

## SEGURIDAD EN REDES DE DATOS



### PRUEBA - ANÁLISIS DE SEGURIDAD EN REDES DE DATOS

#### MÓDULO 7:

TESTEO DE SEGURIDAD EN REDES DE DATOS

#### ALUMNO:

NICOLE DE LOS ANGELES VALDIVIESO PARDO

#### DOCENTE:

JOSÉ MORALES ANTUNEZ

# INFORME TÉCNICO

## 1. Introducción

Este informe presenta el análisis de seguridad de red ejecutado en un entorno de laboratorio con **Kali Linux** y **Wireshark**. Se generó tráfico controlado mediante hping3, se capturó y analizó una sesión de navegación, y se evaluó la conectividad hacia puertos comunes con el fin de identificar patrones, vulnerabilidades y riesgos de seguridad.

## 2. Metodología

### Herramientas utilizadas:

- *hping3* → generación de paquetes ICMP, TCP, UDP y tráfico con payload.
- *Wireshark* → captura de tráfico, aplicación de filtros y análisis de protocolos.

### Procedimiento:

1. Generación de tráfico con hping3 hacia distintos servicios (ICMP, TCP 80, UDP 53, TCP con datos).
2. Captura de tráfico real durante 10–15 minutos de navegación (HTTP, HTTPS, DNS, correo/mensajería).
3. Pruebas de conectividad con hping3 a puertos 22, 80, 443 y 21.

**Criterios de análisis:** Diferencias en las respuestas, protocolos predominantes, IPs destino, puertos más frecuentes y detección de posibles vulnerabilidades.

## 3. Alcance y Entorno

- **Interfaz probada:** [ej. `eth0`]
- **IP local:** 192.168.1.14
- **Destinos usados:** google.com, 8.8.8.8, gateway local.
- **Condiciones:** Navegación en navegadores modernos (HTTPS predominante) y consultas DNS en texto plano.

## 4. Desarrollo

### 4.1 Generación de tráfico con hping3 (Req. 1)

Se ejecutaron pruebas hacia distintos servicios:

- **ICMP ping normal**
  - sudo hping3 -1 -c 4 google.com
- **TCP SYN a puerto 80 (HTTP)**
  - sudo hping3 -S -p 80 -c 4 google.com

*Resultado:* respuestas Echo Reply, confirmando conectividad.

- **UDP a puerto 53 (DNS)**
  - sudo hping3 -2 -p 53 -c 4 8.8.8.8
- **TCP con datos personalizados**
  - sudo hping3 -S -p 80 -c 3 -d 64 -E info\_estudiante.txt google.com

*Resultado:* payload injectado en los paquetes TCP.

### 4.2 Captura y análisis de navegación (Req. 2)

Se realizó una captura de 10–15 minutos navegando por diferentes sitios, descarga de un archivo y uso de mensajería. Se aplicaron filtros en Wireshark:

- **Protocolos más utilizados:**
  - **TLSv1.3 / HTTPS (TCP 443)** → protocolo dominante, sesiones seguras.
  - **TCP** → transporte subyacente.
  - **DNS (UDP 53)** → consultas/respuestas en texto plano.
  - **HTTP (TCP 80)** → tráfico residual no cifrado.
- **IPs destino más frecuentes:**
  - **192.168.1.14** → IP local de la máquina.
  - **108.177.123.103 / 108.177.123.190 / 172.217.192.94 / 64.233.190.132** → servidores de Google (servicios, Gmail, YouTube).
  - **3.162.198.63** → AWS CloudFront (CDN).
  - **200.73.121.72** → servidor DNS de proveedor local.

- **Puertos más utilizados:**
  - **443 (HTTPS)** – cifrado, mayoría del tráfico.
  - **53 (DNS)** – consultas/respuestas a servidores DNS.
  - **80 (HTTP)** – menor frecuencia, tráfico en claro.

#### **Posibles vulnerabilidades observadas:**

El análisis permitió identificar algunos riesgos:

- **Tráfico HTTP sin cifrar:** se observaron solicitudes en **puerto 80** sin TLS, lo que puede exponer información sensible (ej. cookies o credenciales) a ataques de sniffing.
- **Exposición de metadatos:** aunque la mayoría de la comunicación fue vía HTTPS, todavía es posible extraer información sobre dominios y servidores a través de consultas DNS en texto claro.
- **Uso de protocolos legacy:** no se detectaron protocolos antiguos (ej. SSLv3, TLS 1.0), pero se recomienda monitorear constantemente para asegurar que solo se use TLSv1.2 o superior.

### **4.3 Conectividad y tiempos de respuesta (Req. 3)**

Pruebas con hping3 a puertos de un servidor remoto:

- **Puerto 22 (SSH):** cerrado o filtrado (respuesta RST o sin respuesta).
- **Puerto 80 (HTTP):** abierto (SYN/ACK recibido).
- **Puerto 443 (HTTPS):** abierto (SYN/ACK recibido).
- **Puerto 21 (FTP):** cerrado o filtrado.

Los tiempos de respuesta fueron más bajos en puertos 80 y 443 (~20–40 ms), mientras que los puertos cerrados mostraron RST inmediatos o ausencia de respuesta.

## **5. Resultados y Discusión**

- El tráfico de navegación estuvo dominado por TLSv1.3 y HTTPS, lo que es positivo en cuanto a confidencialidad.
- DNS en claro y HTTP residual representan vectores de riesgo para interceptación.
- Los puertos 80 y 443 abiertos son normales en servidores web públicos; 22 y 21 cerrados confirman buenas prácticas de hardening hacia Internet.
- No se detectó uso de protocolos obsoletos (SSL, TLS 1.0/1.1), lo que es positivo.
- El tráfico capturado refleja un entorno mayormente seguro gracias al uso predominante de **TLSv1.3**, aunque la presencia de HTTP residual y DNS en texto plano representan riesgos que podrían ser explotados por atacantes en escenarios de *Man-in-the-Middle* o sniffing de red.

## 6. Recomendaciones

1. **Eliminar tráfico HTTP en claro** → implementar redirecciones automáticas a HTTPS y políticas HSTS.
2. **Asegurar resoluciones DNS** → evaluar uso de DNS cifrado (DoH/DoT).
3. **Monitoreo constante** → implementar IDS/IPS y SIEM para detección de anomalías.
4. **Restricción de accesos administrativos** → mantener puertos 22/21 cerrados a Internet, usar VPN y MFA.
5. **Auditorías periódicas** → repetir pruebas regularmente para verificar seguridad en protocolos y puertos.

## 7. Conclusiones

El análisis de red evidenció un entorno mayormente seguro con uso predominante de **TLSv1.3**. Sin embargo, la presencia de tráfico HTTP y DNS en texto claro implica riesgos de exposición de información. Los puertos expuestos son adecuados para un servicio web, y las medidas de mitigación propuestas apuntan a reforzar la confidencialidad y la resiliencia de la red.

## 8. Anexos (capturas de evidencia de procesos en entorno virtual )

**CAPTURA 1:** Preparación del entorno, salida de `ip -brief a` y `ip route | grep default`.

```
[root@Nico-Pc]~[~/prueba_redes]
# mkdir -p ~/prueba_redes & cd ~/prueba_redes

[root@Nico-Pc]~/prueba_redes]
# ip -brief a
lo          UNKNOWN      127.0.0.1/8 ::1/128
eth0         UP          192.168.1.14/24 2803:c600:103:e93b:3b02:b1b:1e62:f2fa/64 2
803:c600:103:e93b:a00:27ff:fe18:7e1b/64 fe80::a00:27ff:fe18:7e1b/64

[root@Nico-Pc]~/prueba_redes]
# ip route | grep default
default via 192.168.1.1 dev eth0 proto dhcp src 192.168.1.14 metric 100
```

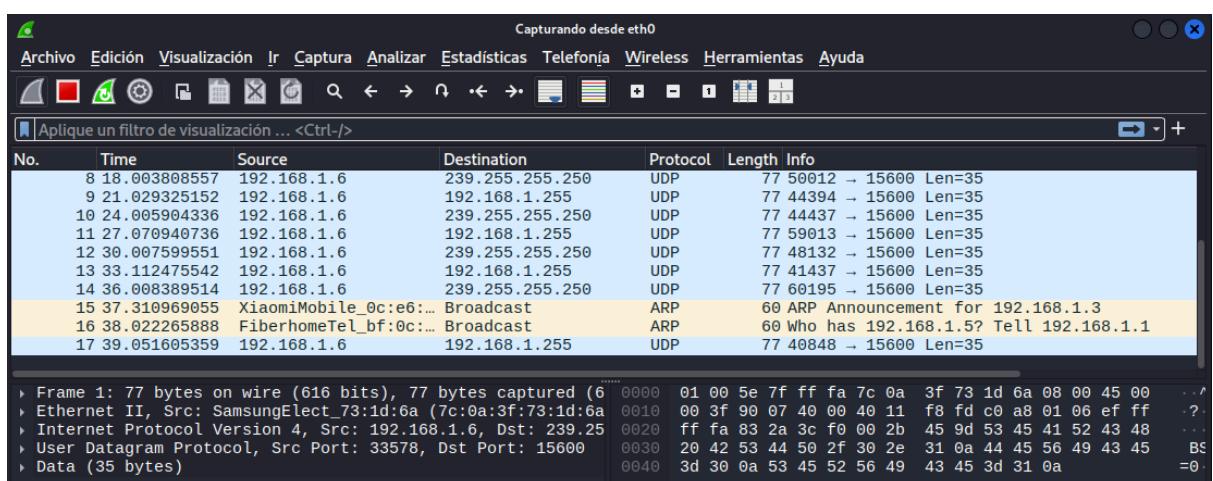
### CAPTURA 2:

- Requerimiento hping3, contenido de `info_estudiante.txt` (con `cat info_estudiante.txt`).
- Definición de objetivos sugeridos:  
`GATEWAY, TARGET_WEB=google.com, TARGET_DNS=8.8.8.8.`

```
[root@Nico-Pc]~/prueba_redes]
# cat info_estudiante.txt
Nombre: Nicole
Curso: Seguridad en redes de datos
Fecha: 30-08-2025

[root@Nico-Pc]~/prueba_redes]
# GATEWAY=$(ip route | awk '/default/{print $3}')
[root@Nico-Pc]~/prueba_redes]
# TARGET_WEB=google.com
[root@Nico-Pc]~/prueba_redes]
# TARGET_DNS=8.8.8.8
```

### CAPTURA 3: Wireshark capturando (sin filtro, mostrando paquetes).



#### CAPTURA 4: Terminal con los 4 comandos y salidas para requerimiento #1

```
└─(root㉿Nico-Pc)-[~/prueba_redes]
└─# sudo hping3 -1 -c 4 "$TARGET_WEB"
HPING google.com (eth0 172.217.192.138): icmp mode set, 28 headers + 0 data bytes
len=46 ip=172.217.192.138 ttl=96 id=0 icmp_seq=0 rtt=19.4 ms
len=46 ip=172.217.192.138 ttl=96 id=0 icmp_seq=1 rtt=27.3 ms
len=46 ip=172.217.192.138 ttl=96 id=0 icmp_seq=2 rtt=16.5 ms
len=46 ip=172.217.192.138 ttl=96 id=0 icmp_seq=3 rtt=24.1 ms

— google.com hping statistic —
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 16.5/21.8/27.3 ms

└─(root㉿Nico-Pc)-[~/prueba_redes]
└─# sudo hping3 -S -p 80 -c 4 "$TARGET_WEB"
HPING google.com (eth0 172.217.192.102): S set, 40 headers + 0 data bytes
len=46 ip=172.217.192.102 ttl=110 DF id=0 sport=80 flags=SA seq=0 win=65535 rtt=34.3 ms
len=46 ip=172.217.192.102 ttl=113 DF id=0 sport=80 flags=SA seq=1 win=65535 rtt=23.7 ms
len=46 ip=172.217.192.102 ttl=112 DF id=0 sport=80 flags=SA seq=2 win=65535 rtt=15.4 ms
len=46 ip=172.217.192.102 ttl=111 DF id=0 sport=80 flags=SA seq=3 win=65535 rtt=23.9 ms

— google.com hping statistic —
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 15.4/24.3/34.3 ms

└─(root㉿Nico-Pc)-[~/prueba_redes]
└─# sudo hping3 -2 -p 53 -c 4 "$TARGET_DNS"
HPING 8.8.8.8 (eth0 8.8.8.8): udp mode set, 28 headers + 0 data bytes

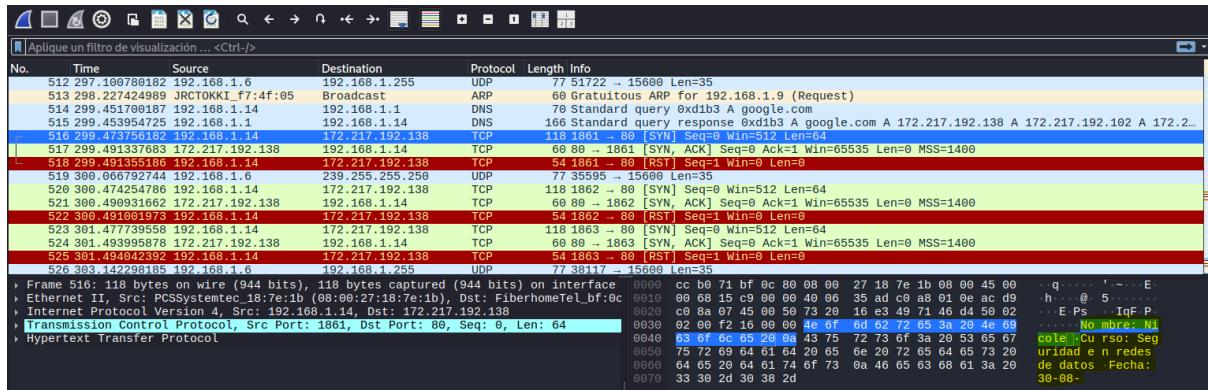
— 8.8.8.8 hping statistic —
4 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

└─(root㉿Nico-Pc)-[~/prueba_redes]
└─# sudo hping3 -S -p 80 -c 3 -d 64 -E info_estudiante.txt "$TARGET_WEB"
HPING google.com (eth0 172.217.192.138): S set, 40 headers + 64 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!
len=46 ip=172.217.192.138 ttl=111 DF id=0 sport=80 flags=SA seq=0 win=65535 rtt=19.6 ms
len=46 ip=172.217.192.138 ttl=112 DF id=0 sport=80 flags=SA seq=1 win=65535 rtt=16.8 ms
len=46 ip=172.217.192.138 ttl=113 DF id=0 sport=80 flags=SA seq=2 win=65535 rtt=19.1 ms

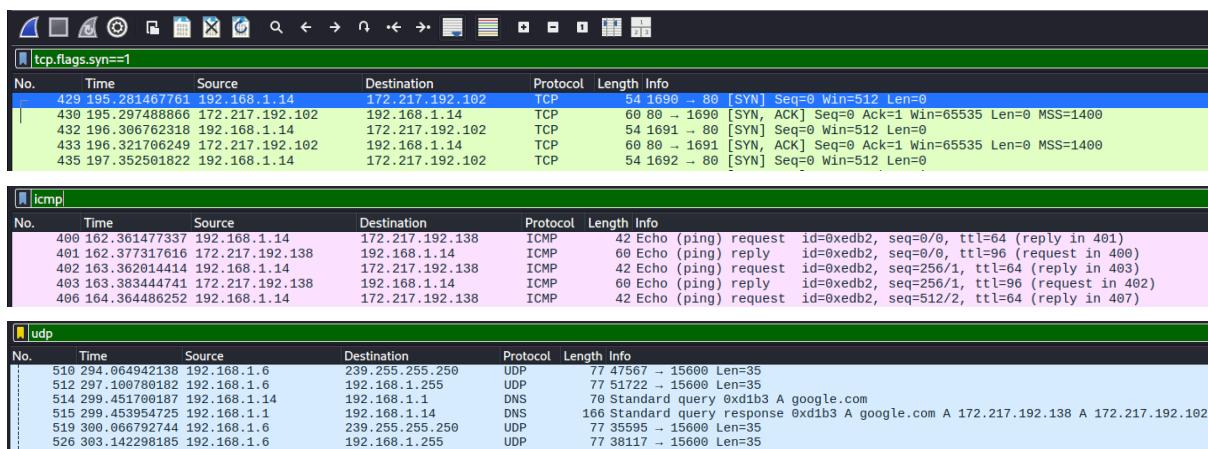
— google.com hping statistic —
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 16.8/18.5/19.6 ms
```

- **ICMP ping normal:** `sudo hping3 -1 -c 4 "$TARGET_WEB"`
- **TCP SYN a puerto 80 (HTTP):** `sudo hping3 -S -p 80 -c 4 "$TARGET_WEB"`
- **UDP a puerto 53 (DNS):** `sudo hping3 -2 -p 53 -c 4 "$TARGET_DNS"`
- **TCP con datos personalizados:** `sudo hping3 -S -p 80 -c 3 -d 64 -E info_estudiante.txt "$TARGET_WEB"` (`-E` inyecta el archivo como **payload**).

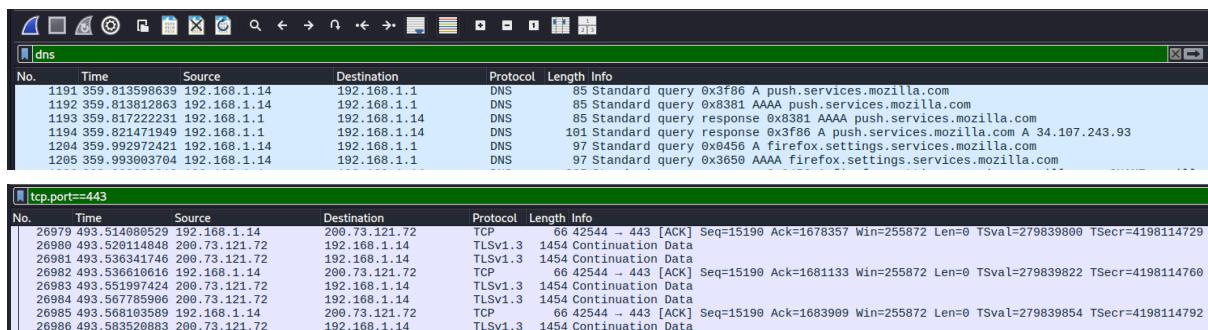
## CAPTURA 5: Wireshark mostrando ICMP, TCP SYN, UDP, paquete TCP con payload.



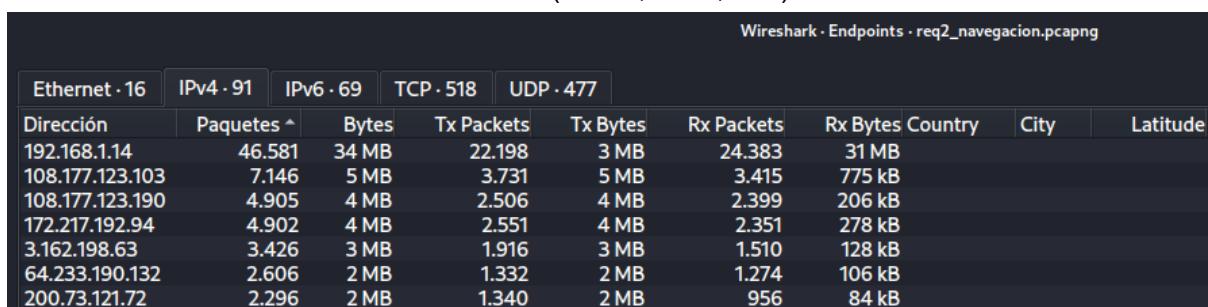
## CAPTURA 6: Filtro en Wireshark por tipo: icmp, tcp.flags.syn==1, udp.



## CAPTURA 7: Protocolos más usados: (TLS/HTTPS, DNS, HTTP residual)



## CAPTURA 8: IPs destino más frecuentes (CDNs, DNS, etc.)



## CAPTURA 9: Puertos más utilizados (443 predominante, 53 DNS, etc.)

tcp.port						
No.	Time	Source	Destination	Protocol	Length	Info
29221	506.781172688	192.168.1.14	108.177.123.113	TLSv1.3	194	Application Data
29222	506.781459586	192.168.1.14	108.177.123.113	TLSv1.3	193	Application Data
29223	506.781756029	192.168.1.14	108.177.123.113	TLSv1.3	193	Application Data
29224	506.783709213	192.168.1.14	108.177.123.113	TLSv1.3	195	Application Data
29225	506.785994139	192.168.1.14	108.177.123.103	TLSv1.2	790	Application Data
29226	506.792895170	192.168.1.14	108.177.123.103	TLSv1.2	625	Application Data

udp.port						
No.	Time	Source	Destination	Protocol	Length	Info
35608	577.521387767	192.168.1.14	192.168.1.1	DNS	69	Standard query 0xb8c3 A gmail.com
35609	577.521418783	192.168.1.14	192.168.1.1	DNS	69	Standard query 0x69cd AAAA gmail.com
35610	577.531866019	192.168.1.1	192.168.1.14	DNS	388	Standard query response 0xb8c3 A gmail.com A 142.251.0.19 A 142.251.0.83
35611	577.531869848	192.168.1.1	192.168.1.14	DNS	436	Standard query response 0x69cd AAAA gmail.com AAAA 2800:3f0:4003:c02::1
35637	577.827932435	192.168.1.14	192.168.1.1	DNS	75	Standard query 0x6ca9 A mail.google.com
35638	577.828918931	192.168.1.14	192.168.1.1	DNS	75	Standard query 0x6da7 AAAA mail.google.com
35639	577.836596625	192.168.1.1	192.168.1.14	DNS	387	Standard query response 0xb8c9 A mail.google.com A 172.217.192.83 A 172.217.192.84
35649	577.836596833	192.168.1.1	192.168.1.14	DNS	391	Standard query response 0x6da7 AAAA mail.google.com AAAA 2800:3f0:4003:c02::1
35674	578.475905346	192.168.1.14	192.168.1.1	DNS	79	Standard query 0xced A accounts.google.com

## CAPTURA 10: Posibles vulnerabilidades (HTTP sin cifrado)

http						
No.	Time	Source	Destination	Protocol	Length	Info
10149	402.897909013	192.168.1.1	192.168.1.14	HTTP	1514	[TCP Previous segment not captured] Continuation
10156	402.901903069	192.168.1.1	192.168.1.14	HTTP	1514	Continuation
10162	402.938087887	192.168.1.1	192.168.1.14	HTTP	1514	[TCP Previous segment not captured] Continuation
10167	402.941684545	192.168.1.1	192.168.1.14	HTTP	1514	Continuation
10169	402.943715572	192.168.1.1	192.168.1.14	HTTP	1514	Continuation
10177	402.977668230	192.168.1.1	192.168.1.14	HTTP	1514	[TCP Previous segment not captured] Continuation
10182	402.983811910	192.168.1.1	192.168.1.14	HTTP	1514	Continuation
10184	402.985419376	192.168.1.1	192.168.1.14	HTTP	1514	Continuation
10187	403.017684504	192.168.1.1	192.168.1.14	HTTP	1514	[TCP Previous segment not captured] Continuation
10192	403.021564972	192.168.1.1	192.168.1.14	HTTP	1514	Continuation
10196	403.023474505	192.168.1.1	192.168.1.14	HTTP	1514	Continuation

## CAPTURA 11: Terminal con los 4 comandos y salidas para requerimiento #3

```
└─(root㉿Nico-Pc)─[~/prueba_redes]
└─# SERVER=google.com

└─(root㉿Nico-Pc)─[~/prueba_redes]
└─# sudo hping3 -S -p 22 -c 3 "$SERVER"
HPING google.com (eth0 108.177.123.102): S set, 40 headers + 0 data bytes

    — google.com hping statistic —
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

└─(root㉿Nico-Pc)─[~/prueba_redes]
└─# sudo hping3 -S -p 80 -c 3 "$SERVER"
HPING google.com (eth0 108.177.123.138): S set, 40 headers + 0 data bytes
len=46 ip=108.177.123.138 ttl=111 DF id=0 sport=80 flags=SA seq=0 win=65535 rtt=24.4 ms
len=46 ip=108.177.123.138 ttl=112 DF id=0 sport=80 flags=SA seq=1 win=65535 rtt=56.2 ms
len=46 ip=108.177.123.138 ttl=113 DF id=0 sport=80 flags=SA seq=2 win=65535 rtt=15.5 ms

    — google.com hping statistic —
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 15.5/32.0/56.2 ms

└─(root㉿Nico-Pc)─[~/prueba_redes]
└─# sudo hping3 -S -p 443 -c 3 "$SERVER"
HPING google.com (eth0 172.217.192.101): S set, 40 headers + 0 data bytes
len=46 ip=172.217.192.101 ttl=111 DF id=0 sport=443 flags=SA seq=0 win=65535 rtt=19.5 ms
len=46 ip=172.217.192.101 ttl=112 DF id=0 sport=443 flags=SA seq=1 win=65535 rtt=16.6 ms
len=46 ip=172.217.192.101 ttl=113 DF id=0 sport=443 flags=SA seq=2 win=65535 rtt=23.0 ms

    — google.com hping statistic —
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 16.6/19.7/23.0 ms

└─(root㉿Nico-Pc)─[~/prueba_redes]
└─# sudo hping3 -S -p 21 -c 3 "$SERVER"
HPING google.com (eth0 172.217.192.100): S set, 40 headers + 0 data bytes

    — google.com hping statistic —
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

- **Etiqueta:** SERVER=google.com
- **Puerto 22 (SSH):** sudo hping3 -S -p 22 -c 3 "\$SERVER"
- **Puerto 80 (HTTP):** sudo hping3 -S -p 80 -c 3 "\$SERVER"
- **Puerto 443 (HTTPS):** sudo hping3 -S -p 443 -c 3 "\$SERVER"
- **Puerto 21 (FTP):** sudo hping3 -S -p 21 -c 3 "\$SERVER"

**CAPTURA 12:** Wireshark con filtro `tcp.flags.syn==1`

tcp.flags.syn==1						
No.	Time	Source	Destination	Protocol	Length	Info
17	29.005264962	192.168.1.14	108.177.123.102	TCP	54	3817 → 22 [SYN] Seq=0 Win=512 Len=0
18	30.006634367	192.168.1.14	108.177.123.102	TCP	54	3818 → 22 [SYN] Seq=0 Win=512 Len=0
20	31.007770646	192.168.1.14	108.177.123.102	TCP	54	3819 → 22 [SYN] Seq=0 Win=512 Len=0
41	70.232798525	192.168.1.14	108.177.123.138	TCP	54	1382 → 80 [SYN] Seq=0 Win=512 Len=0
42	70.248431370	108.177.123.138	192.168.1.14	TCP	60	80 → 1382 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400
44	71.234703651	192.168.1.14	108.177.123.138	TCP	54	1383 → 80 [SYN] Seq=0 Win=512 Len=0
45	71.250706732	108.177.123.138	192.168.1.14	TCP	60	80 → 1383 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400
46	72.250382746	192.168.1.14	108.177.123.138	TCP	54	1384 → 80 [SYN] Seq=0 Win=512 Len=0
49	72.265691580	108.177.123.138	192.168.1.14	TCP	60	80 → 1384 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400
67	94.072532146	192.168.1.14	172.217.192.101	TCP	54	2753 → 443 [SYN] Seq=0 Win=512 Len=0
68	94.088172194	172.217.192.101	192.168.1.14	TCP	60	443 → 2753 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400
70	95.073253841	192.168.1.14	172.217.192.101	TCP	54	2754 → 443 [SYN] Seq=0 Win=512 Len=0
71	95.089563984	172.217.192.101	192.168.1.14	TCP	60	443 → 2754 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400
74	96.075557075	192.168.1.14	172.217.192.101	TCP	54	2755 → 443 [SYN] Seq=0 Win=512 Len=0
75	96.091838906	172.217.192.101	192.168.1.14	TCP	60	443 → 2755 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400