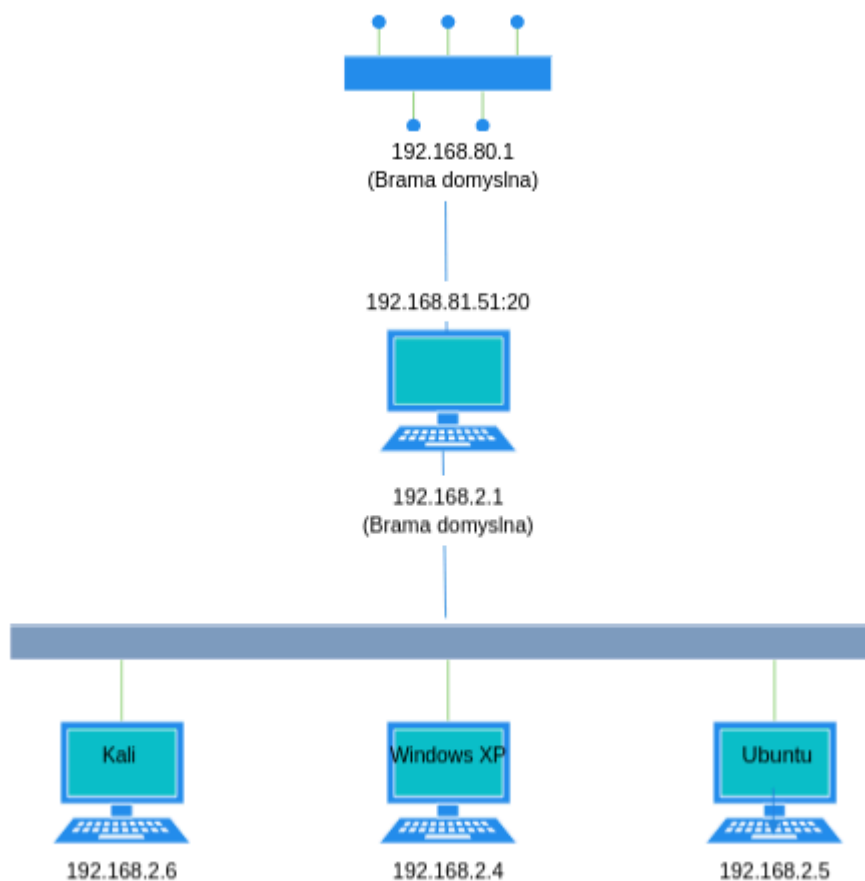


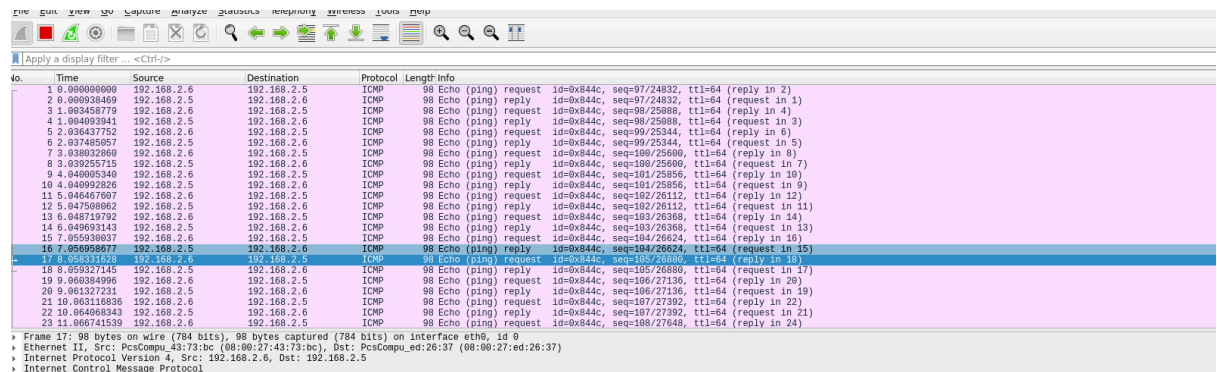
Testy Penetracyjne Lab 2

Julia Sadecka, Cyberbezpieczeństwo

1.

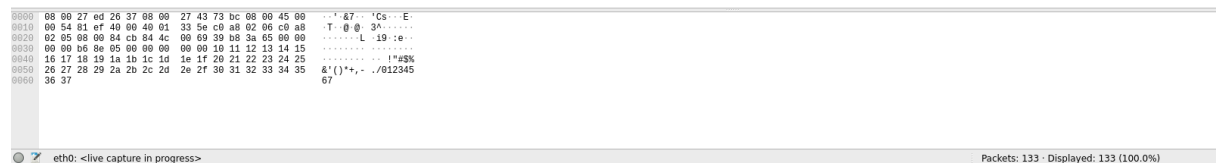


2. Wireshark - przechwycenie pinga z Kali do Ubuntu



Wireshark interface showing a packet capture of ping requests and replies. The packet list on the left shows 24 packets, all of which are ICMP Echo (ping) requests and replies. The packet details pane on the right shows the structure of the ICMP Echo request and reply, including the sequence number and TTL.

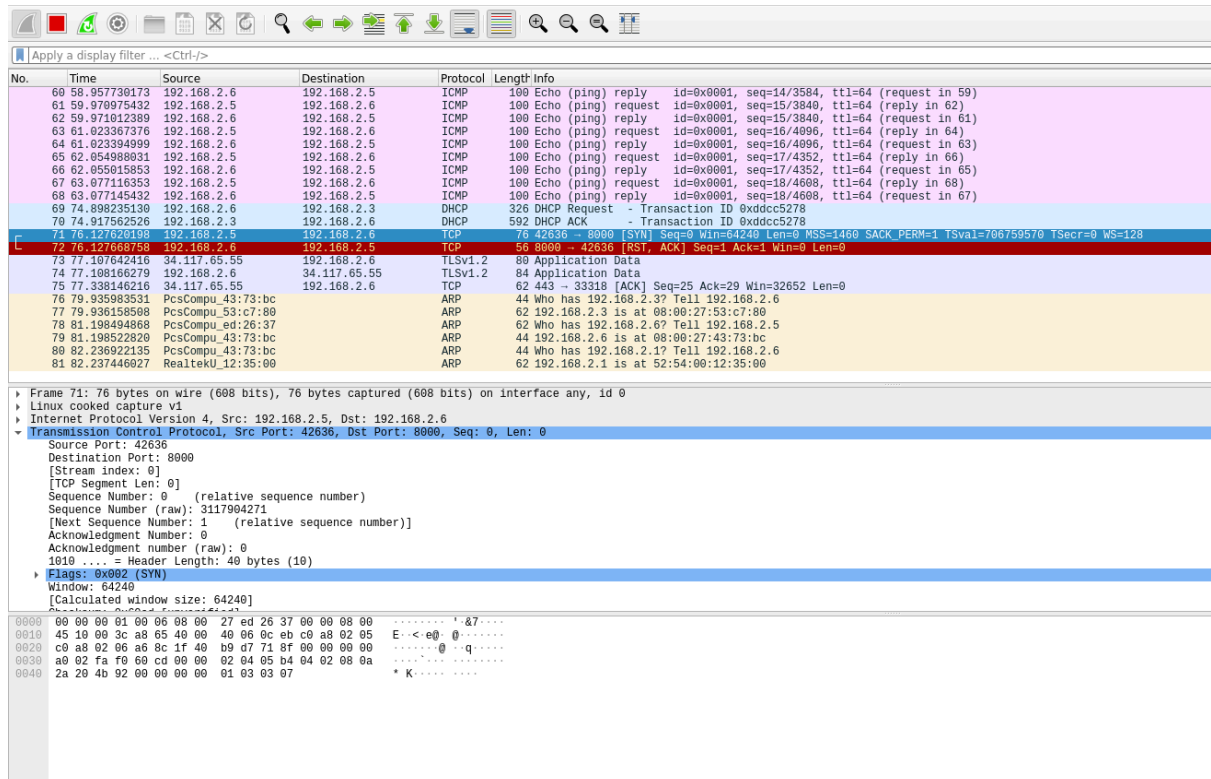
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.2.6	192.168.2.5	ICMP	98	Echo (ping) request id=0x844c, seq=97/24832, ttl=64 (request in 2)
2	0.000038469	192.168.2.5	192.168.2.6	ICMP	98	Echo (ping) reply id=0x844c, seq=97/24832, ttl=64 (request in 1)
3	1.003458779	192.168.2.6	192.168.2.5	ICMP	98	Echo (ping) request id=0x844c, seq=98/25088, ttl=64 (request in 4)
4	1.004093941	192.168.2.5	192.168.2.6	ICMP	98	Echo (ping) reply id=0x844c, seq=98/25088, ttl=64 (request in 3)
5	2.036437752	192.168.2.6	192.168.2.5	ICMP	98	Echo (ping) request id=0x844c, seq=99/25344, ttl=64 (request in 6)
6	2.037485057	192.168.2.5	192.168.2.6	ICMP	98	Echo (ping) reply id=0x844c, seq=99/25344, ttl=64 (request in 5)
7	3.038032868	192.168.2.6	192.168.2.5	ICMP	98	Echo (ping) request id=0x844c, seq=100/25600, ttl=64 (request in 8)
8	3.039255715	192.168.2.5	192.168.2.6	ICMP	98	Echo (ping) reply id=0x844c, seq=100/25600, ttl=64 (request in 7)
9	4.040005348	192.168.2.6	192.168.2.5	ICMP	98	Echo (ping) request id=0x844c, seq=101/25856, ttl=64 (request in 10)
10	4.040992826	192.168.2.5	192.168.2.6	ICMP	98	Echo (ping) reply id=0x844c, seq=101/25856, ttl=64 (request in 9)
11	5.046467607	192.168.2.6	192.168.2.5	ICMP	98	Echo (ping) request id=0x844c, seq=102/26112, ttl=64 (request in 12)
12	5.047508062	192.168.2.5	192.168.2.6	ICMP	98	Echo (ping) reply id=0x844c, seq=102/26112, ttl=64 (request in 11)
13	6.048719792	192.168.2.6	192.168.2.5	ICMP	98	Echo (ping) request id=0x844c, seq=103/26368, ttl=64 (request in 14)
14	6.049693143	192.168.2.5	192.168.2.6	ICMP	98	Echo (ping) reply id=0x844c, seq=103/26368, ttl=64 (request in 13)
15	7.055938037	192.168.2.6	192.168.2.5	ICMP	98	Echo (ping) request id=0x844c, seq=104/26624, ttl=64 (request in 16)
16	7.056908077	192.168.2.5	192.168.2.6	ICMP	98	Echo (ping) reply id=0x844c, seq=104/26624, ttl=64 (request in 15)
17	8.058331624	192.168.2.6	192.168.2.5	ICMP	98	Echo (ping) request id=0x844c, seq=105/26880, ttl=64 (request in 18)
18	8.059327145	192.168.2.5	192.168.2.6	ICMP	98	Echo (ping) reply id=0x844c, seq=105/26880, ttl=64 (request in 17)
19	9.060384096	192.168.2.6	192.168.2.5	ICMP	98	Echo (ping) request id=0x844c, seq=106/27136, ttl=64 (request in 20)
20	9.061327231	192.168.2.5	192.168.2.6	ICMP	98	Echo (ping) reply id=0x844c, seq=106/27136, ttl=64 (request in 19)
21	10.063116836	192.168.2.6	192.168.2.5	ICMP	98	Echo (ping) request id=0x844c, seq=107/27392, ttl=64 (request in 22)
22	10.064060343	192.168.2.5	192.168.2.6	ICMP	98	Echo (ping) reply id=0x844c, seq=107/27392, ttl=64 (request in 21)
23	11.066741539	192.168.2.6	192.168.2.5	ICMP	98	Echo (ping) request id=0x844c, seq=108/27648, ttl=64 (request in 24)



Wireshark interface showing the raw data of a packet capture. The packet list on the left shows 24 packets, all of which are ICMP Echo (ping) requests and replies. The packet details pane on the right shows the structure of the ICMP Echo request and reply, including the sequence number and TTL.

No.	Time	Source	Destination	Protocol	Length	Info
60	58.957736173	192.168.2.6	192.168.2.5	ICMP	100	Echo (ping) reply id=0x0001, seq=14/3584, ttl=64 (request in 59)
61	59.970975432	192.168.2.5	192.168.2.6	ICMP	100	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (request in 62)
62	59.971012389	192.168.2.6	192.168.2.5	ICMP	100	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 61)
63	61.023367376	192.168.2.5	192.168.2.6	ICMP	100	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (request in 64)
64	61.023394999	192.168.2.6	192.168.2.5	ICMP	100	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 63)
65	62.054988031	192.168.2.5	192.168.2.6	ICMP	100	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (request in 66)
66	62.055015853	192.168.2.6	192.168.2.5	ICMP	100	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 65)
67	63.077116353	192.168.2.5	192.168.2.6	ICMP	100	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (request in 68)
68	63.077145432	192.168.2.6	192.168.2.5	ICMP	100	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64 (request in 67)
69	74.898235130	192.168.2.6	192.168.2.3	DHCP	326	DHCP Request - Transaction ID 0x0ddcc5278
70	74.917562526	192.168.2.3	192.168.2.6	DHCP	592	DHCP ACK - Transaction ID 0x0ddcc5278
71	76.127620198	192.168.2.5	192.168.2.6	TCP	76	42636 -> 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=706759570 TSecr=0 WS=128
72	76.127668158	192.168.2.6	192.168.2.5	TCP	58	8000 -> 42636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
73	77.107042416	34.117.65.55	192.168.2.6	TLSv1.2	80	Application Data
74	77.108166279	192.168.2.6	34.117.65.55	TLSv1.2	84	Application Data
75	77.338146216	34.117.65.55	192.168.2.6	TCP	62	443 -> 33318 [ACK] Seq=25 Ack=29 Win=32652 Len=0
76	79.935983531	PcsCompu_43:73:bc		ARP	44	Who has 192.168.2.3? Tell 192.168.2.6
77	79.936158598	PcsCompu_53:c7:80		ARP	62	192.168.2.3 is at 08:00:27:53:c7:80
78	81.198494868	PcsCompu_ed:26:37		ARP	62	Who has 192.168.2.6? Tell 192.168.2.5
79	81.198522820	PcsCompu_43:73:bc		ARP	44	192.168.2.6 is at 08:00:27:43:73:bc
80	82.236922135	PcsCompu_43:73:bc		ARP	44	Who has 192.168.2.1? Tell 192.168.2.6
81	82.237446027	RealtekU_12:35:00		ARP	62	192.168.2.1 is at 52:54:00:12:35:00

3. Telnet



Wireshark interface showing a packet capture of a Telnet session. The packet list on the left shows 81 packets, including Telnet requests and responses, as well as DHCP and ARP traffic. The packet details pane on the right shows the structure of the Telnet session, including the sequence number and window size.

No.	Time	Source	Destination	Protocol	Length	Info
60	58.957736173	192.168.2.6	192.168.2.5	ICMP	100	Echo (ping) reply id=0x0001, seq=14/3584, ttl=64 (request in 59)
61	59.970975432	192.168.2.5	192.168.2.6	ICMP	100	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (request in 62)
62	59.971012389	192.168.2.6	192.168.2.5	ICMP	100	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 61)
63	61.023367376	192.168.2.5	192.168.2.6	ICMP	100	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (request in 64)
64	61.023394999	192.168.2.6	192.168.2.5	ICMP	100	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 63)
65	62.054988031	192.168.2.5	192.168.2.6	ICMP	100	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (request in 66)
66	62.055015853	192.168.2.6	192.168.2.5	ICMP	100	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 65)
67	63.077116353	192.168.2.5	192.168.2.6	ICMP	100	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (request in 68)
68	63.077145432	192.168.2.6	192.168.2.5	ICMP	100	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64 (request in 67)
69	74.898235130	192.168.2.6	192.168.2.3	DHCP	326	DHCP Request - Transaction ID 0x0ddcc5278
70	74.917562526	192.168.2.3	192.168.2.6	DHCP	592	DHCP ACK - Transaction ID 0x0ddcc5278
71	76.127620198	192.168.2.5	192.168.2.6	TCP	76	42636 -> 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=706759570 TSecr=0 WS=128
72	76.127668158	192.168.2.6	192.168.2.5	TCP	58	8000 -> 42636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
73	77.107042416	34.117.65.55	192.168.2.6	TLSv1.2	80	Application Data
74	77.108166279	192.168.2.6	34.117.65.55	TLSv1.2	84	Application Data
75	77.338146216	34.117.65.55	192.168.2.6	TCP	62	443 -> 33318 [ACK] Seq=25 Ack=29 Win=32652 Len=0
76	79.935983531	PcsCompu_43:73:bc		ARP	44	Who has 192.168.2.3? Tell 192.168.2.6
77	79.936158598	PcsCompu_53:c7:80		ARP	62	192.168.2.3 is at 08:00:27:53:c7:80
78	81.198494868	PcsCompu_ed:26:37		ARP	62	Who has 192.168.2.6? Tell 192.168.2.5
79	81.198522820	PcsCompu_43:73:bc		ARP	44	192.168.2.6 is at 08:00:27:43:73:bc
80	82.236922135	PcsCompu_43:73:bc		ARP	44	Who has 192.168.2.1? Tell 192.168.2.6
81	82.237446027	RealtekU_12:35:00		ARP	62	192.168.2.1 is at 52:54:00:12:35:00

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
99	374.866175223	34.117.237.239	192.168.2.6	TCP	62	443 → 42744 [ACK] Seq=798 Ack=1146 Win=31623 Len=0
100	374.939717131	192.168.2.6	192.168.2.3	DHCP	326	DHCP Request - Transaction ID 0x267bce6f
101	374.939387560	192.168.2.3	192.168.2.6	DHCP	592	DHCP ACK - Transaction ID 0x267bce6f
102	375.019948939	34.117.237.239	192.168.2.6	TLSv1.3	254	Application Data
103	375.020845773	192.168.2.6	34.117.237.239	TCP	56	42744 → 443 [ACK] Seq=1146 Ack=996 Win=64028 Len=0
104	375.020852028	192.168.2.6	34.117.237.239	TLSv1.3	95	Application Data
105	375.117917393	34.117.237.239	192.168.2.6	TCP	62	443 → 42744 [ACK] Seq=996 Ack=1185 Win=31584 Len=0
106	377.432582259	34.117.65.55	192.168.2.6	TLSv1.2	80	Application Data
107	377.433863318	192.168.2.6	34.117.65.55	TLSv1.2	84	Application Data
108	377.637393362	34.117.65.55	192.168.2.6	TCP	62	443 → 33518 [ACK] Seq=49 Ack=57 Win=32624 Len=0
109	379.965231859	PcsCompu.43:73:bc	192.168.2.6	ARP	44	Who has 192.168.2.3? Tell 192.168.2.6
110	379.965801354	PcsCompu.53:c7:80	192.168.2.6	ARP	62	192.168.2.3 is at 08:00:27:53:c7:80
111	433.812186798	192.168.2.6	34.117.237.239	TLSv1.3	95	Application Data
112	433.827198594	34.117.237.239	192.168.2.6	TLSv1.3	95	Application Data
113	433.868595927	192.168.2.6	34.117.237.239	TCP	56	42744 → 443 [ACK] Seq=1224 Ack=1035 Win=64028 Len=0
114	440.339193333	192.168.2.6	192.168.80.2	DNS	80	Standard query 0xda27 A dobrewiadomosci.pl
115	440.339167798	192.168.2.6	192.168.80.2	DNS	80	Standard query 0x9421 AAAA dobrewiadomosci.pl
116	440.342777154	192.168.80.2	192.168.2.6	DNS	96	Standard query response 0xda27 A dobrewiadomosci.pl A 91.198.146.229
117	440.343395690	192.168.80.2	192.168.2.6	DNS	138	Standard query response 0x9421 AAAA dobrewiadomosci.pl SOA dns1.tld.pl
118	440.343765145	192.168.2.6	91.198.146.229	TCP	76	54252 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=449506894 TSecr=0 WS=128
119	440.374486318	91.198.146.229	192.168.2.6	TCP	62	443 → 54252 [SYN, ACK] Seq=1146 Ack=1 Win=32768 Len=0 MSS=1460
120	440.374483187	192.168.2.6	91.198.146.229	TCP	56	54252 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0

Frame 118: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface any, id 0

Linux cooked capture v1

Internet Protocol Version 4, Src: 192.168.2.6, Dst: 91.198.146.229

Transmission Control Protocol, Src Port: 54252, Dst Port: 443, Seq: 0, Len: 0

Source Port: 54252

Destination Port: 443

[Stream index: 3]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 953906274

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 0

Acknowledgment number (raw): 0

1010 = Header Length: 40 bytes (10)

Flags: 0x002 (SYN)

Window: 64240

[Calculated window size: 64240]

0000 00 04 00 01 00 06 08 00 27 43 73 bc 00 00 08 00 'Cs'....

0010 45 10 00 3c c5 b7 40 00 40 06 c3 9a c0 a8 02 06 E...<...@... ..

0020 5b c6 92 e5 d3 ec 01 b0 38 d0 74 62 00 00 00 00 [...] 8 tb'....

0030 a0 02 fa f0 d1 88 00 00 02 04 05 b4 04 02 08 0aLE....

0040 1a ca ee 4e 00 00 00 00 01 03 03 07#A'....

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
126	497.988950614	RealTekU.12:35:00	192.168.2.6	ARP	62	192.168.2.1 is at 52:54:00:12:35:00
127	515.125299663	192.168.2.6	91.198.146.229	SSL	61	Continuation Data
128	515.158168359	91.198.146.229	192.168.2.6	TCP	62	443 → 54252 [FIN, ACK] Seq=1 Ack=6 Win=32763 Len=0
129	515.156517178	192.168.2.6	91.198.146.229	TCP	56	54252 → 443 [FIN, ACK] Seq=0 Ack=2 Win=64239 Len=0
130	515.157329088	91.198.146.229	192.168.2.6	TCP	62	443 → 54252 [ACK] Seq=2 Ack=7 Win=32762 Len=0
131	519.461190363	192.168.2.6	192.168.80.2	DNS	80	Standard query 0xe1da A dobrewiadomosci.pl
132	519.461227983	192.168.2.6	192.168.80.2	DNS	80	Standard query 0x4d09 AAAA dobrewiadomosci.pl
133	519.462906461	192.168.80.2	192.168.2.6	DNS	96	Standard query response 0xe1da A dobrewiadomosci.pl A 91.198.146.229
134	519.463100090	192.168.80.2	192.168.2.6	DNS	138	Standard query response 0x4d09 AAAA dobrewiadomosci.pl SOA dns1.tld.pl
135	519.463269788	192.168.2.6	91.198.146.229	TCP	76	36988 → 4443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=449586014 TSecr=0 WS=128
136	520.462267895	192.168.2.6	91.198.146.229	TCP	76	[TCP Retransmission] 36988 → 4443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=449587833 TSecr=0 WS=128
137	522.468134067	192.168.2.6	91.198.146.229	TCP	76	[TCP Retransmission] 36988 → 4443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=449589047 TSecr=0 WS=128
138	526.651751327	192.168.2.6	91.198.146.229	TCP	76	[TCP Retransmission] 36988 → 4443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=449593202 TSecr=0 WS=128
139	534.849777209	192.168.2.6	91.198.146.229	TCP	76	[TCP Retransmission] 36988 → 4443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=449601460 TSecr=0 WS=128
140	545.851840318	192.168.2.6	34.117.237.239	TLSv1.3	95	Application Data
141	545.852352432	192.168.2.6	34.117.237.239	TLSv1.3	80	Application Data
142	545.852570842	192.168.2.6	34.117.237.239	TCP	56	42744 → 443 [FIN, ACK] Seq=1326 Ack=1074 Win=64028 Len=0
143	545.852839026	34.117.237.239	192.168.2.6	TCP	62	443 → 42744 [ACK] Seq=1074 Ack=1326 Win=31443 Len=0
144	545.853077941	34.117.237.239	192.168.2.6	TCP	62	443 → 42744 [ACK] Seq=1074 Ack=1327 Win=31442 Len=0
145	545.867277926	34.117.237.239	192.168.2.6	TCP	62	443 → 42744 [FIN, ACK] Seq=1074 Ack=1327 Win=31442 Len=0
146	545.867346159	192.168.2.6	34.117.237.239	TCP	56	42744 → 443 [ACK] Seq=1327 Ack=1075 Win=64028 Len=0
147	549.743391436	192.168.2.6	91.198.146.229	TCP	76	[TCP Retransmission] 36988 → 4443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=449617526 TSecr=0 WS=128

Frame 135: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface any, id 0

Linux cooked capture v1

Internet Protocol Version 4, Src: 192.168.2.6, Dst: 91.198.146.229

Transmission Control Protocol, Src Port: 36988, Dst Port: 4443, Seq: 0, Len: 0

Source Port: 36988

Destination Port: 4443

[Stream index: 4]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 430722117

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 0

Acknowledgment number (raw): 0

1010 = Header Length: 40 bytes (10)

Flags: 0x002 (SYN)

Window: 64240

[Calculated window size: 64240]

0000 00 04 00 01 00 06 08 00 27 43 73 bc 00 00 08 00 'Cs'....

0010 45 10 00 3c 5d 9f 40 00 40 06 35 13 c0 a8 02 06 E...CT?@ 0 5'....

0020 5b c6 92 e5 90 7c 11 5b 19 ac 4c 45 00 00 00 00 [...] [] ..LE....

0030 a9 02 fa f0 d1 88 00 00 02 04 05 b4 04 02 08 0aLE....

0040 1a cc 23 5e 00 00 00 00 01 03 03 07#A'....

any: <live capture in progress>

Packets: 147 - Displayed: 147 (100.0%)

4. Telnet - odpowiedzi

Podczas każdej z tych prób nie udało się nam wykonać połączenia

- **telnet 192.168.2.6 8000** - ponieważ port ten na maszynie jest zamknięty
- **telnet dobrewiadomosci.pl 443** (https) - port na serwisie jest zamknięty. Dodatkowo może występować problem, ponieważ Telnet jest protokołem tekstowym i nie obsługuje szyfrowania SSL/TLS, które jest standardem w przypadku połączeń HTTPS.

- telnet dobrewiadomosci.pl 4443 - jest to niestandardowy port i jest zamknięty

5. HackThisSite

