ING. REDES INTELIGENTES Y CIBERSEGURIDAD

Universidad Tecnológica de Cancún.

Alumno:

Moo Canul Jesús Enrique

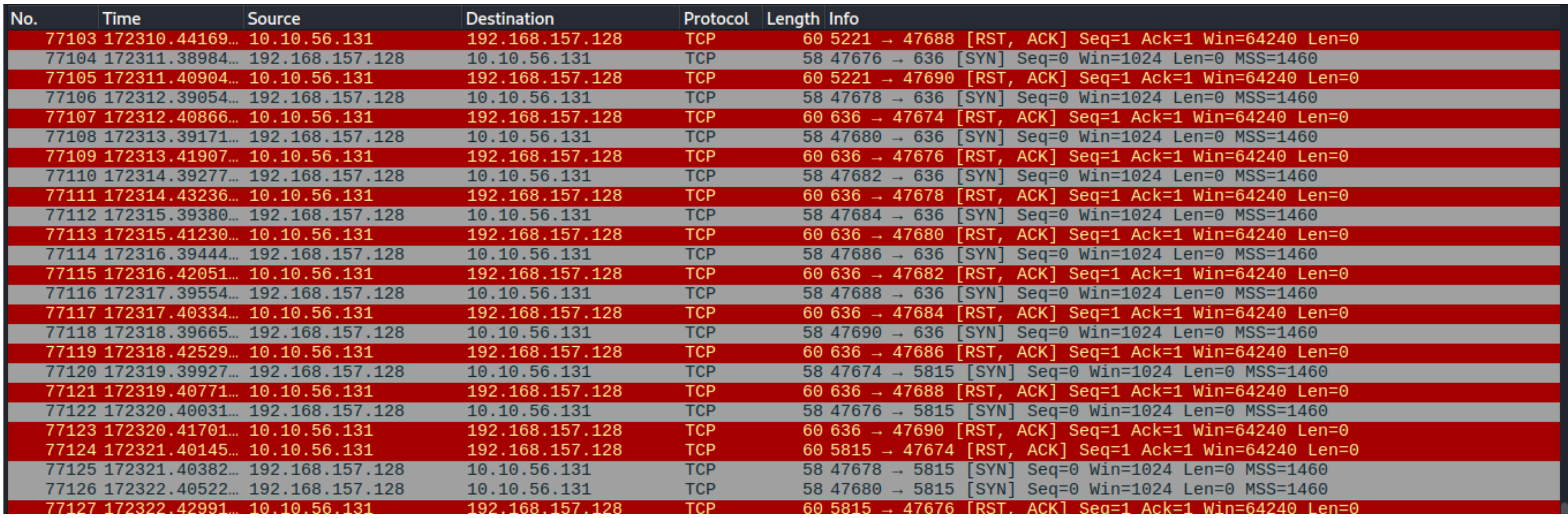
Grupo: IRIYC91

Ejercicio 1: Mapeo completo de tu red local

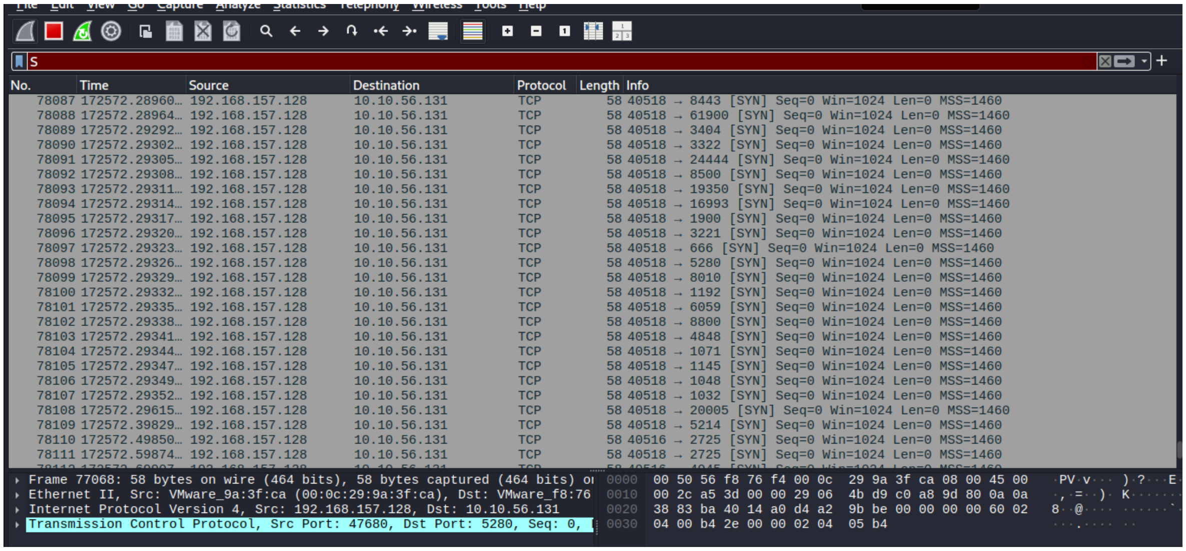
Con base en tu segmento de red, realiza un escaneo que te permita identificar todos los hosts activos y los servicios que están corriendo en cada uno. Analiza qué equipos representan un posible riesgo por los servicios expuestos.

En Wireshark deberían ver:

- Tráfico SYN enviado a múltiples IPs del segmento.
- Respuestas SYN-ACK desde los hosts activos.

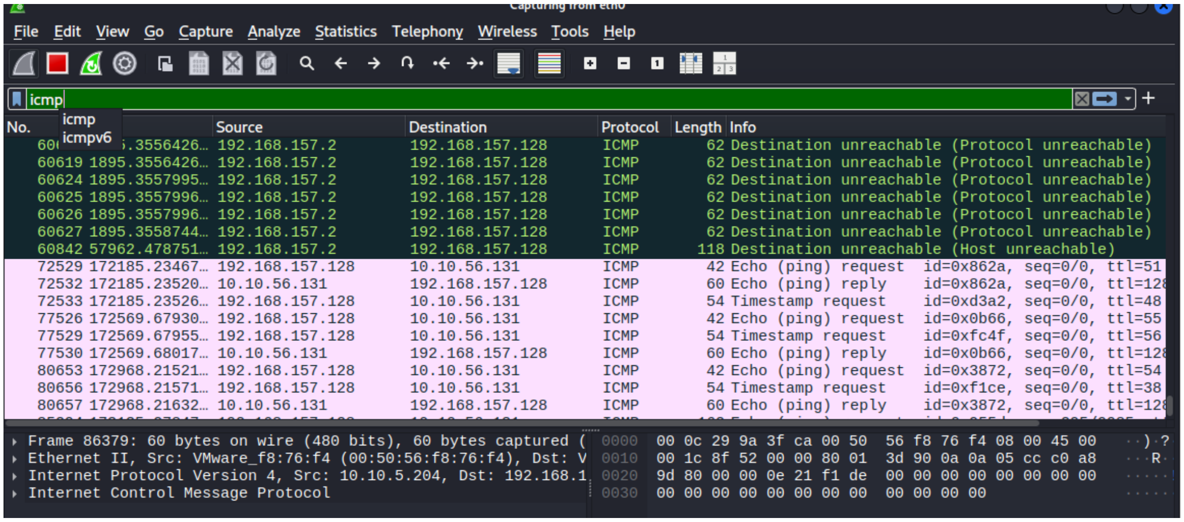


```
No.   Time           Source           Destination      Protocol Length Info
77103 172310.44169… 10.10.56.131     192.168.157.128  TCP      60 5221 → 47688 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
77104 172311.38984… 192.168.157.128  10.10.56.131     TCP      58 47676 → 636 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
77105 172311.40904… 10.10.56.131     192.168.157.128  TCP      60 5221 → 47690 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
77106 172312.39054… 192.168.157.128  10.10.56.131     TCP      58 47678 → 636 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
77107 172312.40866… 10.10.56.131     192.168.157.128  TCP      60 636 → 47674 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
77108 172313.39171… 192.168.157.128  10.10.56.131     TCP      58 47680 → 636 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
77109 172313.41907… 10.10.56.131     192.168.157.128  TCP      60 636 → 47676 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
77110 172314.39277… 192.168.157.128  10.10.56.131     TCP      58 47682 → 636 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
77111 172314.43236… 10.10.56.131     192.168.157.128  TCP      60 636 → 47678 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
77112 172315.39380… 192.168.157.128  10.10.56.131     TCP      58 47684 → 636 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
77113 172315.41230… 10.10.56.131     192.168.157.128  TCP      60 636 → 47680 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
77114 172316.39444… 192.168.157.128  10.10.56.131     TCP      58 47686 → 636 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
77115 172316.42051… 10.10.56.131     192.168.157.128  TCP      60 636 → 47682 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
77116 172317.39554… 192.168.157.128  10.10.56.131     TCP      58 47688 → 636 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
77117 172317.40334… 10.10.56.131     192.168.157.128  TCP      60 636 → 47684 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
77118 172318.39665… 192.168.157.128  10.10.56.131     TCP      58 47690 → 636 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
77119 172318.42529… 10.10.56.131     192.168.157.128  TCP      60 636 → 47686 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
77120 172319.39927… 192.168.157.128  10.10.56.131     TCP      58 47674 → 5815 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
77121 172319.40771… 10.10.56.131     192.168.157.128  TCP      60 636 → 47688 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
77122 172320.40031… 192.168.157.128  10.10.56.131     TCP      58 47676 → 5815 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
77123 172320.41701… 10.10.56.131     192.168.157.128  TCP      60 636 → 47690 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
77124 172321.40145… 10.10.56.131     192.168.157.128  TCP      60 5815 → 47674 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
77125 172321.40382… 192.168.157.128  10.10.56.131     TCP      58 47678 → 5815 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
77126 172322.40522… 192.168.157.128  10.10.56.131     TCP      58 47680 → 5815 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
77127 172322.42991… 10.10.56.131     192.168.157.128  TCP      60 5815 → 47676 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
```



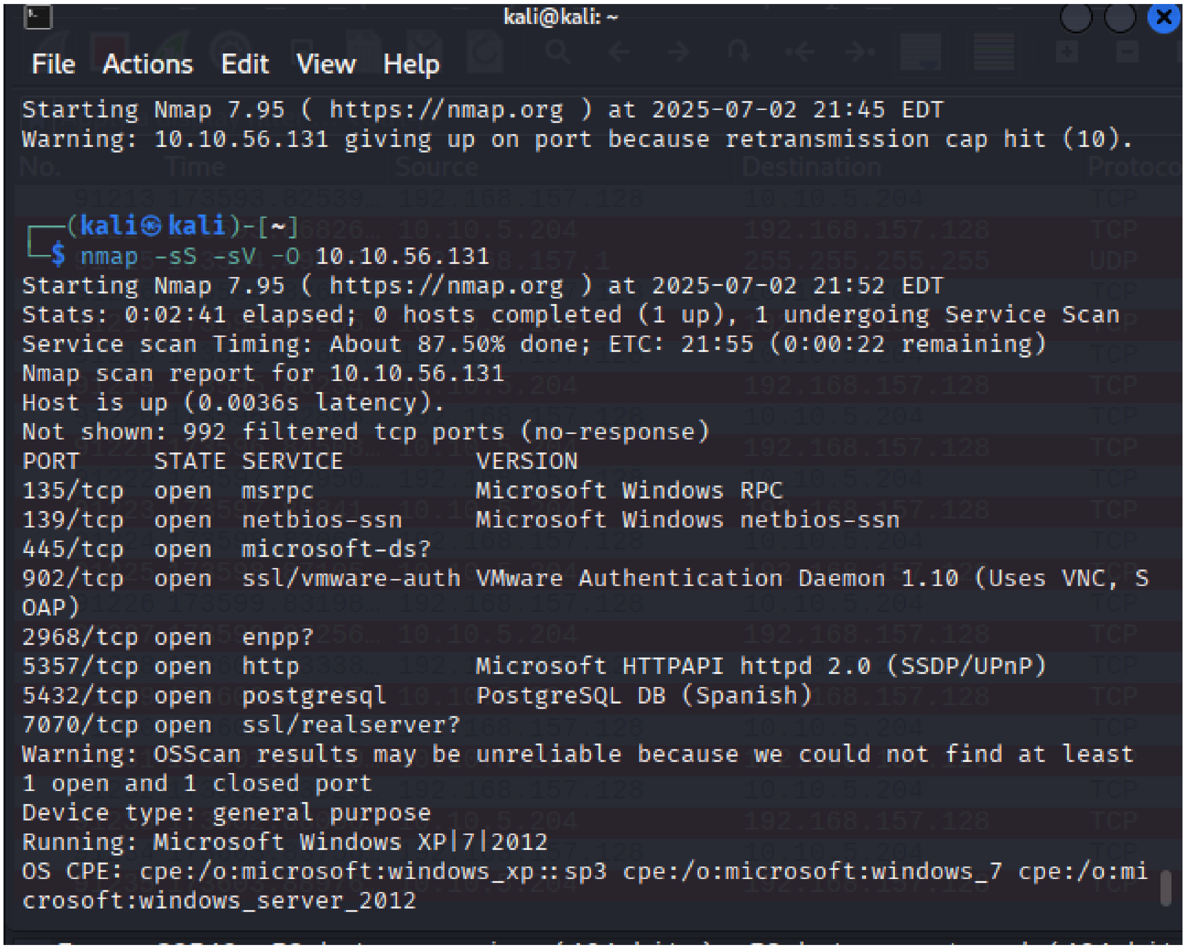
```
S

No.   Time           Source           Destination      Protocol Length Info
78087 172572.28960… 192.168.157.128  10.10.56.131     TCP      58 40518 → 8443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78088 172572.28964… 192.168.157.128  10.10.56.131     TCP      58 40518 → 61900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78089 172572.29292… 192.168.157.128  10.10.56.131     TCP      58 40518 → 3404 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78090 172572.29302… 192.168.157.128  10.10.56.131     TCP      58 40518 → 3322 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78091 172572.29305… 192.168.157.128  10.10.56.131     TCP      58 40518 → 24444 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78092 172572.29308… 192.168.157.128  10.10.56.131     TCP      58 40518 → 8500 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78093 172572.29311… 192.168.157.128  10.10.56.131     TCP      58 40518 → 19350 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78094 172572.29314… 192.168.157.128  10.10.56.131     TCP      58 40518 → 16993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78095 172572.29317… 192.168.157.128  10.10.56.131     TCP      58 40518 → 1900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78096 172572.29320… 192.168.157.128  10.10.56.131     TCP      58 40518 → 3221 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78097 172572.29323… 192.168.157.128  10.10.56.131     TCP      58 40518 → 666 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78098 172572.29326… 192.168.157.128  10.10.56.131     TCP      58 40518 → 5280 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78099 172572.29329… 192.168.157.128  10.10.56.131     TCP      58 40518 → 8010 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78100 172572.29332… 192.168.157.128  10.10.56.131     TCP      58 40518 → 1192 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78101 172572.29335… 192.168.157.128  10.10.56.131     TCP      58 40518 → 6059 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78102 172572.29338… 192.168.157.128  10.10.56.131     TCP      58 40518 → 8800 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78103 172572.29341… 192.168.157.128  10.10.56.131     TCP      58 40518 → 4848 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78104 172572.29344… 192.168.157.128  10.10.56.131     TCP      58 40518 → 1071 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78105 172572.29347… 192.168.157.128  10.10.56.131     TCP      58 40518 → 1145 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78106 172572.29349… 192.168.157.128  10.10.56.131     TCP      58 40518 → 1048 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78107 172572.29352… 192.168.157.128  10.10.56.131     TCP      58 40518 → 1032 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78108 172572.29615… 192.168.157.128  10.10.56.131     TCP      58 40518 → 20005 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78109 172572.39829… 192.168.157.128  10.10.56.131     TCP      58 40518 → 5214 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78110 172572.49850… 192.168.157.128  10.10.56.131     TCP      58 40516 → 2725 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78111 172572.59874… 192.168.157.128  10.10.56.131     TCP      58 40518 → 2725 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

▸ Frame 77068: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) o
▸ Ethernet II, Src: VMware_9a:3f:ca (00:0c:29:9a:3f:ca), Dst: VMware_f8:76
▸ Internet Protocol Version 4, Src: 192.168.157.128, Dst: 10.10.56.131
▸ Transmission Control Protocol, Src Port: 47680, Dst Port: 5280, Seq: 0,

0000  00 50 56 f8 76 f4 00 0c  29 9a 3f ca 08 00 45 00   ·PV·v···)·?···E·
0010  00 2c a5 3d 00 00 29 06  4b d9 c0 a8 9d 80 0a 0a   ·,·=··)·K·······
0020  38 83 ba 40 14 a0 d4 a2  9b be 00 00 00 00 60 02   8··@··········`·
0030  04 00 b4 2e 00 00 02 04  05 b4                     ···.······
```

Tráfico ICMP si usan ping scan.



```
No.                  Source            Destination       Protocol  Length Info
60(   ;.3556426… 192.168.157.2     192.168.157.128   ICMP        62 Destination unreachable (Protocol unreachable)
60619 1895.3556426… 192.168.157.2     192.168.157.128   ICMP        62 Destination unreachable (Protocol unreachable)
60624 1895.3557995… 192.168.157.2     192.168.157.128   ICMP        62 Destination unreachable (Protocol unreachable)
60625 1895.3557996… 192.168.157.2     192.168.157.128   ICMP        62 Destination unreachable (Protocol unreachable)
60626 1895.3557996… 192.168.157.2     192.168.157.128   ICMP        62 Destination unreachable (Protocol unreachable)
60627 1895.3558744… 192.168.157.2     192.168.157.128   ICMP        62 Destination unreachable (Protocol unreachable)
60842 57962.478751… 192.168.157.2     192.168.157.128   ICMP       118 Destination unreachable (Host unreachable)
72529 172185.23467… 192.168.157.128   10.10.56.131      ICMP        42 Echo (ping) request   id=0x862a, seq=0/0, ttl=51
72532 172185.23520… 10.10.56.131      192.168.157.128   ICMP        60 Echo (ping) reply     id=0x862a, seq=0/0, ttl=128
72533 172185.23526… 192.168.157.128   10.10.56.131      ICMP        54 Timestamp request     id=0xd3a2, seq=0/0, ttl=48
77526 172569.67930… 192.168.157.128   10.10.56.131      ICMP        42 Echo (ping) request   id=0x0b66, seq=0/0, ttl=55
77529 172569.67955… 192.168.157.128   10.10.56.131      ICMP        54 Timestamp request     id=0xfc4f, seq=0/0, ttl=56
77530 172569.68017… 10.10.56.131      192.168.157.128   ICMP        60 Echo (ping) reply     id=0x0b66, seq=0/0, ttl=128
80653 172968.21521… 192.168.157.128   10.10.56.131      ICMP        42 Echo (ping) request   id=0x3872, seq=0/0, ttl=54
80656 172968.21571… 192.168.157.128   10.10.56.131      ICMP        54 Timestamp request     id=0xf1ce, seq=0/0, ttl=38
80657 172968.21632… 10.10.56.131      192.168.157.128   ICMP        60 Echo (ping) reply     id=0x3872, seq=0/0, ttl=128

› Frame 86379: 60 bytes on wire (480 bits), 60 bytes captured (   0000  00 0c 29 9a 3f ca 00 50  56 f8 76 f4 08 00 45 00   ··)·?·
› Ethernet II, Src: VMware_f8:76:f4 (00:50:56:f8:76:f4), Dst: V   0010  00 1c 8f 52 00 00 80 01  3d 90 0a 0a 05 cc c0 a8   ···R··
› Internet Protocol Version 4, Src: 10.10.5.204, Dst: 192.168.1   0020  9d 80 00 00 0e 21 f1 de  00 00 00 00 00 00 00 00   ······
› Internet Control Message Protocol                               0030  00 00 00 00 00 00 00 00  00 00 00 00               ·····
```

Escaneos dirigidos a múltiples puertos por host.



```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 21:45 EDT
Warning: 10.10.56.131 giving up on port because retransmission cap hit (10).

┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV -O 10.10.56.131
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 21:52 EDT
Stats: 0:02:41 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 87.50% done; ETC: 21:55 (0:00:22 remaining)
Nmap scan report for 10.10.56.131
Host is up (0.0036s latency).
Not shown: 992 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?
902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, S
OAP)
2968/tcp open  enpp?
5357/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5432/tcp open  postgresql      PostgreSQL DB (Spanish)
7070/tcp open  ssl/realserver?
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows XP|7|2012
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:mi
crosoft:windows_server_2012
```

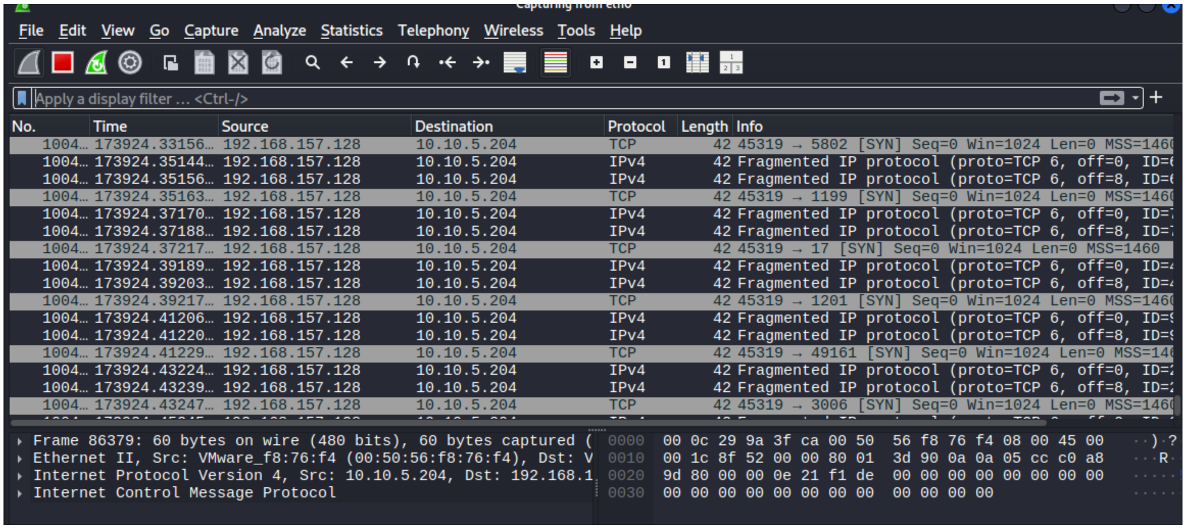
Los comandos utilizados para la realización de este ejercicio fueron: nmap -Ss , nmap -sV y Nmap -O

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.

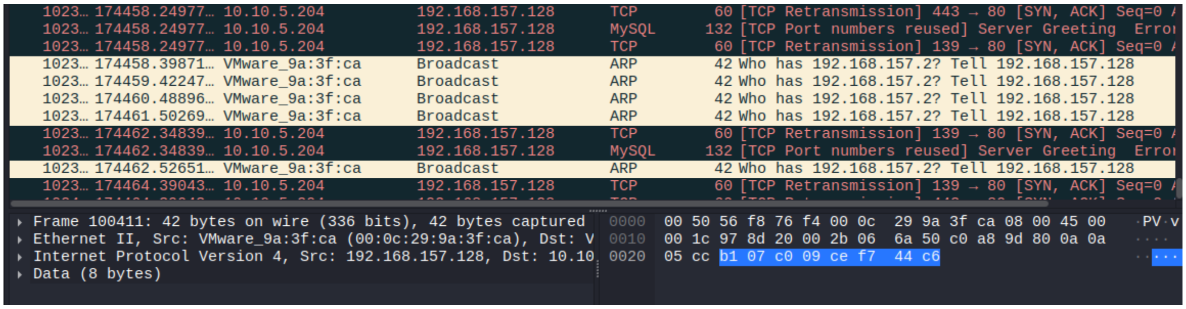
En Wireshark deberían ver:

Tráfico con fragmentación de paquetes TCP/IP.


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

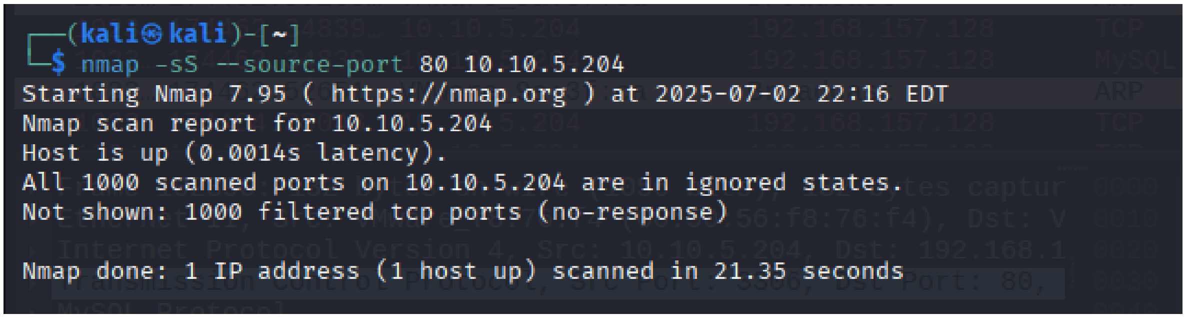
```
No.     Time            Source            Destination     Protocol  Length Info
  1004… 173924.33156… 192.168.157.128  10.10.5.204     TCP          42 45319 → 5802 [SYN] Seq=0 Win=1024 Len=0 MSS=146
  1004… 173924.35144… 192.168.157.128  10.10.5.204     IPv4         42 Fragmented IP protocol (proto=TCP 6, off=0, ID=
  1004… 173924.35156… 192.168.157.128  10.10.5.204     IPv4         42 Fragmented IP protocol (proto=TCP 6, off=8, ID=
  1004… 173924.35163… 192.168.157.128  10.10.5.204     TCP          42 45319 → 1199 [SYN] Seq=0 Win=1024 Len=0 MSS=146
  1004… 173924.37170… 192.168.157.128  10.10.5.204     IPv4         42 Fragmented IP protocol (proto=TCP 6, off=0, ID=
  1004… 173924.37188… 192.168.157.128  10.10.5.204     IPv4         42 Fragmented IP protocol (proto=TCP 6, off=8, ID=
  1004… 173924.37217… 192.168.157.128  10.10.5.204     TCP          42 45319 → 17 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  1004… 173924.39189… 192.168.157.128  10.10.5.204     IPv4         42 Fragmented IP protocol (proto=TCP 6, off=0, ID=
  1004… 173924.39203… 192.168.157.128  10.10.5.204     IPv4         42 Fragmented IP protocol (proto=TCP 6, off=8, ID=
  1004… 173924.39217… 192.168.157.128  10.10.5.204     TCP          42 45319 → 1201 [SYN] Seq=0 Win=1024 Len=0 MSS=146
  1004… 173924.41206… 192.168.157.128  10.10.5.204     IPv4         42 Fragmented IP protocol (proto=TCP 6, off=0, ID=
  1004… 173924.41220… 192.168.157.128  10.10.5.204     IPv4         42 Fragmented IP protocol (proto=TCP 6, off=8, ID=
  1004… 173924.41229… 192.168.157.128  10.10.5.204     TCP          42 45319 → 49161 [SYN] Seq=0 Win=1024 Len=0 MSS=14
  1004… 173924.43224… 192.168.157.128  10.10.5.204     IPv4         42 Fragmented IP protocol (proto=TCP 6, off=0, ID=
  1004… 173924.43239… 192.168.157.128  10.10.5.204     IPv4         42 Fragmented IP protocol (proto=TCP 6, off=8, ID=
  1004… 173924.43247… 192.168.157.128  10.10.5.204     TCP          42 45319 → 3006 [SYN] Seq=0 Win=1024 Len=0 MSS=146

▸ Frame 86379: 60 bytes on wire (480 bits), 60 bytes captured (   0000  00 0c 29 9a 3f ca 00 50  56 f8 76 f4 08 00 45 00   ··)·?
▸ Ethernet II, Src: VMware_f8:76:f4 (00:50:56:f8:76:f4), Dst: V   0010  00 1c 8f 52 00 00 80 01  3d 90 0a 0a 05 cc c0 a8   ···R·
▸ Internet Protocol Version 4, Src: 10.10.5.204, Dst: 192.168.1   0020  9d 80 00 00 0e 21 f1 de  00 00 00 00 00 00 00 00   ·····
▸ Internet Control Message Protocol                                0030  00 00 00 00 00 00 00 00  00 00 00 00               ·····
```

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



```
  1023… 174458.24977… 10.10.5.204       192.168.157.128  TCP         60 [TCP Retransmission] 443 → 80 [SYN, ACK] Seq=0 
  1023… 174458.24977… 10.10.5.204       192.168.157.128  MySQL      132 [TCP Port numbers reused] Server Greeting  Erro
  1023… 174458.24977… 10.10.5.204       192.168.157.128  TCP         60 [TCP Retransmission] 139 → 80 [SYN, ACK] Seq=0 
  1023… 174458.39871… VMware_9a:3f:ca   Broadcast        ARP         42 Who has 192.168.157.2? Tell 192.168.157.128
  1023… 174459.42247… VMware_9a:3f:ca   Broadcast        ARP         42 Who has 192.168.157.2? Tell 192.168.157.128
  1023… 174460.48896… VMware_9a:3f:ca   Broadcast        ARP         42 Who has 192.168.157.2? Tell 192.168.157.128
  1023… 174461.50269… VMware_9a:3f:ca   Broadcast        ARP         42 Who has 192.168.157.2? Tell 192.168.157.128
  1023… 174462.34839… 10.10.5.204       192.168.157.128  TCP         60 [TCP Retransmission] 139 → 80 [SYN, ACK] Seq=0 
  1023… 174462.34839… 10.10.5.204       192.168.157.128  MySQL      132 [TCP Port numbers reused] Server Greeting  Erro
  1023… 174462.52651… VMware_9a:3f:ca   Broadcast        ARP         42 Who has 192.168.157.2? Tell 192.168.157.128
  1023… 174464.39043… 10.10.5.204       192.168.157.128  TCP         60 [TCP Retransmission] 139 → 80 [SYN, ACK] Seq=0 

▸ Frame 100411: 42 bytes on wire (336 bits), 42 bytes captured   0000  00 50 56 f8 76 f4 00 0c  29 9a 3f ca 08 00 45 00   ·PV·v
▸ Ethernet II, Src: VMware_9a:3f:ca (00:0c:29:9a:3f:ca), Dst: V  0010  00 1c 97 8d 20 00 2b 06  6a 50 c0 a8 9d 80 0a 0a   ····
▸ Internet Protocol Version 4, Src: 192.168.157.128, Dst: 10.10  0020  05 cc b1 07 c0 09 ce f7  44 c6                     ·····
▸ Data (8 bytes)
```

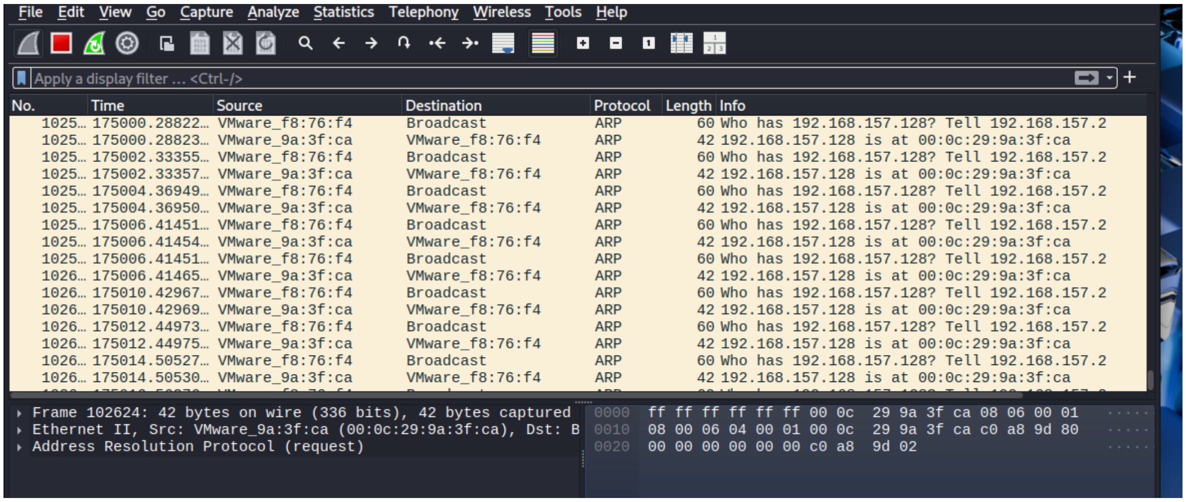
Coloque el puerto 80 ya que no me detecto otros equipo y detecto el mysql de mi equipo



```
┌──(kali㉿kali)-[~]
└─$ nmap -sS --source-port 80 10.10.5.204
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 22:16 EDT
Nmap scan report for 10.10.5.204
Host is up (0.0014s latency).
All 1000 scanned ports on 10.10.5.204 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.35 seconds
```

Comando: nmap -Ss –source port 80

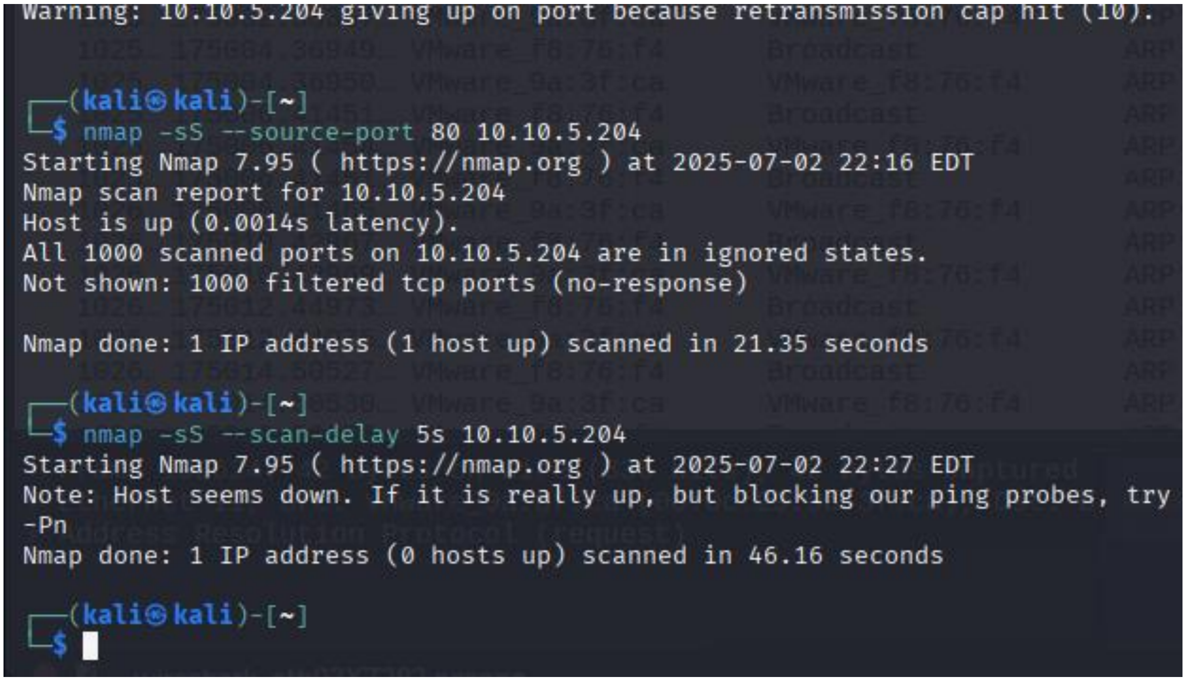
- Intervalos largos entre los paquetes (bajo volumen).



No.	Time	Source	Destination	Protocol	Length	Info
1025…	175000.28822…	VMware_f8:76:f4	Broadcast	ARP	60	Who has 192.168.157.128? Tell 192.168.157.2
1025…	175000.28823…	VMware_9a:3f:ca	VMware_f8:76:f4	ARP	42	192.168.157.128 is at 00:0c:29:9a:3f:ca
1025…	175002.33355…	VMware_f8:76:f4	Broadcast	ARP	60	Who has 192.168.157.128? Tell 192.168.157.2
1025…	175002.33357…	VMware_9a:3f:ca	VMware_f8:76:f4	ARP	42	192.168.157.128 is at 00:0c:29:9a:3f:ca
1025…	175004.36949…	VMware_f8:76:f4	Broadcast	ARP	60	Who has 192.168.157.128? Tell 192.168.157.2
1025…	175004.36950…	VMware_9a:3f:ca	VMware_f8:76:f4	ARP	42	192.168.157.128 is at 00:0c:29:9a:3f:ca
1025…	175006.41451…	VMware_f8:76:f4	Broadcast	ARP	60	Who has 192.168.157.128? Tell 192.168.157.2
1025…	175006.41454…	VMware_9a:3f:ca	VMware_f8:76:f4	ARP	42	192.168.157.128 is at 00:0c:29:9a:3f:ca
1025…	175006.41451…	VMware_f8:76:f4	Broadcast	ARP	60	Who has 192.168.157.128? Tell 192.168.157.2
1026…	175006.41465…	VMware_9a:3f:ca	VMware_f8:76:f4	ARP	42	192.168.157.128 is at 00:0c:29:9a:3f:ca
1026…	175010.42967…	VMware_f8:76:f4	Broadcast	ARP	60	Who has 192.168.157.128? Tell 192.168.157.2
1026…	175010.42969…	VMware_9a:3f:ca	VMware_f8:76:f4	ARP	42	192.168.157.128 is at 00:0c:29:9a:3f:ca
1026…	175012.44973…	VMware_f8:76:f4	Broadcast	ARP	60	Who has 192.168.157.128? Tell 192.168.157.2
1026…	175012.44975…	VMware_9a:3f:ca	VMware_f8:76:f4	ARP	42	192.168.157.128 is at 00:0c:29:9a:3f:ca
1026…	175014.50527…	VMware_f8:76:f4	Broadcast	ARP	60	Who has 192.168.157.128? Tell 192.168.157.2
1026…	175014.50530…	VMware_9a:3f:ca	VMware_f8:76:f4	ARP	42	192.168.157.128 is at 00:0c:29:9a:3f:ca

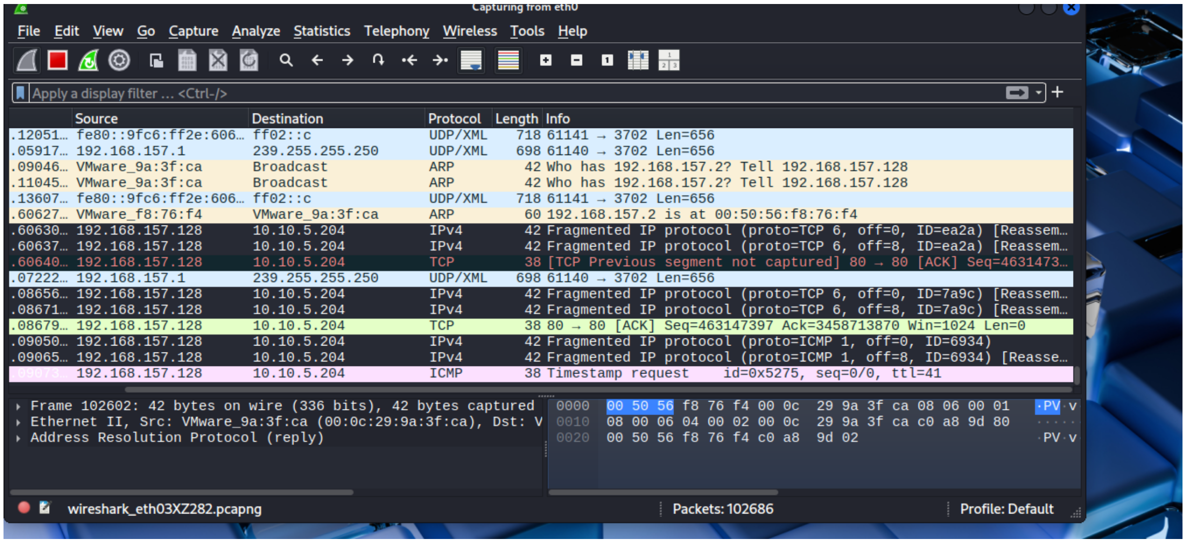
```
› Frame 102624: 42 bytes on wire (336 bits), 42 bytes captured
› Ethernet II, Src: VMware_9a:3f:ca (00:0c:29:9a:3f:ca), Dst: B
› Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 0c  29 9a 3f ca 08 06 00 01
0010  08 00 06 04 00 01 00 0c  29 9a 3f ca c0 a8 9d 80
0020  00 00 00 00 00 00 c0 a8  9d 02
```



```
Warning: 10.10.5.204 giving up on port because retransmission cap hit (10).

┌──(kali㉿kali)-[~]
└─$ nmap -sS --source-port 80 10.10.5.204
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 22:16 EDT
Nmap scan report for 10.10.5.204
Host is up (0.0014s latency).
All 1000 scanned ports on 10.10.5.204 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.35 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sS --scan-delay 5s 10.10.5.204
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 22:27 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 46.16 seconds

┌──(kali㉿kali)-[~]
└─$ █
```

- Tráfico que no completa handshakes TCP.

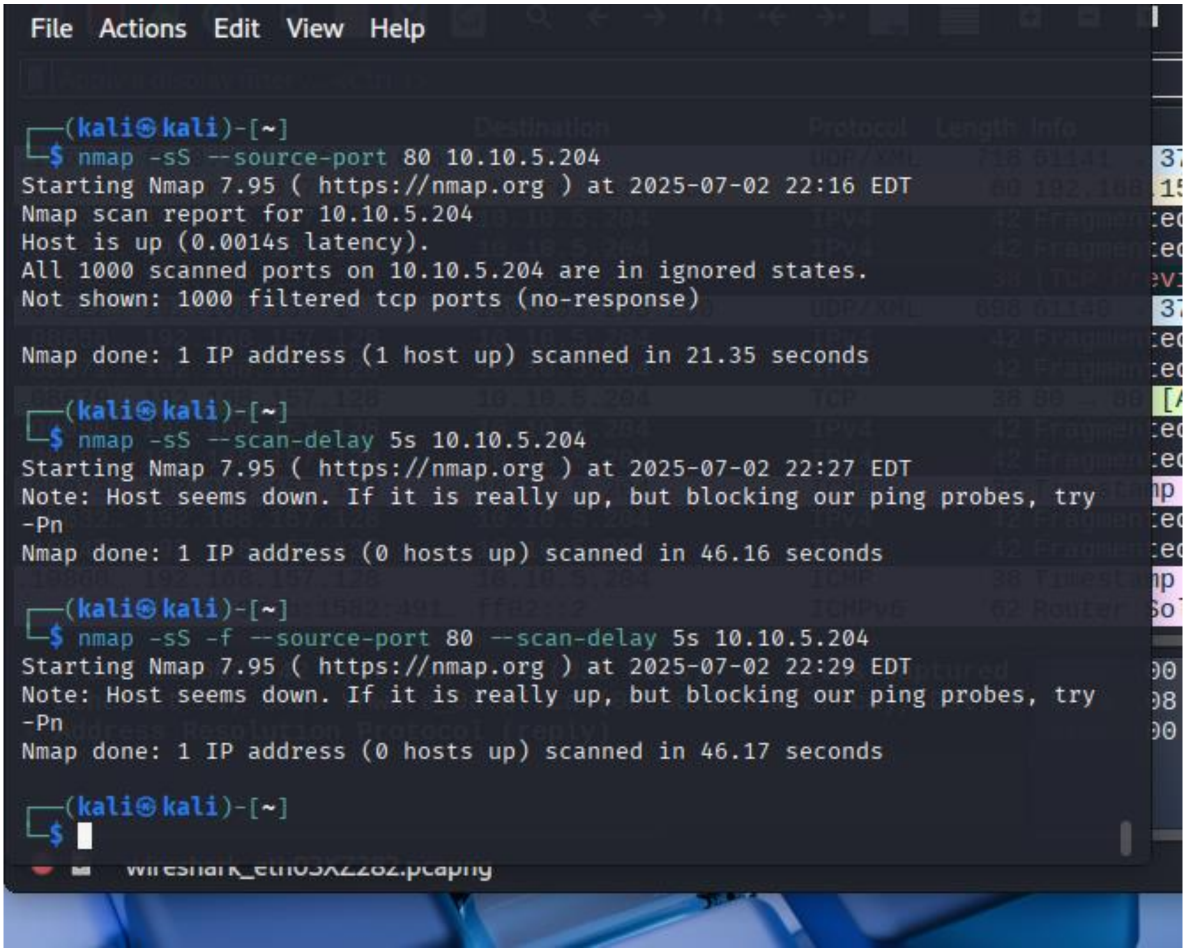


```
          Source                 Destination      Protocol Length Info
.12051… fe80::9fc6:ff2e:606… ff02::c          UDP/XML   718 61141 → 3702 Len=656
.05917… 192.168.157.1        239.255.255.250  UDP/XML   698 61140 → 3702 Len=656
.09046… VMware_9a:3f:ca      Broadcast        ARP        42 Who has 192.168.157.2? Tell 192.168.157.128
.11045… VMware_9a:3f:ca      Broadcast        ARP        42 Who has 192.168.157.2? Tell 192.168.157.128
.13607… fe80::9fc6:ff2e:606… ff02::c          UDP/XML   718 61141 → 3702 Len=656
.60627… VMware_f8:76:f4      VMware_9a:3f:ca  ARP        60 192.168.157.2 is at 00:50:56:f8:76:f4
.60630… 192.168.157.128      10.10.5.204      IPv4       42 Fragmented IP protocol (proto=TCP 6, off=0, ID=ea2a) [Reassem…
.60637… 192.168.157.128      10.10.5.204      IPv4       42 Fragmented IP protocol (proto=TCP 6, off=8, ID=ea2a) [Reassem…
.60640… 192.168.157.128      10.10.5.204      TCP        38 [TCP Previous segment not captured] 80 → 80 [ACK] Seq=4631473…
.07222… 192.168.157.1        239.255.255.250  UDP/XML   698 61140 → 3702 Len=656
.08656… 192.168.157.128      10.10.5.204      IPv4       42 Fragmented IP protocol (proto=TCP 6, off=0, ID=7a9c) [Reassem…
.08671… 192.168.157.128      10.10.5.204      IPv4       42 Fragmented IP protocol (proto=TCP 6, off=8, ID=7a9c) [Reassem…
.08679… 192.168.157.128      10.10.5.204      TCP        38 80 → 80 [ACK] Seq=463147397 Ack=3458713870 Win=1024 Len=0
.09050… 192.168.157.128      10.10.5.204      IPv4       42 Fragmented IP protocol (proto=ICMP 1, off=0, ID=6934)
.09065… 192.168.157.128      10.10.5.204      IPv4       42 Fragmented IP protocol (proto=ICMP 1, off=8, ID=6934) [Reasse…
.09073… 192.168.157.128      10.10.5.204      ICMP       38 Timestamp request    id=0x5275, seq=0/0, ttl=41
```

```
› Frame 102602: 42 bytes on wire (336 bits), 42 bytes captured
› Ethernet II, Src: VMware_9a:3f:ca (00:0c:29:9a:3f:ca), Dst: V
› Address Resolution Protocol (reply)
```

```
0000  00 50 56 f8 76 f4 00 0c  29 9a 3f ca 08 06 00 01   ·PV·v
0010  08 00 06 04 00 02 00 0c  29 9a 3f ca c0 a8 9d 80   ·····
0020  00 50 56 f8 76 f4 c0 a8  9d 02                     ·PV·v
```

wireshark_eth03XZ282.pcapng   Packets: 102686   Profile: Default



```
┌──(kali㉿kali)-[~]
└─$ nmap -sS --source-port 80 10.10.5.204
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 22:16 EDT
Nmap scan report for 10.10.5.204
Host is up (0.0014s latency).
All 1000 scanned ports on 10.10.5.204 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.35 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sS --scan-delay 5s 10.10.5.204
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 22:27 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 46.16 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sS -f --source-port 80 --scan-delay 5s 10.10.5.204
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 22:29 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 46.17 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

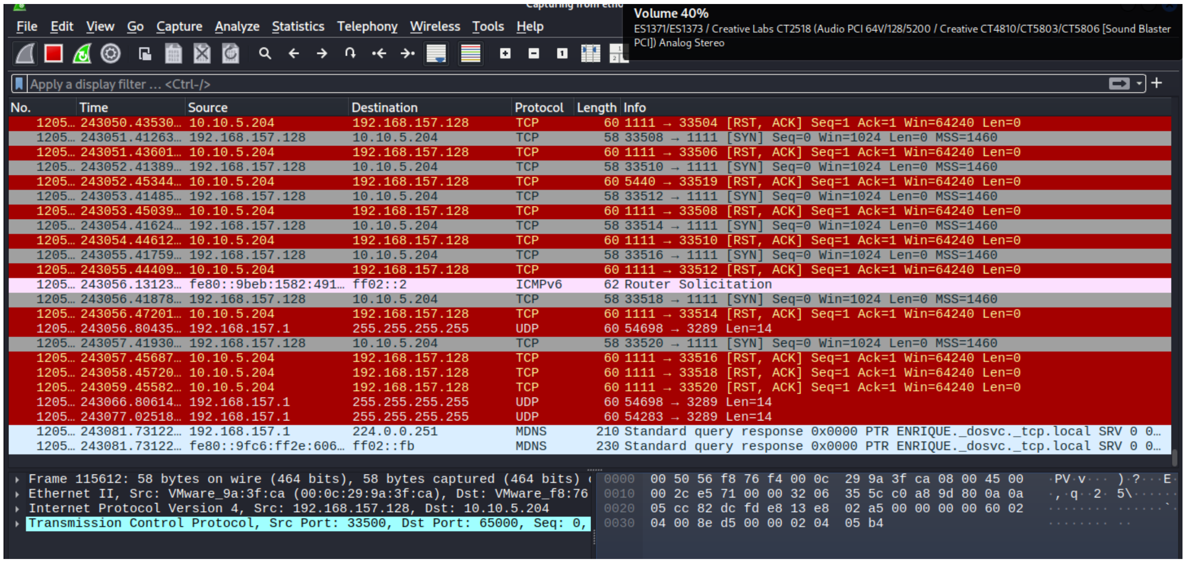
Ejercicio 3: Enumeración avanzada de servicios

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:

Fitros: tcp.port == 21 || tcp.port == 22 || tcp.port == 80 || tcp.port == 443

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

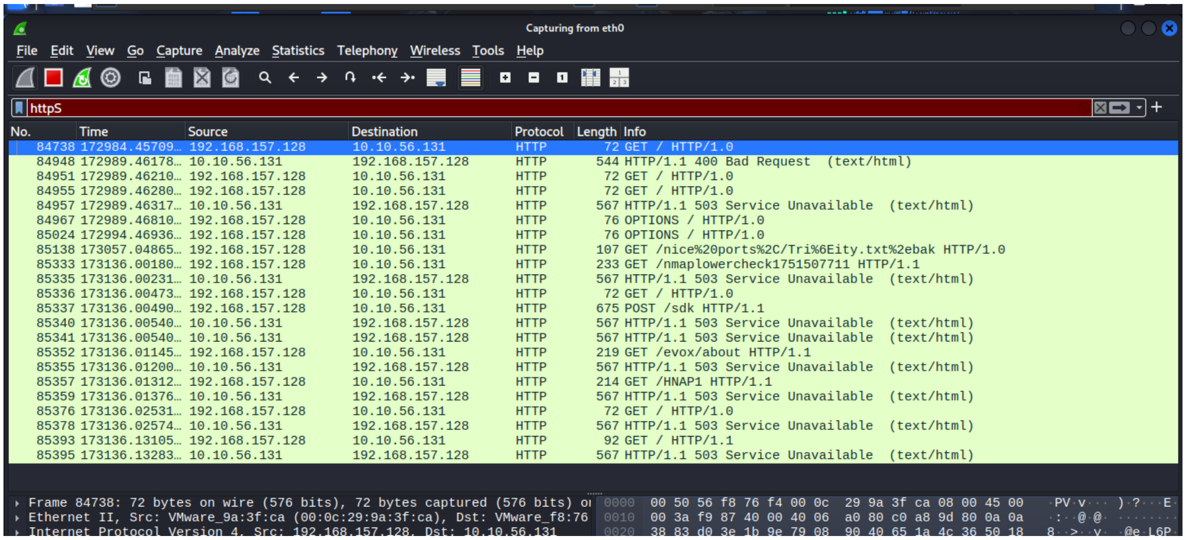


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Volume 40%
ES1371/ES1373 / Creative Labs CT2518 (Audio PCI 64V/128/5200 / Creative CT4810/CT5803/CT5806 [Sound Blaster PCI]) Analog Stereo
Apply a display filter … <Ctrl-/>

```
No.     Time            Source                  Destination       Protocol  Length Info
  1205… 243050.43530… 10.10.5.204             192.168.157.128   TCP         60 1111 → 33504 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
  1205… 243051.41263… 192.168.157.128         10.10.5.204       TCP         58 33508 → 1111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  1205… 243051.43601… 10.10.5.204             192.168.157.128   TCP         60 1111 → 33506 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
  1205… 243052.41389… 192.168.157.128         10.10.5.204       TCP         58 33510 → 1111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  1205… 243052.45344… 10.10.5.204             192.168.157.128   TCP         60 5440 → 33519 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
  1205… 243053.41485… 192.168.157.128         10.10.5.204       TCP         58 33512 → 1111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  1205… 243053.45039… 10.10.5.204             192.168.157.128   TCP         60 1111 → 33508 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
  1205… 243054.41624… 192.168.157.128         10.10.5.204       TCP         58 33514 → 1111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  1205… 243054.44612… 10.10.5.204             192.168.157.128   TCP         60 1111 → 33510 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
  1205… 243055.41759… 192.168.157.128         10.10.5.204       TCP         58 33516 → 1111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  1205… 243055.44409… 10.10.5.204             192.168.157.128   TCP         60 1111 → 33512 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
  1205… 243056.13123… fe80::9beb:1582:491… ff02::2           ICMPv6      62 Router Solicitation
  1205… 243056.41878… 192.168.157.128         10.10.5.204       TCP         58 33518 → 1111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  1205… 243056.47201… 10.10.5.204             192.168.157.128   TCP         60 1111 → 33514 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
  1205… 243056.80435… 192.168.157.1           255.255.255.255   UDP         60 54698 → 3289 Len=14
  1205… 243057.41930… 192.168.157.128         10.10.5.204       TCP         58 33520 → 1111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  1205… 243057.45687… 10.10.5.204             192.168.157.128   TCP         60 1111 → 33516 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
  1205… 243058.45720… 10.10.5.204             192.168.157.128   TCP         60 1111 → 33518 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
  1205… 243059.45582… 10.10.5.204             192.168.157.128   TCP         60 1111 → 33520 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
  1205… 243066.80614… 192.168.157.1           255.255.255.255   UDP         60 54698 → 3289 Len=14
  1205… 243077.02518… 192.168.157.1           255.255.255.255   UDP         60 54283 → 3289 Len=14
  1205… 243081.73122… 192.168.157.1           224.0.0.251       MDNS       210 Standard query response 0x0000 PTR ENRIQUE._dosvc._tcp.local SRV 0 0…
  1205… 243081.73122… fe80::9fc6:ff2e:606… ff02::fb          MDNS       230 Standard query response 0x0000 PTR ENRIQUE._dosvc._tcp.local SRV 0 0…

› Frame 115612: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) (   0000  00 50 56 f8 76 f4 00 0c  29 9a 3f ca 08 00 45 00   ·PV·v··· )·?···E·
› Ethernet II, Src: VMware_9a:3f:ca (00:0c:29:9a:3f:ca), Dst: VMware_f8:76   0010  00 2c e5 71 00 00 32 06  35 5c c0 a8 9d 80 0a 0a   ·,·q··2· 5\······
› Internet Protocol Version 4, Src: 192.168.157.128, Dst: 10.10.5.204         0020  05 cc 82 dc fd e8 13 e8  02 a5 00 00 00 00 60 02   ········ ······`·
› Transmission Control Protocol, Src Port: 33500, Dst Port: 65000, Seq: 0,    0030  04 00 8e d5 00 00 02 04  05 b4                     ········ ··
```

Comandos utilizados sudo nmap -sV --script=banner -p 21,22,80,443

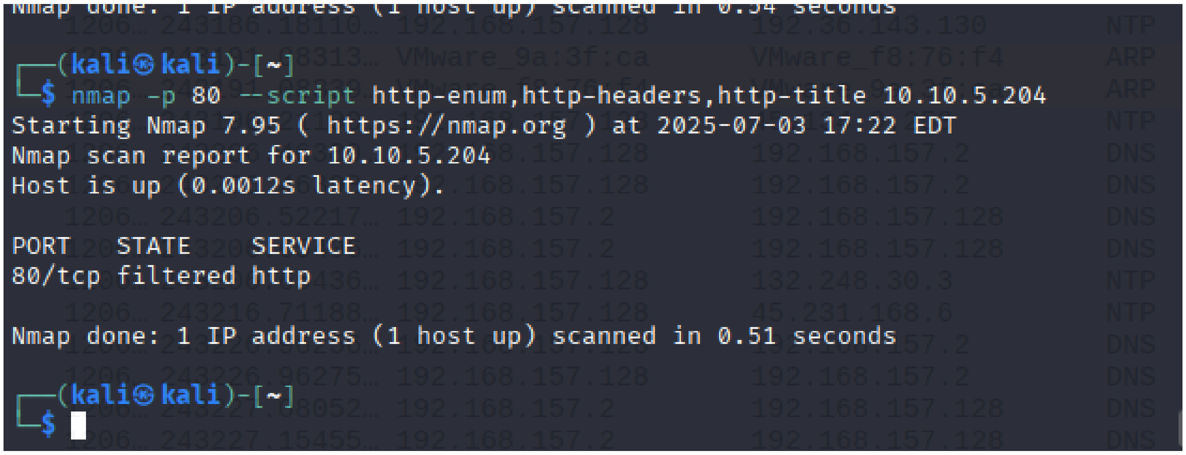
- Tráfico con comandos FTP, HTTP o SSH.



Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
httpS

```
No.     Time            Source            Destination       Protocol  Length Info
  84738 172984.45709… 192.168.157.128   10.10.56.131      HTTP        72 GET / HTTP/1.0
  84948 172989.46178… 10.10.56.131      192.168.157.128   HTTP       544 HTTP/1.1 400 Bad Request  (text/html)
  84951 172989.46210… 192.168.157.128   10.10.56.131      HTTP        72 GET / HTTP/1.0
  84955 172989.46280… 192.168.157.128   10.10.56.131      HTTP        72 GET / HTTP/1.0
  84957 172989.46317… 10.10.56.131      192.168.157.128   HTTP       567 HTTP/1.1 503 Service Unavailable  (text/html)
  84967 172989.46810… 192.168.157.128   10.10.56.131      HTTP        76 OPTIONS / HTTP/1.0
  85024 172994.46936… 192.168.157.128   10.10.56.131      HTTP        76 OPTIONS / HTTP/1.0
  85138 173057.04865… 192.168.157.128   10.10.56.131      HTTP       107 GET /nice%20ports%2C/Tri%6Eity.txt%2ebak HTTP/1.0
  85333 173136.00180… 192.168.157.128   10.10.56.131      HTTP       233 GET /nmaplowercheck1751507711 HTTP/1.1
  85335 173136.00231… 10.10.56.131      192.168.157.128   HTTP       567 HTTP/1.1 503 Service Unavailable  (text/html)
  85336 173136.00473… 192.168.157.128   10.10.56.131      HTTP        72 GET / HTTP/1.0
  85337 173136.00490… 192.168.157.128   10.10.56.131      HTTP       675 POST /sdk HTTP/1.1
  85340 173136.00540… 10.10.56.131      192.168.157.128   HTTP       567 HTTP/1.1 503 Service Unavailable  (text/html)
  85341 173136.00540… 10.10.56.131      192.168.157.128   HTTP       567 HTTP/1.1 503 Service Unavailable  (text/html)
  85352 173136.01145… 192.168.157.128   10.10.56.131      HTTP       219 GET /evox/about HTTP/1.1
  85355 173136.01200… 10.10.56.131      192.168.157.128   HTTP       567 HTTP/1.1 503 Service Unavailable  (text/html)
  85357 173136.01312… 192.168.157.128   10.10.56.131      HTTP       214 GET /HNAP1 HTTP/1.1
  85359 173136.01376… 10.10.56.131      192.168.157.128   HTTP       567 HTTP/1.1 503 Service Unavailable  (text/html)
  85376 173136.02531… 192.168.157.128   10.10.56.131      HTTP        72 GET / HTTP/1.0
  85378 173136.02574… 10.10.56.131      192.168.157.128   HTTP       567 HTTP/1.1 503 Service Unavailable  (text/html)
  85393 173136.13105… 192.168.157.128   10.10.56.131      HTTP        92 GET / HTTP/1.1
  85395 173136.13283… 10.10.56.131      192.168.157.128   HTTP       567 HTTP/1.1 503 Service Unavailable  (text/html)

› Frame 84738: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) o   0000  00 50 56 f8 76 f4 00 0c  29 9a 3f ca 08 00 45 00   ·PV·v··· )·?···E·
› Ethernet II, Src: VMware_9a:3f:ca (00:0c:29:9a:3f:ca), Dst: VMware_f8:76   0010  00 3a f9 87 40 00 40 06  a0 80 c0 a8 9d 80 0a 0a   ·:··@·@· ········
› Internet Protocol Version 4, Src: 192.168.157.128, Dst: 10.10.56.131        0020  38 83 d0 3e 1b 9e 79 08  90 40 65 1a 4c 36 50 18   8··>··y· ·@e·L6P·
```

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



```
Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -p 80 --script http-enum,http-headers,http-title 10.10.5.204
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-03 17:22 EDT
Nmap scan report for 10.10.5.204
Host is up (0.0012s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

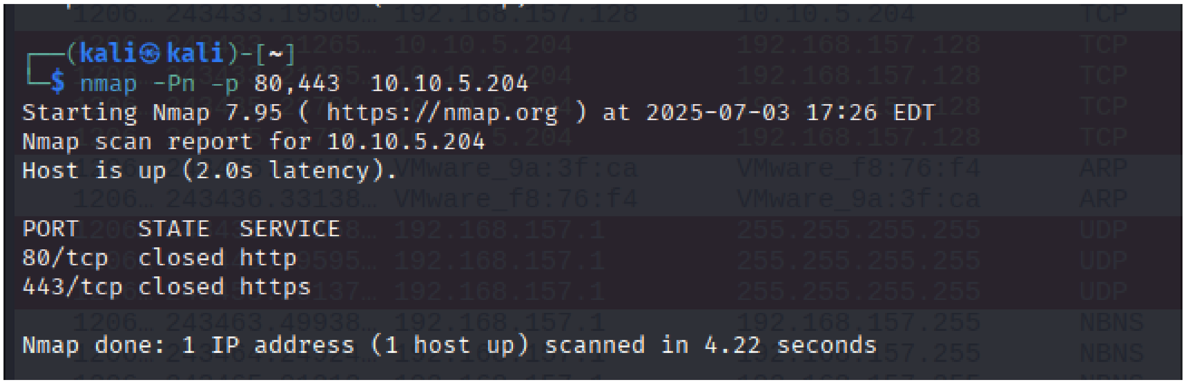
nmap -p 80 --script http-enum,http-headers,http-title

Ejercicio 4: Detección de hosts sin ICMP habilitado

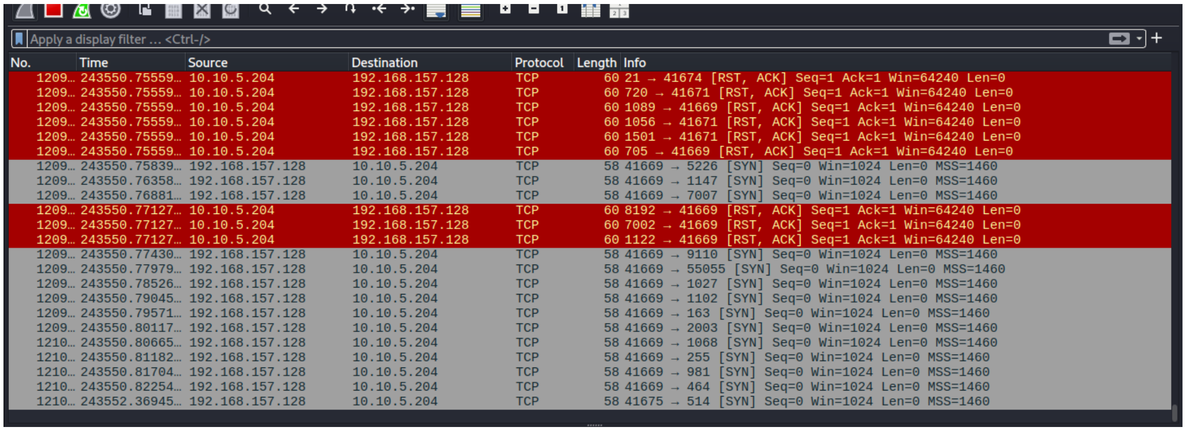
Encuentra dentro de tu red aquellos hosts que no responden a ping (ICMP), pero que tienen puertos abiertos accesibles. Analiza si puedes detectarlos sin depender de ICMP.

En Wireshark deberían ver:

- Escaneos TCP sin tráfico ICMP.



```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -p 80,443  10.10.5.204
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-03 17:26 EDT
Nmap scan report for 10.10.5.204
Host is up (2.0s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 4.22 seconds
```

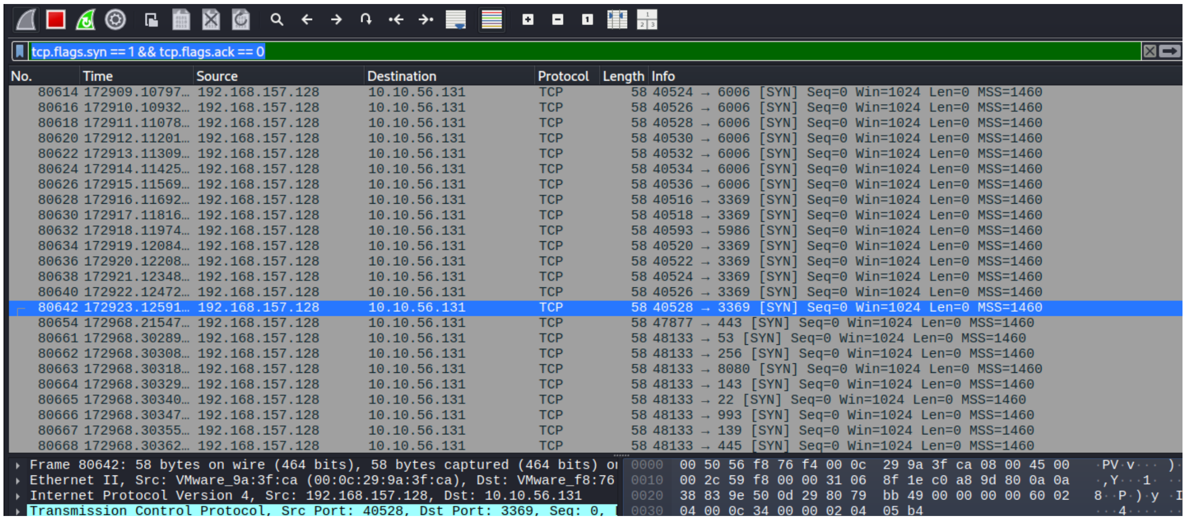


```
Apply a display filter … <Ctrl-/>
No.      Time             Source            Destination       Protocol  Length Info
  1209… 243550.75559… 10.10.5.204       192.168.157.128   TCP          60 21 → 41674 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
  1209… 243550.75559… 10.10.5.204       192.168.157.128   TCP          60 720 → 41671 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
  1209… 243550.75559… 10.10.5.204       192.168.157.128   TCP          60 1089 → 41669 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
  1209… 243550.75559… 10.10.5.204       192.168.157.128   TCP          60 1056 → 41671 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
  1209… 243550.75559… 10.10.5.204       192.168.157.128   TCP          60 1501 → 41671 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
  1209… 243550.75559… 10.10.5.204       192.168.157.128   TCP          60 705 → 41669 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
  1209… 243550.75839… 192.168.157.128   10.10.5.204       TCP          58 41669 → 5226 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  1209… 243550.76358… 192.168.157.128   10.10.5.204       TCP          58 41669 → 1147 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  1209… 243550.76881… 192.168.157.128   10.10.5.204       TCP          58 41669 → 7007 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  1209… 243550.77127… 10.10.5.204       192.168.157.128   TCP          60 8192 → 41669 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
  1209… 243550.77127… 10.10.5.204       192.168.157.128   TCP          60 7002 → 41669 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
  1209… 243550.77127… 10.10.5.204       192.168.157.128   TCP          60 1122 → 41669 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
  1209… 243550.77430… 192.168.157.128   10.10.5.204       TCP          58 41669 → 9110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  1209… 243550.77979… 192.168.157.128   10.10.5.204       TCP          58 41669 → 55055 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  1209… 243550.78526… 192.168.157.128   10.10.5.204       TCP          58 41669 → 1027 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  1209… 243550.79045… 192.168.157.128   10.10.5.204       TCP          58 41669 → 1102 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  1209… 243550.79571… 192.168.157.128   10.10.5.204       TCP          58 41669 → 163 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  1209… 243550.80117… 192.168.157.128   10.10.5.204       TCP          58 41669 → 2003 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  1210… 243550.80665… 192.168.157.128   10.10.5.204       TCP          58 41669 → 1068 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  1210… 243550.81182… 192.168.157.128   10.10.5.204       TCP          58 41669 → 255 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  1210… 243550.81704… 192.168.157.128   10.10.5.204       TCP          58 41669 → 981 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  1210… 243550.82254… 192.168.157.128   10.10.5.204       TCP          58 41669 → 464 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  1210… 243552.36945… 192.168.157.128   10.10.5.204       TCP          58 41675 → 514 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

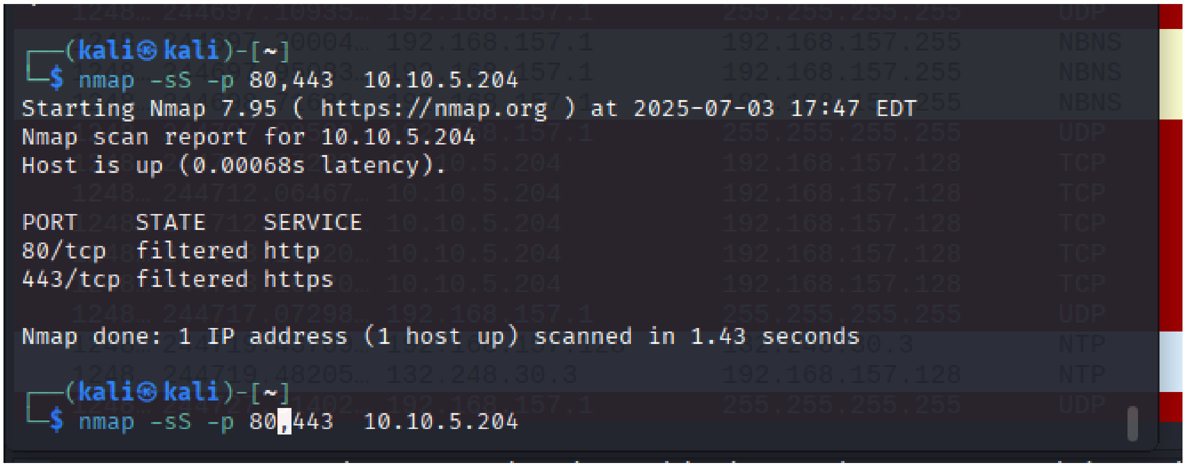
Utilice el comndo nmap -Pn -p 80,443, pero me marcaba que ese puerto estaba bloquedo, por lo que decidí realizarlo hacia todos los puertos

- Solicitudes TCP SYN enviadas directamente a puertos específicos.

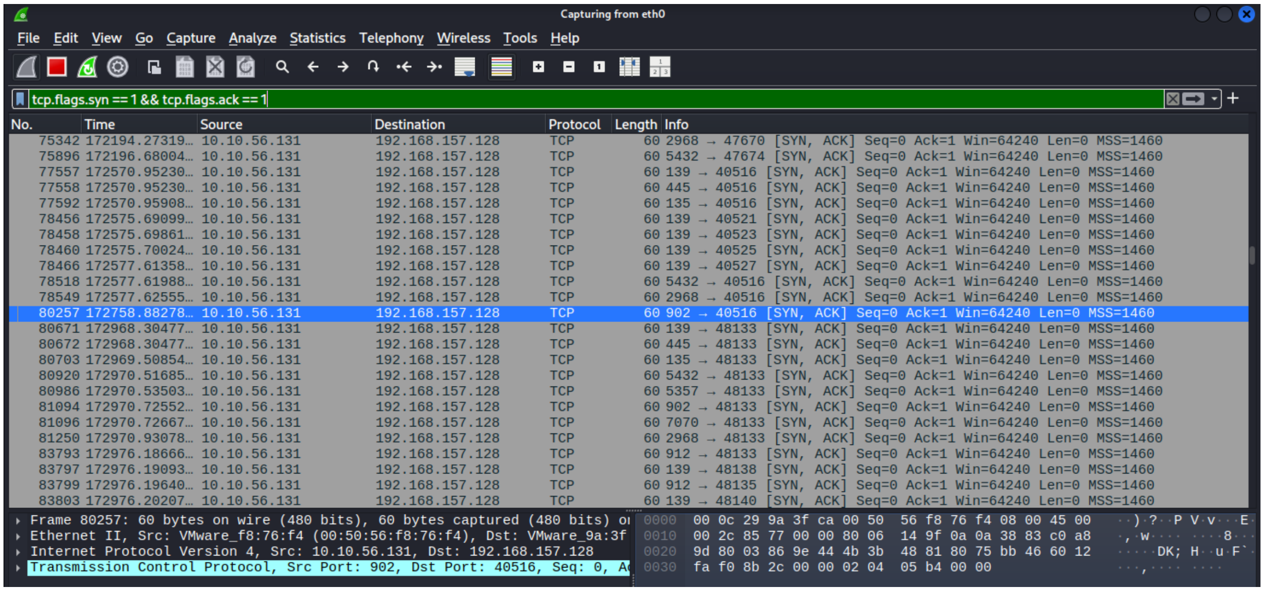
Fitros: tcp.flags.syn == 1 && tcp.flags.ack == 0 y tcp.flags.syn == 0 && tcp.flags.ack == 1



```
tcp.flags.syn == 1 && tcp.flags.ack == 0
No.     Time             Source            Destination       Protocol  Length Info
  80614 172909.10797… 192.168.157.128   10.10.56.131      TCP          58 40524 → 6006 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80616 172910.10932… 192.168.157.128   10.10.56.131      TCP          58 40526 → 6006 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80618 172911.11078… 192.168.157.128   10.10.56.131      TCP          58 40528 → 6006 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80620 172912.11201… 192.168.157.128   10.10.56.131      TCP          58 40530 → 6006 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80622 172913.11309… 192.168.157.128   10.10.56.131      TCP          58 40532 → 6006 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80624 172914.11425… 192.168.157.128   10.10.56.131      TCP          58 40534 → 6006 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80626 172915.11569… 192.168.157.128   10.10.56.131      TCP          58 40536 → 6006 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80628 172916.11692… 192.168.157.128   10.10.56.131      TCP          58 40516 → 3369 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80630 172917.11816… 192.168.157.128   10.10.56.131      TCP          58 40518 → 3369 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80632 172918.11974… 192.168.157.128   10.10.56.131      TCP          58 40593 → 5986 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80634 172919.12084… 192.168.157.128   10.10.56.131      TCP          58 40520 → 3369 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80636 172920.12208… 192.168.157.128   10.10.56.131      TCP          58 40522 → 3369 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80638 172921.12348… 192.168.157.128   10.10.56.131      TCP          58 40524 → 3369 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80640 172922.12472… 192.168.157.128   10.10.56.131      TCP          58 40526 → 3369 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80642 172923.12591… 192.168.157.128   10.10.56.131      TCP          58 40528 → 3369 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80654 172968.21547… 192.168.157.128   10.10.56.131      TCP          58 47877 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80661 172968.30289… 192.168.157.128   10.10.56.131      TCP          58 48133 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80662 172968.30308… 192.168.157.128   10.10.56.131      TCP          58 48133 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80663 172968.30318… 192.168.157.128   10.10.56.131      TCP          58 48133 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80664 172968.30329… 192.168.157.128   10.10.56.131      TCP          58 48133 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80665 172968.30340… 192.168.157.128   10.10.56.131      TCP          58 48133 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80666 172968.30347… 192.168.157.128   10.10.56.131      TCP          58 48133 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80667 172968.30355… 192.168.157.128   10.10.56.131      TCP          58 48133 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  80668 172968.30362… 192.168.157.128   10.10.56.131      TCP          58 48133 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

▸ Frame 80642: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) o   0000  00 50 56 f8 76 f4 00 0c  29 9a 3f ca 08 00 45 00   ·PV·v··· )
▸ Ethernet II, Src: VMware_9a:3f:ca (00:0c:29:9a:3f:ca), Dst: VMware_f8:76   0010  00 2c 59 f8 00 00 31 06  8f 1e c0 a8 9d 80 0a 0a   ·,Y···1·
▸ Internet Protocol Version 4, Src: 192.168.157.128, Dst: 10.10.56.131       0020  38 83 9e 50 0d 29 80 79  bb 49 00 00 00 00 60 02   8··P·)·y ·I
▸ Transmission Control Protocol, Src Port: 40528, Dst Port: 3369, Seq: 0,    0030  04 00 0c 34 00 00 02 04  05 b4                     ···4····
```

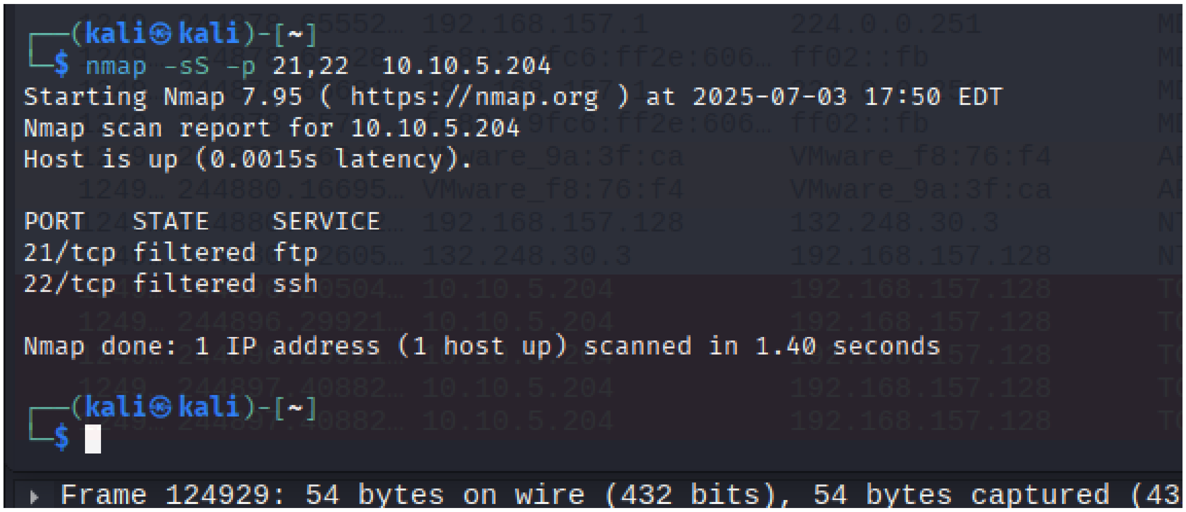


```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -p 80,443  10.10.5.204
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-03 17:47 EDT
Nmap scan report for 10.10.5.204
Host is up (0.00068s latency).

PORT    STATE    SERVICE
80/tcp  filtered http
443/tcp filtered https

Nmap done: 1 IP address (1 host up) scanned in 1.43 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sS -p 80,443  10.10.5.204
```



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

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

No.   Time            Source         Destination      Protocol Length Info
75342 172194.27319…  10.10.56.131   192.168.157.128  TCP      60 2968 → 47670 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
75896 172196.68004…  10.10.56.131   192.168.157.128  TCP      60 5432 → 47674 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
77557 172570.95230…  10.10.56.131   192.168.157.128  TCP      60 139 → 40516 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
77558 172570.95230…  10.10.56.131   192.168.157.128  TCP      60 445 → 40516 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
77592 172570.95908…  10.10.56.131   192.168.157.128  TCP      60 135 → 40516 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
78456 172575.69099…  10.10.56.131   192.168.157.128  TCP      60 139 → 40521 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
78458 172575.69861…  10.10.56.131   192.168.157.128  TCP      60 139 → 40523 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
78460 172575.70024…  10.10.56.131   192.168.157.128  TCP      60 139 → 40525 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
78466 172577.61358…  10.10.56.131   192.168.157.128  TCP      60 139 → 40527 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
78518 172577.61988…  10.10.56.131   192.168.157.128  TCP      60 5432 → 40516 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
78549 172577.62555…  10.10.56.131   192.168.157.128  TCP      60 2968 → 40516 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
80257 172758.88278…  10.10.56.131   192.168.157.128  TCP      60 902 → 40516 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
80671 172968.30477…  10.10.56.131   192.168.157.128  TCP      60 139 → 48133 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
80672 172968.30477…  10.10.56.131   192.168.157.128  TCP      60 445 → 48133 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
80703 172969.50854…  10.10.56.131   192.168.157.128  TCP      60 135 → 48133 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
80920 172970.51685…  10.10.56.131   192.168.157.128  TCP      60 5432 → 48133 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
80986 172970.53503…  10.10.56.131   192.168.157.128  TCP      60 5357 → 48133 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
81094 172970.72552…  10.10.56.131   192.168.157.128  TCP      60 902 → 48133 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
81096 172970.72667…  10.10.56.131   192.168.157.128  TCP      60 7070 → 48133 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
81250 172970.93078…  10.10.56.131   192.168.157.128  TCP      60 2968 → 48133 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
83793 172976.18666…  10.10.56.131   192.168.157.128  TCP      60 912 → 48133 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
83797 172976.19093…  10.10.56.131   192.168.157.128  TCP      60 139 → 48138 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
83799 172976.19640…  10.10.56.131   192.168.157.128  TCP      60 912 → 48135 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
83803 172976.20207…  10.10.56.131   192.168.157.128  TCP      60 139 → 48140 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460

▸ Frame 80257: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) o
▸ Ethernet II, Src: VMware_f8:76:f4 (00:50:56:f8:76:f4), Dst: VMware_9a:3f
▸ Internet Protocol Version 4, Src: 10.10.56.131, Dst: 192.168.157.128
▸ Transmission Control Protocol, Src Port: 902, Dst Port: 40516, Seq: 0, A

0000  00 0c 29 9a 3f ca 00 50  56 f8 76 f4 08 00 45 00   ··)·?··P V·v···E·
0010  00 2c 85 77 00 00 80 06  14 9f 0a 0a 38 83 c0 a8   ·,·w···· ····8···
0020  9d 80 03 86 9e 44 4b 3b  48 81 80 75 bb 46 60 12   ·····DK; H··u·F`·
0030  fa f0 8b 2c 00 00 02 04  05 b4 00 00               ···,···· ····
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -p 21,22  10.10.5.204
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-03 17:50 EDT
Nmap scan report for 10.10.5.204
Host is up (0.0015s latency).

PORT   STATE    SERVICE
21/tcp filtered ftp
22/tcp filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds

┌──(kali㉿kali)-[~]
└─$ 

▸ Frame 124929: 54 bytes on wire (432 bits), 54 bytes captured (43
```