UNIVERSIDAD DEL ISTMO

UNISTMO TEHUANTEPEC

DOCENTE:

ING. CARLOS MIJANGOS.

ASIGNATURA:

REDES DE COMPUTADORAS II.

TEMA:

ANÁLISIS DE ESCANEOS Y MEDIDAS DEFENSIVAS

ALUMNOS:

JEOVANI PACHECO RUEDA

CARRERA:

INGENIERÍA EN COMPUTACIÓN.

GRUPO:

704.

SANTO DOMINGO TEHUANTEPEC, OAXACA; 20 DE OCTUBRE DE 2025.

Índice

1. Introducción

En el campo de la ciberseguridad, comprender cómo se comunican los sistemas y cómo se exponen sus servicios es esencial para proteger cualquier infraestructura digital. Antes de poder defender una red, es necesario conocerla a fondo: qué equipos la integran, qué servicios ofrecen y qué puertas de entrada pueden representar un riesgo. Este principio guía las auditorías de seguridad, donde las herramientas de escaneo y monitoreo se convierten en los ojos del analista.

El propósito de esta práctica fue explorar el funcionamiento y la eficacia de dos herramientas fundamentales en la auditoría de redes: Nmap (Network Mapper) [1] y Wireshark [2], aplicadas tanto desde una perspectiva ofensiva como defensiva. El ejercicio se desarrolló dentro de un entorno controlado o sandbox, lo que permitió simular ataques de reconocimiento de forma segura y luego observar sus efectos en tiempo real.

Nmap es una herramienta de código abierto ampliamente utilizada para el descubrimiento de hosts, servicios y puertos dentro de una red. Su capacidad para identificar sistemas operativos, versiones de software y configuraciones expuestas la convierte en un recurso esencial para evaluar la superficie de ataque y localizar posibles vulnerabilidades.

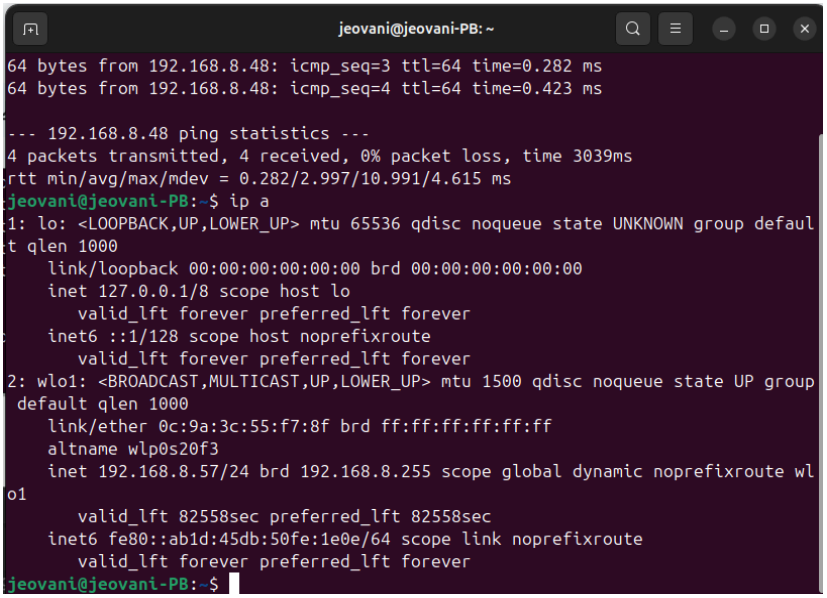
Por otro lado, Wireshark actúa como un microscopio del tráfico de red: un analizador de protocolos capaz de capturar, decodificar y examinar cada paquete que circula por una interfaz. Gracias a su nivel de detalle y a la potencia de sus filtros, permite detectar comportamientos anómalos, rastrear escaneos y correlacionar eventos sospechosos con su origen.

Para el correcto desarrollo de la práctica se requieren permisos administrativos, conectividad local y la configuración de la tarjeta de red en modo promiscuo, permitiendo la captura completa del tráfico entre los equipos del entorno de prueba. Con estas condiciones establecidas, el alumno pudo observar de forma práctica cómo las acciones de reconocimiento se reflejan en el tráfico de red y cómo una correcta monitorización puede servir como defensa temprana ante intentos de intrusión.

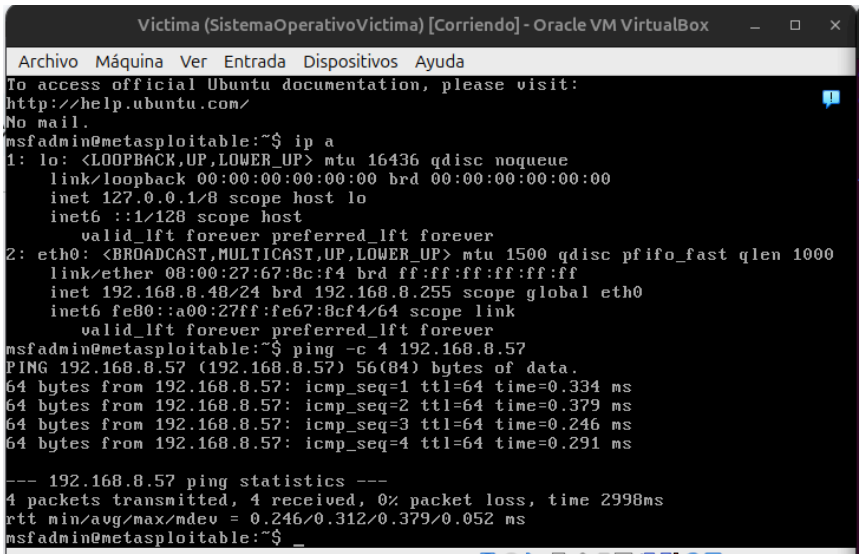
2. Creación del Sandbox

Para realizar la práctica de forma segura, se configuró un entorno controlado (sandbox) [3] dentro de una red local. Este espacio aislado permitió ejecutar escaneos sin afectar sistemas reales ni vulnerar políticas de red. Se utilizaron dos equipos: uno actuó como atacante con Nmap, y el otro como víctima y monitor de tráfico mediante Wireshark, ambos conectados bajo la misma subred.

IP ATACANTE: 192.168.8.57



IP VICTIMA: 192.168.8.48

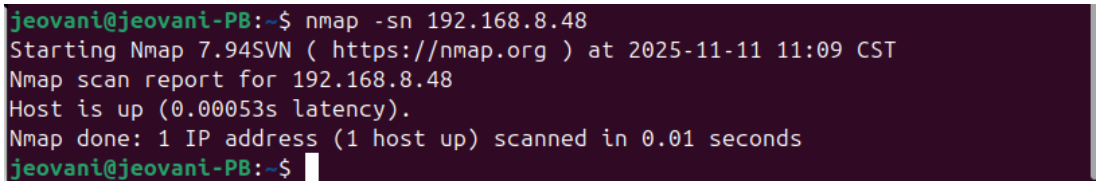


Comprobamos que ambos equipos están conectados, y permiten hacer ping entre ellos.

3. Escaneos con Nmap (Máquina Atacante).

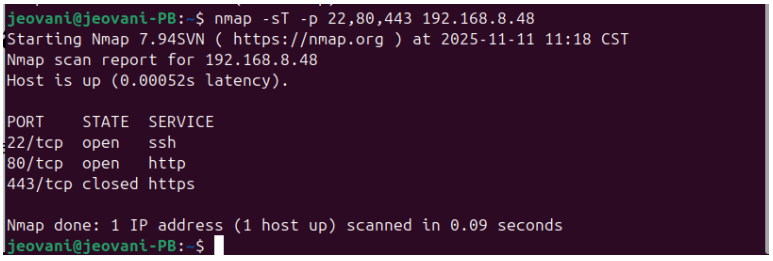
- **Ping scan:** Envía sondeo para ver qué hosts responden en la subred. No escanea puertos. Útil para saber qué máquinas están encendidas.

  cmd: nmap -sn 192.168.8.48



- **Escaneo TCP (Protocolo de Control de Transmisión):** Intenta completar la conexión TCP usando las llamadas normales del sistema operativo . Es más ruidoso que SYN [4] pero funciona sin privilegios y evita necesitar sudo.

  nmap -sT -p 22,80,443 192.168.8.48



- **Escaneo SYN:** Envía SYN y analiza respuestas sin completar el handshake [5]. Muy usado para descubrimiento rápido de puertos. Necesita permisos de root.

  sudo nmap -sS -p 1-1000 192.168.8.48

```
jeovani@jeovani-PB:~$ sudo nmap -sS -p 1-1000 192.168.8.48
[sudo] contraseña para jeovani:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-11 11:22 CST
Nmap scan report for 192.168.8.48
Host is up (0.00045s latency).
Not shown: 988 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
512/tcp open  exec
513/tcp open  login
514/tcp open  shell
MAC Address: 08:00:27:67:8C:F4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
jeovani@jeovani-PB:~$
```

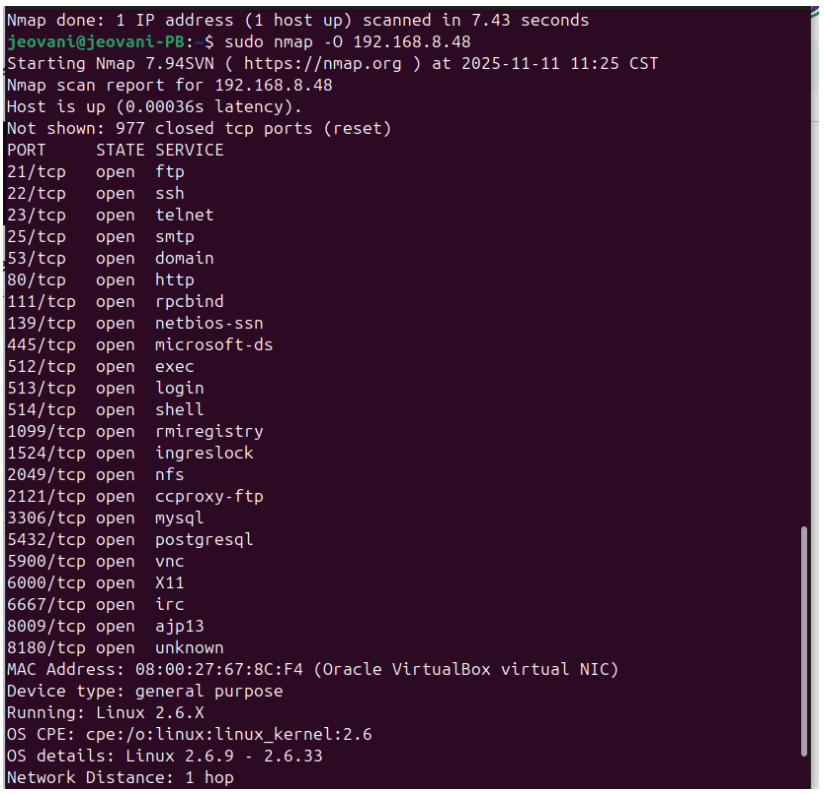
- **Detección de versión de servicio:** Intenta identificar software y versiones que corren en los puertos encontrados. Útil para inventario y para evaluar si hay servicios desactualizados.

  sudo nmap -sV -p 22,80 192.168.8.48

```
jeovani@jeovani-PB:~$ sudo nmap -sV -p 22,80 192.168.8.48
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-11 11:23 CST
Nmap scan report for 192.168.8.48
Host is up (0.00047s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 08:00:27:67:8C:F4 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.43 seconds
jeovani@jeovani-PB:~$
```

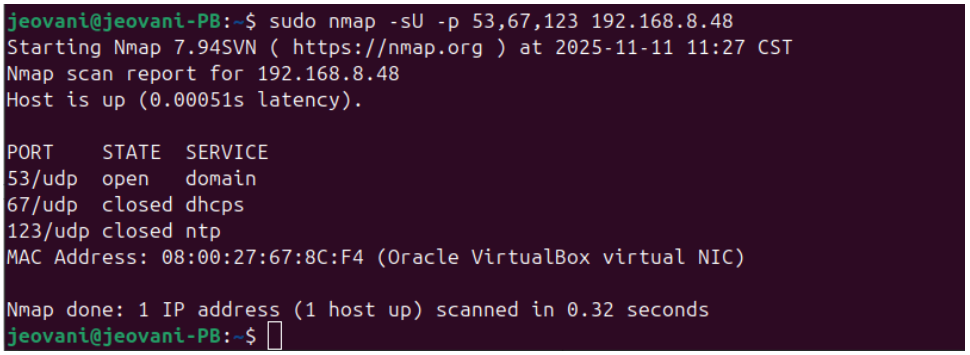
- **Detección de sistema operativo:** Recolecta huellas del stack TCP/IP para inferir el sistema operativo. No siempre es 100% fiable. Requiere permisos y genera tráfico que puede ser conspicuo.

  sudo nmap -O 192.168.8.48



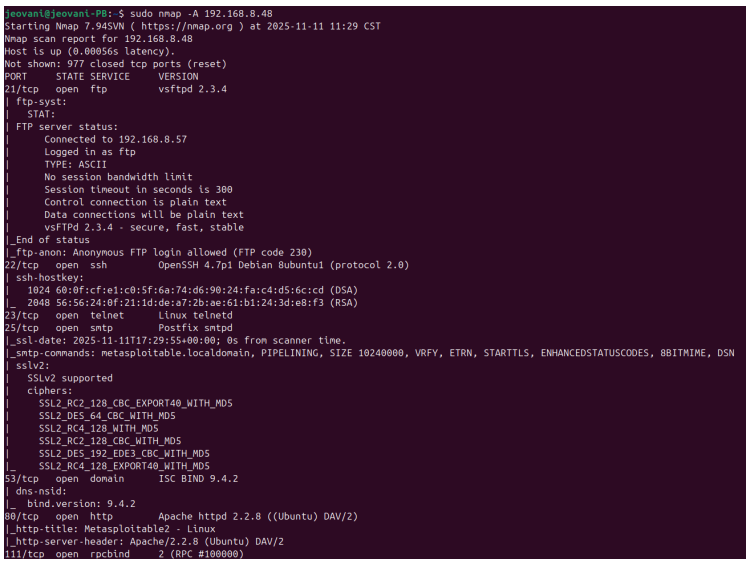
- **Escaneo UDP:** Prueba puertos UDP (DNS, DHCP, NTP). UDP es inherentemente más lento por retransmisiones y timeouts.

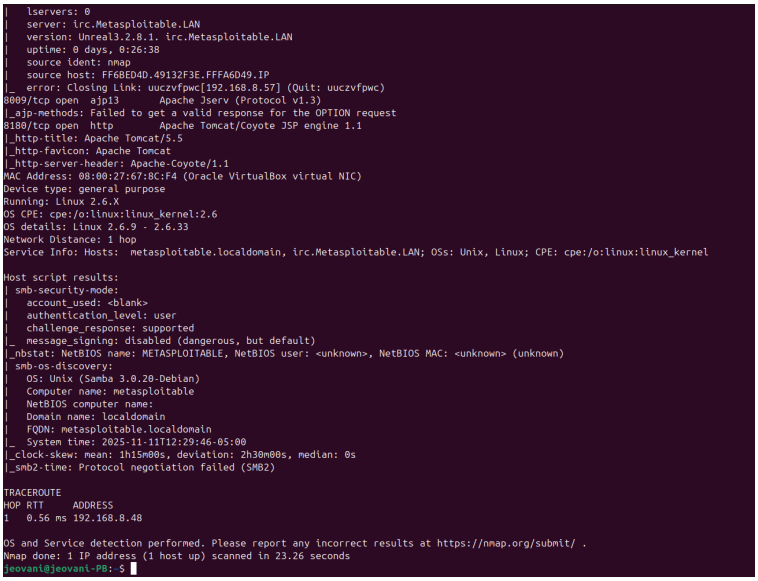
  sudo nmap -sU -p 53,67,123 192.168.8.48



- **Escaneo "agresivo":** Combina detección de OS, versión, scripts y traceroute. Muy informativo pero ruidoso,es sólo usado en laboratorio o con permiso explícito.

  sudo nmap -A 192.168.8.48





4. Medidas de seguridad (Máquina Víctima).

Configurar un firewall local: Un firewall local actúa como una barrera entre tu equipo y el resto de la red. Su función es controlar el tráfico entrante y saliente según reglas definidas: qué puertos, direcciones IP o protocolos están permitidos o bloqueados.

Al configurarlo correctamente, puedes bloquear intentos de conexión no solicitados, es decir, evitar que alguien desde fuera escanee o intente conectarse a tus servicios sin autorización. Solo el tráfico que tú declares explícitamente como permitido podrá pasar.

```
# instalar
sudo apt update
sudo apt install ufw -y

# política por defecto: bloquear entradas, permitir salidas
sudo ufw default deny incoming
sudo ufw default allow outgoing

# permitir SSH con rate limit (evita brute force)
sudo ufw limit ssh

# permitir sólo puertos necesarios
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp

# activar
sudo ufw enable

# ver reglas
sudo ufw status verbose
```

Cortar scans rápidos con reglas de tasa: Otra forma de defensa es aplicar reglas de limitación de tasa, que permiten conexiones normales pero bloquean o descartan aquellas que generan demasiadas solicitudes en poco tiempo.

Durante un escaneo rápido, el atacante envía una gran cantidad de paquetes SYN por segundo hacia distintos puertos. Este comportamiento no es típico del uso legítimo de un servicio, por lo que se puede filtrar fácilmente.

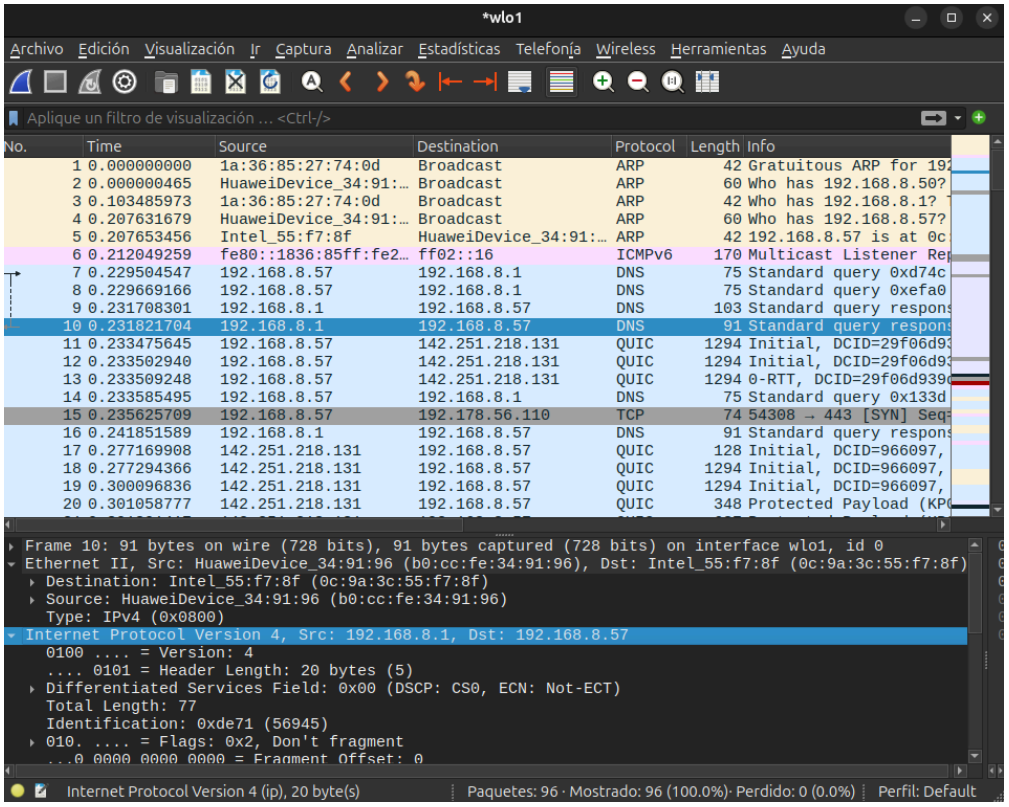
```
sudo apt install nftables -y
sudo systemctl enable --now nftables

sudo nft add table inet filter
sudo nft 'add chain inet filter input { type filter hook input priority 0; }'
sudo nft 'add rule inet filter input ct state established,related accept'
sudo nft 'add rule inet filter input tcp flags syn ct count over 20/second drop'
```

Detección de escaneos en registros firewall: Además de bloquear conexiones sospechosas, un buen firewall también puede detectar patrones de escaneo al analizar sus propios registros (logs). Cuando un atacante realiza un escaneo puerto a puerto, el sistema recibe múltiples intentos de conexión seguidos a diferentes puertos desde una misma dirección IP. Estos eventos, registrados en los logs del firewall, pueden interpretarse como una señal de reconocimiento o ataque.

Mediante herramientas de monitoreo o scripts de análisis, se pueden establecer alertas automáticas que avisen al administrador si una IP genera demasiadas solicitudes en poco tiempo o intenta acceder a puertos no autorizados.

```
sudo apt install psad -y
sudo psad --sig-update
sudo psad --Status
```

WireShark: Esta herramienta captura y muestra cada pieza de información que viaja por la red. Cada fila que ves en la lista es un "paquete" de datos individual. Piensa en cada paquete como una pequeña carta digital.



Wireshark te permite ver "detrás de cámaras" cómo se comunican tus dispositivos con Internet. Las columnas te dicen:

- Source (Fuente): Qué dispositivo envió la "carta".
- Destination (Destino): Para quién era la "carta".

- Protocol (Protocolo): Qué "idioma" o conjunto de reglas se usó para escribir la carta.
- Info (Información): Un resumen de lo que dice la carta.

IP (Internet Protocol):

- Es el "sistema de correo" de internet. Su trabajo es ponerle una dirección (la dirección IP) a cada paquete de datos para que los routers sepan a dónde enviarlo. No garantiza que llegue, solo pone la dirección y lo envía.

TCP (Transmission Control Protocol):

- Es el "servicio de mensajería con acuse de recibo". Trabaja junto con IP y se asegura de que todos los datos lleguen, que lleguen en el orden correcto y sin errores. Si un paquete se pierde, TCP lo pide de nuevo.

UDP (User Datagram Protocol):

- Es el "servicio de mensajería rápido". También trabaja con IP, pero su prioridad es la velocidad, no la fiabilidad. Envía los paquetes y no le importa si algunos se pierden o llegan en desorden.

HTTP (Hypertext Transfer Protocol):

- **E**s el idioma que usa tu navegador para pedir y recibir páginas web. Cuando escribes una dirección “http://”, estás usando este protocolo.

HTTPS (HTTP Secure):

- Es la versión segura de HTTP. Hace lo mismo (pedir páginas web), pero toda la conversación entre tu navegador y el servidor está cifrada. Es el "candado" que ves en la barra de direcciones y garantiza que nadie pueda espiar lo que envías o recibes.

DNS (Domain Name System):

- Es la "agenda telefónica" de internet. Los humanos usamos nombres fáciles de recordar, pero las computadoras usan números. DNS es el servicio que traduce esos nombres a sus IPs correspondientes.

FTP (File Transfer Protocol):

- Un protocolo diseñado específicamente para transferir archivos (subir y bajar) desde y hacia un servidor.

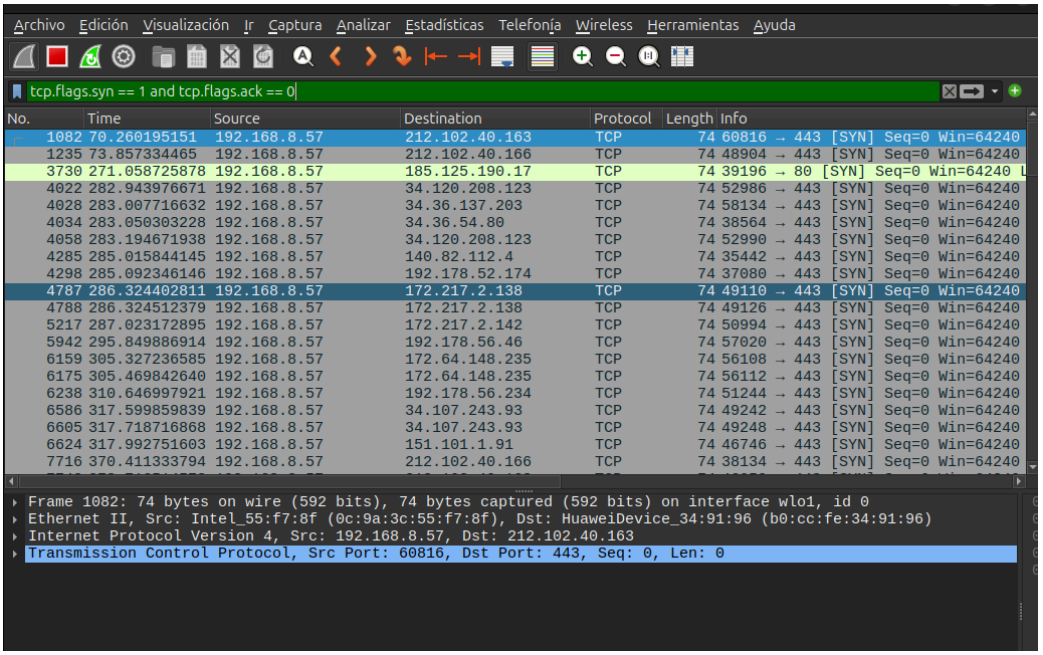
5. ¿Por qué usar Wireshark?

Una de las principales fortalezas de Wireshark es su capacidad para usar filtros de captura y de visualización, lo que permite enfocar el análisis en paquetes específicos dentro del tráfico de red. Gracias a esta función, es posible identificar patrones típicos de escaneo o comportamientos anómalos que podrían indicar un intento de reconocimiento o ataque.

Como medida de protección, estos filtros se convierten en una herramienta valiosa: permiten detectar escaneos en tiempo real, registrar evidencias y generar alertas tempranas.

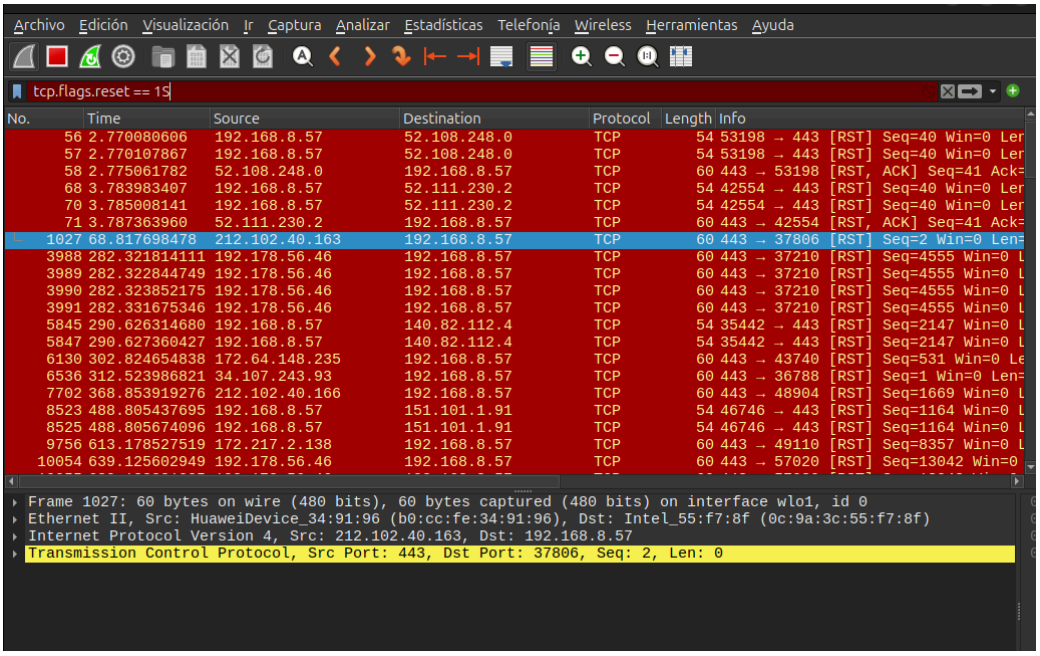
Escaneo SYN (half-open): Muestra los paquetes TCP SYN , sin el flag ACK. Un escaneo tipo SYN, como el que usa nmap -sS, envía solo ese paquete SYN para ver si el puerto responde con un SYN-ACK (abierto) o un RST (cerrado). No completa la conexión, y así evita dejar registros evidentes en el sistema destino.

tcp.flags.syn == 1 and tcp.flags.ack == 0



- **Conexiones con RST masivas:** Si ves muchos RST consecutivos provenientes del mismo destino, suele significar que alguien está probando varios puertos a la vez, lo que es típico de un escaneo SYN o Connect.

  tcp.flags.reset == 1



- **Escaneo UDP:** Muestra todas las respuestas ICMP que indican puertos UDP cerrados, revelando que alguien podría estar probando puertos UDP en tu máquina.

icmp.type == 3 and icmp.code == 3

- **Ping sweep / hosts que responden a ICMP:** Este filtro te deja ver quién está enviando o recibiendo pings ICMP, algo típico en un *ping sweep*, que es una técnica usada para descubrir qué equipos están activos dentro de una red.

  icmp.type == 0 or icmp.type == 8

- **Tráfico a muchos puertos desde una misma IP:** Este filtro mostrará todo el tráfico TCP proveniente de una IP concreta.Si ves que esa IP envía paquetes a muchos puertos distintos de forma continua, eso suele indicar un escaneo de puertos TCP.

  ip.src == 10.0.0.5 and tc

Conclusiones:

Al realizar tanto los escaneos con Nmap como la monitorización con Wireshark, comprendí de forma práctica cómo interactúan el ataque y la defensa dentro de una red. Nmap permitió descubrir los servicios expuestos y entender la superficie de ataque, mientras que Wireshark evidenció las trazas que esos escaneos dejan en el tráfico, revelando los patrones que pueden alertar sobre una actividad sospechosa.

Esta experiencia conjunta me ayudó a conectar la teoría con la práctica: interpretar paquetes, detectar anomalías y analizar los resultados desde ambos lados del proceso. En conjunto, ambas herramientas demostraron su valor para una auditoría de seguridad completa, que no solo busca vulnerabilidades, sino que también enseña a reconocerlas y mitigarlas mediante observación, análisis y registro técnico riguroso.

Referencias bibliográficas

[1] *Nmap: The network mapper - Free Security Scanner*. (n.d.). Nmap.org. Retrieved November 12, 2025, from https://nmap.org/

[2] *Wireshark • go deep*. (n.d.). Wireshark. Retrieved November 12, 2025, from https://www.wireshark.org/

[3] *Oracle VirtualBox*. (n.d.). Virtualbox.org. Retrieved November 12, 2025, from https://www.virtualbox.org/

[4] (N.d.-b). Akamai.com. Retrieved November 12, 2025, from https://www.akamai.com/es/glossary/what-are-syn-flood-ddos-attacks

[5] (N.d.). Ninjaone.com. Retrieved November 12, 2025, from https://www.ninjaone.com/es/it-hub/endpoint-management/handshake/

E. (n.d.). *NMAP 6: Listado de comandos*. Gva.Es. Retrieved November 12, 2025, from https://csirtcv.gva.es/wp-content/uploads/2020/05/NMAP-6_-Listado-de-comandos.pdf

(N.d.). Ninjaone.com. Retrieved November 12, 2025, from https://www.ninjaone.com/es/blog/utilizar-nmap-guia-completa/

Conceptos Básicos de Redes. (n.d.). FIRST Robotics Competition Documentation. Retrieved November 12, 2025, from https://docs.wpilib.org/es/latest/docs/networking/networking-introduction/networking-basics.html

Support. (2007, May 4). Cisco. https://www.cisco.com/en/US/docs/security/vpn5000/manager/reference/guide/appA.html

(N.d.-b). Labex.Io. Retrieved November 12, 2025, from https://labex.io/es/tutorials/nmap-how-to-ensure-the-security-of-nmap-scan-data-415518

Wireshark-filter(4). (n.d.). Wireshark.org. Retrieved November 12, 2025, from https://www.wireshark.org/docs/man-pages/wireshark-filter.html

Luz, S. (2020, July 4). *Cómo usar Wireshark para capturar y analizar el tráfico de red*. RedesZone. https://www.redeszone.net/tutoriales/redes-cable/wireshark-capturar-analizar-trafico-red/