{desafío} latam_ Academia de talentos digitales

Prueba - Análisis de Seguridad en Redes de Datos

Nombre: Nicolás Pérez
Fecha:04/09/2025
Curso:G1
Prueba módulo 7

En esta prueba validaremos nuestros conocimientos de la aplicación de herramientas y metodologías de análisis de seguridad para la identificación y análisis de tráfico en redes de datos corporativas. Para lograrlo, necesitarás aplicar los requerimientos que serán solicitados utilizando las herramientas Kali Linux y Wireshark.

Lee todo el documento antes de comenzar el desarrollo individual para asegurarte de tener el máximo de puntaje y enfocar bien los esfuerzos.

Tiempo asociado: 3 horas cronológicas.

Descripción

La empresa Desafío Latam ha implementado una red corporativa en donde deberás realizar una serie de análisis de tráfico y pruebas de conectividad que permita evaluar el comportamiento de la red desde el punto de vista de seguridad, así como la identificación de patrones de tráfico y posibles anomalías.

Introducción

El Objetivo de realizar este informe es analizar el comportamiento de la red mediante herramientas de análisis de tráfico y además realizando pruebas de conectividad. Para esto se utiliza en Kali Linux, herramientas como Hping3 para generar tráfico de prueba y Wireshark para simular uso de red y analizar las respuestas. Se realizaron pruebas enfocadas al DNS de google 8.8.8.8 para recopilar información sobre una red relacionada a la seguridad.

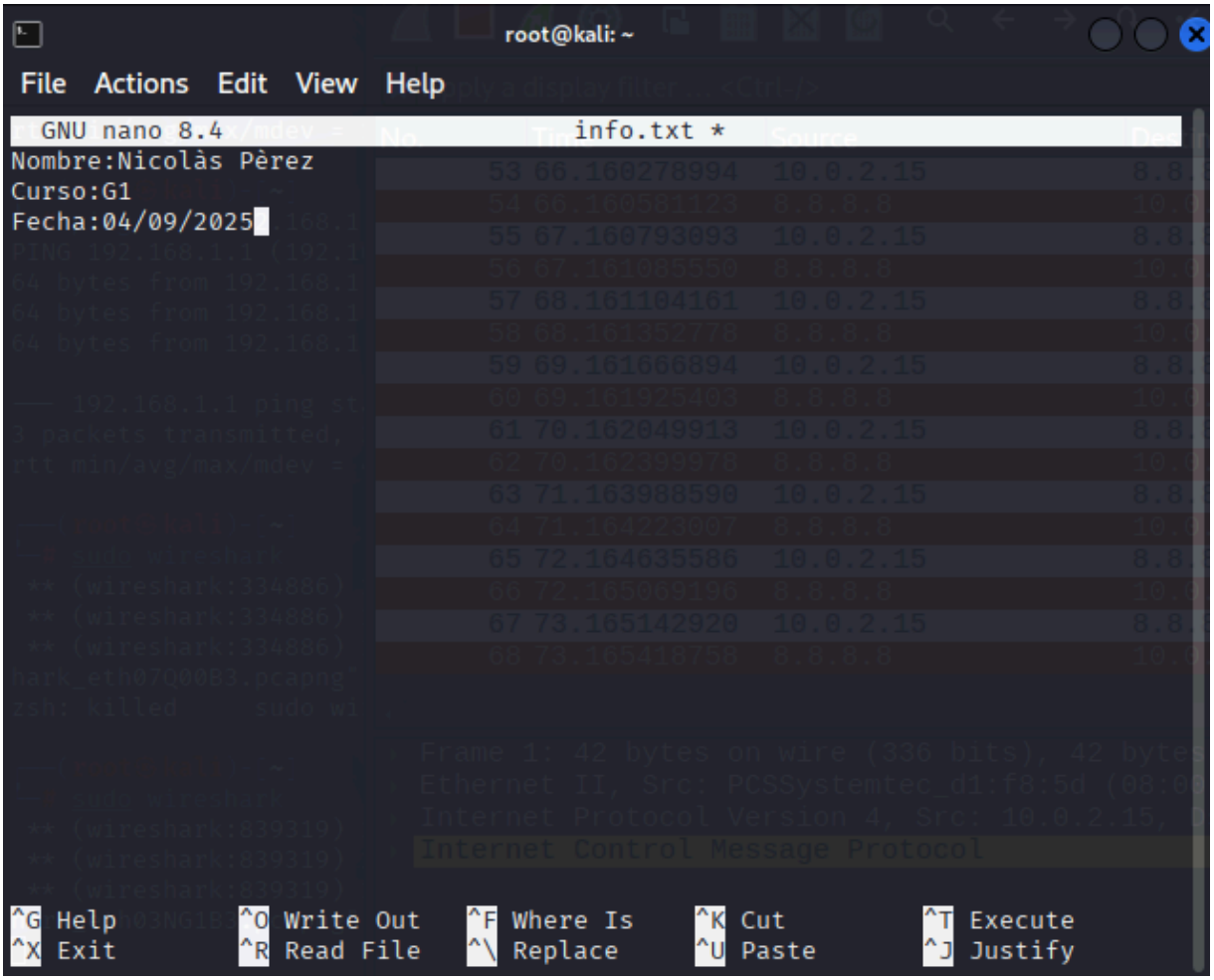
Desarrollo

Requerimientos de la Prueba:

1. Análisis de Tráfico con hping3 en Kali Linux

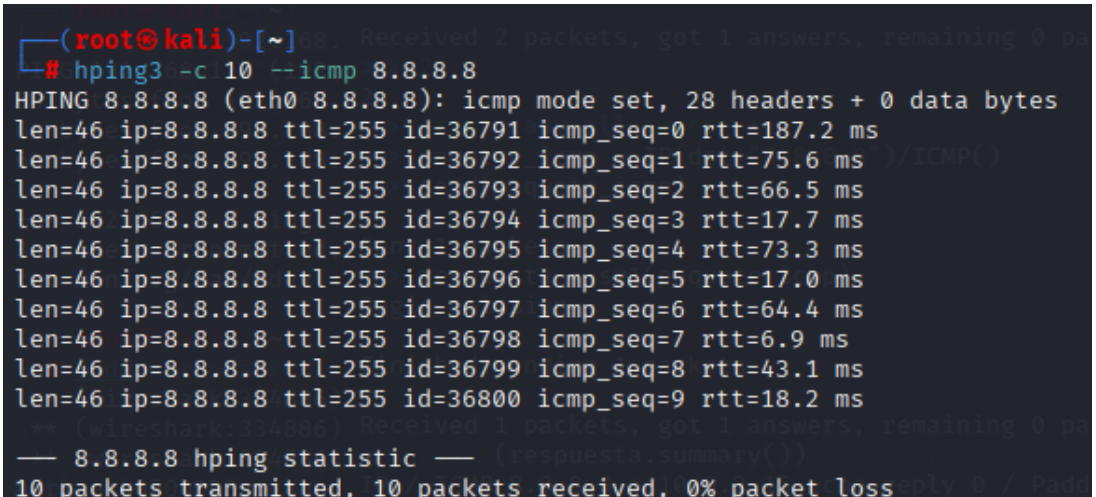
Utilizando Kali Linux, deberás realizar las siguientes actividades con la herramienta hping3:

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

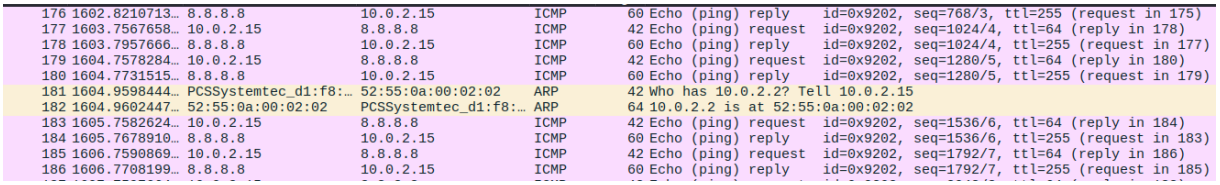


- **b)** Utilizar hping3 para enviar diferentes tipos de paquetes a un host objetivo (puede ser google.com o la puerta de enlace local):

  ICMP ping normal = Enviara 10 paquetes al ICMP al dns 8.8.8.8

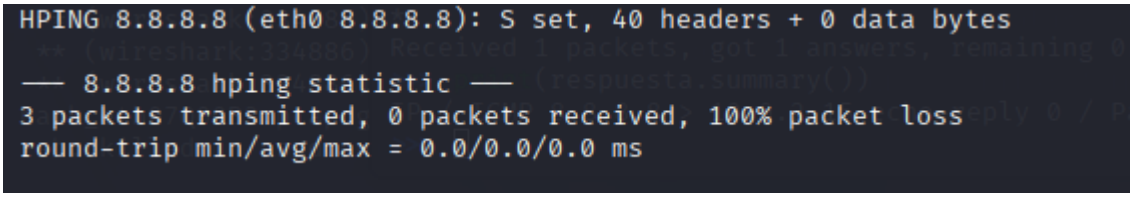


Comunicación exitosa el servidor responde por medio de ICMP



176	1602.8210713…	8.8.8.8	10.0.2.15	ICMP	60	Echo (ping) reply id=0x9202, seq=768/3, ttl=255 (request in 175)
177	1603.7567658…	10.0.2.15	8.8.8.8	ICMP	42	Echo (ping) request id=0x9202, seq=1024/4, ttl=64 (reply in 178)
178	1603.7957666…	8.8.8.8	10.0.2.15	ICMP	60	Echo (ping) reply id=0x9202, seq=1024/4, ttl=255 (request in 177)
179	1604.7578284…	10.0.2.15	8.8.8.8	ICMP	42	Echo (ping) request id=0x9202, seq=1280/5, ttl=64 (reply in 180)
180	1604.7731515…	8.8.8.8	10.0.2.15	ICMP	60	Echo (ping) reply id=0x9202, seq=1280/5, ttl=255 (request in 179)
181	1604.9598444…	PCSSystemtec_d1:f8:…	52:55:0a:00:02:02	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
182	1604.9602447…	52:55:0a:00:02:02	PCSSystemtec_d1:f8:…	ARP	64	10.0.2.2 is at 52:55:0a:00:02:02
183	1605.7582624…	10.0.2.15	8.8.8.8	ICMP	42	Echo (ping) request id=0x9202, seq=1536/6, ttl=64 (reply in 184)
184	1605.7678910…	8.8.8.8	10.0.2.15	ICMP	60	Echo (ping) reply id=0x9202, seq=1536/6, ttl=255 (request in 183)
185	1606.7590869…	10.0.2.15	8.8.8.8	ICMP	42	Echo (ping) request id=0x9202, seq=1792/7, ttl=64 (reply in 186)
186	1606.7708199…	8.8.8.8	10.0.2.15	ICMP	60	Echo (ping) reply id=0x9202, seq=1792/7, ttl=255 (request in 185)

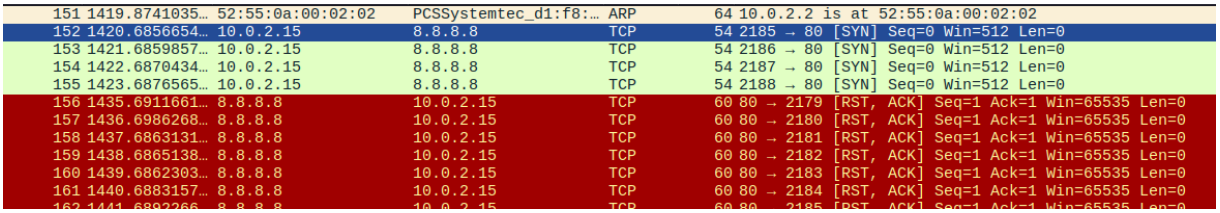
- TCP SYN a puerto 80 = Enviara 10 paquetes TCP con flag SYN al Puerto HTTP(80)



```
HPING 8.8.8.8 (eth0 8.8.8.8): S set, 40 headers + 0 data bytes

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

El servidor descarta la comunicación denegando comunicación



151	1419.8741035…	52:55:0a:00:02:02	PCSSystemtec_d1:f8:…	ARP	64	10.0.2.2 is at 52:55:0a:00:02:02
152	1420.6856654…	10.0.2.15	8.8.8.8	TCP	54	2185 → 80 [SYN] Seq=0 Win=512 Len=0
153	1421.6859857…	10.0.2.15	8.8.8.8	TCP	54	2186 → 80 [SYN] Seq=0 Win=512 Len=0
154	1422.6870434…	10.0.2.15	8.8.8.8	TCP	54	2187 → 80 [SYN] Seq=0 Win=512 Len=0
155	1423.6876565…	10.0.2.15	8.8.8.8	TCP	54	2188 → 80 [SYN] Seq=0 Win=512 Len=0
156	1435.6911661…	8.8.8.8	10.0.2.15	TCP	60	80 → 2179 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
157	1436.6986268…	8.8.8.8	10.0.2.15	TCP	60	80 → 2180 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
158	1437.6863131…	8.8.8.8	10.0.2.15	TCP	60	80 → 2181 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
159	1438.6865138…	8.8.8.8	10.0.2.15	TCP	60	80 → 2182 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
160	1439.6862303…	8.8.8.8	10.0.2.15	TCP	60	80 → 2183 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
161	1440.6883157…	8.8.8.8	10.0.2.15	TCP	60	80 → 2184 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0

- UDP a puerto 53 = Enviara 10 paquetes UDP al puerto 53

```
┌──(root㉿kali)-[~]
└─# sudo hping3 -c 10 -U -p 53 8.8.8.8
HPING 8.8.8.8 (eth0 8.8.8.8): U set, 40 headers + 0 data bytes
len=46 ip=8.8.8.8 ttl=255 id=36813 sport=53 flags=RA seq=0 win=0 rtt=7.5 ms
len=46 ip=8.8.8.8 ttl=255 id=36815 sport=53 flags=RA seq=1 win=0 rtt=7.8 ms
len=46 ip=8.8.8.8 ttl=255 id=36816 sport=53 flags=RA seq=2 win=0 rtt=3.0 ms
len=46 ip=8.8.8.8 ttl=255 id=36817 sport=53 flags=RA seq=3 win=0 rtt=6.9 ms
len=46 ip=8.8.8.8 ttl=255 id=36818 sport=53 flags=RA seq=4 win=0 rtt=2.9 ms
len=46 ip=8.8.8.8 ttl=255 id=36819 sport=53 flags=RA seq=5 win=0 rtt=2.0 ms
len=46 ip=8.8.8.8 ttl=255 id=36820 sport=53 flags=RA seq=6 win=0 rtt=4.9 ms
len=46 ip=8.8.8.8 ttl=255 id=36821 sport=53 flags=RA seq=7 win=0 rtt=0.8 ms
len=46 ip=8.8.8.8 ttl=255 id=36822 sport=53 flags=RA seq=8 win=0 rtt=4.6 ms
len=46 ip=8.8.8.8 ttl=255 id=36823 sport=53 flags=RA seq=9 win=0 rtt=8.2 ms

── 8.8.8.8 hping statistic ──
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 0.8/4.9/8.2 ms
```

El servidor no está aceptando conexión envía paquetes RST resetear conexión

No.	Time	Source	Destination	Protocol	Length	Info
125	769.434866908	8.8.8.8	10.0.2.15	TCP	60	53 → 2361 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
126	770.435106112	10.0.2.15	8.8.8.8	TCP	54	2362 → 53 [URG] Seq=1 Win=512 Urg=0 Len=0
127	770.435335258	8.8.8.8	10.0.2.15	TCP	60	53 → 2362 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
128	770.655988434	PCSSystemtec_d1:f8:…	52:55:0a:00:02:02	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
129	770.656368567	52:55:0a:00:02:02	PCSSystemtec_d1:f8:…	ARP	64	10.0.2.2 is at 52:55:0a:00:02:02
130	771.435890750	10.0.2.15	8.8.8.8	TCP	54	2363 → 53 [URG] Seq=1 Win=512 Urg=0 Len=0
131	771.436889513	8.8.8.8	10.0.2.15	TCP	60	53 → 2363 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
132	772.436053761	10.0.2.15	8.8.8.8	TCP	54	2364 → 53 [URG] Seq=1 Win=512 Urg=0 Len=0
133	772.436293211	8.8.8.8	10.0.2.15	TCP	60	53 → 2364 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
134	773.436469196	10.0.2.15	8.8.8.8	TCP	54	2365 → 53 [URG] Seq=1 Win=512 Urg=0 Len=0
135	773.436654997	8.8.8.8	10.0.2.15	TCP	60	53 → 2365 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

- TCP con datos personalizados adjunta los datos de tu archivo de texto al paquete TCP y los envía al puerto HTTP

```
└─# hping3 -c 10 -S -p 80 -E info.txt -d 25 8.8.8.8
HPING 8.8.8.8 (eth0 8.8.8.8): S set, 40 headers + 25 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!

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

El servidor rechazo la conexión por el puerto 80

101	493.407871479	52:55:0a:00:02:02	PCSSystemtec_d1:f8:…	ARP	64	10.0.2.2 is at 52:55:0a:00:02:02
102	494.283391163	10.0.2.15	8.8.8.8	TCP	79	1378 → 80 [SYN] Seq=0 Win=512 Len=25[Malformed Packet]
103	495.283817222	10.0.2.15	8.8.8.8	TCP	79	1379 → 80 [SYN] Seq=0 Win=512 Len=25[Malformed Packet]
104	496.284552989	10.0.2.15	8.8.8.8	TCP	79	1380 → 80 [SYN] Seq=0 Win=512 Len=25[Malformed Packet]
105	497.285810258	10.0.2.15	8.8.8.8	TCP	79	1381 → 80 [SYN] Seq=0 Win=512 Len=25[Malformed Packet]
106	509.293071542	8.8.8.8	10.0.2.15	TCP	60	80 → 1372 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
107	510.279773324	8.8.8.8	10.0.2.15	TCP	60	80 → 1373 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
108	511.279725362	8.8.8.8	10.0.2.15	TCP	60	80 → 1374 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
109	512.282841411	8.8.8.8	10.0.2.15	TCP	60	80 → 1375 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
110	513.281995829	8.8.8.8	10.0.2.15	TCP	60	80 → 1376 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
111	514.283537647	8.8.8.8	10.0.2.15	TCP	60	80 → 1377 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0

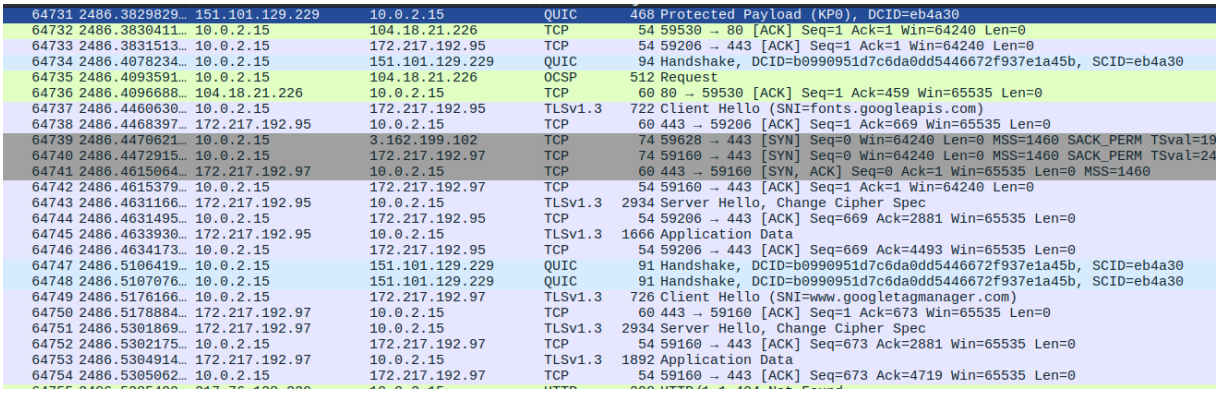
- **c)** Documentar los comandos utilizados y explicar las diferencias en las respuestas Respuestas en cada punto
- **d)** Capturar el tráfico generado con Wireshark durante las pruebas

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:

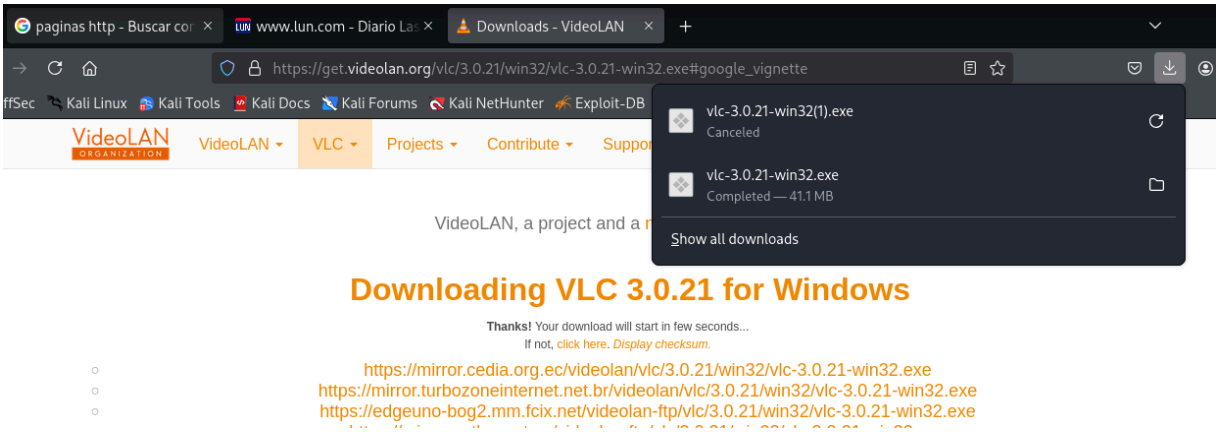
- **a)** Acceder a al menos 5 sitios web diferentes (incluir HTTP y HTTPS)

Se ingresa a páginas de HTTP y HTTPS

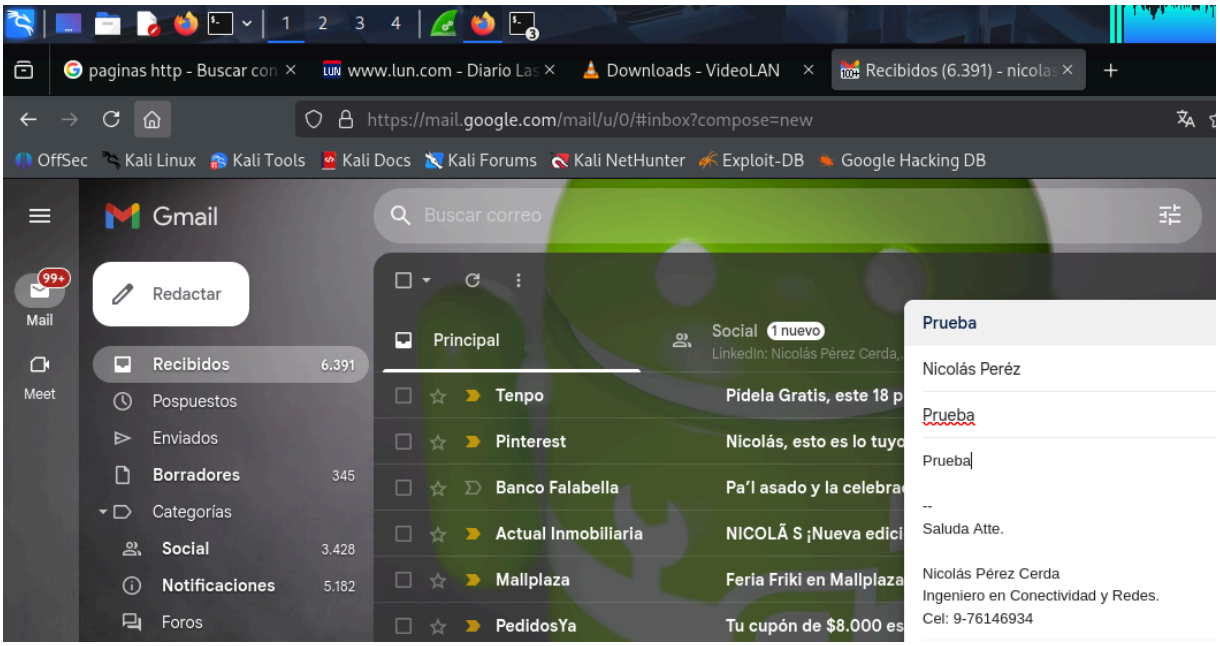


64731	2486.3829829…	151.101.129.229	10.0.2.15	QUIC	468 Protected Payload (KP0), DCID=eb4a30
64732	2486.3830411…	10.0.2.15	104.18.21.226	TCP	54 59530 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
64733	2486.3831513…	10.0.2.15	172.217.192.95	TCP	54 59206 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
64734	2486.4078234…	10.0.2.15	151.101.129.229	QUIC	94 Handshake, DCID=b0990951d7c6da0dd5446672f937e1a45b, SCID=eb4a30
64735	2486.4093591…	10.0.2.15	104.18.21.226	OCSP	512 Request
64736	2486.4096688…	104.18.21.226	10.0.2.15	TCP	60 80 → 59530 [ACK] Seq=1 Ack=459 Win=65535 Len=0
64737	2486.4460630…	10.0.2.15	172.217.192.95	TLSv1.3	722 Client Hello (SNI=fonts.googleapis.com)
64738	2486.4468397…	172.217.192.95	10.0.2.15	TCP	60 443 → 59206 [ACK] Seq=1 Ack=669 Win=65535 Len=0
64739	2486.4470621…	10.0.2.15	3.162.199.102	TCP	74 59628 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=19
64740	2486.4472915…	10.0.2.15	172.217.192.97	TCP	74 59160 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=24
64741	2486.4615064…	172.217.192.97	10.0.2.15	TCP	60 443 → 59160 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
64742	2486.4615379…	10.0.2.15	172.217.192.97	TCP	54 59160 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
64743	2486.4631166…	172.217.192.95	10.0.2.15	TLSv1.3	2934 Server Hello, Change Cipher Spec
64744	2486.4631495…	10.0.2.15	172.217.192.95	TCP	54 59206 → 443 [ACK] Seq=669 Ack=2881 Win=65535 Len=0
64745	2486.4633930…	172.217.192.95	10.0.2.15	TLSv1.3	1666 Application Data
64746	2486.4634173…	10.0.2.15	172.217.192.95	TCP	54 59206 → 443 [ACK] Seq=669 Ack=4493 Win=65535 Len=0
64747	2486.5106419…	10.0.2.15	151.101.129.229	QUIC	91 Handshake, DCID=b0990951d7c6da0dd5446672f937e1a45b, SCID=eb4a30
64748	2486.5107076…	10.0.2.15	151.101.129.229	QUIC	91 Handshake, DCID=b0990951d7c6da0dd5446672f937e1a45b, SCID=eb4a30
64749	2486.5176166…	10.0.2.15	172.217.192.97	TLSv1.3	726 Client Hello (SNI=www.googletagmanager.com)
64750	2486.5178884…	172.217.192.97	10.0.2.15	TCP	60 443 → 59160 [ACK] Seq=1 Ack=673 Win=65535 Len=0
64751	2486.5301869…	172.217.192.97	10.0.2.15	TLSv1.3	2934 Server Hello, Change Cipher Spec
64752	2486.5302175…	10.0.2.15	172.217.192.97	TCP	54 59160 → 443 [ACK] Seq=673 Ack=2881 Win=65535 Len=0
64753	2486.5304914…	172.217.192.97	10.0.2.15	TLSv1.3	1892 Application Data
64754	2486.5305062…	10.0.2.15	172.217.192.97	TCP	54 59160 → 443 [ACK] Seq=673 Ack=4719 Win=65535 Len=0

- **b)** Realizar una descarga de archivo pequeño



- **c)** Enviar un correo electrónico o usar una aplicación de mensajería



- **d)** Aplicar los siguientes filtros en Wireshark y documentar los resultados:
  - http - Tráfico HTTP

http

No.	Time	Source	Destination	Protocol	Length	Info
1054…	2939.0927593…	10.0.2.15	108.177.123.94	OCSP	481	Request
1055…	2939.2876523…	10.0.2.15	108.177.123.94	OCSP	481	Request
1055…	2939.2887740…	10.0.2.15	108.177.123.94	OCSP	481	Request
1055…	2939.2977997…	10.0.2.15	108.177.123.94	OCSP	481	Request
1055…	2939.3004789…	108.177.123.94	10.0.2.15	OCSP	1156	Response
1055…	2939.3091259…	10.0.2.15	108.177.123.94	OCSP	481	Request
1055…	2939.5005525…	108.177.123.94	10.0.2.15	OCSP	1156	Response
1055…	2939.5010143…	108.177.123.94	10.0.2.15	OCSP	1156	Response
1055…	2939.5010146…	108.177.123.94	10.0.2.15	OCSP	1156	Response
1055…	2939.5011733…	108.177.123.94	10.0.2.15	OCSP	1156	Response
1072…	2942.0102251…	10.0.2.15	108.177.123.94	OCSP	482	Request
1072…	2942.0187948…	10.0.2.15	108.177.123.94	OCSP	482	Request
1072…	2942.0196501…	10.0.2.15	108.177.123.94	OCSP	481	Request
1073…	2942.1288867…	10.0.2.15	108.177.123.94	OCSP	481	Request
1074…	2942.4860238…	108.177.123.94	10.0.2.15	OCSP	1157	Response
1074…	2942.4875493…	108.177.123.94	10.0.2.15	OCSP	1157	Response
1074…	2942.5029118…	108.177.123.94	10.0.2.15	OCSP	1156	Response
1076…	2942.6350013…	108.177.123.94	10.0.2.15	OCSP	1156	Response
1090…	2991.5975001…	10.0.2.15	108.177.123.94	OCSP	482	Request
1090…	2991.7766865…	108.177.123.94	10.0.2.15	OCSP	1157	Response
1091…	2992.3365635…	10.0.2.15	108.177.123.94	OCSP	482	Request
1091…	2992.4920436…	108.177.123.94	10.0.2.15	OCSP	1157	Response
1105…	3003.6767393…	10.0.2.15	108.177.123.94	OCSP	482	Request
1105…	3003.8504819…	108.177.123.94	10.0.2.15	OCSP	1157	Response

  - dns - Consultas DNS

dns

No.	Time	Source	Destination	Protocol	Length	Info
1221…	3203.6693600…	10.0.2.15	10.0.2.3	DNS	77	Standard query 0x751d A fonts.gstatic.com
1221…	3203.6694000…	10.0.2.15	10.0.2.3	DNS	77	Standard query 0x271b AAAA fonts.gstatic.com
1221…	3203.7640814…	10.0.2.3	10.0.2.15	DNS	93	Standard query response 0x751d A fonts.gstatic.com A 64.233.190.94
1221…	3203.7640820…	10.0.2.3	10.0.2.15	DNS	105	Standard query response 0x271b AAAA fonts.gstatic.com AAAA 2800:3f0:4…
1225…	3205.6523047…	10.0.2.15	10.0.2.3	DNS	80	Standard query 0x4a19 A accounts.youtube.com
1225…	3205.6939643…	10.0.2.3	10.0.2.15	DNS	204	Standard query response 0x4a19 A accounts.youtube.com CNAME www3.l.go…
1225…	3205.6941734…	10.0.2.15	10.0.2.3	DNS	80	Standard query 0xff1d AAAA accounts.youtube.com
1225…	3205.7062620…	10.0.2.3	10.0.2.15	DNS	220	Standard query response 0xff1d AAAA accounts.youtube.com CNAME www3.l…
1225…	3205.8796357…	10.0.2.15	10.0.2.3	DNS	75	Standard query 0x33a9 A www.gstatic.com
1225…	3205.8809664…	10.0.2.15	10.0.2.3	DNS	77	Standard query 0xbb02 A fonts.gstatic.com
1225…	3205.9592157…	10.0.2.3	10.0.2.15	DNS	93	Standard query response 0xbb02 A fonts.gstatic.com A 64.233.190.94
1225…	3205.9592161…	10.0.2.3	10.0.2.15	DNS	91	Standard query response 0x33a9 A www.gstatic.com A 172.217.192.94
1226…	3205.9594641…	10.0.2.15	10.0.2.3	DNS	75	Standard query 0x3aaa AAAA www.gstatic.com
1226…	3205.9594921…	10.0.2.15	10.0.2.3	DNS	77	Standard query 0x8000 AAAA fonts.gstatic.com
1226…	3205.9774367…	10.0.2.3	10.0.2.15	DNS	103	Standard query response 0x3aaa AAAA www.gstatic.com AAAA 2800:3f0:400…
1226…	3206.0052045…	10.0.2.3	10.0.2.15	DNS	105	Standard query response 0x8000 AAAA fonts.gstatic.com AAAA 2800:3f0:4…
1227…	3207.7964411…	10.0.2.15	10.0.2.3	DNS	85	Standard query 0x363a A push.services.mozilla.com
1227…	3207.7964833…	10.0.2.15	10.0.2.3	DNS	85	Standard query 0x033d AAAA push.services.mozilla.com
1227…	3207.8327398…	10.0.2.3	10.0.2.15	DNS	101	Standard query response 0x363a A push.services.mozilla.com A 34.107.2…
1227…	3207.8328989…	10.0.2.3	10.0.2.15	DNS	166	Standard query response 0x033d AAAA push.services.mozilla.com SOA ns-…
1228…	3231.1251533…	10.0.2.15	10.0.2.3	DNS	75	Standard query 0x5cda A ssl.gstatic.com
1228…	3231.1632358…	10.0.2.3	10.0.2.15	DNS	91	Standard query response 0x5cda A ssl.gstatic.com A 108.177.123.94
1228…	3231.1659485…	10.0.2.15	10.0.2.3	DNS	75	Standard query 0x4adf AAAA ssl.gstatic.com
1228…	3231.1848849…	10.0.2.3	10.0.2.15	DNS	103	Standard query response 0x4adf AAAA ssl.gstatic.com AAAA 2800:3f0:400…

- tcp.port == 443 - Tráfico HTTPS

tcp.port == 443

No.	Time	Source	Destination	Protocol	Length	Info
1229…	3264.2833183…	64.233.190.94	10.0.2.15	TLSv1.3	93	Application Data
1229…	3264.2863581…	64.233.186.138	10.0.2.15	TLSv1.3	93	Application Data
1229…	3264.3237336…	10.0.2.15	172.217.192.94	TCP	54	46378 → 443 [ACK] Seq=890 Ack=4818 Win=59423 Len=0
1229…	3264.3277143…	10.0.2.15	64.233.186.138	TCP	54	60144 → 443 [ACK] Seq=1366 Ack=20372 Win=43869 Len=0
1229…	3264.3277622…	10.0.2.15	64.233.190.94	TCP	54	60792 → 443 [ACK] Seq=892 Ack=4817 Win=59424 Len=0
1229…	3266.2605734…	10.0.2.15	34.107.243.93	TLSv1.3	93	Application Data
1229…	3266.2616816…	34.107.243.93	10.0.2.15	TCP	60	443 → 49998 [ACK] Seq=3730 Ack=900 Win=65535 Len=0
1229…	3266.2747754…	34.107.243.93	10.0.2.15	TLSv1.3	93	Application Data
1229…	3266.3158650…	10.0.2.15	34.107.243.93	TCP	54	49998 → 443 [ACK] Seq=900 Ack=3769 Win=64008 Len=0
1229…	3282.2190551…	10.0.2.15	64.233.186.95	TCP	74	54028 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2239…
1229…	3282.3004024…	64.233.186.95	10.0.2.15	TCP	60	443 → 54028 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
1229…	3282.3004618…	10.0.2.15	64.233.186.95	TCP	54	54028 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1230…	3282.3043131…	10.0.2.15	64.233.186.95	TLSv1.3	1303	Client Hello (SNI=signaler-pa.clients6.google.com)
1230…	3282.3046483…	64.233.186.95	10.0.2.15	TCP	60	443 → 54028 [ACK] Seq=1 Ack=1250 Win=65535 Len=0
1230…	3282.3049259…	10.0.2.15	64.233.186.95	TLSv1.3	60	Change Cipher Spec
1230…	3282.3050039…	10.0.2.15	64.233.186.95	TLSv1.3	146	Application Data
1230…	3282.3052311…	64.233.186.95	10.0.2.15	TCP	60	443 → 54028 [ACK] Seq=1 Ack=1256 Win=65535 Len=0
1230…	3282.3052313…	64.233.186.95	10.0.2.15	TCP	60	443 → 54028 [ACK] Seq=1 Ack=1348 Win=65535 Len=0
1230…	3282.3197959…	64.233.186.95	10.0.2.15	TLSv1.3	915	Server Hello, Change Cipher Spec, Application Data, Application Data,…
1230…	3282.3198412…	10.0.2.15	64.233.186.95	TCP	54	54028 → 443 [ACK] Seq=1348 Ack=862 Win=63379 Len=0
1230…	3282.3217488…	10.0.2.15	64.233.186.95	TLSv1.3	138	Application Data, Application Data
1230…	3282.3220946…	64.233.186.95	10.0.2.15	TCP	60	443 → 54028 [ACK] Seq=862 Ack=1432 Win=65535 Len=0
1230…	3282.3237351…	10.0.2.15	64.233.186.95	TLSv1.3	85	Application Data
1230…	3282.3240344…	64.233.186.95	10.0.2.15	TCP	60	443 → 54028 [ACK] Seq=862 Ack=1463 Win=65535 Len=0

- icmp - Tráfico ICMP

icmp

No.	Time	Source	Destination	Protocol	Length	Info
178	1603.7957666…	8.8.8.8	10.0.2.15	ICMP	60	Echo (ping) reply id=0x9202, seq=1024/4, ttl=255 (request in 177)
179	1604.7578284…	10.0.2.15	8.8.8.8	ICMP	42	Echo (ping) request id=0x9202, seq=1280/5, ttl=64 (reply in 180)
180	1604.7731515…	8.8.8.8	10.0.2.15	ICMP	60	Echo (ping) reply id=0x9202, seq=1280/5, ttl=255 (request in 179)
183	1605.7582624…	10.0.2.15	8.8.8.8	ICMP	42	Echo (ping) request id=0x9202, seq=1536/6, ttl=64 (reply in 184)
184	1605.7678910…	8.8.8.8	10.0.2.15	ICMP	60	Echo (ping) reply id=0x9202, seq=1536/6, ttl=255 (request in 183)
185	1606.7590869…	10.0.2.15	8.8.8.8	ICMP	42	Echo (ping) request id=0x9202, seq=1792/7, ttl=64 (reply in 186)
186	1606.7708199…	8.8.8.8	10.0.2.15	ICMP	60	Echo (ping) reply id=0x9202, seq=1792/7, ttl=255 (request in 185)
187	1607.7597664…	10.0.2.15	8.8.8.8	ICMP	42	Echo (ping) request id=0x9202, seq=2048/8, ttl=64 (reply in 188)
188	1607.8223959…	8.8.8.8	10.0.2.15	ICMP	60	Echo (ping) reply id=0x9202, seq=2048/8, ttl=255 (request in 187)
→ 189	1608.7599104…	10.0.2.15	8.8.8.8	ICMP	42	Echo (ping) request id=0x9202, seq=2304/9, ttl=64 (reply in 190)
← 190	1608.7705446…	8.8.8.8	10.0.2.15	ICMP	60	Echo (ping) reply id=0x9202, seq=2304/9, ttl=255 (request in 189)
74585	2750.4948656…	10.0.2.15	104.16.118.43	ICMP	561	Destination unreachable (Port unreachable)
74587	2750.4951313…	10.0.2.15	104.16.118.43	ICMP	105	Destination unreachable (Port unreachable)
74636	2751.2285734…	10.0.2.15	104.16.118.43	ICMP	561	Destination unreachable (Port unreachable)
74639	2751.2289433…	10.0.2.15	104.16.118.43	ICMP	105	Destination unreachable (Port unreachable)
74776	2752.6756856…	10.0.2.15	104.16.118.43	ICMP	561	Destination unreachable (Port unreachable)
74777	2752.6757203…	10.0.2.15	104.16.118.43	ICMP	105	Destination unreachable (Port unreachable)
74828	2755.5820262…	10.0.2.15	104.16.118.43	ICMP	561	Destination unreachable (Port unreachable)
74830	2755.5822030…	10.0.2.15	104.16.118.43	ICMP	105	Destination unreachable (Port unreachable)
74859	2761.4060012…	10.0.2.15	104.16.118.43	ICMP	561	Destination unreachable (Port unreachable)
74861	2761.4061910…	10.0.2.15	104.16.118.43	ICMP	105	Destination unreachable (Port unreachable)
74901	2773.0815754…	10.0.2.15	104.16.118.43	ICMP	561	Destination unreachable (Port unreachable)
74903	2773.0817612…	10.0.2.15	104.16.118.43	ICMP	105	Destination unreachable (Port unreachable)
1150…	3048.1518253…	10.0.2.15	108.177.123.138	ICMP	112	Destination unreachable (Port unreachable)

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

ip.addr == 10.0.2.15

No.	Time	Source	Destination	Protocol	Length	Info
1233…	3388.7041298…	10.0.2.15	108.177.123.100	QUIC	1399	Protected Payload (KP0), DCID=f1c88ab676cff34c
1233…	3388.7045120…	10.0.2.15	108.177.123.100	QUIC	1399	Protected Payload (KP0), DCID=f1c88ab676cff34c
1233…	3388.7090271…	10.0.2.15	108.177.123.100	QUIC	588	Protected Payload (KP0), DCID=f1c88ab676cff34c
1233…	3388.7539738…	10.0.2.15	108.177.123.100	QUIC	1399	Protected Payload (KP0), DCID=f1c88ab676cff34c
1233…	3388.7540655…	10.0.2.15	108.177.123.100	QUIC	1399	Protected Payload (KP0), DCID=f1c88ab676cff34c
1233…	3388.7559034…	10.0.2.15	108.177.123.100	QUIC	1399	Protected Payload (KP0), DCID=f1c88ab676cff34c
1233…	3388.7577757…	10.0.2.15	108.177.123.100	QUIC	1399	Protected Payload (KP0), DCID=f1c88ab676cff34c
1233…	3388.7578480…	10.0.2.15	108.177.123.100	QUIC	612	Protected Payload (KP0), DCID=f1c88ab676cff34c
1233…	3388.7858907…	108.177.123.100	10.0.2.15	QUIC	171	Protected Payload (KP0), DCID=607f85
1233…	3388.7861236…	108.177.123.100	10.0.2.15	QUIC	68	Protected Payload (KP0), DCID=607f85
1233…	3388.7861238…	108.177.123.100	10.0.2.15	QUIC	898	Protected Payload (KP0), DCID=607f85
1233…	3388.7861239…	108.177.123.100	10.0.2.15	QUIC	127	Protected Payload (KP0), DCID=607f85
1233…	3388.7879267…	10.0.2.15	108.177.123.100	QUIC	81	Protected Payload (KP0), DCID=f1c88ab676cff34c
1233…	3388.7911923…	108.177.123.100	10.0.2.15	QUIC	68	Protected Payload (KP0), DCID=607f85
1233…	3388.7911929…	108.177.123.100	10.0.2.15	QUIC	68	Protected Payload (KP0), DCID=607f85
1233…	3388.7914888…	108.177.123.100	10.0.2.15	QUIC	165	Protected Payload (KP0), DCID=607f85
1233…	3388.7921592…	108.177.123.100	10.0.2.15	QUIC	68	Protected Payload (KP0), DCID=607f85
1233…	3388.7939264…	10.0.2.15	108.177.123.100	QUIC	75	Protected Payload (KP0), DCID=f1c88ab676cff34c
1233…	3399.6851870…	10.0.2.15	64.233.186.95	TLSv1.3	93	Application Data
1233…	3399.6858863…	64.233.186.95	10.0.2.15	TCP	60	443 → 54028 [ACK] Seq=901 Ack=1541 Win=65535 Len=0
1233…	3399.6941543…	64.233.186.95	10.0.2.15	TLSv1.3	93	Application Data
1233…	3399.6942104…	10.0.2.15	64.233.186.95	TCP	54	54028 → 443 [ACK] Seq=1541 Ack=940 Win=63301 Len=0
1233…	3405.1164662…	64.233.186.95	10.0.2.15	QUIC	123	Protected Payload (KP0), DCID=6f27a3
1233…	3405.1183665…	10.0.2.15	64.233.186.95	QUIC	76	Protected Payload (KP0), DCID=f18cc134e46ab297

- **e)** Identificar y explicar:
  - Protocolos más utilizados
    Quic: Protocolo Google para encapsular HTTPS
    Tlsv1.3 versión más resiente de HTTPS
    DNS
  - Direcciones IP de destino más frecuentes
    10.0.2.15
    8.8.8.8
  - Puertos más utilizados
    443
    53
  - Posibles vulnerabilidades observadas (tráfico no cifrado, etc.)
    HTTP vulnerabilidad de confiabilidad por que los datos no están cifrados

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:
  - Puerto 22 (SSH)

```
┌──(root㉿kali)-[~]
└─# hping3 -S -p 22 -c 10 8.8.8.8
HPING 8.8.8.8 (eth0 8.8.8.8): S set, 40 headers + 0 data bytes

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

1238…	3692.3739637…	108.177.123.101	10.0.2.15	TCP	60	443 → 53276 [ACK] Seq=6620 Ack=820 Win=65535 Len=0
1238…	3692.3802350…	108.177.123.101	10.0.2.15	QUIC	69	Protected Payload (KP0), DCID=e8d60c
1238…	3692.3929195…	108.177.123.101	10.0.2.15	TLSv1.3	699	Application Data, Application Data, Application Data
1238…	3692.3929741…	10.0.2.15	108.177.123.101	TCP	54	53276 → 443 [ACK] Seq=820 Ack=7265 Win=65535 Len=0
1238…	3692.3944085…	10.0.2.15	108.177.123.101	TLSv1.3	85	Application Data
1238…	3692.3947926…	108.177.123.101	10.0.2.15	TCP	60	443 → 53276 [ACK] Seq=7265 Ack=851 Win=65535 Len=0
1238…	3692.6279344…	10.0.2.15	8.8.8.8	TCP	54	2320 → 22 [SYN] Seq=0 Win=512 Len=0
1238…	3704.6220069…	8.8.8.8	10.0.2.15	TCP	60	22 → 2311 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
1238…	3705.6260107…	8.8.8.8	10.0.2.15	TCP	60	22 → 2312 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
1238…	3706.6239287…	8.8.8.8	10.0.2.15	TCP	60	22 → 2313 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
1238…	3707.6251298…	8.8.8.8	10.0.2.15	TCP	60	22 → 2314 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
1238…	3708.6233803…	8.8.8.8	10.0.2.15	TCP	60	22 → 2315 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
1238…	3709.6292971…	8.8.8.8	10.0.2.15	TCP	60	22 → 2316 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0

  - Puerto 80 (HTTP)

```
└─# hping3 -S -p 80 -c 10 8.8.8.8
HPING 8.8.8.8 (eth0 8.8.8.8): S set, 40 headers + 0 data bytes

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

```
1240… 3772.2765475… 64.233.186.95      10.0.2.15          QUIC      73 Protected Payload (KP0), DCID=6f27a3
1240… 3772.2769592… 10.0.2.15          64.233.186.95      QUIC      74 Protected Payload (KP0), DCID=f18cc134e46ab297
1240… 3772.3571482… 64.233.186.95      10.0.2.15          QUIC     130 Protected Payload (KP0), DCID=6f27a3
1240… 3772.3595981… 10.0.2.15          64.233.186.95      QUIC      80 Protected Payload (KP0), DCID=f18cc134e46ab297
1240… 3772.4148788… 64.233.186.95      10.0.2.15          QUIC      69 Protected Payload (KP0), DCID=6f27a3
1240… 3776.8636883… PCSSystemtec_d1:f8:… 52:55:0a:00:02:02 ARP       42 Who has 10.0.2.2? Tell 10.0.2.15
1240… 3776.8639138… 52:55:0a:00:02:02  PCSSystemtec_d1:f8:… ARP       64 10.0.2.2 is at 52:55:0a:00:02:02
1240… 3784.0067881… 8.8.8.8            10.0.2.15          TCP       60 80 → 2716 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
1240… 3785.0286877… 8.8.8.8            10.0.2.15          TCP       60 80 → 2717 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
1240… 3786.0205709… 8.8.8.8            10.0.2.15          TCP       60 80 → 2718 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
1240… 3787.0194685… 8.8.8.8            10.0.2.15          TCP       60 80 → 2719 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
1240… 3788.0283487… 8.8.8.8            10.0.2.15          TCP       60 80 → 2720 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
```

- Puerto 443 (HTTPS)

```
HPING 8.8.8.8 (eth0 8.8.8.8): S set, 40 headers + 0 data bytes
len=46 ip=8.8.8.8 ttl=64 id=36841 sport=443 flags=SA seq=0 win=65535 rtt=12.0
 ms
len=46 ip=8.8.8.8 ttl=64 id=36842 sport=443 flags=SA seq=1 win=65535 rtt=18.1
 ms
len=46 ip=8.8.8.8 ttl=64 id=36843 sport=443 flags=SA seq=2 win=65535 rtt=17.7
 ms
len=46 ip=8.8.8.8 ttl=64 id=36844 sport=443 flags=SA seq=3 win=65535 rtt=64.9
 ms
len=46 ip=8.8.8.8 ttl=64 id=36845 sport=443 flags=SA seq=4 win=65535 rtt=15.8
 ms
len=46 ip=8.8.8.8 ttl=64 id=36846 sport=443 flags=SA seq=5 win=65535 rtt=51.4
 ms
len=46 ip=8.8.8.8 ttl=64 id=36847 sport=443 flags=SA seq=6 win=65535 rtt=30.2
 ms
len=46 ip=8.8.8.8 ttl=64 id=36848 sport=443 flags=SA seq=7 win=65535 rtt=13.9
 ms
len=46 ip=8.8.8.8 ttl=64 id=36849 sport=443 flags=SA seq=8 win=65535 rtt=13.7
 ms
len=46 ip=8.8.8.8 ttl=64 id=36850 sport=443 flags=SA seq=9 win=65535 rtt=41.1
 ms

--- 8.8.8.8 hping statistic ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 12.0/27.9/64.9 ms
```

```
1241… 3838.8728818… 10.0.2.15          8.8.8.8            TCP       54 2618 → 443 [SYN] Seq=0 Win=512 Len=0
1241… 3838.8821281… 8.8.8.8            10.0.2.15          TCP       60 443 → 2618 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
1241… 3838.8821580… 10.0.2.15          8.8.8.8            TCP       54 2618 → 443 [RST] Seq=1 Win=0 Len=0
1241… 3839.8733516… 10.0.2.15          8.8.8.8            TCP       54 2619 → 443 [SYN] Seq=0 Win=512 Len=0
1241… 3839.8840654… 8.8.8.8            10.0.2.15          TCP       60 443 → 2619 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
1241… 3839.8841348… 10.0.2.15          8.8.8.8            TCP       54 2619 → 443 [RST] Seq=1 Win=0 Len=0
1241… 3840.8740087… 10.0.2.15          8.8.8.8            TCP       54 2620 → 443 [SYN] Seq=0 Win=512 Len=0
1241… 3840.8847432… 8.8.8.8            10.0.2.15          TCP       60 443 → 2620 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
1241… 3840.8848006… 10.0.2.15          8.8.8.8            TCP       54 2620 → 443 [RST] Seq=1 Win=0 Len=0
1241… 3841.8748915… 10.0.2.15          8.8.8.8            TCP       54 2621 → 443 [SYN] Seq=0 Win=512 Len=0
1241… 3841.9367770… 8.8.8.8            10.0.2.15          TCP       60 443 → 2621 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
1241… 3841.9368321… 10.0.2.15          8.8.8.8            TCP       54 2621 → 443 [RST] Seq=1 Win=0 Len=0
1241… 3842.8758410… 10.0.2.15          8.8.8.8            TCP       54 2622 → 443 [SYN] Seq=0 Win=512 Len=0
1241… 3842.8863657… 8.8.8.8            10.0.2.15          TCP       60 443 → 2622 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
1241… 3842.8864101… 10.0.2.15          8.8.8.8            TCP       54 2622 → 443 [RST] Seq=1 Win=0 Len=0
```

- Puerto 21 (FTP)

```
1243… 3933.1480244… 8.8.8.8            10.0.2.15          TCP       60 21 → 2033 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
1243… 3934.1463172… 8.8.8.8            10.0.2.15          TCP       60 21 → 2034 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
1243… 3935.1573023… 8.8.8.8            10.0.2.15          TCP       60 21 → 2035 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
1243… 3935.8515762… 64.233.186.95      10.0.2.15          QUIC     123 Protected Payload (KP0), DCID=6f27a3
1243… 3935.9527684… 10.0.2.15          64.233.186.95      QUIC      79 Protected Payload (KP0), DCID=f18cc134e46ab297
```

```
┌──(root㉿kali)-[~]
└─# hping3 -S -p 21 -c 10 8.8.8.8
HPING 8.8.8.8 (eth0 8.8.8.8): S set, 40 headers + 0 data bytes

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

- **b)** Documentar qué puertos están abiertos, cerrados o filtrados
  Puerto 22 Cerrado
  Puerto 80 Cerrado
  Puerto 443 abierto
  Puerto 21 Cerrado
- **c)** Analizar los tiempos de respuesta y patrones de conectividad
  Los valores de RTT muestran que la conexión a 8.8.8.8 tiene tiempo e latencia baja en la mayoría de los casos.

Recomendaciones

-Las recordaciones enfocando en Desafío Latam son:
-Implementar sistemas de detección de intrusos IDS o también IPS sistema de prevención de intrusos

-Políticas estricta en Firewall para restringir acceso a puertos innecesarios (como es el caso google)
-Enumeración con Hacking Ético para recopilar información sobre una red en relación a la seguridad.

Conclusiones

El análisis de tráfico de red generado por medio de Hping3 demostró las medidas de seguridad de Google, que bloquean de forma activa los intentos de conexión a puertos no esencial esto se vio por medio de Wireshark. Dejando solo los servicios esenciales para el buen funcionamiento de sus servicios.