

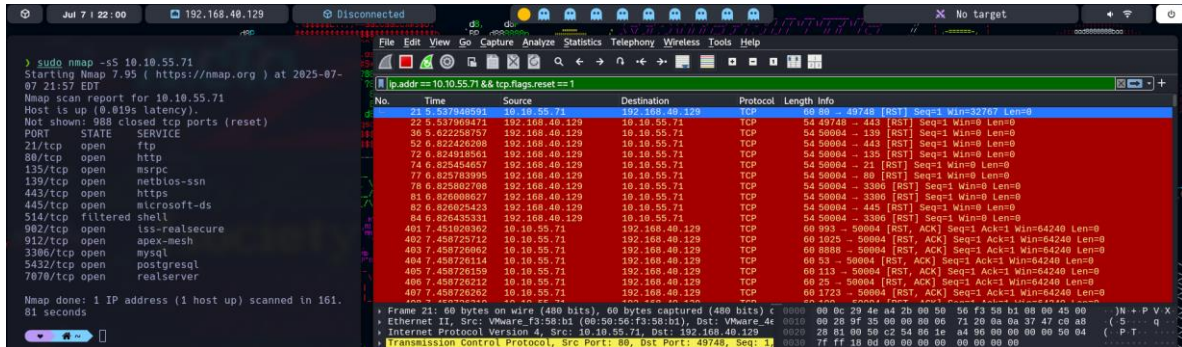
EXAMEN KALI LINUX

Dzul Zárate Jorge
Emmanuel

PREGUNTA 1 – Escaneo SYN (-sS)

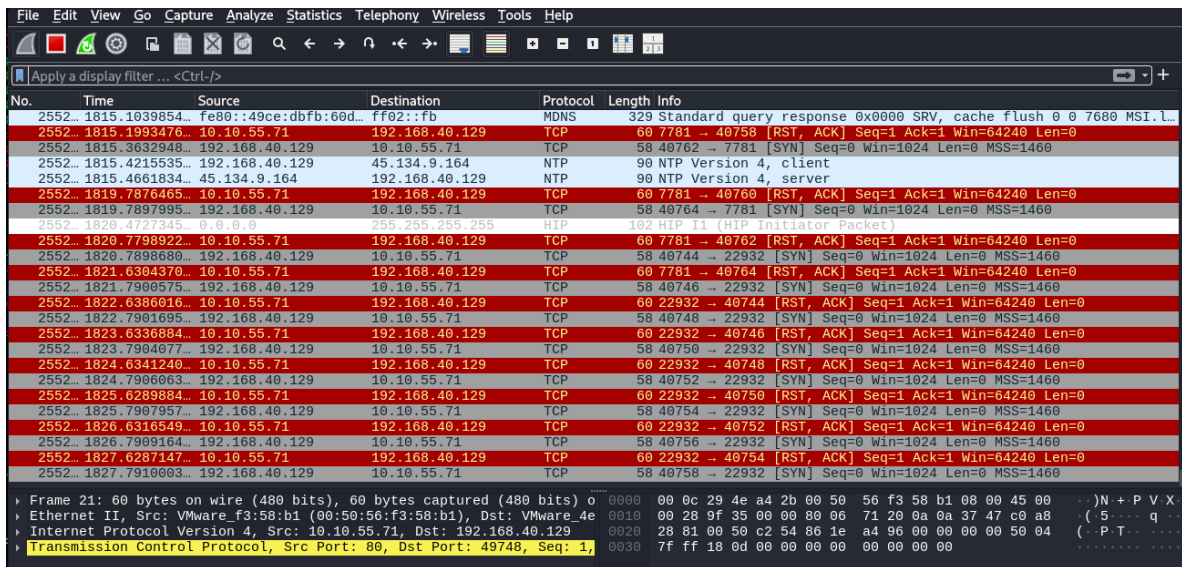
Comando: `sudo nmap -sS 10.10.55.71`

Filtro: `ip.addr == 10.10.55.71 && tcp.flags.reset == 1`



PREGUNTA 2 – Escaneos SYN (stealth scan)

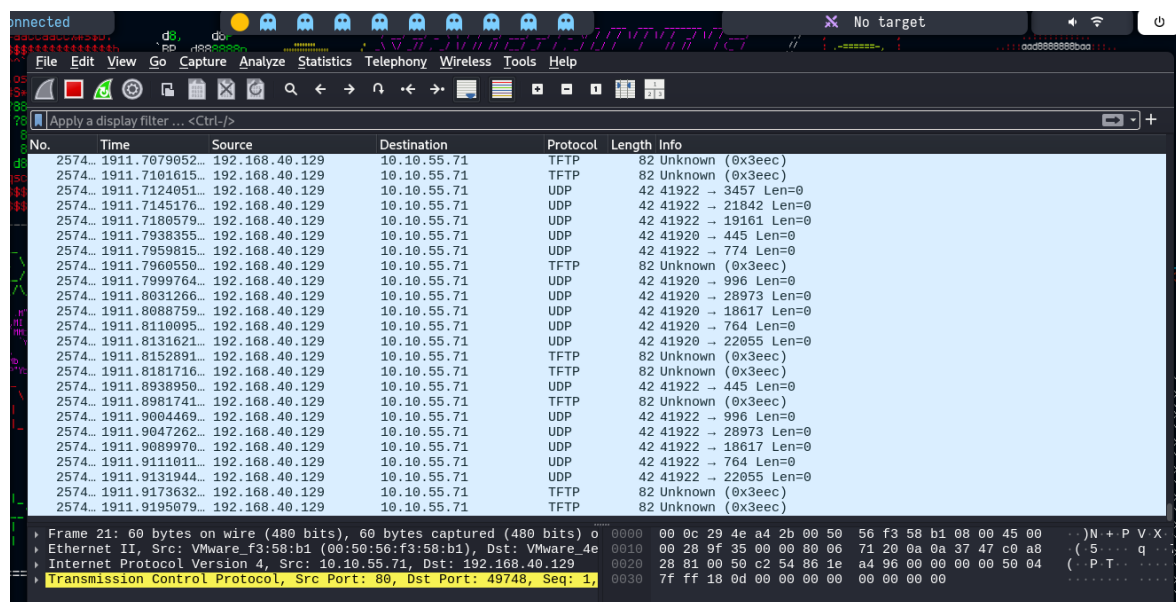
Comandos: `sudo nmap -sS 10.10.55.71`, `sudo nmap -sS -p- 10.10.55.71`



PREGUNTA 4 – Escaneo UDP

sudo nmap -sU 10.10.55.71

```
> sudo nmap -sU 10.10.55.71
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-
07 22:10 EDT
```



The image shows a Wireshark packet capture of a UDP scan. The packet list table contains 20 entries, all of which are UDP packets from 192.168.40.129 to 10.10.55.71. The packet details pane shows the structure of a UDP packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (though it's a UDP scan, the protocol field is still TCP in the capture).

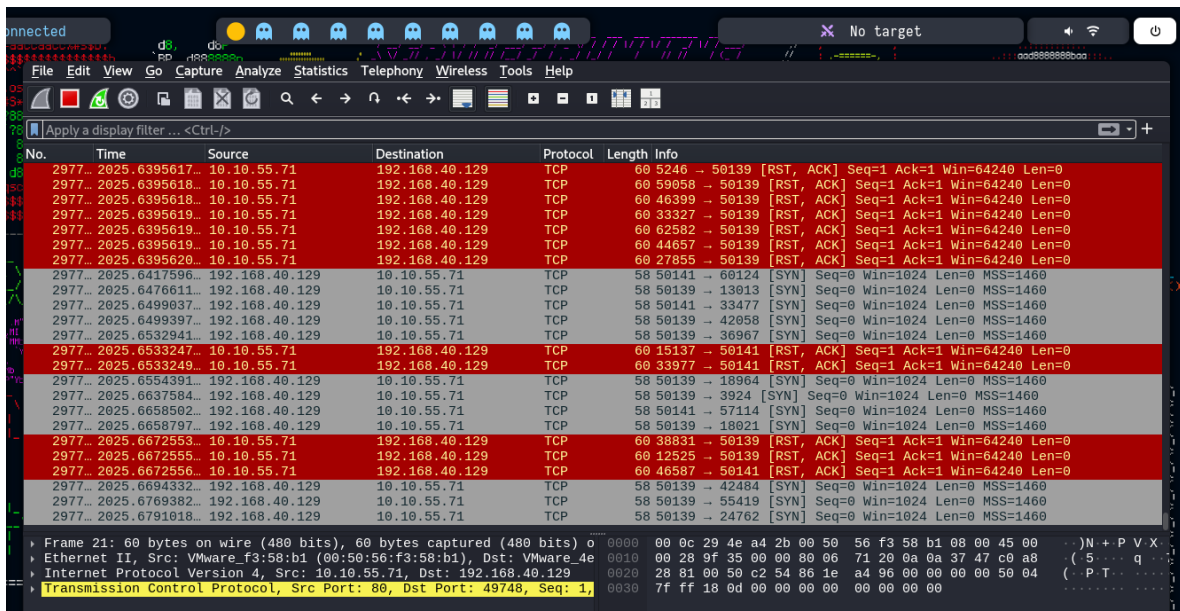
No.	Time	Source	Destination	Protocol	Length	Info
2574	1911.7079052	192.168.40.129	10.10.55.71	TFTP	82	Unknown (0x3eec)
2574	1911.7101615	192.168.40.129	10.10.55.71	TFTP	82	Unknown (0x3eec)
2574	1911.7124051	192.168.40.129	10.10.55.71	UDP	42	41922 → 3457 Len=0
2574	1911.7145176	192.168.40.129	10.10.55.71	UDP	42	41922 → 21842 Len=0
2574	1911.7180579	192.168.40.129	10.10.55.71	UDP	42	41922 → 19161 Len=0
2574	1911.7938355	192.168.40.129	10.10.55.71	UDP	42	41920 → 445 Len=0
2574	1911.7959815	192.168.40.129	10.10.55.71	UDP	42	41922 → 774 Len=0
2574	1911.7960550	192.168.40.129	10.10.55.71	TFTP	82	Unknown (0x3eec)
2574	1911.7999764	192.168.40.129	10.10.55.71	UDP	42	41920 → 996 Len=0
2574	1911.8031266	192.168.40.129	10.10.55.71	UDP	42	41920 → 28973 Len=0
2574	1911.8088759	192.168.40.129	10.10.55.71	UDP	42	41920 → 18617 Len=0
2574	1911.8110095	192.168.40.129	10.10.55.71	UDP	42	41920 → 764 Len=0
2574	1911.8131621	192.168.40.129	10.10.55.71	UDP	42	41920 → 22055 Len=0
2574	1911.8152891	192.168.40.129	10.10.55.71	TFTP	82	Unknown (0x3eec)
2574	1911.8181716	192.168.40.129	10.10.55.71	TFTP	82	Unknown (0x3eec)
2574	1911.8938950	192.168.40.129	10.10.55.71	UDP	42	41922 → 445 Len=0
2574	1911.8981741	192.168.40.129	10.10.55.71	TFTP	82	Unknown (0x3eec)
2574	1911.9004469	192.168.40.129	10.10.55.71	UDP	42	41922 → 996 Len=0
2574	1911.9047262	192.168.40.129	10.10.55.71	UDP	42	41922 → 28973 Len=0
2574	1911.9089970	192.168.40.129	10.10.55.71	UDP	42	41922 → 18617 Len=0
2574	1911.9111011	192.168.40.129	10.10.55.71	UDP	42	41922 → 764 Len=0
2574	1911.9131944	192.168.40.129	10.10.55.71	UDP	42	41922 → 22055 Len=0
2574	1911.9173632	192.168.40.129	10.10.55.71	TFTP	82	Unknown (0x3eec)
2574	1911.9195079	192.168.40.129	10.10.55.71	TFTP	82	Unknown (0x3eec)

Frame 21: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on
Ethernet II, Src: VMware_f3:58:b1 (00:50:56:f3:58:b1), Dst: VMware_4e
Internet Protocol Version 4, Src: 10.10.55.71, Dst: 192.168.40.129
Transmission Control Protocol, Src Port: 80, Dst Port: 49748, Seq: 1,

PREGUNTA 5 – Escaneo SYN en todos los puertos

sudo nmap -sS -p- 10.10.55.71

```
> sudo nmap -sS -p- 10.10.55.71
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-
07 22:12 EDT
```

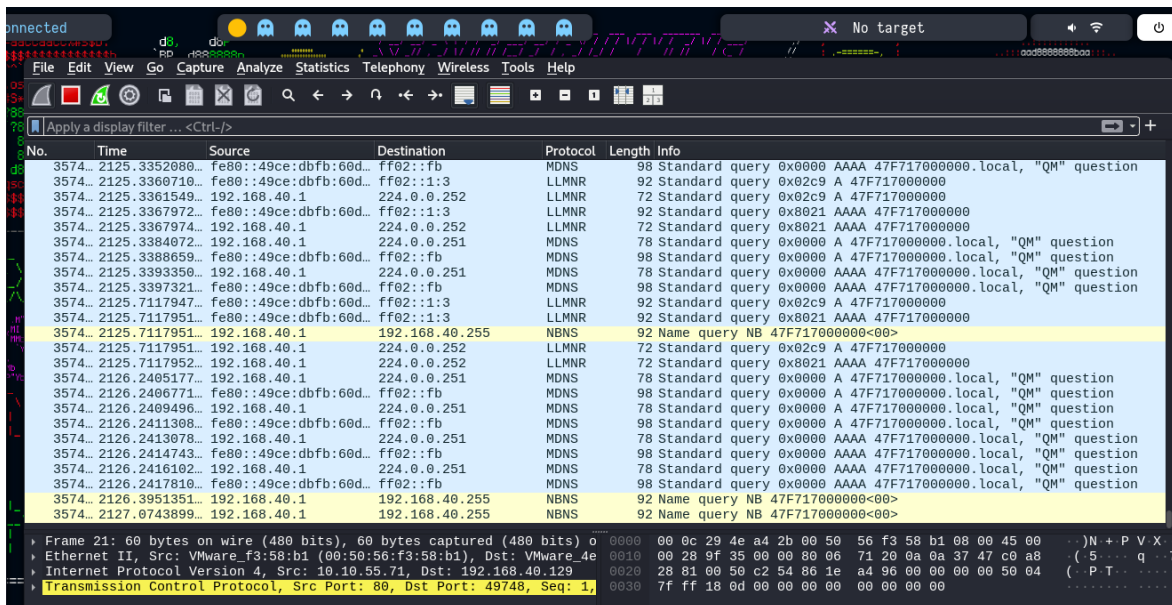


PREGUNTA 7 – Escaneo de versión (¿qué hay en el puerto 80?)

`sudo nmap -sV -p 80 10.10.55.71`

```
> sudo nmap -sV -p 80 10.10.55.71
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-07 22:13 EDT
Nmap scan report for 10.10.55.71
Host is up (0.00080s latency).

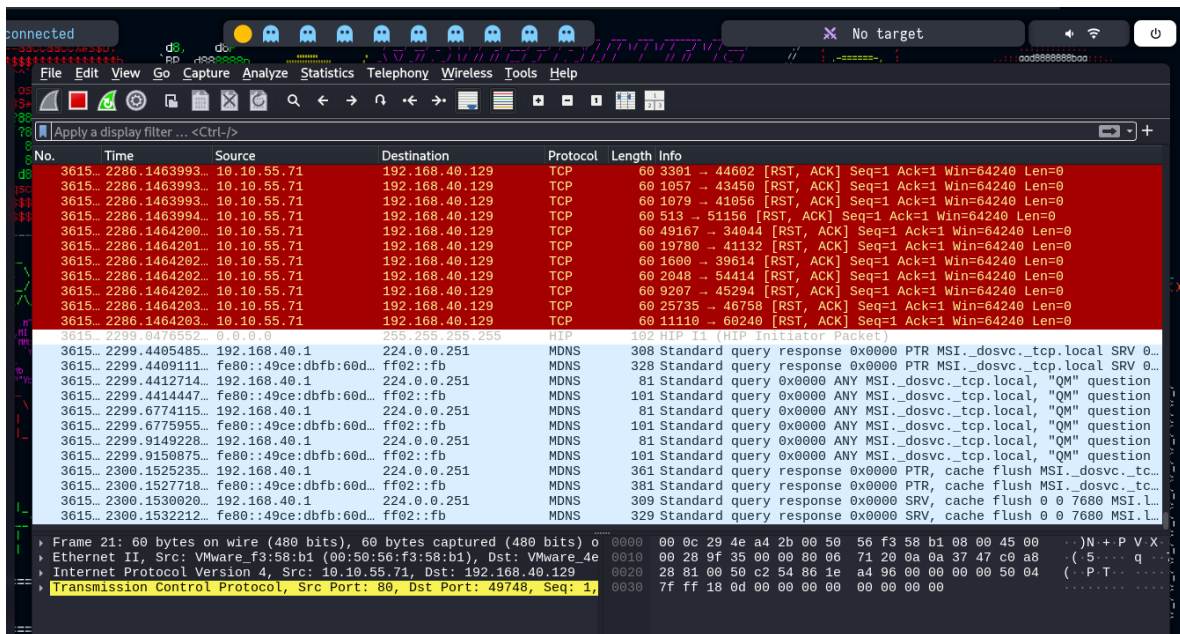
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)
```



PREGUNTA 8 – Escaneo TCP completo

nmap -sT 10.10.55.71

```
> sudo nmap -sT 10.10.55.71
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-07 22:16 EDT
Nmap scan report for 10.10.55.71
Host is up (0.0011s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
3306/tcp  open  mysql
5432/tcp  open  postgresql
```

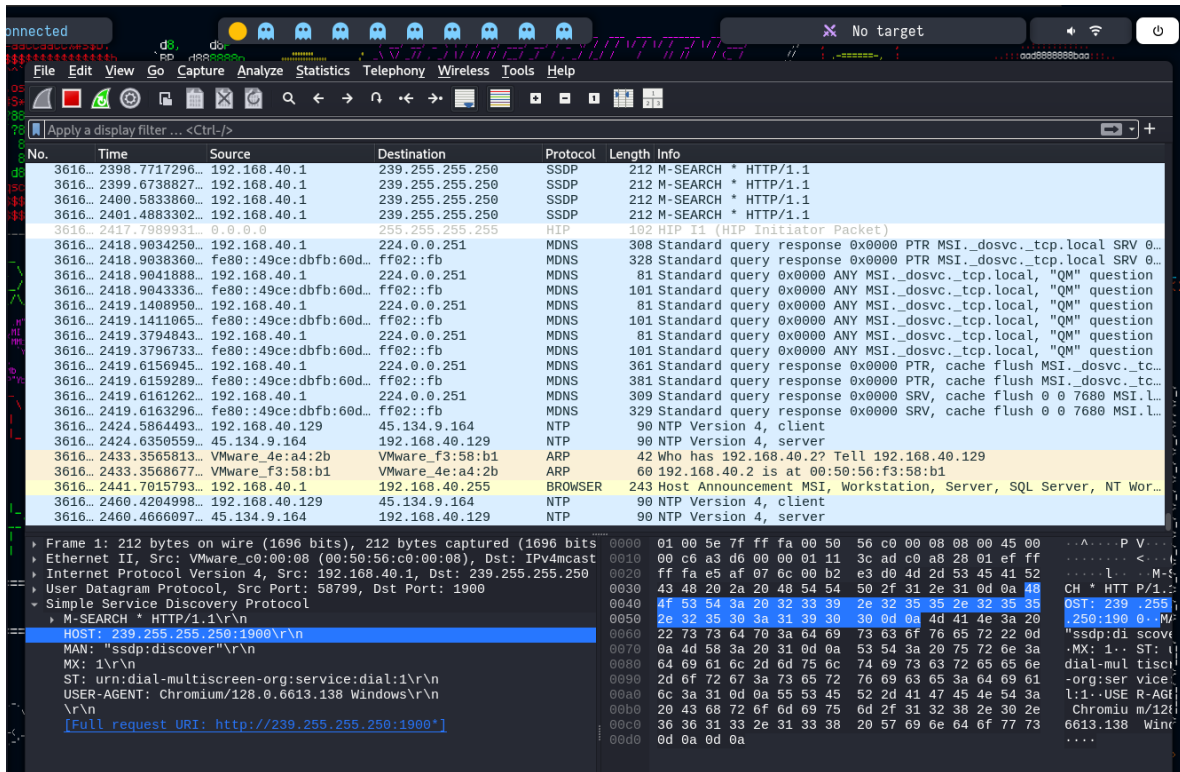


PREGUNTA 9 – Escaneo UDP a puertos 53 y 161

Coamdo: `sudo nmap -sU -p 53,161 10.10.55.71`

```
> sudo nmap -sU -p 53,161 10.10.55.71
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-07 22:18 EDT
Nmap scan report for 10.10.55.71
Host is up (0.0010s latency).

PORT      STATE      SERVICE
53/udp    open|filtered domain
161/udp   open|filtered snmp
```

PREGUNTA 10 – Detectar escaneo desde otra máquina

Filtro: tcp.flags.syn == 1 && tcp.flags.ack == 0

