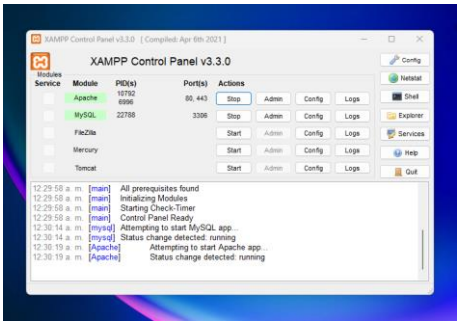
Escanea rápidamente todos los puertos de todos los equipos en la red 192.168.1.0/24 usando técnicas agresivas y muestra solo los puertos que están realmente abiertos.

Resultados:

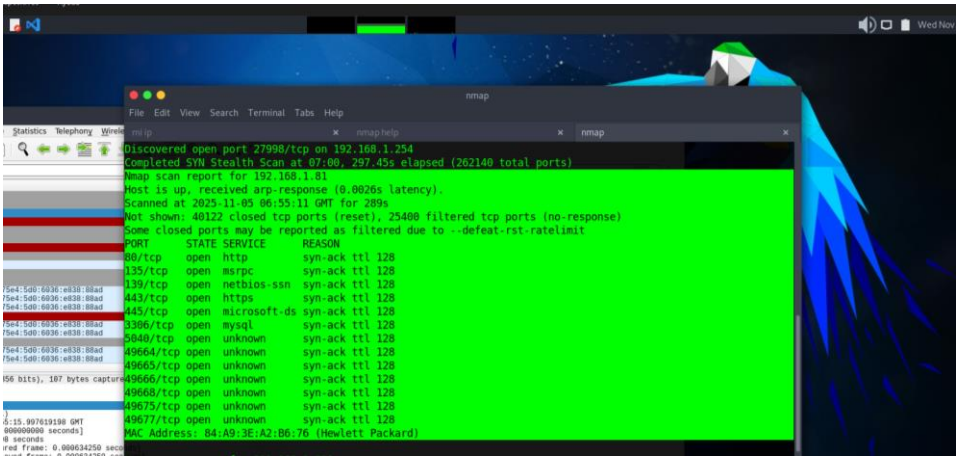
Al finalizar, mostrará los resultados de cada cliente conectado según lo que haya encontrado.

Lo que nos interesa en este caso, fue detectar los puertos que abrimos con XAMPP en nuestro equipo con Windows.

Resultados obtenidos del escaneo con Nmap:



(Captura de la aplicación XAMPP ejecutándose).

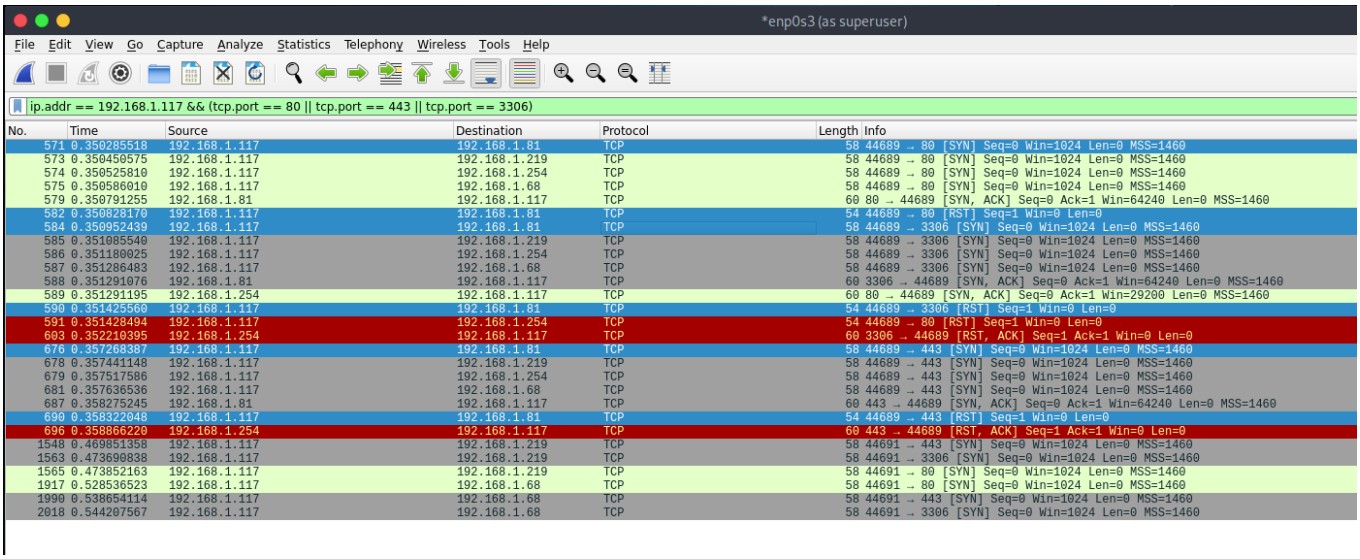


(Resultados del escaneo con Nmap).

En nuestro caso, al estar aplicando esta práctica en un entorno controlado, podemos conocer la ip de nuestra máquina victima (Windows) con el comando “ipconfig” en nuestra terminal y confirmar los resultados obtenidos.

Resultados de la intercepción de paquetes en Wireshark:

una vez finalizado el escaneo con Nmap, detuvimos la intercepción de paquetes y posteriormente aplicamos el filtro: *ip.addr == [IP_PARROT_Sin_corchetes] && (tcp.port == 80 || tcp.port == 443 || tcp.port == 3306)*



Conclusión:

Se cumplieron con éxito los objetivos de la práctica, logrando realizar una auditoría de ataque y defensa de forma simultánea.

Resultados Obtenidos (Ataque): El escaneo de **Nmap** fue exitoso. Se identificaron correctamente los servicios expuestos por XAMPP en la máquina víctima, incluyendo Apache (puertos 80 y 443) y MySQL (puerto 3306).

Análisis de Defensa (Wireshark): El uso de **Wireshark** demostró ser una medida de seguridad (Blue Team) altamente eficaz. Al capturar el tráfico *durante* el escaneo, se observó un flujo masivo de paquetes SYN. Este patrón es un **"comportamiento**

anómalo" evidente que permite a un analista de seguridad detectar un reconocimiento de red en tiempo real, cumpliendo el objetivo de la rúbrica.

Análisis de Sigilo (Nmap): En cuanto al objetivo de "medidas para no ser detectado", el comando nmap --min-rate 5000 utilizado fue intencionalmente **extremadamente ruidoso** y fácil de detectar. Esta agresividad, si bien es rápida, es lo opuesto al sigilo. Una medida real para "no ser detectado" implicaría sacrificar la velocidad, utilizando *timings* más lentos (como nmap -T2 o -T1) para espaciar los paquetes y simular tráfico legítimo.

Referencias:

1. Shah, M., Ahmed, S., Saeed, K., Junaid, M., Khan, H., & Ata-ur-rehman. (2019). Penetration testing active reconnaissance phase – Optimized port scanning with nmap tool. En *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (IComET)*. IEEE. https://doi.org/10.1109/ICOMET.2019.8673520
2. Chowhan, S., & Saxena, A. K. (2024). Advanced techniques in network traffic analysis: Utilizing wireshark for in-depth live data packet inspection and information capture. En *2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI)*. IEEE. https://ieeexplore.ieee.org/document/10421631
3. Apache Friends. (2021). XAMPP Control Panel (Versión 3.3.0). [Software]. Recuperado de https://www.apachefriends.org
4. Insecure.Com LLC. (2025). Nmap (Network Mapper) (Versión 7.93). [Software]. Recuperado de https://nmap.org
5. Oracle Corporation. (2025). Oracle VM VirtualBox (Versión 7.2.4). [Software]. Recuperado de https://www.virtualbox.org
6. Parrot Security. (2025). ParrotOS Security Edition. [Sistema operativo]. Recuperado de https://parrotsec.org
7. The Wireshark Foundation. (2025). Wireshark (Versión 4.0.4). [Software]. Recuperado de https://www.wireshark.org