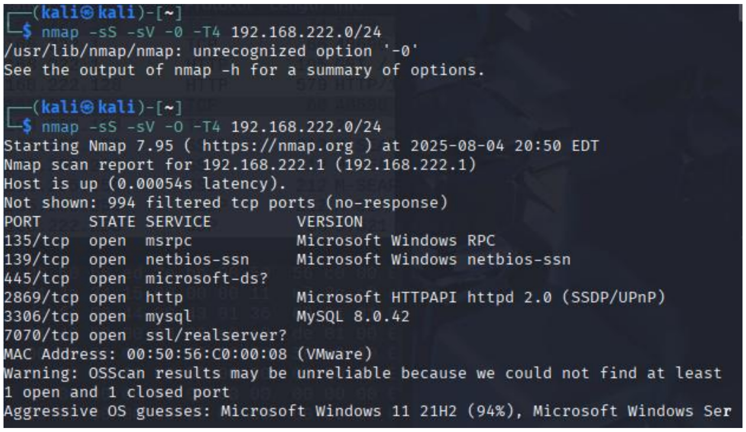
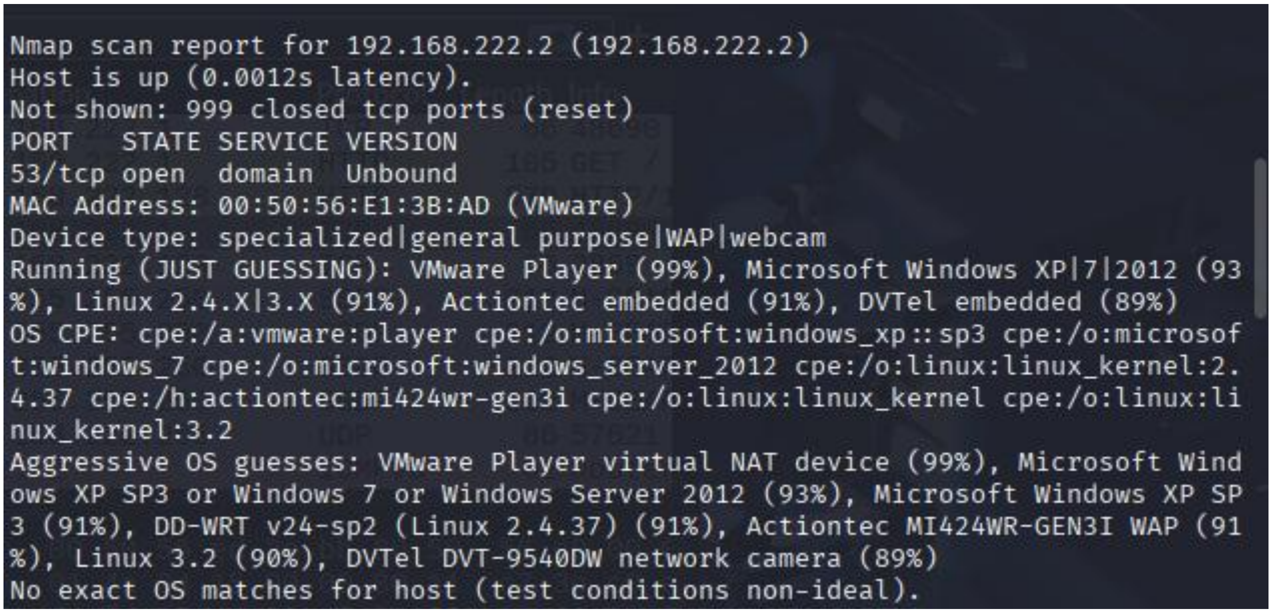
Ejercicio 1: Mapeo completo de tu red local

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.

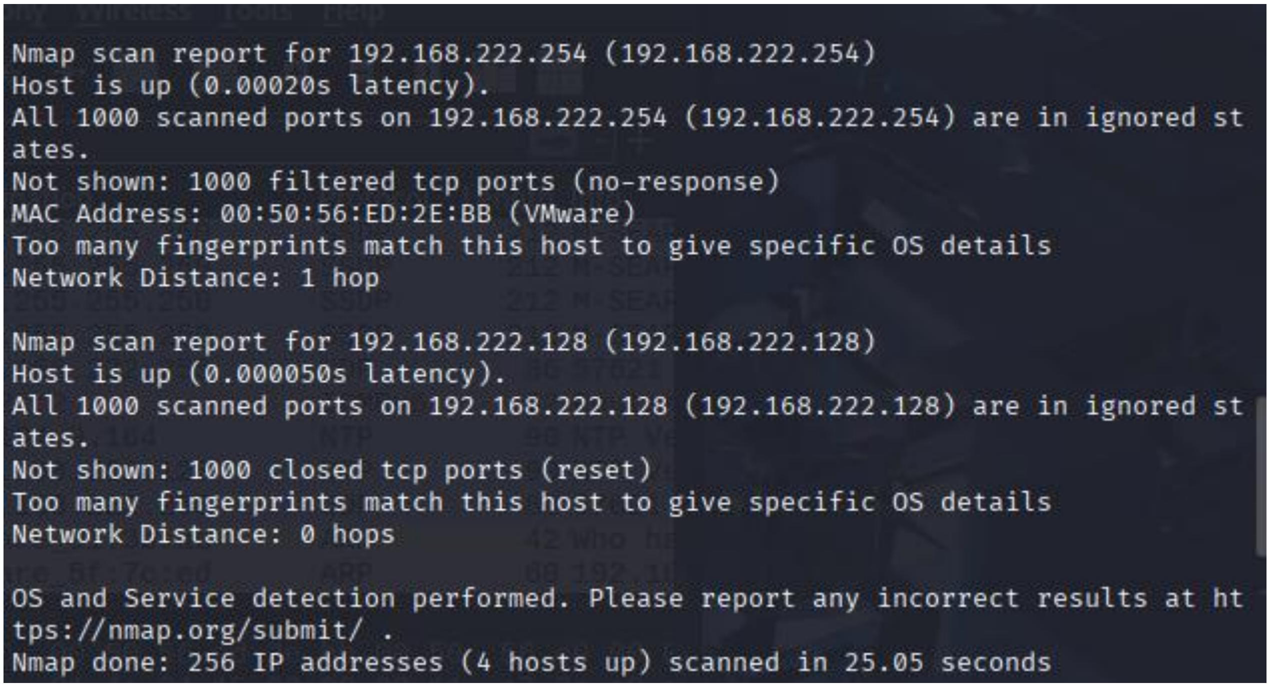
Hosts:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV -0 -T4 192.168.222.0/24
/usr/lib/nmap/nmap: unrecognized option '-0'
See the output of nmap -h for a summary of options.

┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV -O -T4 192.168.222.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 20:50 EDT
Nmap scan report for 192.168.222.1 (192.168.222.1)
Host is up (0.00054s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE         VERSION
135/tcp  open  msrpc           Microsoft Windows RPC
139/tcp  open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2869/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3306/tcp open  mysql           MySQL 8.0.42
7070/tcp open  ssl/realserver?
MAC Address: 00:50:56:C0:00:08 (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 11 21H2 (94%), Microsoft Windows Ser
```



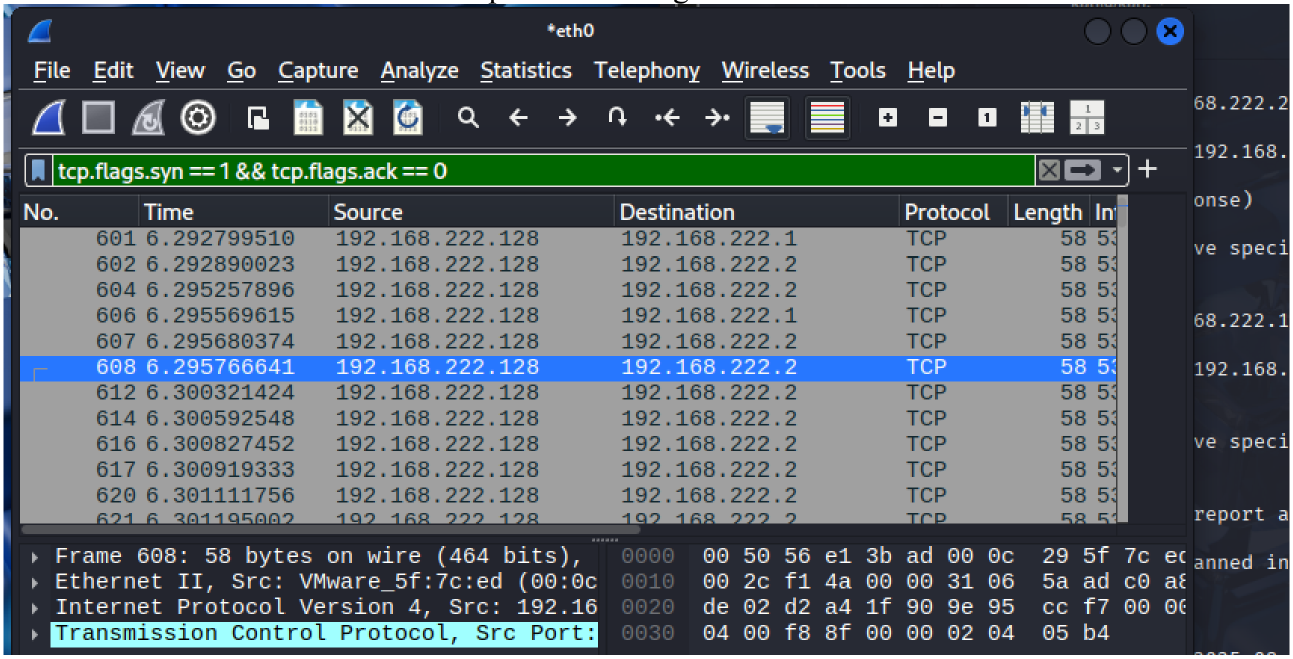
```
Nmap scan report for 192.168.222.2 (192.168.222.2)
Host is up (0.0012s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  Unbound
MAC Address: 00:50:56:E1:3B:AD (VMware)
Device type: specialized|general purpose|WAP|webcam
Running (JUST GUESSING): VMware Player (99%), Microsoft Windows XP|7|2012 (93
%), Linux 2.4.X|3.X (91%), Actiontec embedded (91%), DVTel embedded (89%)
OS CPE: cpe:/a:vmware:player cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsof
t:windows_7 cpe:/o:microsoft:windows_server_2012 cpe:/o:linux:linux_kernel:2.
4.37 cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:li
nux_kernel:3.2
Aggressive OS guesses: VMware Player virtual NAT device (99%), Microsoft Wind
ows XP SP3 or Windows 7 or Windows Server 2012 (93%), Microsoft Windows XP SP
3 (91%), DD-WRT v24-sp2 (Linux 2.4.37) (91%), Actiontec MI424WR-GEN3I WAP (91
%), Linux 3.2 (90%), DVTel DVT-9540DW network camera (89%)
No exact OS matches for host (test conditions non-ideal).
```



```
Nmap scan report for 192.168.222.254 (192.168.222.254)
Host is up (0.00020s latency).
All 1000 scanned ports on 192.168.222.254 (192.168.222.254) are in ignored st
ates.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:ED:2E:BB (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.222.128 (192.168.222.128)
Host is up (0.000050s latency).
All 1000 scanned ports on 192.168.222.128 (192.168.222.128) are in ignored st
ates.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 25.05 seconds
```

En Wireshark deberían ver:

- Tráfico SYN enviado a múltiples IPs del segmento.

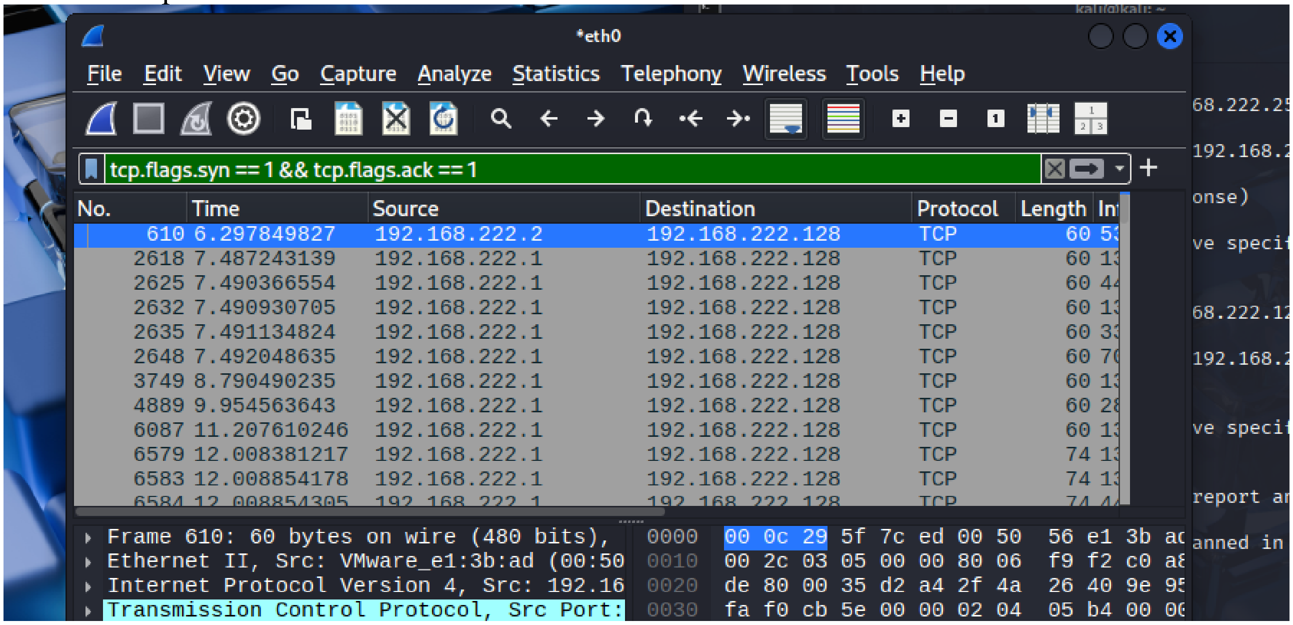


```
tcp.flags.syn == 1 && tcp.flags.ack == 0
```

```
No.  Time         Source           Destination      Protocol  Length  In
 601 6.292799510  192.168.222.128  192.168.222.1    TCP         58 5
 602 6.292890023  192.168.222.128  192.168.222.2    TCP         58 5
 604 6.295257896  192.168.222.128  192.168.222.2    TCP         58 5
 606 6.295569615  192.168.222.128  192.168.222.1    TCP         58 5
 607 6.295680374  192.168.222.128  192.168.222.2    TCP         58 5
 608 6.295766641  192.168.222.128  192.168.222.2    TCP         58 5
 612 6.300321424  192.168.222.128  192.168.222.2    TCP         58 5
 614 6.300592548  192.168.222.128  192.168.222.2    TCP         58 5
 616 6.300827452  192.168.222.128  192.168.222.2    TCP         58 5
 617 6.300919333  192.168.222.128  192.168.222.2    TCP         58 5
 620 6.301111756  192.168.222.128  192.168.222.2    TCP         58 5
 621 6.301195002  192.168.222.128  192.168.222.2    TCP         58 5
```

```
Frame 608: 58 bytes on wire (464 bits),       0000  00 50 56 e1 3b ad 00 0c  29 5f 7c ed
Ethernet II, Src: VMware_5f:7c:ed (00:0c      0010  00 2c f1 4a 00 00 31 06  5a ad c0 a8
Internet Protocol Version 4, Src: 192.16      0020  de 02 d2 a4 1f 90 9e 95  cc f7 00 00
Transmission Control Protocol, Src Port:      0030  04 00 f8 8f 00 00 02 04  05 b4
```

- Respuestas SYN-ACK desde los hosts activos.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
kali@kali: ~

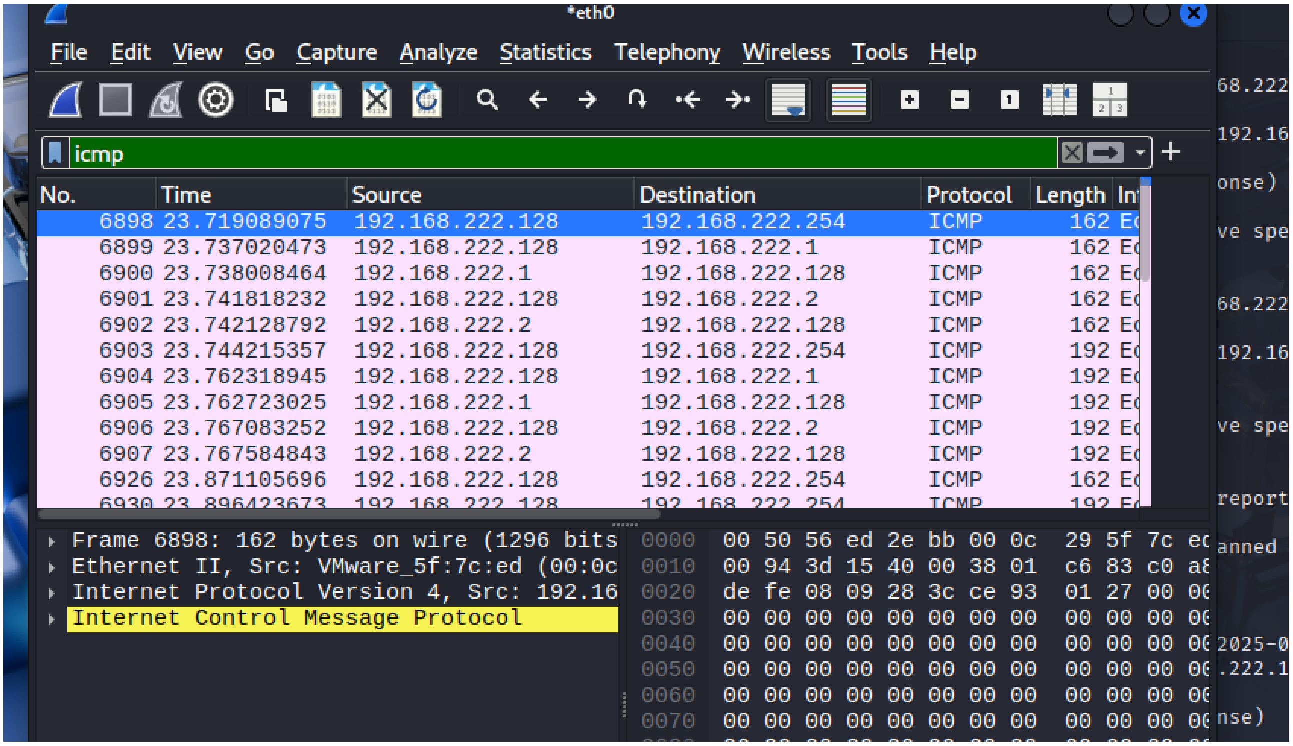
```
tcp.flags.syn == 1 && tcp.flags.ack == 1
```

```
No.       Time           Source           Destination        Protocol  Length In
      610 6.297849827    192.168.222.2    192.168.222.128    TCP           60 53
     2618 7.487243139    192.168.222.1    192.168.222.128    TCP           60 13
     2625 7.490366554    192.168.222.1    192.168.222.128    TCP           60 44
     2632 7.490930705    192.168.222.1    192.168.222.128    TCP           60 13
     2635 7.491134824    192.168.222.1    192.168.222.128    TCP           60 33
     2648 7.492048635    192.168.222.1    192.168.222.128    TCP           60 70
     3749 8.790490235    192.168.222.1    192.168.222.128    TCP           60 13
     4889 9.954563643    192.168.222.1    192.168.222.128    TCP           60 28
     6087 11.207610246   192.168.222.1    192.168.222.128    TCP           60 13
     6579 12.008381217   192.168.222.1    192.168.222.128    TCP           74 13
     6583 12.008854178   192.168.222.1    192.168.222.128    TCP           74 13
     6584 12.008854305   192.168.222.1    192.168.222.128    TCP           74 44
```

```
▸ Frame 610: 60 bytes on wire (480 bits),      0000  00 0c 29 5f 7c ed 00 50  56 e1 3b ac
▸ Ethernet II, Src: VMware_e1:3b:ad (00:50     0010  00 2c 03 05 00 00 80 06  f9 f2 c0 a8
▸ Internet Protocol Version 4, Src: 192.16     0020  de 80 00 35 d2 a4 2f 4a  26 40 9e 95
▸ Transmission Control Protocol, Src Port:     0030  fa f0 cb 5e 00 00 02 04  05 b4 00 00
```

```
68.222.25
192.168.2
onse)
ve specif
68.222.12
192.168.2
ve specif
report an
anned in
```

- Tráfico ICMP si usan ping scan.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length In

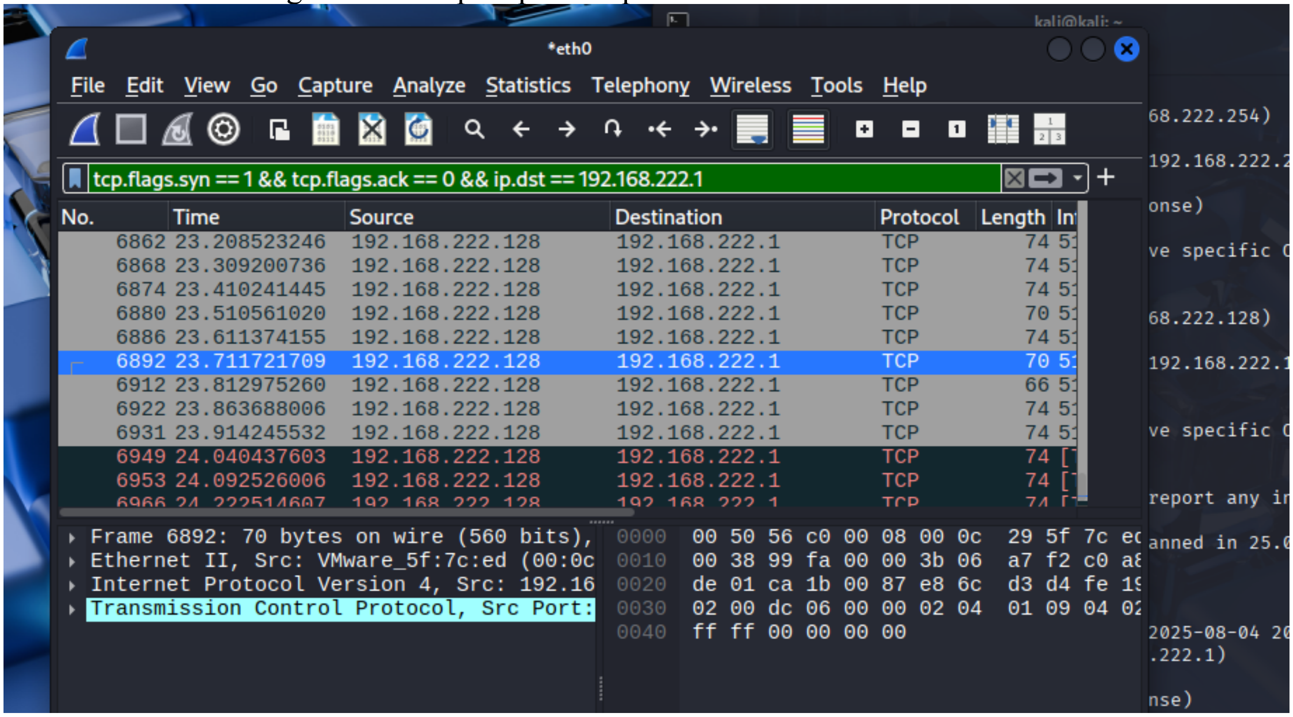
```
icmp
```

```
 6898 23.719089075  192.168.222.128   192.168.222.254   ICMP     162 E
 6899 23.737020473  192.168.222.128   192.168.222.1     ICMP     162 E
 6900 23.738008464  192.168.222.1     192.168.222.128   ICMP     162 E
 6901 23.741818232  192.168.222.128   192.168.222.2     ICMP     162 E
 6902 23.742128792  192.168.222.2     192.168.222.128   ICMP     162 E
 6903 23.744215357  192.168.222.128   192.168.222.254   ICMP     192 E
 6904 23.762318945  192.168.222.128   192.168.222.1     ICMP     192 E
 6905 23.762723025  192.168.222.1     192.168.222.128   ICMP     192 E
 6906 23.767083252  192.168.222.128   192.168.222.2     ICMP     192 E
 6907 23.767584843  192.168.222.2     192.168.222.128   ICMP     192 E
 6926 23.871105696  192.168.222.128   192.168.222.254   ICMP     162 E
 6930 23.896423673  192.168.222.128   192.168.222.254   ICMP     192 E
```

```
› Frame 6898: 162 bytes on wire (1296 bits      0000  00 50 56 ed 2e bb 00 0c  29 5f 7c ec
› Ethernet II, Src: VMware_5f:7c:ed (00:0c      0010  00 94 3d 15 40 00 38 01  c6 83 c0 a8
› Internet Protocol Version 4, Src: 192.16      0020  de fe 08 09 28 3c ce 93  01 27 00 00
› Internet Control Message Protocol             0030  00 00 00 00 00 00 00 00  00 00 00 00
                                                0040  00 00 00 00 00 00 00 00  00 00 00 00
                                                0050  00 00 00 00 00 00 00 00  00 00 00 00
                                                0060  00 00 00 00 00 00 00 00  00 00 00 00
                                                0070  00 00 00 00 00 00 00 00  00 00 00 00
```

```
68.222
192.16
onse)
ve spe
68.222
192.16
ve spe
report
anned
2025-0
.222.1
nse)
```

- Escaneos dirigidos a múltiples puertos por host.


kali@kali: ~
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length In

```
tcp.flags.syn == 1 && tcp.flags.ack == 0 && ip.dst == 192.168.222.1
```

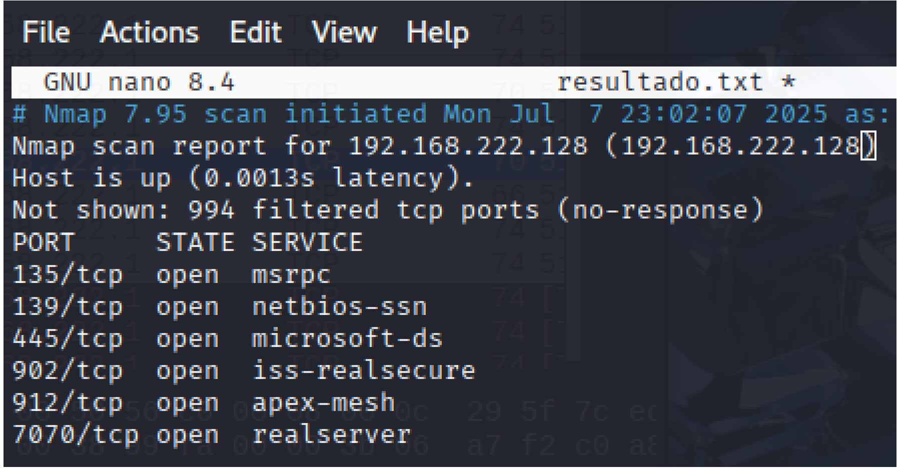
```
 6862 23.208523246  192.168.222.128   192.168.222.1   TCP    74 5
 6868 23.309200736  192.168.222.128   192.168.222.1   TCP    74 5
 6874 23.410241445  192.168.222.128   192.168.222.1   TCP    74 5
 6880 23.510561020  192.168.222.128   192.168.222.1   TCP    70 5
 6886 23.611374155  192.168.222.128   192.168.222.1   TCP    74 5
 6892 23.711721709  192.168.222.128   192.168.222.1   TCP    70 5
 6912 23.812975260  192.168.222.128   192.168.222.1   TCP    66 5
 6922 23.863688006  192.168.222.128   192.168.222.1   TCP    74 5
 6931 23.914245532  192.168.222.128   192.168.222.1   TCP    74 5
 6949 24.040437603  192.168.222.128   192.168.222.1   TCP    74 [
 6953 24.092526006  192.168.222.128   192.168.222.1   TCP    74 [
 6966 24.222514607  192.168.222.128   192.168.222.1   TCP    74 [
```

```
› Frame 6892: 70 bytes on wire (560 bits),      0000  00 50 56 c0 00 08 00 0c  29 5f 7c ec
› Ethernet II, Src: VMware_5f:7c:ed (00:0c      0010  00 38 99 fa 00 00 3b 06  a7 f2 c0 a8
› Internet Protocol Version 4, Src: 192.16      0020  de 01 ca 1b 00 87 e8 6c  d3 d4 fe 19
› Transmission Control Protocol, Src Port:      0030  02 00 dc 06 00 00 02 04  01 09 04 02
                                                0040  ff ff 00 00 00 00
```

```
68.222.254)
192.168.222.2
onse)
ve specific C
68.222.128)
192.168.222.1
ve specific C
report any in
anned in 25.0
2025-08-04 20
.222.1)
nse)
```

Ejercicio 2: Escaneo sigiloso a un host en tu red

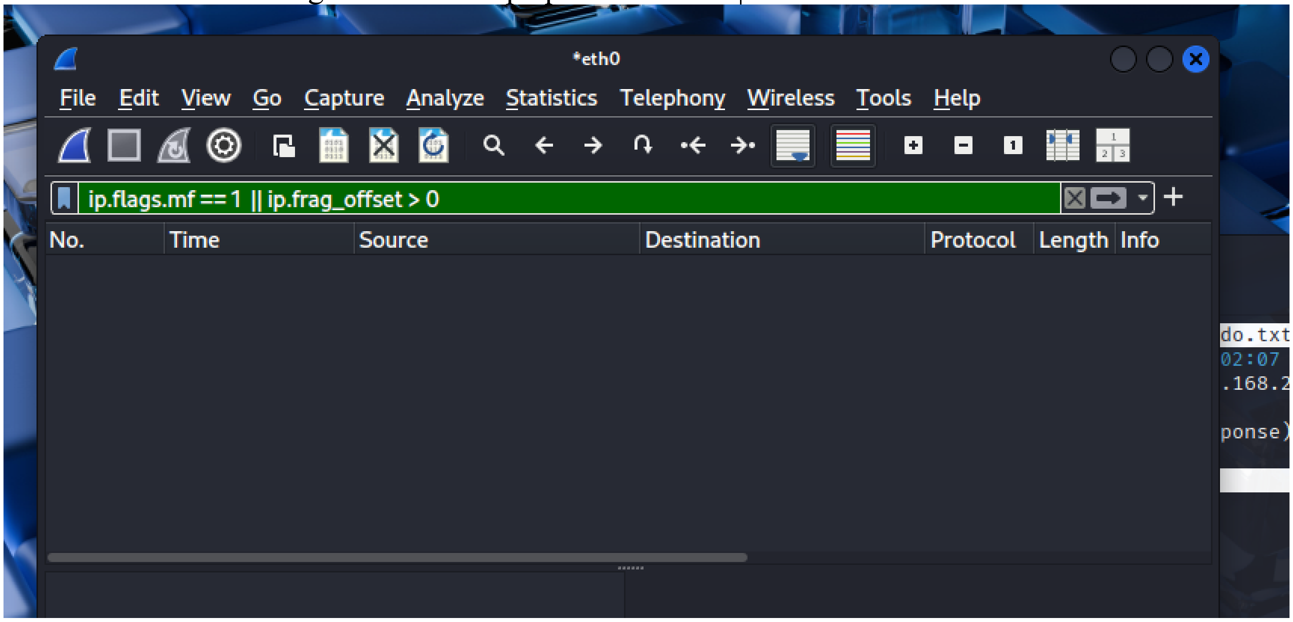
Escoge un host dentro de tu red y realiza un escaneo que utilice técnicas de evasión para evitar su detección por firewalls o sistemas de monitoreo. Evalúa si lograste obtener información sin generar tráfico evidente.



```
 GNU nano 8.4                    resultado.txt *
# Nmap 7.95 scan initiated Mon Jul  7 23:02:07 2025 as:
Nmap scan report for 192.168.222.128 (192.168.222.128)
Host is up (0.0013s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
7070/tcp open  realserver
```

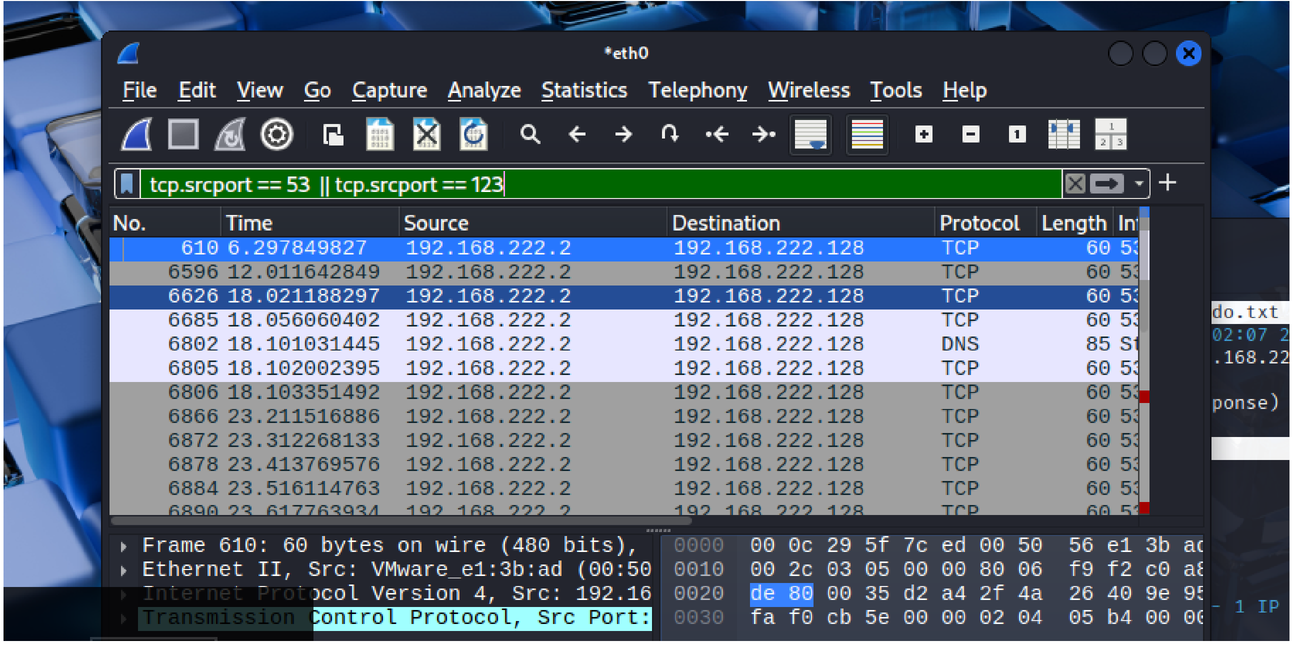
En Wireshark deberían ver:

- Tráfico con fragmentación de paquetes TCP/IP. |



```
ip.flags.mf == 1 || ip.frag_offset > 0
```

- Uso de un puerto fuente no estándar (ej. 53, 123).

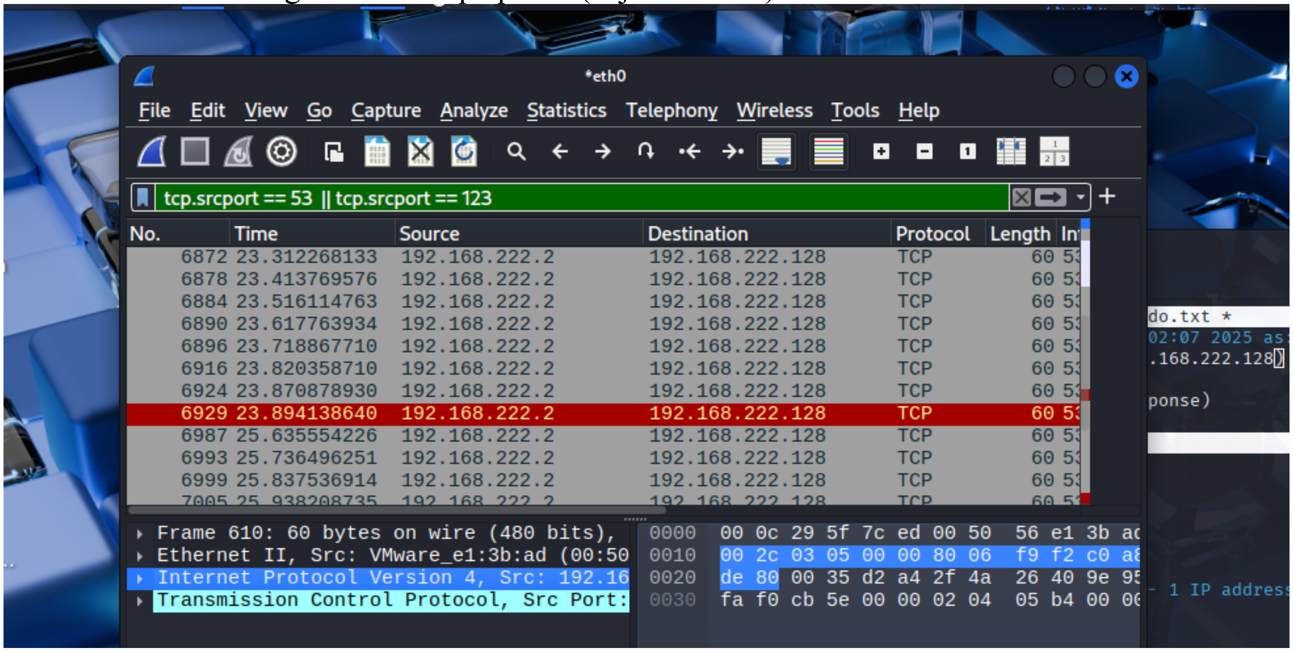

*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
do.txt
02:07 2
.168.22
ponse)
- 1 IP

tcp.srcport == 53 || tcp.srcport == 123

```
No.    Time          Source          Destination      Protocol Length In
   610 6.297849827   192.168.222.2   192.168.222.128  TCP        60 5
  6596 12.011642849  192.168.222.2   192.168.222.128  TCP        60 5
  6626 18.021188297  192.168.222.2   192.168.222.128  TCP        60 5
  6685 18.056060402  192.168.222.2   192.168.222.128  TCP        60 5
  6802 18.101031445  192.168.222.2   192.168.222.128  DNS        85 St
  6805 18.102002395  192.168.222.2   192.168.222.128  TCP        60 5
  6806 18.103351492  192.168.222.2   192.168.222.128  TCP        60 5
  6866 23.211516886  192.168.222.2   192.168.222.128  TCP        60 5
  6872 23.312268133  192.168.222.2   192.168.222.128  TCP        60 5
  6878 23.413769576  192.168.222.2   192.168.222.128  TCP        60 5
  6884 23.516114763  192.168.222.2   192.168.222.128  TCP        60 5
  6890 23.617763934  192.168.222.2   192.168.222.128  TCP        60 5
```

```
▸ Frame 610: 60 bytes on wire (480 bits),      0000  00 0c 29 5f 7c ed 00 50  56 e1 3b ac
▸ Ethernet II, Src: VMware_e1:3b:ad (00:50     0010  00 2c 03 05 00 00 80 06  f9 f2 c0 a8
▸ Internet Protocol Version 4, Src: 192.16     0020  de 80 00 35 d2 a4 2f 4a  26 40 9e 95
▸ Transmission Control Protocol, Src Port:     0030  fa f0 cb 5e 00 00 02 04  05 b4 00 00
```

- Intervalos largos entre los paquetes (bajo volumen).

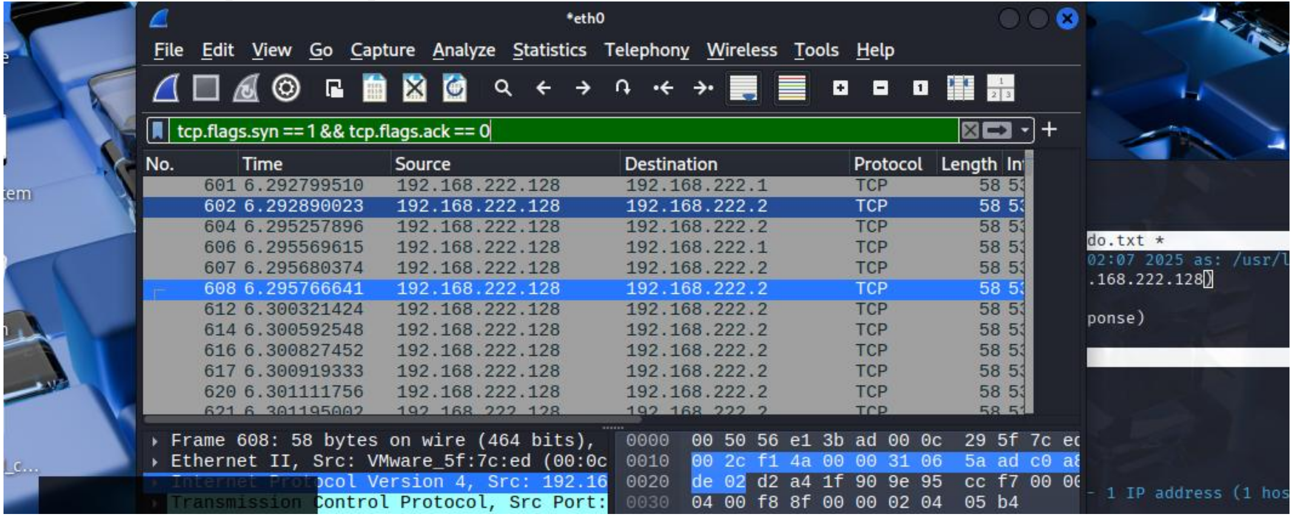

*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
do.txt *
02:07 2025 as
.168.222.128
ponse)
- 1 IP address

tcp.srcport == 53 || tcp.srcport == 123

```
No.    Time          Source          Destination      Protocol Length In
  6872 23.312268133  192.168.222.2   192.168.222.128  TCP        60 5
  6878 23.413769576  192.168.222.2   192.168.222.128  TCP        60 5
  6884 23.516114763  192.168.222.2   192.168.222.128  TCP        60 5
  6890 23.617763934  192.168.222.2   192.168.222.128  TCP        60 5
  6896 23.718867710  192.168.222.2   192.168.222.128  TCP        60 5
  6916 23.820358710  192.168.222.2   192.168.222.128  TCP        60 5
  6924 23.870878930  192.168.222.2   192.168.222.128  TCP        60 5
  6929 23.894138640  192.168.222.2   192.168.222.128  TCP        60 5
  6987 25.635554226  192.168.222.2   192.168.222.128  TCP        60 5
  6993 25.736496251  192.168.222.2   192.168.222.128  TCP        60 5
  6999 25.837536914  192.168.222.2   192.168.222.128  TCP        60 5
  7005 25.938208735  192.168.222.2   192.168.222.128  TCP        60 5
```

```
▸ Frame 610: 60 bytes on wire (480 bits),      0000  00 0c 29 5f 7c ed 00 50  56 e1 3b ac
▸ Ethernet II, Src: VMware_e1:3b:ad (00:50     0010  00 2c 03 05 00 00 80 06  f9 f2 c0 a8
▸ Internet Protocol Version 4, Src: 192.16     0020  de 80 00 35 d2 a4 2f 4a  26 40 9e 95
▸ Transmission Control Protocol, Src Port:     0030  fa f0 cb 5e 00 00 02 04  05 b4 00 00
```

- Tráfico que no completa handshakes TCP.



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.flags.syn == 1 && tcp.flags.ack == 0
```

```
No.  Time          Source           Destination      Protocol Length In
 601 6.292799510   192.168.222.128  192.168.222.1    TCP       58 53
 602 6.292890023   192.168.222.128  192.168.222.2    TCP       58 53
 604 6.295257896   192.168.222.128  192.168.222.2    TCP       58 53
 606 6.295569615   192.168.222.128  192.168.222.1    TCP       58 53
 607 6.295680374   192.168.222.128  192.168.222.2    TCP       58 53
 608 6.295766641   192.168.222.128  192.168.222.2    TCP       58 53
 612 6.300321424   192.168.222.128  192.168.222.2    TCP       58 53
 614 6.300592548   192.168.222.128  192.168.222.2    TCP       58 53
 616 6.300827452   192.168.222.128  192.168.222.2    TCP       58 53
 617 6.300919333   192.168.222.128  192.168.222.2    TCP       58 53
 620 6.301111756   192.168.222.128  192.168.222.2    TCP       58 53
 621 6.301195002   192.168.222.128  192.168.222.2    TCP       58 5
```

```
› Frame 608: 58 bytes on wire (464 bits),     0000  00 50 56 e1 3b ad 00 0c  29 5f 7c ed
› Ethernet II, Src: VMware_5f:7c:ed (00:0c    0010  00 2c f1 4a 00 00 31 06  5a ad c0 a8
› Internet Protocol Version 4, Src: 192.16    0020  de 02 d2 a4 1f 90 9e 95  cc f7 00 00
› Transmission Control Protocol, Src Port:    0030  04 00 f8 8f 00 00 02 04  05 b4
```

```
do.txt *
02:07 2025 as: /usr/l
.168.222.128

ponse)

- 1 IP address (1 hos
```

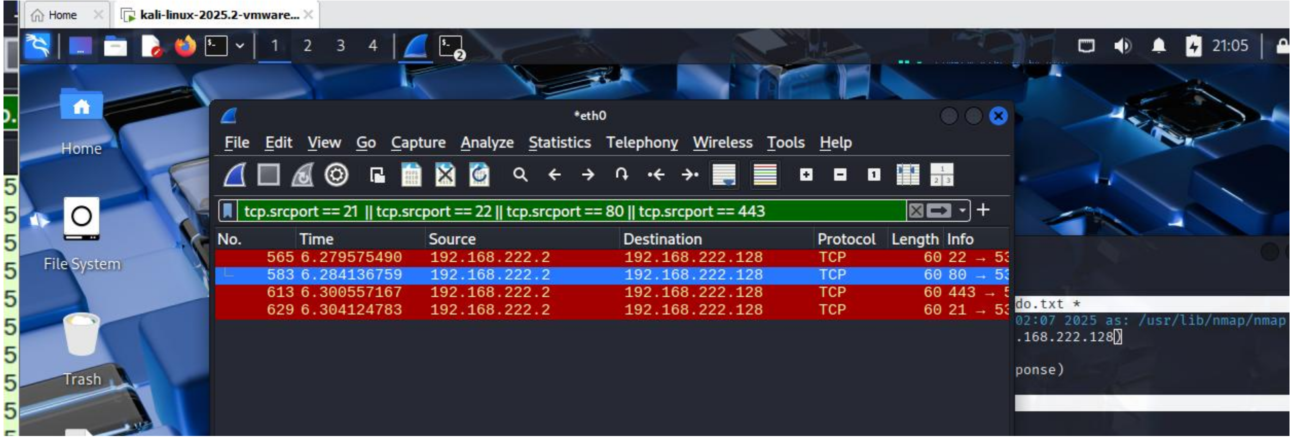
Ejercicio 3: Enumeración avanzada de servicios

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.).

NO se cuenta

En Wireshark deberían ver:

- Solicitudes hacia puertos 21, 22, 80, 443, u otros comunes.



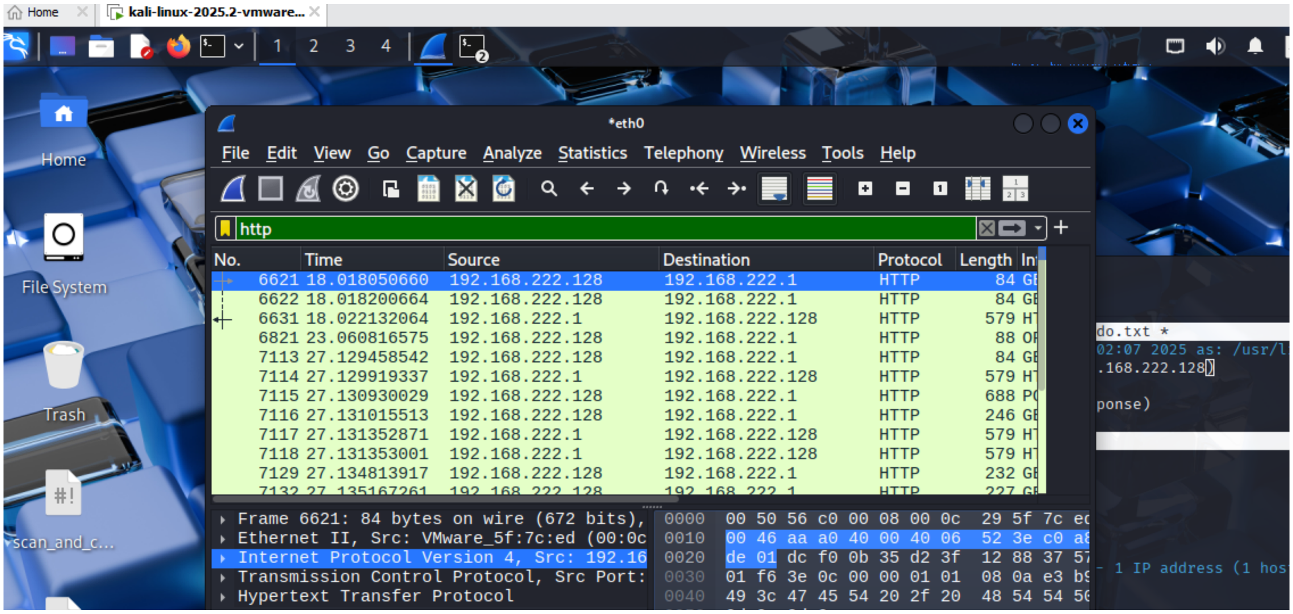
Home
kali-linux-2025.2-vmware...
1
2
3
4
21:05
Home
File System
Trash
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.srcport == 21 || tcp.srcport == 22 || tcp.srcport == 80 || tcp.srcport == 443

No.  Time         Source          Destination      Protocol Length Info
 565 6.279575490  192.168.222.2   192.168.222.128  TCP          60 22 → 53
 583 6.284136759  192.168.222.2   192.168.222.128  TCP          60 80 → 53
 613 6.300557167  192.168.222.2   192.168.222.128  TCP          60 443 → 5
 629 6.304124783  192.168.222.2   192.168.222.128  TCP          60 21 → 53
```

```
do.txt *
02:07 2025 as: /usr/lib/nmap/nmap
.168.222.128

ponse)
```

- Tráfico con comandos FTP, HTTP o SSH.

HTTP:



Home
kali-linux-2025.2-vmware...
1
2
3
4
Home
File System
Trash
scan_and_c...
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

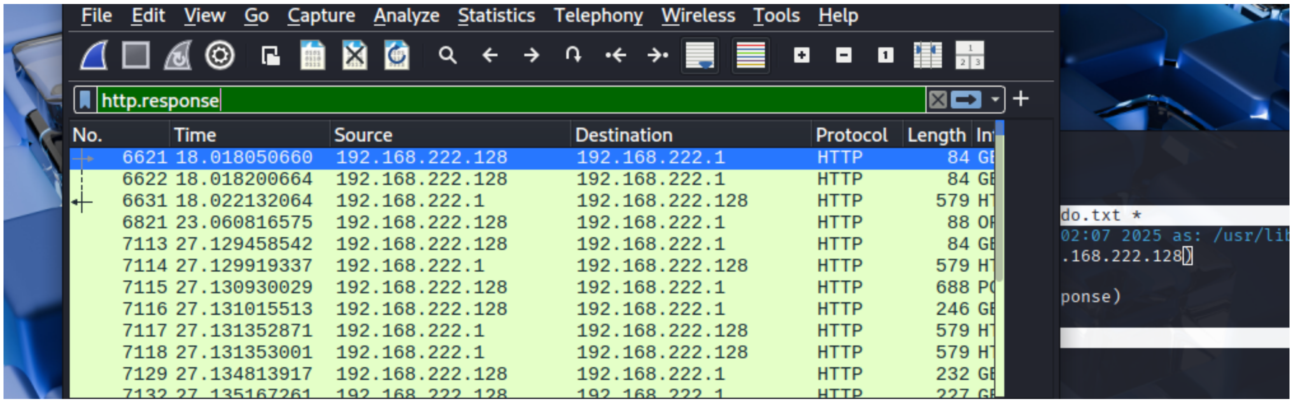
```
http

No.   Time          Source           Destination      Protocol Length In
 6621 18.018050660  192.168.222.128  192.168.222.1    HTTP         84 GE
 6622 18.018200664  192.168.222.128  192.168.222.1    HTTP         84 GE
 6631 18.022132064  192.168.222.1    192.168.222.128  HTTP        579 HT
 6821 23.060816575  192.168.222.128  192.168.222.1    HTTP         88 OF
 7113 27.129458542  192.168.222.128  192.168.222.1    HTTP         84 GE
 7114 27.129919337  192.168.222.1    192.168.222.128  HTTP        579 HT
 7115 27.130930029  192.168.222.128  192.168.222.1    HTTP        688 PO
 7116 27.131015513  192.168.222.128  192.168.222.1    HTTP        246 GE
 7117 27.131352871  192.168.222.1    192.168.222.128  HTTP        579 HT
 7118 27.131353001  192.168.222.1    192.168.222.128  HTTP        579 HT
 7129 27.134813917  192.168.222.128  192.168.222.1    HTTP        232 GE
 7132 27.135167261  192.168.222.128  192.168.222.1    HTTP        227 GE
```

```
› Frame 6621: 84 bytes on wire (672 bits),     0000  00 50 56 c0 00 08 00 0c  29 5f 7c ed
› Ethernet II, Src: VMware_5f:7c:ed (00:0c     0010  00 46 aa a0 40 00 40 06  52 3e c0 a8
› Internet Protocol Version 4, Src: 192.16     0020  de 01 dc f0 0b 35 d2 3f  12 88 37 57
› Transmission Control Protocol, Src Port:     0030  01 f6 3e 0c 00 00 01 01  08 0a e3 b9
› Hypertext Transfer Protocol                  0040  49 3c 47 45 54 20 2f 20  48 54 54 50
```

```
do.txt *
02:07 2025 as: /usr/l
.168.222.128

ponse)

- 1 IP address (1 hos
```

- Respuestas con datos identificables: versiones de servicios, encabezados HTTP, mensajes de bienvenida de FTP/SSH.

HTTP.RESPONSE:



http.response

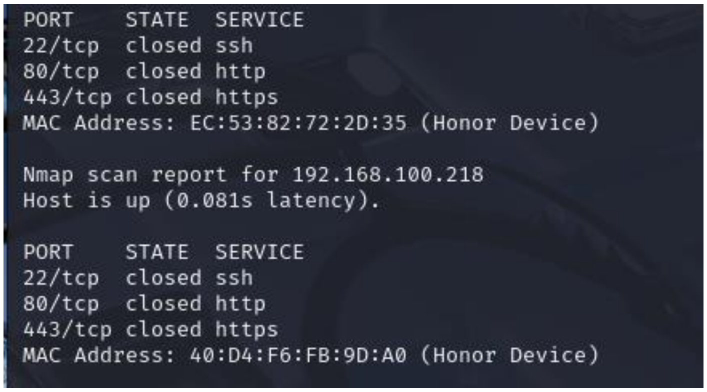
No.	Time	Source	Destination	Protocol	Length	In
6621	18.018050660	192.168.222.128	192.168.222.1	HTTP	84	GE
6622	18.018200664	192.168.222.128	192.168.222.1	HTTP	84	GE
6631	18.022132064	192.168.222.1	192.168.222.128	HTTP	579	HT
6821	23.060816575	192.168.222.128	192.168.222.1	HTTP	88	OF
7113	27.129458542	192.168.222.128	192.168.222.1	HTTP	84	GE
7114	27.129919337	192.168.222.1	192.168.222.128	HTTP	579	HT
7115	27.130930029	192.168.222.128	192.168.222.1	HTTP	688	PO
7116	27.131015513	192.168.222.128	192.168.222.1	HTTP	246	GE
7117	27.131352871	192.168.222.1	192.168.222.128	HTTP	579	HT
7118	27.131353001	192.168.222.1	192.168.222.128	HTTP	579	HT
7129	27.134813917	192.168.222.128	192.168.222.1	HTTP	232	GE
7132	27.135167261	192.168.222.128	192.168.222.1	HTTP	227	GE

```
do.txt *
02:07 2025 as: /usr/li
.168.222.128

ponse)
```

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:



```
PORT    STATE  SERVICE
22/tcp  closed ssh
80/tcp  closed http
443/tcp closed https
MAC Address: EC:53:82:72:2D:35 (Honor Device)

Nmap scan report for 192.168.100.218
Host is up (0.081s latency).

PORT    STATE  SERVICE
22/tcp  closed ssh
80/tcp  closed http
443/tcp closed https
MAC Address: 40:D4:F6:FB:9D:A0 (Honor Device)
```

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