

Trabajo Práctico 7 - Redes - Rando - 14004

Tomás Rando

Junio 2024

1 Introducción

Se realiza el informe correspondiente al trabajo práctico número 7 de la materia "Redes de computadoras" del año 2024. Se realizaron todas las actividades incluyendo la opcional

Índice

1	Introducción	1
2	Actividades.	2
2.1	Actividad 1.	2
2.2	Actividad 2.	3
2.3	Actividad 3.	4
2.4	Actividad 4.	5
2.4.1	ARP spoofing con Nping	5
2.4.2	DoS con hping3	5
2.4.3	DoS por inundación con hping3	6
2.4.4	Actividad opcional.	6
2.5	Actividad 5.	7

2 Actividades.

2.1 Actividad 1.

La actividad 1 fue respondida en el cuestionario correspondiente al TP N°7 en el aula abierta. Para ilustrar la realización de la actividad, se incluye una imagen correspondiente al certificado de la página del punto 1.

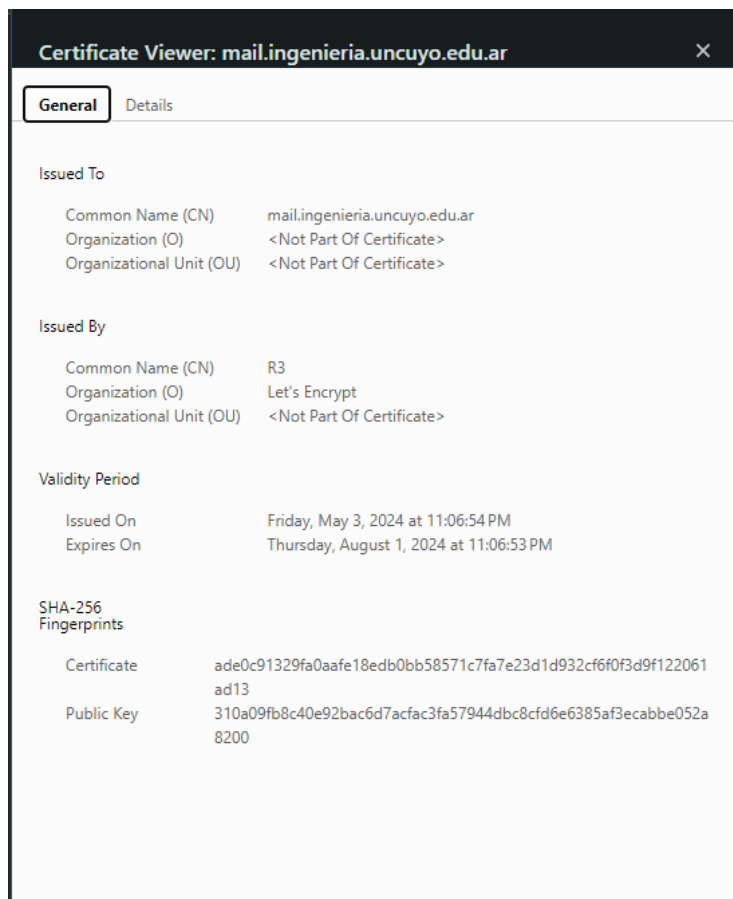


Figure 1: Certificado de la página

2.2 Actividad 2.

En la actividad 2 se clonó la página web del banco solicitado y se modificó el código para que cuando se inicie sesión se invoque un procedimiento escrito en PHP (contenido en el archivo verificar.php) que almacene el usuario y contraseña en un .txt con este formato: "usuario - contraseña".

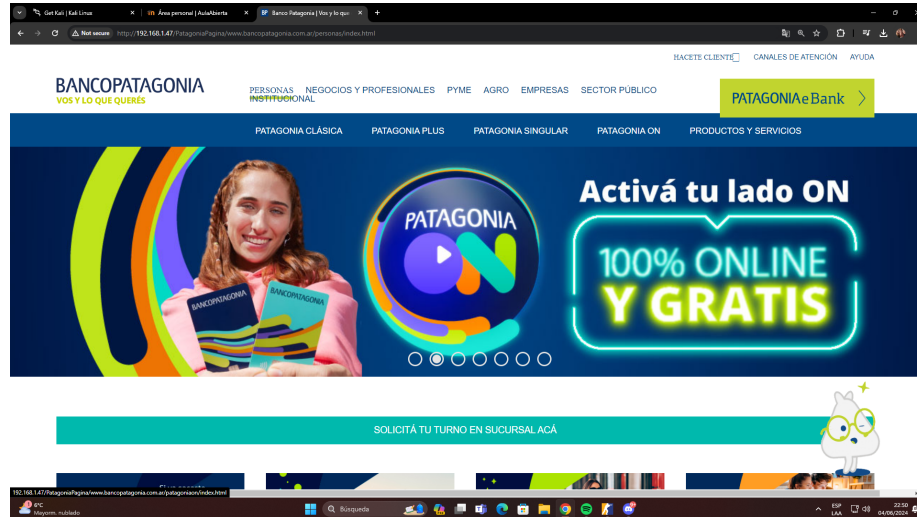


Figure 2: Inicio de la página del banco clonada

2.3 Actividad 3.

En wireshark se pudo observar como la información de los paquetes http si pueden ser vistos. Por ello, se generó el certificado con el procedimiento brindado. Luego, se volvió a analizar los paquetes y se confirmó que la información quedó encriptada, por lo que no pudo ser leída mediante wireshark.



Figure 3: Página web con HTTPS

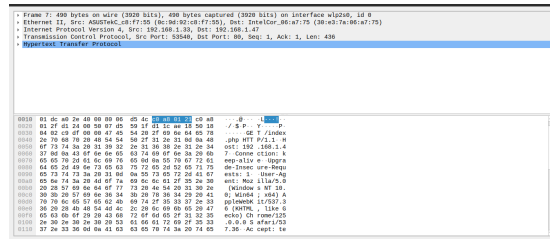


Figure 4: Paquetes antes del certificado

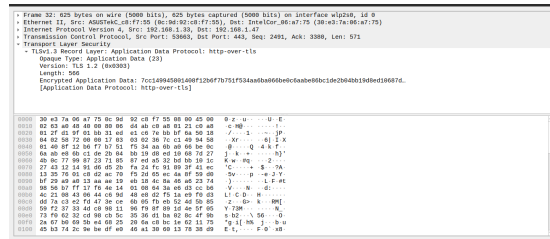


Figure 5: Paquetes luego del certificado

2.4 Actividad 4.

2.4.1 ARP spoofing con Nping

Se respondió la pregunta en el cuestionario asociada a esta actividad, pero se muestra una imagen de la realización de la actividad.

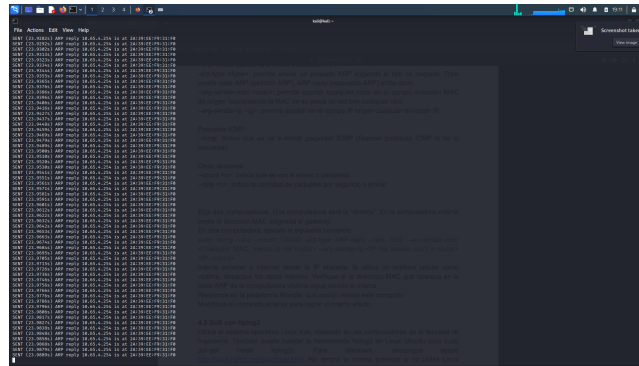


Figure 6: Consola con ARP spoofing

2.4.2 DoS con hping3

Se muestra una imagen correspondiente al wireshark con los paquetes enviados con el comando utilizado.

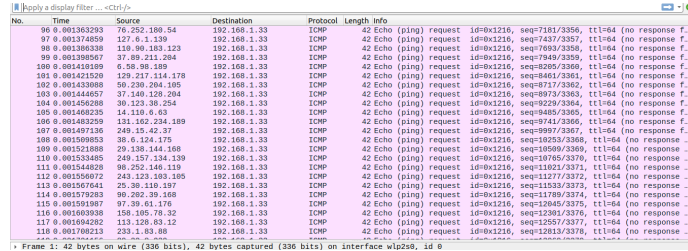
No.	Time	Source	Destination	Protocol	Length	Info
1006	1927.982988	192.168.1.33	192.168.1.35	ICMP	42	Echo (ping) request id=0xb13, seq=15628/3133, ttl=64 (no response ...)
1006	1927.9932383	192.168.1.33	192.168.1.35	ICMP	42	Echo (ping) request id=0xb13, seq=15884/3134, ttl=64 (no response ...)
1006	1928.0034732	192.168.1.33	192.168.1.35	ICMP	42	Echo (ping) request id=0xb13, seq=16140/3135, ttl=64 (no response ...)
1006	1928.0136565	192.168.1.33	192.168.1.35	ICMP	42	Echo (ping) request id=0xb13, seq=16396/3136, ttl=64 (no response ...)
1006	1928.0238707	192.168.1.33	192.168.1.35	ICMP	42	Echo (ping) request id=0xb13, seq=16652/3137, ttl=64 (no response ...)
1006	1928.0341425	192.168.1.33	192.168.1.35	ICMP	42	Echo (ping) request id=0xb13, seq=16908/3138, ttl=64 (no response ...)
1006	1928.0444827	192.168.1.33	192.168.1.35	ICMP	42	Echo (ping) request id=0xb13, seq=17164/3139, ttl=64 (no response ...)
1006	1928.0547325	192.168.1.33	192.168.1.35	ICMP	42	Echo (ping) request id=0xb13, seq=17420/3140, ttl=64 (no response ...)
1006	1928.0649894	192.168.1.33	192.168.1.35	ICMP	42	Echo (ping) request id=0xb13, seq=17676/3141, ttl=64 (no response ...)
1006	1928.0750713	192.168.1.33	192.168.1.35	ICMP	42	Echo (ping) request id=0xb13, seq=17932/3142, ttl=64 (no response ...)
1006	1928.0798434	192.168.1.100	239.255.255.250	SSDP	393	NOTIFY * HTTP/1.1
1006	1928.0803774	192.168.1.100	239.255.255.250	SSDP	393	NOTIFY * HTTP/1.1
1006	1928.0840306	192.168.1.100	239.255.255.250	SSDP	393	NOTIFY * HTTP/1.1
1006	1928.0891919	192.168.1.33	192.168.1.35	ICMP	42	Echo (ping) request id=0xb13, seq=18188/3143, ttl=64 (no response ...)
1006	1928.0953782	192.168.1.33	192.168.1.35	ICMP	42	Echo (ping) request id=0xb13, seq=18444/3144, ttl=64 (no response ...)
1006	1928.1055155	192.168.1.33	192.168.1.35	ICMP	42	Echo (ping) request id=0xb13, seq=18700/3145, ttl=64 (no response ...)
1006	1928.1156803	192.168.1.33	192.168.1.35	ICMP	42	Echo (ping) request id=0xb13, seq=18956/3146, ttl=64 (no response ...)
1006	1928.1258456	192.168.1.33	192.168.1.35	ICMP	42	Echo (ping) request id=0xb13, seq=19212/3147, ttl=64 (no response ...)
1006	1928.1360172	192.168.1.33	192.168.1.35	ICMP	42	Echo (ping) request id=0xb13, seq=19468/3148, ttl=64 (no response ...)
1006	1928.1461713	192.168.1.33	192.168.1.35	ICMP	42	Echo (ping) request id=0xb13, seq=19724/3149, ttl=64 (no response ...)
1006	1928.1563278	192.168.1.33	192.168.1.35	ICMP	42	Echo (ping) request id=0xb13, seq=19980/3150, ttl=64 (no response ...)
1006	1928.1664827	192.168.1.33	192.168.1.35	ICMP	42	Echo (ping) request id=0xb13, seq=20236/3151, ttl=64 (no response ...)
1006	1928.1766322	192.168.1.33	192.168.1.35	ICMP	42	Echo (ping) request id=0xb13, seq=20492/3152, ttl=64 (no response ...)

* Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp2s0, id 0
* Ethernet II, Src: IntelCor_86:a7:75 (30:e3:7a:86:a7:75), Dst: ASUSTekC_8c:7f:55 (8c:9d:92:c8:7f:55)
* Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.35

Figure 7: DoS con hping3

2.4.3 DoS por inundación con hping3

Se utilizó el comando con la PC de ip 192.168.1.33. El efecto que tuvo en ella fue la imposibilidad de utilizar el servicio de internet. Se muestra en la imagen el wireshark con una captura de los paquetes enviados a esa PC.

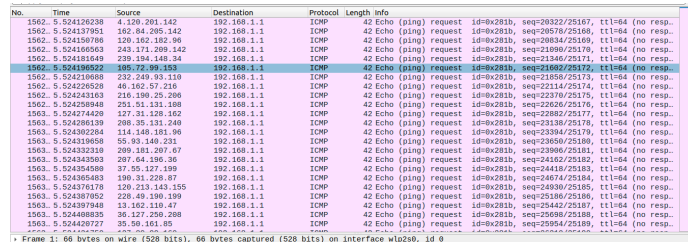


No.	Time	Source	Destination	Protocol	Length	Info
96	0.001363293	76.252.188.54	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=7181/3356, ttl=64 (no response f...
97	0.001374059	127.0.1.1	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=7437/3357, ttl=64 (no response f...
98	0.001386338	110.90.183.123	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=7693/3356, ttl=64 (no response f...
99	0.001398567	37.89.211.264	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=7949/3359, ttl=64 (no response f...
100	0.001410809	6.58.90.189	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=8205/3360, ttl=64 (no response f...
101	0.001421520	129.217.114.178	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=8461/3361, ttl=64 (no response f...
102	0.001433088	50.230.204.105	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=8717/3362, ttl=64 (no response f...
103	0.001444657	37.140.128.264	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=8973/3363, ttl=64 (no response f...
104	0.001456286	30.123.38.254	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=9229/3364, ttl=64 (no response f...
105	0.001468235	14.110.0.43	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=9485/3365, ttl=64 (no response f...
106	0.001483259	131.162.234.189	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=9741/3366, ttl=64 (no response f...
107	0.001497136	249.15.42.37	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=9997/3367, ttl=64 (no response f...
108	0.001509853	38.6.124.175	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=10253/3368, ttl=64 (no response f...
109	0.001521988	29.130.144.168	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=10509/3369, ttl=64 (no response f...
110	0.001533485	249.157.134.139	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=10765/3370, ttl=64 (no response f...
111	0.001545428	96.252.146.115	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=11021/3371, ttl=64 (no response f...
112	0.001556872	243.123.103.185	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=11277/3372, ttl=64 (no response f...
113	0.001567641	25.38.110.197	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=11533/3373, ttl=64 (no response f...
114	0.001579263	86.282.38.168	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=11789/3374, ttl=64 (no response f...
115	0.001591987	97.39.61.176	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=12045/3375, ttl=64 (no response f...
116	0.001603930	158.105.78.32	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=12301/3376, ttl=64 (no response f...
117	0.001616422	113.128.83.12	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=12557/3377, ttl=64 (no response f...
118	0.001628213	233.1.83.88	192.168.1.33	ICMP	42	Echo (ping) request id=0x1216, seq=12813/3378, ttl=64 (no response f...

Figure 8: DoS por inundación con hping3

2.4.4 Actividad opcional.

Se atacó la IP del router (En este caso, 192.168.1.1) desde 2 computadoras a la vez. El resultado obtenido fue que se imposibilitó usar el servicio de internet desde cualquier dispositivo conectado. Se adjunta una imagen de wireshark con los paquetes enviados.



No.	Time	Source	Destination	Protocol	Length	Info
1562	5.524126238	4.120.201.142	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=20322/25167, ttl=64 (no resp...
1562	5.524137951	162.84.208.142	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=20578/25168, ttl=64 (no resp...
1562	5.524138766	126.162.162.96	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=20834/25169, ttl=64 (no resp...
1562	5.524160563	243.171.209.142	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=21090/25170, ttl=64 (no resp...
1562	5.524151649	239.134.140.34	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=21346/25171, ttl=64 (no resp...
1562	5.524196522	185.72.99.153	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=21602/25172, ttl=64 (no resp...
1562	5.524218688	232.249.93.110	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=21858/25173, ttl=64 (no resp...
1562	5.524229520	46.162.57.210	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=22114/25174, ttl=64 (no resp...
1562	5.524243163	216.190.25.206	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=22370/25175, ttl=64 (no resp...
1562	5.524250848	251.51.131.188	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=22626/25176, ttl=64 (no resp...
1563	5.524274428	127.31.128.162	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=22882/25177, ttl=64 (no resp...
1562	5.524283120	208.35.531.240	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=23138/25178, ttl=64 (no resp...
1563	5.524382284	114.148.181.96	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=23394/25179, ttl=64 (no resp...
1563	5.524319958	55.83.148.231	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=23650/25180, ttl=64 (no resp...
1563	5.524323218	289.181.207.67	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=23906/25181, ttl=64 (no resp...
1563	5.524343593	297.64.196.36	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=24162/25182, ttl=64 (no resp...
1563	5.524354088	37.55.157.199	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=24418/25183, ttl=64 (no resp...
1563	5.524385483	190.31.228.87	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=24674/25184, ttl=64 (no resp...
1563	5.524376178	126.213.143.155	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=24930/25185, ttl=64 (no resp...
1563	5.524387052	228.49.190.199	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=25186/25186, ttl=64 (no resp...
1563	5.524387948	13.162.110.47	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=25442/25187, ttl=64 (no resp...
1563	5.524408830	36.127.206.260	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=25698/25188, ttl=64 (no resp...
1563	5.524428727	35.50.161.85	192.168.1.1	ICMP	42	Echo (ping) request id=0x281b, seq=25954/25189, ttl=64 (no resp...

Figure 9: DoS por inundación con hping3 al router

2.5 Actividad 5.

Se realizó la actividad con el gufw solicitado. Se pudo verificar que la primera vez que lo activamos no se pudo acceder a la página desde otra computadora.

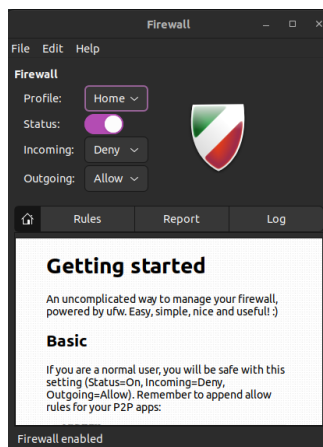


Figure 10: GUFW con la primera configuración solicitada

Despues de realizar la segunda configuración que se solicitó, es decir, luego de agregar la regla, se intentó nuevamente. En esta ocasión, pudimos comprobar que sí se pudo ingresar correctamente a la página web realizada desde otra computadora.

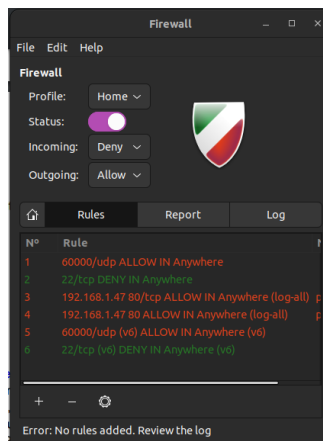


Figure 11: GUFW con la segunda configuración solicitada