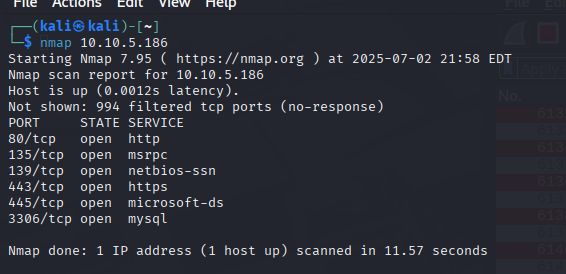
**Ejercicio 1: Mapeo completo de tu red local**

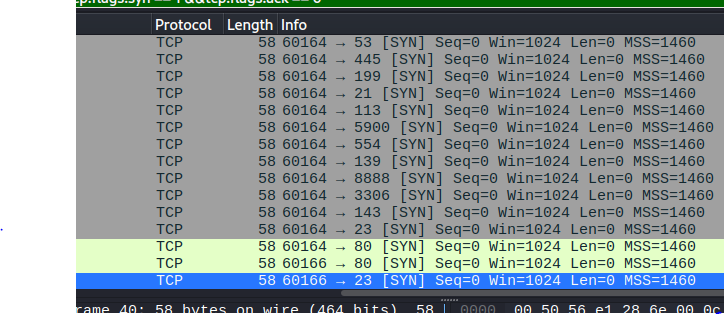
Con base en tu segmento de red, realiza un escaneo que te permita identificar todos los hosts activos y los servicios que están corriendo en cada uno. Analiza qué equipos representan un posible riesgo por los servicios expuestos.



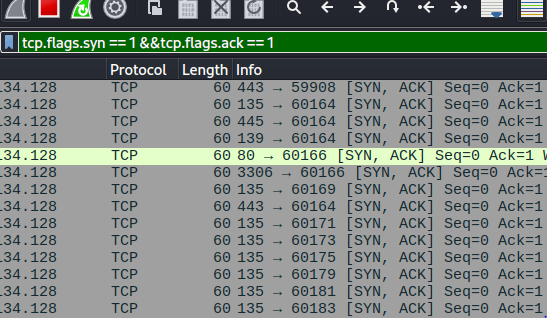
**En Wireshark deberían ver:**

* Tráfico SYN enviado a múltiples IPs del segmento.
* Respuestas SYN-ACK desde los hosts activos.
* Tráfico ICMP si usan ping scan.
* Escaneos dirigidos a múltiples puertos por host.

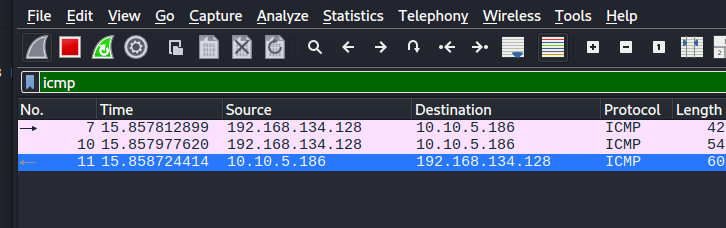
SYN:



SYN-ACK



ICMP:

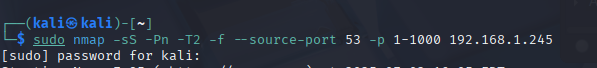


**Ejercicio 2: Escaneo sigiloso a un host en tu red**

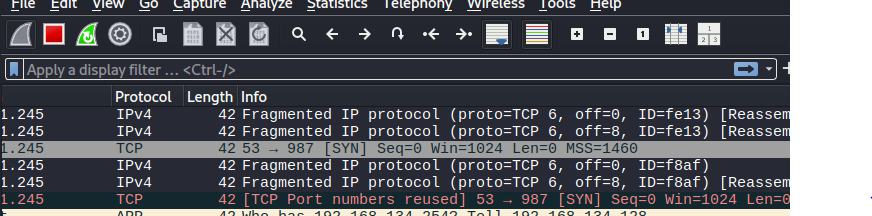
Escoge un host dentro de tu red y realiza un escaneo que utilice técnicas de evasión para evitar su detección por firewalls o sistemas de monitoreo. Evalúa si lograste obtener información sin generar tráfico evidente.

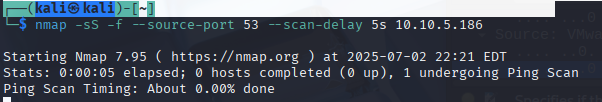
**En Wireshark deberían ver:**

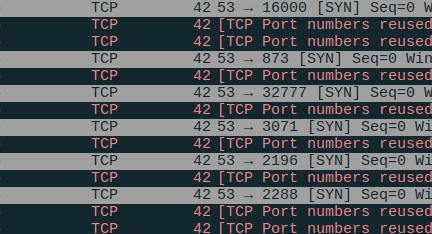
* Tráfico con fragmentación de paquetes TCP/IP.
* Uso de un puerto fuente no estándar (ej. 53, 123).
* Intervalos largos entre los paquetes (bajo volumen).
* Tráfico que no completa handshakes TCP.



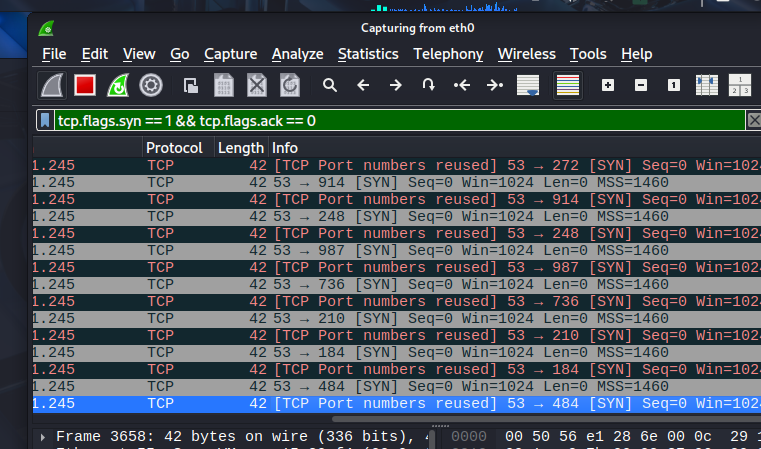
Fragmentado:







Tráfico que no completa Handshakes:

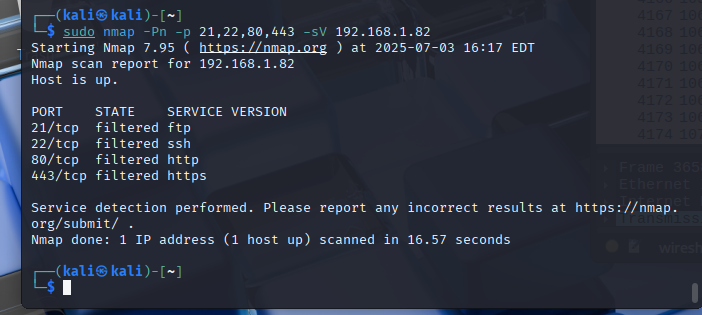


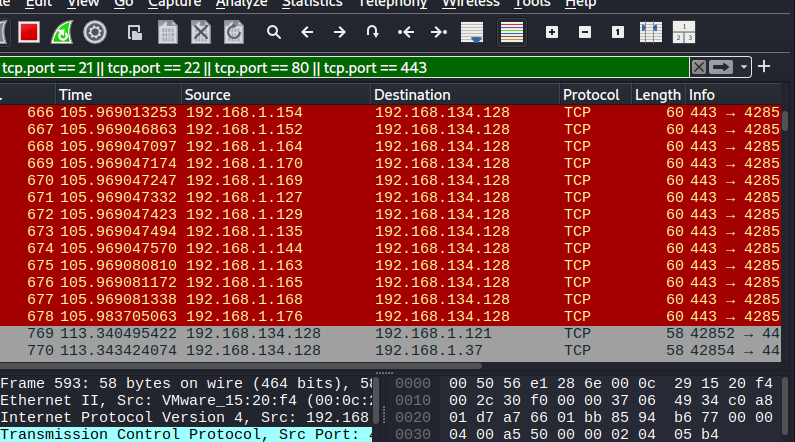
**Ejercicio 3: Enumeración avanzada de servicios**

Identifica un host dentro de tu red que tenga servicios web, FTP, o SSH, y utiliza técnicas avanzadas para obtener información detallada de esos servicios (como banners, versiones, métodos HTTP, etc.).

**En Wireshark deberían ver:**

* Solicitudes hacia puertos 21, 22, 80, 443, u otros comunes.
* Tráfico con comandos FTP, HTTP o SSH.
* Respuestas con datos identificables: versiones de servicios, encabezados HTTP, mensajes de bienvenida de FTP/SSH.





**Ejercicio 4: Detección de hosts sin ICMP habilitado**

Encuentra dentro de tu red aquellos hosts que no responden a ping (ICMP), pero que tienen puertos abiertos accesibles. Analiza si puedes detectarlos sin depender de ICMP.

**En Wireshark deberían ver:**

* Escaneos TCP sin tráfico ICMP.
* Solicitudes TCP SYN enviadas directamente a puertos específicos.
* Respuestas SYN-ACK de hosts que no respondieron al ping.

