

# INFORME TÉCNICO

## Análisis de Seguridad en Redes de Datos.

Aplicación de herramientas y metodologías de análisis de seguridad para la identificación y análisis de tráfico en redes de datos corporativas.

Felipe Oyanedel Beltran

## Índice de Contenido

Introducción .....	2
Objetivo General .....	2
Objetivos Específicos .....	2
Alcance .....	2
Desarrollo .....	3
1.    Análisis de tráfico con hping3 en Kali Linux .....	3
a)    Crear un archivo de texto plano con información personal (nombre, curso, fecha) .....	3
b)    Utilizar hping3 para enviar diferentes tipos de paquetes a un host objetivo (puede ser google.com o la puerta de enlace local) .....	3
c)    Documentar los comandos utilizados y explicar las diferencias en las respuestas .....	6
2.    Captura y Análisis de tráfico con Wireshark .....	9
3.    Análisis de conectividad y respuesta de red .....	13
Recomendaciones .....	16
Conclusiones .....	17

## **Introducción**

El presente informe tiene como propósito analizar el comportamiento de la red corporativa implementada en la empresa Desafío Latam, mediante la realización de pruebas controladas de tráfico y conectividad. Para ello se emplearán las herramientas hping3 y Wireshark, que permiten generar, capturar y examinar distintos tipos de paquetes de red, posibilitando así una evaluación desde el punto de vista de seguridad y detección de posibles anomalías.

El análisis busca comprender cómo interactúa la red frente a diferentes escenarios de comunicación, identificando protocolos utilizados, puertos en uso, direcciones IP frecuentes y posibles vulnerabilidades derivadas de tráfico no cifrado o servicios expuestos. Con estos resultados se pretende aportar información clave para mejorar la eficiencia y la seguridad de la infraestructura tecnológica.

## **Objetivo General**

Evaluar el comportamiento de la red corporativa de Desafío Latam a través de pruebas de tráfico y conectividad, con el fin de identificar patrones de comunicación, detectar posibles vulnerabilidades y analizar la seguridad de los servicios expuestos.

## **Objetivos Específicos**

Generar diferentes tipos de tráfico con hping3 (ICMP, TCP, UDP) y documentar las respuestas obtenidas.

Capturar y analizar tráfico con Wireshark, identificando protocolos más utilizados, direcciones IP de destino y puertos más frecuentes.

Aplicar filtros de tráfico en Wireshark para observar comunicaciones específicas (HTTP, HTTPS, DNS, ICMP).

Evaluar la conectividad de distintos puertos de un servidor remoto (22, 80, 443, 21), determinando si se encuentran abiertos, cerrados o filtrados.

Identificar posibles anomalías o riesgos de seguridad presentes en las pruebas (tráfico no cifrado, exposición de servicios, etc.).

## **Alcance**

El análisis se limita a pruebas de laboratorio realizadas en entornos controlados utilizando Kali Linux y herramientas de captura de tráfico. No contempla la ejecución de ataques reales ni la alteración de servicios en producción, por lo que los resultados se centran exclusivamente en la detección de patrones, comportamiento esperado de la red y posibles vulnerabilidades a nivel de tráfico y conectividad.

## Desarrollo

### 1. Análisis de tráfico con hping3 en Kali Linux

- a) Crear un archivo de texto plano con información personal (nombre, curso, fecha)

Se procede con la creación del archivo "info.txt" haciendo uso del comando **nano info.txt**.

```
(root@kali)-[/home/kali]
# cat info.txt
Nombre : Felipe Oyanedel B
Curso : Seguridad en Redes de Datos
Fecha : 25 de Agosto del 2025
```

- b) Utilizar hping3 para enviar diferentes tipos de paquetes a un host objetivo (puede ser google.com o la puerta de enlace local)

- ICMP ping normal

El modo **-1** es para tráfico ICMP y **-c 5** cuenta la cantidad de paquetes ICMP a enviar hacia la dirección IP de destino, para así tener una muestra más clara.

```
(root@kali)-[/home/kali]
# hping3 -1 -c 5 192.168.1.1
HPING 192.168.1.1 (eth1 192.168.1.1): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.1.1 ttl=64 id=54455 icmp_seq=0 rtt=11.6 ms
len=46 ip=192.168.1.1 ttl=64 id=54544 icmp_seq=1 rtt=10.9 ms
len=46 ip=192.168.1.1 ttl=64 id=54573 icmp_seq=2 rtt=7.2 ms
len=46 ip=192.168.1.1 ttl=64 id=54669 icmp_seq=3 rtt=13.0 ms
len=46 ip=192.168.1.1 ttl=64 id=54709 icmp_seq=4 rtt=10.4 ms

— 192.168.1.1 hping statistic —
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.2/10.6/13.0 ms

(root@kali)-[/home/kali]
#
```

No.	Time	Source	Destination	Protocol	Length	Info
12	3.319582814	192.168.1.21	192.168.1.1	ICMP	42	Echo (ping) request id=0xa510, seq=0/0, ttl=64 (reply in 13)
13	3.324708362	192.168.1.1	192.168.1.21	ICMP	60	Echo (ping) reply id=0xa510, seq=0/0, ttl=64 (request in 12)
17	4.321814847	192.168.1.21	192.168.1.1	ICMP	42	Echo (ping) request id=0xa510, seq=256/1, ttl=64 (reply in 18)
18	4.323719578	192.168.1.1	192.168.1.21	ICMP	60	Echo (ping) reply id=0xa510, seq=256/1, ttl=64 (request in 17)
30	5.322552587	192.168.1.21	192.168.1.1	ICMP	42	Echo (ping) request id=0xa510, seq=512/2, ttl=64 (reply in 31)
31	5.324406555	192.168.1.1	192.168.1.21	ICMP	60	Echo (ping) reply id=0xa510, seq=512/2, ttl=64 (request in 30)
33	6.323954209	192.168.1.21	192.168.1.1	ICMP	42	Echo (ping) request id=0xa510, seq=768/3, ttl=64 (reply in 34)
34	6.327277604	192.168.1.1	192.168.1.21	ICMP	60	Echo (ping) reply id=0xa510, seq=768/3, ttl=64 (request in 33)
35	7.325163378	192.168.1.21	192.168.1.1	ICMP	42	Echo (ping) request id=0xa510, seq=1024/4, ttl=64 (reply in 36)
36	7.331037042	192.168.1.1	192.168.1.21	ICMP	60	Echo (ping) reply id=0xa510, seq=1024/4, ttl=64 (request in 35)

<p>Frame 12: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth1</p> <p>Ethernet II, Src: PCSSystemtec e0:64:1e:08:00:27:e0:64:1e, Dst: zte_36:55:7c (14:ca:00:10:00:00:14:ca:00:10:00:00:14:ca:00:10:00:00:14:ca)</p> <p>Internet Protocol Version 4, Src: 192.168.1.21, Dst: 192.168.1.1</p> <p>Internet Control Message Protocol</p> <p>Type: 0 (Echo (ping) request)</p> <p>Code: 0</p> <p>Checksum: 0x52ef [correct]</p> <p>[Checksum Status: Good]</p> <p>Identifier (BE): 42256 (0xa510)</p> <p>Identifier (LE): 4261 (0x10a5)</p> <p>Sequence Number (BE): 0 (0x0000)</p> <p>Sequence Number (LE): 0 (0x0000)</p> <p>[Response Frame: 13]</p>	<pre>0000 14 ca 56 36 55 7c 08 00 27 e0 64 1e 08 00 45 00 ..V6U]...d...E 0010 00 1c bb ee 00 00 40 01 3b 8c c0 a8 01 15 c0 a8 .....@;..... 0020 01 01 08 00 52 ef a5 10 00 00 .....R.....</pre>
---	---

- TCP SYN a puerto 80

El modo **-S** establece el flag SYN en el paquete a enviar. El modo **-p 80** indica que el envío de paquetes apunta al puerto 80 HTTP.

```
(root@kali)-[/home/kali]
# hping3 -S -p 80 -c 5 192.168.1.1
HPING 192.168.1.1 (eth1 192.168.1.1): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.1 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=29200 rtt=4.7 ms
len=46 ip=192.168.1.1 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=29200 rtt=4.9 ms
len=46 ip=192.168.1.1 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=29200 rtt=11.4 ms
len=46 ip=192.168.1.1 ttl=64 DF id=0 sport=80 flags=SA seq=3 win=29200 rtt=5.2 ms
len=46 ip=192.168.1.1 ttl=64 DF id=0 sport=80 flags=SA seq=4 win=29200 rtt=8.6 ms

— 192.168.1.1 hping statistic —
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 4.7/6.9/11.4 ms

(root@kali)-[/home/kali]
#
```

ip.addr == 192.168.1.21 && ip.addr == 192.168.1.1 && tcp.port

No.	Time	Source	Destination	Protocol	Length	Info
1127	9.157286514	192.168.1.21	192.168.1.1	TCP	54	2436 → 80 [SYN] Seq=0 Win=512 Len=0
1128	9.162825747	192.168.1.1	192.168.1.21	TCP	60	80 → 2436 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
1129	9.162859245	192.168.1.21	192.168.1.1	TCP	54	2436 → 80 [RST] Seq=0 Win=0 Len=0
1137	10.180683940	192.168.1.21	192.168.1.1	TCP	54	2437 → 80 [SYN] Seq=0 Win=512 Len=0
1138	10.186285879	192.168.1.1	192.168.1.21	TCP	60	80 → 2437 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
1139	10.186349396	192.168.1.21	192.168.1.1	TCP	54	2437 → 80 [RST] Seq=1 Win=0 Len=0
1146	11.187462891	192.168.1.21	192.168.1.1	TCP	54	2438 → 80 [SYN] Seq=0 Win=512 Len=0
1147	11.189298418	192.168.1.1	192.168.1.21	TCP	60	80 → 2438 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
1148	11.189474865	192.168.1.21	192.168.1.1	TCP	54	2438 → 80 [RST] Seq=1 Win=0 Len=0
1174	12.186699988	192.168.1.21	192.168.1.1	TCP	54	2439 → 80 [SYN] Seq=0 Win=512 Len=0
1175	12.191419920	192.168.1.1	192.168.1.21	TCP	60	80 → 2439 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
1176	12.191463431	192.168.1.21	192.168.1.1	TCP	54	2439 → 80 [RST] Seq=1 Win=0 Len=0
1186	13.188979639	192.168.1.21	192.168.1.1	TCP	54	2440 → 80 [SYN] Seq=0 Win=512 Len=0
1187	13.190844422	192.168.1.1	192.168.1.21	TCP	60	80 → 2440 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
1188	13.190896846	192.168.1.21	192.168.1.1	TCP	54	2440 → 80 [RST] Seq=1 Win=0 Len=0

Frame 1127: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0  
 Ethernet II, Src: PCSysstemec\_e0:04:1e:08:00:27:e0:04:1e, Dst: zte\_36:55:7c (14:c2:56:00:36:55:7c)  
 Internet Protocol Version 4, Src: 192.168.1.21, Dst: 192.168.1.1  
 Transmission Control Protocol, Src Port: 2436, Dst Port: 80, Seq: 0, Len: 0  
 Source Port: 2436  
 Destination Port: 80  
 [Stream index: 14]  
 [Stream Packet Number: 1]  
 [Conversation completeness: Incomplete, SYN\_SENT (1)]  
 [TCP Segment Len: 0]  
 Sequence Number: 0 (relative sequence number)  
 Sequence Number (raw): 576823462  
 [Next Sequence Number: 1 (relative sequence number)]  
 Acknowledgment Number: 99985729  
 Acknowledgment number (raw): 99985729  
 0101 ... = Header Length: 20 bytes (5)  
 [Initials: SYN] [SYN]

- UDP a puerto 53

El modo **-2** es para UDP. El modo **-p 53** apunta al puerto DNS. Cabe destacar que el protocolo UDP no verifica el bien recibimiento ni las condiciones del paquete enviado.

```
(root@kali)-[/home/kali]
# hping3 -2 -p 53 -c 5 192.168.1.1
HPING 192.168.1.1 (eth1 192.168.1.1): udp mode set, 28 headers + 0 data bytes

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

(root@kali)-[/home/kali]
#
```

udp.port == 53 && ip.src_host == 192.168.1.21									
No.	Time	Source	Destination	Protocol	Length	Info			
86035	499.516321005	192.168.1.21	192.168.1.1	UDP	42	1985 → 53 Len=0			
86225	491.519898341	192.168.1.21	192.168.1.1	UDP	42	1986 → 53 Len=0			
86237	492.520930110	192.168.1.21	192.168.1.1	UDP	42	1987 → 53 Len=0			
86238	493.521818125	192.168.1.21	192.168.1.1	UDP	42	1988 → 53 Len=0			
86241	494.543113607	192.168.1.21	192.168.1.1	UDP	42	1989 → 53 Len=0			

Frame 86035: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface e... Ethernet II, Src: PCSSystemtec e0:64:1e (08:00:27:e0:64:1e), Dst: zte_36:55:7c (14:ca... Internet Protocol Version 4, Src: 192.168.1.21, Dst: 192.168.1.1 User Datagram Protocol, Src Port: 1985, Dst Port: 53									
Source Port: 1985									
Destination Port: 53									
Length: 8									
Checksum: 0x7481 [unverified]									
[Checksum Status: Unverified]									
[Stream Index: 66]									
[Stream Packet Number: 1]									
[Timestamps]									

- TCP con datos personalizados

Este comando envía un único paquete SYN (-S -c 1) al puerto 80, cuyo archivo con datos creado previamente es el payload de datos (-E info.txt) que tiene exactamente el tamaño del archivo (-d \$(stat -c%s info.txt)).

```
(root@kali)-[/home/kali]
# hping3 -S -p 80 -d $(stat -c%s info.txt) -E info.txt -c 1 192.168.1.1

HPING 192.168.1.1 (eth1 192.168.1.1): S set, 40 headers + 94 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!
len=46 ip=192.168.1.1 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=29200 rtt=7.0 ms

— 192.168.1.1 hping statistic —
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 7.0/7.0/7.0 ms

(root@kali)-[/home/kali]
#
```

tcp.stream eq 6									
No.	Time	Source	Destination	Protocol	Length	Info			
940	-26.207065184	192.168.1.21	192.168.1.1	TCP	148	1235 → 80 [SYN] Seq=0 Win=512 Len=94			
941	-26.204328277	192.168.1.1	192.168.1.21	TCP	60	80 → 1235 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460			
942	-26.204306945	192.168.1.21	192.168.1.1	TCP	54	1235 → 80 [RST] Seq=1 Win=0 Len=0			

Wireshark - Follow TCP Stream (tcp.stream eq 6) - eth1									
Nombre : Felipe Oyanedel B Curso : Seguridad en Redes de Datos Fecha : 25 de Agosto del 2025									
Sequence Number (raw): 1019011444									
[Next Sequence Number: 95 (relative sequence num]									
Acknowledgment Number: 1823670574									
Acknowledgment number (raw): 1823670574									
0101 ... = Header Length: 20 bytes (5)									
Flags: 0x002 (SYN)									
Window: 512									
[Calculated window size: 512]									
Checksum: 0xe7c4 [unverified]									
[Checksum Status: Unverified]									
Urgent Pointer: 0									
[Timestamps]									
[SEQ/ACK analysis]									
[Bytes in flight: 94]									
[Bytes sent since last PSH flag: 94]									
TCP payload (94 bytes)									

### c) Documentar los comandos utilizados y explicar las diferencias en las respuestas

#### ICMP ping normal

Comando utilizado: `hping3 -1 -c 5 192.168.1.1`

```
(root@kali)~/home/kali
# hping3 -1 -c 5 192.168.1.1
HPING 192.168.1.1 (eth1 192.168.1.1): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.1.1 ttl=64 id=54455 icmp_seq=0 rtt=11.6 ms
len=46 ip=192.168.1.1 ttl=64 id=54544 icmp_seq=1 rtt=10.9 ms
len=46 ip=192.168.1.1 ttl=64 id=54573 icmp_seq=2 rtt=7.2 ms
len=46 ip=192.168.1.1 ttl=64 id=54669 icmp_seq=3 rtt=13.0 ms
len=46 ip=192.168.1.1 ttl=64 id=54709 icmp_seq=4 rtt=10.4 ms

— 192.168.1.1 hping statistic —
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.2/10.6/13.0 ms

(root@kali)~/home/kali
```

La dirección IP destino (192.168.1.1) respondió a todos los paquetes ICMP Echo Request con respuestas Echo Reply, como se evidencia en las líneas **len=46 ip=192.168.1.1....** El 0% de pérdida de paquetes y los bajos tiempos de respuesta (rtt promedio de 10.6 ms) confirman que el host está activo en la red y que la conectividad a nivel de capa 3 (red) del modelo OSI es excelente.

#### TCP SYN a puerto 80

Comando utilizado: `hping3 -S -p 80 -c 5 192.168.1.1`

```
(root@kali)~/home/kali
# hping3 -S -p 80 -c 5 192.168.1.1
HPING 192.168.1.1 (eth1 192.168.1.1): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.1 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=29200 rtt=4.7 ms
len=46 ip=192.168.1.1 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=29200 rtt=4.9 ms
len=46 ip=192.168.1.1 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=29200 rtt=11.4 ms
len=46 ip=192.168.1.1 ttl=64 DF id=0 sport=80 flags=SA seq=3 win=29200 rtt=5.2 ms
len=46 ip=192.168.1.1 ttl=64 DF id=0 sport=80 flags=SA seq=4 win=29200 rtt=8.6 ms

— 192.168.1.1 hping statistic —
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 4.7/6.9/11.4 ms

(root@kali)~/home/kali
```

La respuesta para cada uno de los 5 paquetes fue **flags=SA (SYN-ACK)**. Esto significa que el puerto **TCP 80** está abierto y escuchando en el host destino **192.168.1.1**. El servicio aceptó activamente la solicitud de conexión enviando un paquete **SYN-ACK** como dicta el handshake de comunicación. El 0% de pérdida de paquetes y el bajo RTT confirman que el servicio es accesible y responde de manera confiable.

#### UDP a puerto 53

Comando utilizado: `hping3 -2 -p 53 -c 5 192.168.1.1`

```
(root@kali)~/home/kali
# hping3 -2 -p 53 -c 5 192.168.1.1
HPING 192.168.1.1 (eth1 192.168.1.1): udp mode set, 28 headers + 0 data bytes

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

(root@kali)~/home/kali
```



El resultado fue **100% packet loss**. Para investigar, se realizó un escaneo UDP con **nmap -SU 192.168.1.1** el cual reveló que el puerto UDP 53 está realmente abierto (**53/udp open domain**). La discrepancia se debe a la metodología de cada herramienta: **hping3**, por defecto, envía paquetes UDP vacíos, que son ignorados silenciosamente por el servicio DNS. Por lo tanto, la prueba con hping3 demostró efectivamente el comportamiento de un servicio UDP ante tráfico no solicitado o mal formado, no el estado como tal del puerto.

## TCP con datos personalizados

Comando utilizado: **hping3 -S -p 80 -d \$(stat -c%s info.txt) -E info.txt -c 1 192.168.1.1**

```
(root@kali)~/home/kali
# hping3 -S -p 80 -d $(stat -c%s info.txt) -E info.txt -c 1 192.168.1.1

HPING 192.168.1.1 (eth1 192.168.1.1): S set, 40 headers + 94 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!
len=46 ip=192.168.1.1 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=29200 rtt=7.0 ms

— 192.168.1.1 hping statistic —
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 7.0/7.0/7.0 ms

(root@kali)~/home/kali
#
```

La respuesta fue **flags=SA (SYN-ACK)** y **0% packet loss**. Esto indica que el comando se ejecutó con éxito. El paquete **TCP SYN**, que contenía un payload de datos de **94 bytes** con la información personal del archivo **info.txt**, fue recibido correctamente por el servicio **HTTP (puerto 80)** en el host **192.168.1.1**. El servidor no solo confirmó que el puerto está abierto, sino que también aceptó la solicitud de conexión que incluía los datos personalizados en el mismo paquete de inicialización de la conexión (**SYN**)

Capturar el tráfico generado con Wireshark durante las pruebas

## ICMP ping normal

The image shows a Wireshark capture of ICMP ping traffic. The packet list at the top shows several echo requests and replies between source IP 192.168.1.21 and destination IP 192.168.1.1. The packet details pane for packet 8 (an echo request) is expanded, showing the following fields:

- Protocol: ICMP (1)
- Header Checksum: 0x9a81 [validation disabled]
- Header checksum status: Unverified
- Source Address: 192.168.1.21
- Destination Address: 192.168.1.1
- Internet Control Message Protocol
- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0x05f2 [correct]
- Checksum status: Good
- Identifier (ID): 61964 (0xf20c)
- Identifier (ID): 3314 (0x0cf2)
- Sequence Number (SEQ): 0 (0x0000)
- Sequence Number (SEQ): 0 (0x0000)

El análisis de Wireshark al ejecutar el comando relacionado a **ICMP ping normal** arroja resultado exitoso en cuanto a la comunicación bidireccional entre la dirección IP del host origen y la dirección IP del host destino. Si analizamos uno de los paquetes, tenemos **Type 8**, correspondiente a solicitudes ICMP y **Code 0**, indicando que no se presentan errores en el paquete. La presencia constante de estos valores, junto con la correlación que hace Wireshark de cada solicitud con su respectiva respuesta (**'reply in X'**), confirma que el protocolo **ICMP** funcionó a la perfección para verificar la conectividad de red.



## TCP SYN a puerto 80

No.	Time	Source	Destination	Protocol	Length	Info
1127	9.157286514	192.168.1.21	192.168.1.1	TCP	54	2436 → 80 [SYN] Seq=0 Win=512 Len=0
1128	9.162825747	192.168.1.1	192.168.1.21	TCP	60	80 → 2436 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
1129	9.162855915	192.168.1.21	192.168.1.1	TCP	54	2436 → 80 [RST] Seq=1 Win=0 Len=0
1137	10.180683940	192.168.1.21	192.168.1.1	TCP	54	2437 → 80 [SYN] Seq=0 Win=512 Len=0
1138	10.186285879	192.168.1.1	192.168.1.21	TCP	60	80 → 2437 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
1139	10.186349396	192.168.1.21	192.168.1.1	TCP	54	2437 → 80 [RST] Seq=1 Win=0 Len=0
1146	11.187402891	192.168.1.21	192.168.1.1	TCP	54	2438 → 80 [SYN] Seq=0 Win=512 Len=0
1147	11.189298418	192.168.1.1	192.168.1.21	TCP	60	80 → 2438 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
1148	11.189474865	192.168.1.21	192.168.1.1	TCP	54	2438 → 80 [RST] Seq=1 Win=0 Len=0
1174	12.186999988	192.168.1.21	192.168.1.1	TCP	54	2439 → 80 [SYN] Seq=0 Win=512 Len=0
1175	12.191419920	192.168.1.1	192.168.1.21	TCP	60	80 → 2439 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
1176	12.191463431	192.168.1.21	192.168.1.1	TCP	54	2439 → 80 [RST] Seq=1 Win=0 Len=0
1186	13.188979639	192.168.1.21	192.168.1.1	TCP	54	2440 → 80 [SYN] Seq=0 Win=512 Len=0
1187	13.190844422	192.168.1.1	192.168.1.21	TCP	60	80 → 2440 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
1188	13.190896846	192.168.1.21	192.168.1.1	TCP	54	2440 → 80 [RST] Seq=1 Win=0 Len=0

La captura de Wireshark valida el comportamiento del comando **hping3**. Se observa el envío de paquetes **SYN** y las respuestas **SYN/ACK** desde la IP del host de destino, lo que demuestra que el **puerto 80** en el host **192.168.1.1** está abierto y escuchando conexiones. La posterior respuesta **RST** es un comportamiento esperado, ya que hping3 está realizando un escaneo de puertos en lugar de intentar establecer una conexión TCP completa, en donde reinicia el orden en el envío de las flags por paquete.

## UDP a puerto 53

No.	Time	Source	Destination	Protocol	Length	Info
3000	27.526965266	192.168.1.21	192.168.1.1	UDP	42	1343 → 53 Len=0
3173	28.528252485	192.168.1.21	192.168.1.1	UDP	42	1344 → 53 Len=0
3389	29.528423145	192.168.1.21	192.168.1.1	UDP	42	1345 → 53 Len=0
3483	30.533218137	192.168.1.21	192.168.1.1	UDP	42	1346 → 53 Len=0
3511	31.538139576	192.168.1.21	192.168.1.1	UDP	42	1347 → 53 Len=0

Captura de tráfico que muestra el resultado del **escaneo UDP al puerto 53**. Se observan los paquetes UDP enviados desde la IP **192.168.1.21** hacia el **puerto 53 de 192.168.1.1**, pero ninguna respuesta desde el destino, resultando en una pérdida del 100% reportada por hping3. Esto puede deberse a que el destino ignora sondas vacías (**len=0**) y a su vez, no hay respuesta dada la poca confiabilidad del tráfico UDP.

## TCP con datos personalizados

tcp.stream eq 6

No.	Time	Source	Destination	Protocol	Length	Info
940	-26.207065184	192.168.1.21	192.168.1.1	TCP	148	1235 → 80 [SYN] Seq=0 Win=512 Len=94
941	-26.204328277	192.168.1.1	192.168.1.21	TCP	60	80 → 1235 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
942	-26.204306945	192.168.1.21	192.168.1.1	TCP	54	1235 → 80 [RST] Seq=1 Win=0 Len=0

Wireshark - Follow TCP Stream (tcp.stream eq 6) - eth1

Nombre : Felipe Oyanedel B  
Curso : Seguridad en Redes de Datos  
Fecha : 25 de Agosto del 2025

Sequence Number (raw): 1019011444  
[Next Sequence Number: 95 (relative sequence num)]  
Acknowledgment Number: 1823670574  
Acknowledgment number (raw): 1823670574  
0101 ... = Header Length: 20 bytes (5)  
Flags: 0x002 (SYN)  
Window: 512  
[Calculated window size: 512]  
Checksum: 0xe7c4 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
[Timestamps]  
[SEQ/ACK analysis]  
[Bytes in flight: 94]  
[Bytes sent since last PSH flag: 94]  
TCP payload (94 bytes)

Captura que muestra el paquete **TCP SYN** con datos personalizados enviado al **puerto 80**. El campo **Len=94** indica el tamaño de los datos adjuntos, que corresponden al contenido del archivo **info.txt**.

## 2. Captura y Análisis de tráfico con Wireshark

Realizar una sesión de captura de tráfico de red durante 10-15 minutos mientras navegas por diferentes sitios web:

- Acceder a al menos 5 sitios web diferentes (incluir HTTP y HTTPS)
- Realizar una descarga de archivo pequeño
- Enviar un correo electrónico o usar una aplicación de mensajería

Aplicar los siguientes filtros en Wireshark y documentar los resultados:

- http - Tráfico HTTP

ip.src==192.168.1.21 && http

No.	Time	Source	Destination	Protocol	Length	Info
1446	74.201487475	192.168.1.21	108.177.123.94	OCSP	493	Request
1565	80.072172087	192.168.1.21	108.177.123.94	OCSP	493	Request
1972	108.130437675	192.168.1.21	45.77.235.56	HTTP	463	GET /login HTTP/1.1
1983	108.558976371	192.168.1.21	45.77.235.56	HTTP	432	GET /favicon.ico HTTP/1.1
2048	116.811146143	192.168.1.21	45.77.235.56	HTTP	620	POST /sessions HTTP/1.1 (application/x-www-form-urlencoded)
2190	135.830767105	192.168.1.21	52.234.209.94	HTTP	495	GET / HTTP/1.1
2203	136.007548082	192.168.1.21	52.234.209.94	HTTP	561	GET /static/prism.css HTTP/1.1
2204	136.007868351	192.168.1.21	52.234.209.94	HTTP	561	GET /static/style.css HTTP/1.1
2270	136.133809298	192.168.1.21	52.234.209.94	HTTP	531	GET /static/prism.js HTTP/1.1
2276	136.140122638	192.168.1.21	52.234.209.94	HTTP	616	GET /static/cube.png HTTP/1.1
2285	136.151110993	192.168.1.21	52.234.209.94	HTTP	544	GET /static/fork.png HTTP/1.1
2378	148.718004670	192.168.1.21	108.177.123.94	OCSP	493	Request
2389	148.812742171	192.168.1.21	108.177.123.94	OCSP	493	Request
2441	152.075918286	192.168.1.21	108.177.123.94	OCSP	493	Request
2571	152.256166593	192.168.1.21	108.177.123.94	OCSP	493	Request
2613	152.306741738	192.168.1.21	108.177.123.94	OCSP	493	Request
2660	152.387770363	192.168.1.21	108.177.123.94	OCSP	493	Request
2667	152.388134004	192.168.1.21	108.177.123.94	OCSP	493	Request
2711	152.460309143	192.168.1.21	108.177.123.94	OCSP	493	Request
2966	161.006425922	192.168.1.21	45.77.235.56	HTTP	463	GET /login HTTP/1.1
3325	169.298551055	192.168.1.21	45.77.235.56	HTTP	463	GET /login HTTP/1.1
4252	169.434818921	192.168.1.21	45.77.235.56	HTTP	463	GET /login HTTP/1.1
4849	170.083440566	192.168.1.21	45.77.235.56	HTTP	463	GET /login HTTP/1.1
5054	171.185186795	192.168.1.21	45.77.235.56	HTTP	463	GET /login HTTP/1.1
5074	171.248681416	192.168.1.21	45.77.235.56	HTTP	463	GET /login HTTP/1.1
5569	172.526409774	192.168.1.21	45.77.235.56	HTTP	463	GET /login HTTP/1.1
5570	172.527084074	192.168.1.21	45.77.235.56	HTTP	463	GET /login HTTP/1.1
5784	174.040061042	192.168.1.21	45.77.235.56	HTTP	463	GET /login HTTP/1.1

Wireshark - Packet 2048 - eth1

Frame 2048: 620 bytes on wire (4960 bits), 620 bytes captured (4960 bits) on interface eth1, id 0  
Ethernet II, Src: PCSSystemtec\_e0:64:1e (08:00:27:e0:64:1e), Dst: zte\_36:55:7c (14:ca:56:36:55:7c)  
Internet Protocol Version 4, Src: 192.168.1.21, Dst: 45.77.235.56  
Transmission Control Protocol, Src Port: 53240, Dst Port: 80, Seq: 398, Ack: 595, Len: 554  
Hypertext Transfer Protocol  
HTML Form URL Encoded: application/x-www-form-urlencoded  
Form item: "utf8" = ""  
Form item: "username" = "mmmm"  
Key: username  
Value: mmmm  
Form item: "password" = "mmmmmm"  
Key: password  
Value: mmmmm  
Form item: "commit" = "Sign in"

• dns - Consultas DNS

No.	Time	Source	Destination	Protocol	Length	Info
448	52.892596944	192.168.1.1	192.168.1.21	DNS	93	Standard query response 0xdice A fonts.gstatic.com A 64.233.190.94
449	52.893668986	192.168.1.1	192.168.1.21	DNS	105	Standard query response 0x9ac9 AAAA Fonts.gstatic.com AAAA 2800:3f0:4003:c01::5e
638	56.383308750	fe80::51a6:1264:df0_	fe80::1	DNS	94	Standard query 0xc807 A assets.msn.com
639	56.390343189	fe80::1	fe80::51a6:1264:df0_	DNS	266	Standard query response 0xc807 A assets.msn.com CNAME assets-msn-com-world-atm-default.traff
728	62.420172317	192.168.1.17	192.168.1.1	DNS	75	Standard query 0xedc4 A play.google.com
729	62.421179233	192.168.1.17	192.168.1.1	DNS	75	Standard query 0xe64a HTTPS play.google.com
730	62.422970557	192.168.1.1	192.168.1.17	DNS	171	Standard query response 0xedc4 A play.google.com A 172.217.192.138 A 172.217.192.102 A 172.217.192.104
731	62.429472724	192.168.1.1	192.168.1.17	DNS	125	Standard query response 0xe64a HTTPS play.google.com SOA ns1.google.com
761	62.723699887	192.168.1.1	192.168.1.17	DNS	125	Standard query response 0xe64a HTTPS play.google.com SOA ns1.google.com
779	65.318362609	192.168.1.21	192.168.1.1	DNS	81	Standard query 0xa74b A opencart.abstracta.us
780	65.318853758	192.168.1.21	192.168.1.1	DNS	81	Standard query 0xb8b7 AAAA opencart.abstracta.us
781	65.321157065	192.168.1.1	192.168.1.21	DNS	97	Standard query response 0xa74b A opencart.abstracta.us A 13.52.135.157
783	65.326666469	192.168.1.1	192.168.1.21	DNS	226	Standard query response 0xb8b7 AAAA opencart.abstracta.us CNAME ec2-13-52-135-157.us-west-1
1150	73.109354531	192.168.1.21	192.168.1.1	DNS	80	Standard query 0x769d A fonts.googleapis.com
1151	73.109690848	192.168.1.21	192.168.1.1	DNS	80	Standard query 0xa830 AAAA fonts.googleapis.com
1152	73.111814144	192.168.1.1	192.168.1.21	DNS	96	Standard query response 0x769d A fonts.googleapis.com A 172.217.192.95
1153	73.111814635	192.168.1.1	192.168.1.21	DNS	108	Standard query response 0xa830 AAAA fonts.googleapis.com AAAA 2800:3f0:4003:c0f::5f
1154	73.111814731	192.168.1.1	192.168.1.21	DNS	70	Standard query response 0xa830 AAAA fonts.googleapis.com

Frame 779: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface eth0  
 Ethernet II, Src: POSSystemtec\_e0:64:1e (08:00:27:e0:64:1e), Dst: zte\_36:55:7c (14:c4:56:36:55:7c)  
 Internet Protocol Version 4, Src: 192.168.1.21, Dst: 192.168.1.1  
 User Datagram Protocol, Src Port: 35423, Dst Port: 53  
 Domain Name System (query)  
 Transaction ID: 0xa74b  
 Flags: 0x0100 Standard query  
 Questions: 1  
 Answer RRs: 0  
 Authority RRs: 0  
 Additional RRs: 0  
 Queries  
 opencart.abstracta.us: type A, class IN  
 Name: opencart.abstracta.us  
 Type: A  
 Class: IN  
 TTL: 300  
 Data Length: 4  
 Data: 13.52.135.157

• tcp.port == 443 - Tráfico HTTPS

No.	Time	Source	Destination	Protocol	Length	Info
291	49.176542214	192.168.1.17	52.123.128.14	TCP	66	58219 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
292	49.184165315	52.123.128.14	192.168.1.17	TCP	66	443 → 58219 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
293	49.184165567	192.168.1.17	52.123.128.14	TCP	66	58219 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
294	49.184541860	192.168.1.17	52.123.128.14	TLSv1.2	541	Client Hello (SHA256WithRSAEncryption)
295	49.194739899	52.123.128.14	192.168.1.17	TCP	60	443 → 58219 [ACK] Seq=1 Ack=488 Win=12583168 Len=0
296	49.196501635	52.123.128.14	192.168.1.17	TLSv1.2	6029	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
297	49.196501886	192.168.1.17	52.123.128.14	TCP	60	58219 → 443 [ACK] Seq=488 Ack=5976 Win=262144 Len=0
298	49.206067919	192.168.1.17	52.123.128.14	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
299	49.220470176	52.123.128.14	192.168.1.17	TCP	60	443 → 58219 [ACK] Seq=5976 Ack=646 Win=12582912 Len=0
300	49.220470697	52.123.128.14	192.168.1.17	TLSv1.2	396	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
301	49.220470777	192.168.1.17	52.123.128.14	TCP	60	58219 → 443 [ACK] Seq=646 Ack=6318 Win=261632 Len=0
302	49.220726591	192.168.1.17	52.123.128.14	TLSv1.2	674	Application Data
303	49.237604398	52.123.128.14	192.168.1.17	TCP	60	443 → 58219 [ACK] Seq=6318 Ack=1266 Win=12582400 Len=0
305	49.433252643	52.123.128.14	192.168.1.17	TLSv1.2	934	Application Data
306	49.433253085	192.168.1.17	52.123.128.14	TCP	60	58219 → 443 [ACK] Seq=1266 Ack=7198 Win=260864 Len=0
305	52.174512135	192.168.1.21	172.217.192.95	TCP	74	33880 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3159798192 TSecr=0 WS=128
306	52.181550824	172.217.192.95	192.168.1.21	TCP	74	443 → 33880 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM TSval=4240105330 TSecr=3159798192
307	52.181550835	192.168.1.21	172.217.192.95	TCP	66	33880 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3159798192 TSecr=4240105330

Frame 291: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0  
 Ethernet II, Src: Intel\_f8:0f:a7 (98:43:fa:fd:0f:a7), Dst: zte\_36:55:7c (14:c4:56:36:55:7c)  
 Internet Protocol Version 4, Src: 192.168.1.17, Dst: 52.123.128.14  
 Transmission Control Protocol, Src Port: 58219, Dst Port: 443, Seq: 0, Len: 0

• icmp - Tráfico ICMP

No.	Time	Source	Destination	Protocol	Length	Info
408	10.848248310	192.168.1.21	192.168.1.1	ICMP	166	Destination unreachable (Port unreachable)

Internet Control Message Protocol  
 Type: 3 (Destination unreachable)  
 Code: 3 (Port unreachable)  
 Checksum: 0x80dd [correct]  
 [Checksum Status: Good]  
 Unused: 00000000  
 Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.21  
 User Datagram Protocol, Src Port: 53, Dst Port: 34732  
 Destination Port: 34732  
 Length: 164  
 Checksum: 0xfac6 [unverified]  
 [Checksum Status: Unverified]  
 [Stream index: 22]  
 UDP payload (96 bytes)  
 Domain Name System (response)

- ip.addr == [tu\_IP] - Todo el tráfico de tu máquina

No.	Time	Source	Destination	Protocol	Length	Info
401	10.783183962	44.212.204.177	192.168.1.21	TCP	74	443 → 55988 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1460 SACK_PERM TSval=1263350485 TSecr=...
402	10.783183953	44.212.204.177	192.168.1.21	TCP	74	443 → 55974 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1460 SACK_PERM TSval=1263350486 TSecr=...
403	10.783845731	192.168.1.21	44.212.204.177	TCP	66	55988 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=705532135 TSecr=1263350485
404	10.784124882	192.168.1.21	44.212.204.177	TCP	66	55974 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=705532136 TSecr=1263350486
405	10.785798267	192.168.1.21	44.212.204.177	TLSv1.2	874	Client Hello (SNI=collector.unsplash.com)
406	10.786511756	192.168.1.21	44.212.204.177	TLSv1.2	874	Client Hello (SNI=collector.unsplash.com)
407	10.847405911	192.168.1.1	192.168.1.21	DNS	138	Standard query response 0x5934 AAAA ad.doubleclick.net SOA ns1.google.com
408	10.848245110	192.168.1.21	192.168.1.1	ICMP	160	Destination unreachable (Port unreachable)
409	10.871129365	3.213.228.90	192.168.1.21	TCP	74	443 → 33514 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1460 SACK_PERM TSval=1919021940 TSecr=...
410	10.871206042	192.168.1.21	3.213.228.90	TCP	66	33514 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1546275436 TSecr=1919021940
411	10.872175100	192.168.1.21	3.213.228.90	TLSv1.3	1105	Client Hello (SNI=e-10457.adzerk.net)
412	10.965826018	44.212.204.177	192.168.1.21	TCP	66	443 → 55988 [ACK] Seq=1 Ack=809 Win=44800 Len=0 TSval=1263350672 TSecr=705532138
413	10.965826389	44.212.204.177	192.168.1.21	TLSv1.2	2962	Server Hello
414	10.965856699	192.168.1.21	44.212.204.177	TCP	66	55988 → 443 [ACK] Seq=809 Ack=2897 Win=70144 Len=0 TSval=705532318 TSecr=1263350672
415	10.966826128	44.212.204.177	192.168.1.21	TLSv1.2	1469	Certificate, Server Key Exchange, Server Hello Done
416	10.966871292	192.168.1.21	44.212.204.177	TCP	66	55988 → 443 [ACK] Seq=809 Ack=4300 Win=72960 Len=0 TSval=705532319 TSecr=1263350673
417	10.967306232	44.212.204.177	192.168.1.21	TCP	66	443 → 55974 [ACK] Seq=1 Ack=809 Win=44800 Len=0 TSval=1263350674 TSecr=705532139
418	10.967306382	44.212.204.177	192.168.1.21	TLSv1.2	2962	Server Hello
419	10.967313741	192.168.1.21	44.212.204.177	TCP	66	55974 → 443 [ACK] Seq=809 Ack=2897 Win=70144 Len=0 TSval=705532319 TSecr=1263350674
420	10.968532739	44.212.204.177	192.168.1.21	TLSv1.2	1469	Certificate, Server Key Exchange, Server Hello Done
421	10.968542223	192.168.1.21	44.212.204.177	TCP	66	55974 → 443 [ACK] Seq=809 Ack=4300 Win=72960 Len=0 TSval=705532321 TSecr=1263350675
422	10.969824358	192.168.1.21	44.212.204.177	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
423	10.970832782	192.168.1.21	44.212.204.177	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
424	11.004918217	3.213.228.90	192.168.1.21	TCP	66	443 → 33514 [ACK] Seq=1 Ack=1040 Win=44800 Len=0 TSval=1919022074 TSecr=1546275437
425	11.004918638	3.213.228.90	192.168.1.21	TLSv1.3	2962	Server Hello, Change Cipher Spec, Application Data
426	11.004978990	192.168.1.21	3.213.228.90	TCP	66	33514 → 443 [ACK] Seq=1040 Ack=2897 Win=70144 Len=0 TSval=1546275570 TSecr=1919022074
427	11.006078303	3.213.228.90	192.168.1.21	TLSv1.3	1541	Application Data, Application Data, Application Data
428	11.006132628	192.168.1.21	3.213.228.90	TCP	66	33514 → 443 [ACK] Seq=1040 Ack=4372 Win=73088 Len=0 TSval=1546275571 TSecr=1919022075
429	11.018469377	192.168.1.21	3.213.228.90	TLSv1.3	138	Change Cipher Spec, Application Data
430	11.018469377	192.168.1.21	3.213.228.90	TLSv1.3	138	Change Cipher Spec, Application Data

Identificar y explicar:

- **Protocolos más utilizados**

Los protocolos que se observan con mayor frecuencia en las capturas son:

**DNS:** Se utiliza para la resolución de nombres de dominio, convirtiendo nombres como web.whatsapp.com en direcciones IP.

No.	Time	Source	Destination	Protocol	Length	Info
517	12.838053990	192.168.1.1	192.168.1.21	DNS	128	Standard query type A
518	12.891115087	192.168.1.1	192.168.1.21	DNS	128	Standard query response type A
528	12.914354372	192.168.1.21	192.168.1.1	DNS	128	Standard query type A
531	12.922558469	192.168.1.1	192.168.1.21	DNS	128	Standard query response type A

```

Class: IN (0x0001)
  Answers
    web.whatsapp.com: type CNAME, class IN, cname mmx-ds.cdn.whatsapp.net
      Name: web.whatsapp.com
      Type: CNAME (5) (Canonical NAME for an alias)
      Class: IN (0x0001)
      Time to live: 1958 (32 minutes, 38 seconds)
      Data length: 25
      CNAME: mmx-ds.cdn.whatsapp.net
    mmx-ds.cdn.whatsapp.net: type A, class IN, addr 157.240.204.60
      Name: mmx-ds.cdn.whatsapp.net
  
```

**TCP:** Es un protocolo de transporte fundamental que establece conexiones para el intercambio de datos.

**TLSv1.2 (Transport Layer Security):** Una versión de un protocolo criptográfico que proporciona comunicación segura y cifrada a través de la red, comúnmente utilizada para HTTPS.

**HTTP (Hypertext Transfer Protocol):** El protocolo base para la World Wide Web, utilizado para la transferencia de información de páginas web.

**ICMP (Internet Control Message Protocol):** Se utiliza para enviar mensajes de error y diagnósticos, como los mensajes de "Destino inalcanzable" que se observan.

- **Direcciones IP de destino más frecuentes**

En cuanto a direcciones IP de destino fueron variadas, dado que se navegó en diferentes sitios web, algunos HTTP y otros HTTPS, entre otros. Para hablarlo a grandes rasgos, podemos tomar como indicador las direcciones IP relacionadas a servidores DNS de Google y sus direcciones IP derivadas.

A su vez, la dirección IP correspondiente a la puerta de enlace fue una de las mas recurrentes, dado que muchas de las peticiones inicialmente se dirigían a tal dirección.

- **Puertos más utilizados**

En las capturas se identifican los siguientes puertos, asociados a los protocolos mencionados:

**Puerto 53 (DNS):** Utilizado para las consultas y respuestas del sistema de nombres de dominio, en donde la comunicación era entre nuestra maquina Kali Linux y la puerta de enlace configurada en el router de nuestra red local.

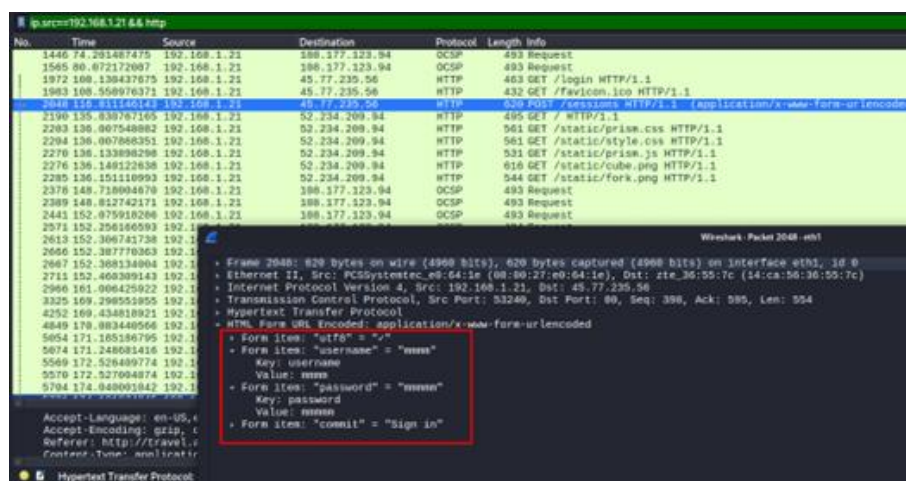
**Puerto 443 (HTTPS/TLS):** El puerto estándar para la comunicación web segura y cifrada, como se ve en las conexiones TLSv1.2.

**Puerto 80 (HTTP):** El puerto estándar para la comunicación web no cifrada, evidenciado por la transferencia de datos en texto plano, haciéndolo un protocolo potencialmente vulnerable.

**Puertos dinámicos/efímeros (> 1023):** Los puertos de origen, asignados aleatoriamente por el sistema operativo de nuestra máquina local para cada conexión saliente.

- **Posibles vulnerabilidades observadas (tráfico no cifrado, etc.)**

La vulnerabilidad más crítica que se puede observar en toda esta captura de tráfico es la transmisión de credenciales en texto plano a través de HTTP. Al momento de navegar por sitios HTTP, se simuló un caso hipotético de ingreso de credenciales de usuario al portal de Login, teniendo como consecuencia que en la captura de pantalla muestra claramente un formulario de inicio de sesión donde el nombre de usuario aleatorio (mmm) y la contraseña (mmm) se envían sin cifrar en el detalle del paquete.



Cualquier persona con acceso a la red (como un atacante en la misma red Wi-Fi o un administrador de red malicioso) podría capturar y leer esta información fácilmente, comprometiendo la cuenta del usuario. La solución para este problema es utilizar HTTPS para cifrar todo el tráfico web, especialmente en los formularios de inicio de sesión.



### 3. Análisis de conectividad y respuesta de red

Utilizando tanto hping3 como Wireshark:

a) Realizar un análisis de conectividad a diferentes puertos de un servidor remoto:

a. Puerto 22 (SSH)

```
(root@kali)-[/home/kali]
# hping3 -S -p 22 -c 1 192.168.1.1
HPING 192.168.1.1 (eth1 192.168.1.1): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.1 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=29200 rtt=3.5 ms

— 192.168.1.1 hping statistic —
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 3.5/3.5/3.5 ms

(root@kali)-[/home/kali]
```

ip.addr == 192.168.1.21 && ip.addr == 192.168.1.1

No.	Time	Source	Destination	Protocol	Length	Info
477	74.588631974	192.168.1.21	192.168.1.1	TCP	54	3022 → 22 [SYN] Seq=0 Win=512 Len=0
478	74.590591972	192.168.1.1	192.168.1.21	TCP	60	22 → 3022 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
479	74.590617707	192.168.1.21	192.168.1.1	TCP	54	3022 → 22 [RST] Seq=1 Win=0 Len=0

Frame 477: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0  
 Ethernet II, Src: PCSSystemtec\_e0:64:1e (08:00:27:e0:64:1e), Dst: zte\_36:55:7c (14:ca:00:00:36:55:7c)  
 Internet Protocol Version 4, Src: 192.168.1.21, Dst: 192.168.1.1  
 Transmission Control Protocol, Src Port: 3022, Dst Port: 22, Seq: 0, Len: 0

Source Port: 3022  
 Destination Port: 22  
 [Stream index: 13]  
 [Stream Packet Number: 1]  
 [Conversation completeness: Incomplete (35)]  
 [TCP Segment Len: 0]  
 Sequence Number: 0 (relative sequence number)  
 Sequence Number (raw): 681077507  
 [Next Sequence Number: 1 (relative sequence number)]  
 Acknowledgment Number: 1802049751  
 Acknowledgment number (raw): 1802049751  
 0101 .... = Header Length: 20 bytes (5)  
 Flags: 0x002 (SYN)  
 Window: 512  
 [Calculated window size: 512]  
 Checksum: 0x00bc [unverified]  
 [Checksum Status: Unverified]  
 Urgent Pointer: 0  
 [Timestamps]

b. Puerto 80 (HTTP)

```
(root@kali)-[/home/kali]
# hping3 -S -p 80 -c 1 192.168.1.1
HPING 192.168.1.1 (eth1 192.168.1.1): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.1 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=29200 rtt=2.6 ms

— 192.168.1.1 hping statistic —
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 2.6/2.6/2.6 ms
```

ip.addr == 192.168.1.21 && ip.addr == 192.168.1.1

No.	Time	Source	Destination	Protocol	Length	Info
101	12.233010257	192.168.1.21	192.168.1.1	TCP	54	1646 → 80 [SYN] Seq=0 Win=512 Len=0
102	12.234838730	192.168.1.1	192.168.1.21	TCP	60	80 → 1646 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
103	12.234895764	192.168.1.21	192.168.1.1	TCP	54	1646 → 80 [RST] Seq=1 Win=0 Len=0

Frame 101: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0  
 Ethernet II, Src: PCSSystemtec\_e0:64:1e (08:00:27:e0:64:1e), Dst: zte\_36:55:7c (14:ca:00:00:36:55:7c)  
 Internet Protocol Version 4, Src: 192.168.1.21, Dst: 192.168.1.1  
 Transmission Control Protocol, Src Port: 1646, Dst Port: 80, Seq: 0, Len: 0

Source Port: 1646  
 Destination Port: 80  
 [Stream index: 11]  
 [Stream Packet Number: 1]  
 [Conversation completeness: Incomplete (35)]  
 [TCP Segment Len: 0]  
 Sequence Number: 0 (relative sequence number)  
 Sequence Number (raw): 1481856526  
 [Next Sequence Number: 1 (relative sequence number)]  
 Acknowledgment Number: 1242915196  
 Acknowledgment number (raw): 1242915196  
 0101 .... = Header Length: 20 bytes (5)  
 Flags: 0x002 (SYN)  
 Window: 512  
 [Calculated window size: 512]  
 Checksum: 0xc9ca [unverified]  
 [Checksum Status: Unverified]  
 Urgent Pointer: 0  
 [Timestamps]



c. Puerto 443 (HTTPS)

```
(root@kali)-[/home/kali]
# hping3 -S -p 443 -c 1 192.168.1.1
HPING 192.168.1.1 (eth1 192.168.1.1): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.1 ttl=64 DF id=0 sport=443 flags=SA seq=0 win=29200 rtt=3.6 ms

— 192.168.1.1 hping statistic —
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 3.6/3.6/3.6 ms
```

ip.addr == 192.168.1.21 && ip.addr == 192.168.1.1

No.	Time	Source	Destination	Protocol	Length	Info
41	7.771691371	192.168.1.21	192.168.1.1	TCP	54	2005 → 443 [SYN] Seq=0 Win=0 Len=0
42	7.774979856	192.168.1.1	192.168.1.21	TCP	60	443 → 2005 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
43	7.774998532	192.168.1.21	192.168.1.1	TCP	54	2005 → 443 [RST] Seq=1 Win=0 Len=0

Frame 41: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth1  
 Ethernet II, Src: PCSSystemtec e0:64:1e (08:00:27:00:64:1e), Dst: zte\_36:55:7c (14:ca  
 Internet Protocol Version 4, Src: 192.168.1.21, Dst: 192.168.1.1  
 Transmission Control Protocol, Src Port: 2005, Dst Port: 443, Seq: 0, Len: 0  
 Source Port: 2005  
 Destination Port: 443  
 [Stream index: 8]  
 [Stream Packet Number: 1]  
 [Conversation completeness: Incomplete (35)]  
 [TCP Segment Len: 0]  
 Sequence Number: 0 (relative sequence number)  
 Sequence Number (raw): 89957142  
 [Next Sequence Number: 1 (relative sequence number)]  
 Acknowledgment Number: 307659783  
 Acknowledgment number (raw): 307659783  
 0101 ... = Header Length: 20 bytes (5)  
 Flags: 0x002 (SYN)  
 Window: 512  
 [Calculated window size: 512]  
 Checksum: 0x5788 [unverified]  
 [Checksum Status: Unverified]  
 Urgent Pointer: 0  
 [Timestamps]

d. Puerto 21 (FTP)

```
(root@kali)-[/home/kali]
# hping3 -S -p 21 -c 1 192.168.1.1
HPING 192.168.1.1 (eth1 192.168.1.1): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.1 ttl=64 DF id=43908 sport=21 flags=RA seq=0 win=0 rtt=7.9 ms

— 192.168.1.1 hping statistic —
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 7.9/7.9/7.9 ms
```

ip.addr == 192.168.1.21 && ip.addr == 192.168.1.1

No.	Time	Source	Destination	Protocol	Length	Info
60	7.277297220	192.168.1.21	192.168.1.1	TCP	54	1555 → 21 [SYN] Seq=0 Win=512 Len=0
61	7.282142080	192.168.1.1	192.168.1.21	TCP	60	21 → 1555 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Frame 60: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth1  
 Ethernet II, Src: PCSSystemtec e0:64:1e (08:00:27:00:64:1e), Dst: zte\_36:55:7c (14:ca  
 Internet Protocol Version 4, Src: 192.168.1.21, Dst: 192.168.1.1  
 Transmission Control Protocol, Src Port: 1555, Dst Port: 21, Seq: 0, Len: 0  
 Source Port: 1555  
 Destination Port: 21  
 [Stream index: 9]  
 [Stream Packet Number: 1]  
 [Conversation completeness: Incomplete, SYN\_SENT (1)]  
 [TCP Segment Len: 0]  
 Sequence Number: 0 (relative sequence number)  
 Sequence Number (raw): 1776365676  
 [Next Sequence Number: 1 (relative sequence number)]  
 Acknowledgment Number: 1698048915  
 Acknowledgment number (raw): 1698048915  
 0101 ... = Header Length: 20 bytes (5)  
 Flags: 0x002 (SYN)  
 Window: 512  
 [Calculated window size: 512]  
 Checksum: 0xfcc0 [unverified]  
 [Checksum Status: Unverified]  
 Urgent Pointer: 0  
 [Timestamps]

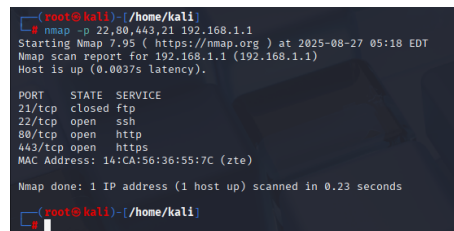
**b) Documentar qué puertos están abiertos, cerrados o filtrados**

En vista de las respuestas al comando **hping3 -S -p [puerto] -c 1 [ip de puerta de enlace]**, los puertos escaneados figuran de la siguiente manera:

**Puertos 22 – 80 – 443** : Puertos abiertos, dado que al capturar tráfico a través de Wireshark se visualiza que el host de destino responde a la sonda **SYN** con un paquete **SYN,ACK**. Esto confirma que hay un servicio escuchando en esos puertos y listo para establecer una conexión.

**Puerto 21** : Puerto cerrado, dado que al capturar tráfico a través de Wireshark se visualiza que el host de destino responde a la sonda **SYN** con un paquete **RST,ACK**, lo cual es una señal inequívoca de que el puerto no cuenta con ningún servicio en escucha y/o se encuentra cerrado.

Se procedió a validar de todas formas haciendo un escaneo simple de puertos con **nmap**, esto dado que es la herramienta estándar para obtener este tipo de información de manera más rápida y gráfica:



```
(root@kali) - /home/kali
$ nmap -p 22,80,443,21 192.168.1.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-27 05:18 EDT
Nmap scan report for 192.168.1.1 (192.168.1.1)
Host is up (0.0037s latency).

PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
MAC Address: 14:CA:56:36:55:7C (zte)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
(root@kali) - /home/kali
```

**c) Analizar los tiempos de respuesta y patrones de conectividad**

El análisis de los datos obtenidos de hping3 y las capturas de tráfico de Wireshark permite evaluar tanto el estado de los puertos como el rendimiento de la red.

**Puertos Abiertos (22, 80 y 443)** : Los escaneos a los puertos 22, 80 y 443 mostraron que el host de destino está activo y los servicios están en funcionamiento.

**Tiempos de Respuesta (RTT)**: La salida de hping3 para estos puertos mostró un tiempo de ida y vuelta (RTT) promedio de 3.23 ms. Esto indica una conexión de muy baja latencia, lo cual es ideal para una comunicación de red eficiente.

**Patrones de Conectividad**: Las capturas de Wireshark confirmaron que, en respuesta a cada paquete SYN enviado, el host de destino respondió con un paquete SYN-ACK. Este es el comportamiento estándar y esperado para un puerto abierto, confirmando que un servicio está escuchando y listo para establecer una conexión TCP. El paquete RST posterior, enviado desde mi máquina, es el resultado del kernel del sistema operativo que rechaza la respuesta SYN-ACK, ya que no hay un proceso de aplicación real esperando esa conexión.

**Puerto Cerrado (21)** : El escaneo del puerto 21 reveló que el servicio de FTP no está activo o no es accesible.

**Tiempo de Respuesta (RTT)**: La salida de hping3 para este puerto mostró un tiempo de ida y vuelta de 7.9 ms. La latencia es comparable a la de los puertos abiertos dado que no es tan alta, lo que confirma que el host está en línea y es accesible dentro de la red.

**Patrones de Conectividad**: La captura de Wireshark mostró que, al enviar un paquete SYN al puerto 21, el host de destino respondió inmediatamente con un paquete RST,ACK. Este es un patrón inequívoco de un puerto cerrado. El host recibe la solicitud, pero la rechaza explícitamente porque no hay ningún servicio escuchando en dicho puerto, lo cual coincide con el resultado de Nmap.

## Recomendaciones

Para darle más robustez al análisis, ejecutamos un barrido de puertos con el comando

**nmap -Sv -p- 192.168.1.1**

El análisis de la salida de Nmap arrojó los siguientes resultados:

Se identificaron cinco puertos abiertos:

- Puerto 22 (SSH): Ejecuta el servicio Dropbear sshd 2022.83. Este es un servidor SSH ligero, común en dispositivos de red.
- Puerto 53 (DNS): Ejecuta el servicio Unbound, un servidor DNS que gestiona las solicitudes de la red interna.
- Puerto 80 (HTTP): Aunque está abierto, el servicio no fue reconocido por Nmap, lo que es común en las interfaces web de administración de routers.
- Puerto 443 (HTTPS): El servicio fue marcado como tcpwrapped, lo que indica que una conexión TCP se completó, pero el servicio cerró la conexión inmediatamente, sugiriendo un firewall o un mecanismo de seguridad activo.

Se confirmó que la gran mayoría de los puertos (65,530) están cerrados, lo cual es una buena práctica de seguridad.

El puerto 23 (Telnet) fue identificado como filtered, lo que demuestra la presencia de un firewall que bloquea el tráfico hacia este puerto, impidiendo el uso de este protocolo obsoleto e inseguro.

En vista de esto y si bien las configuraciones cumplen con una seguridad sólida hacia la red interna, de igual forma se dedujeron las siguientes recomendaciones a tomar en consideración:

- Actualizar el Firmware del Router: Contactar al proveedor (ZTE) para verificar si hay actualizaciones de firmware disponibles. Las actualizaciones suelen incluir parches de seguridad críticos que protegen contra vulnerabilidades conocidas.
- Cambiar las Credenciales de Acceso por Defecto: Acceder a la interfaz de administración web y cambiar la contraseña de fábrica por una contraseña fuerte y única.
- Deshabilitar el Acceso Remoto Innecesario: Si no se requiere acceder a la configuración del router desde Internet, desactivar los servicios SSH y HTTP para el acceso externo. Esto evita que los atacantes intenten acceder al dispositivo desde fuera de la red local.
- Limitar el Acceso al Servidor DNS: Configurar el servicio Unbound para que solo responda a consultas DNS provenientes de la red interna. Esto previene que el dispositivo sea utilizado en ataques de amplificación DNS.
- Revisar la Configuración del Firewall: Asegurarse de que el firewall integrado del router esté correctamente configurado para bloquear el tráfico en todos los puertos que no son necesarios, como se vio en el caso del puerto 23.

## Conclusiones

El análisis de seguridad realizado en la red corporativa de Desafío Latam mediante las herramientas **hping3** y **Wireshark** permitió obtener una visión detallada del comportamiento de la red, la exposición de servicios y la identificación de posibles vulnerabilidades.

A continuación, se destacan los hallazgos más relevantes:

Se confirmó la correcta conectividad a nivel de red mediante pruebas ICMP, con tiempos de respuesta bajos y 0% de pérdida de paquetes. Los puertos 22 (SSH), 80 (HTTP) y 443 (HTTPS) se encuentran abiertos y respondiendo adecuadamente, lo que indica que los servicios asociados están activos y accesibles. El puerto 21 (FTP) se identificó como cerrado, lo cual es positivo desde el punto de vista de seguridad, al reducir la superficie de ataque.

Las pruebas con hping3 hacia el puerto 53 (DNS) mostraron un 100% de pérdida de paquetes, lo que no necesariamente indica que el servicio esté caído, sino que responde de manera selectiva a consultas bien formadas. Esto fue confirmado con nmap, que detectó el servicio Unbound en ejecución.

Uno de los hallazgos más relevantes fue que se detectó tráfico HTTP sin cifrar durante la navegación web, donde de manera hipotética y sabida, se expusieron credenciales de usuario en texto plano. Esto representa un riesgo crítico de seguridad si fuese un usuario y contexto más real, especialmente en redes compartidas o públicas.

Los protocolos más utilizados fueron DNS, TCP, TLSv1.2, HTTP e ICMP, con una predominancia de puertos estándar como 53, 80 y 443, junto con puertos efímeros para conexiones salientes. El escaneo con nmap confirmó que la mayoría de los puertos están cerrados, lo que refleja una configuración base segura por parte del fabricante del router.

Se identificó que el puerto 443 presenta un comportamiento tcpwrapped, sugiriendo la intervención de un firewall o mecanismo de seguridad que limita el acceso no autorizado. El puerto 23 (Telnet) está filtrado, lo que evita el uso de protocolos inseguros y demuestra una configuración defensiva activa.

En resumen, si bien la red presenta una configuración base sólida y varios mecanismos de protección activos, la exposición de tráfico no cifrado y la presencia de servicios expuestos como SSH y HTTP requieren atención inmediata para elevar el nivel de seguridad y prevenir posibles incidentes.