

Lab 20

Abriremos el archivo **general101b.pcapng**

En el paquete numero aplicaremos “flags” como filtro

The screenshot shows the Wireshark interface with the file 'general101b.pcapng' open. The 'Display Filter' bar at the top contains the filter 'tcp.flags == 0x002'. The packet list on the left shows packets 1 through 14. The packet details pane on the right shows the selected packet (packet 1) with its TCP flags set to 0x002. The packet bytes pane at the bottom shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Host
1	0.000000	24.6.173.220	216.115.212.254	TCP	Host
2	0.017273	24.6.173.220	67.217.65.244	TCP	Host
3	0.000227	24.6.173.220	64.74.80.187	TCP	Host
4	0.000401	24.6.173.220	202.173.28.250	TCP	Host
5	0.018962	24.6.173.220	216.115.212.254	TCP	Host
6	0.000194	24.6.173.220	67.217.65.244	TCP	Host
7	0.086583	24.6.173.220	64.74.80.187	TCP	Host
8	0.010868	24.6.173.220	202.173.28.250	TCP	Host
9	0.075160	24.6.173.220	216.115.212.254	TCP	Host
10	0.000201	24.6.173.220	67.217.65.244	TCP	Host
11	0.010283	24.6.173.220	64.74.80.187	TCP	Host
12	0.005195	24.6.173.220	202.173.28.250	TCP	Host
13	0.000129	24.6.173.220	216.115.212.254	TCP	Host
14	0.009862	24.6.173.220	199.47.216.174	TCP	Host

Visualizaremos este filtro

The screenshot shows the Wireshark interface with the file 'general101b.pcapng' open. The 'Display Filter' bar at the top contains the filter 'tcp.flags == 0x002'. The packet list on the left shows packets 1 through 16, all of which are filtered by the display filter. The packet details pane on the right shows the selected packet (packet 1) with its TCP flags set to 0x002. The packet bytes pane at the bottom shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Host
1	0.000000	24.6.173.220	216.115.212.254	TCP	Host
7	0.086583	24.6.173.220	67.217.65.244	TCP	Host
8	0.010868	24.6.173.220	64.74.80.187	TCP	Host
19	0.084391	24.6.173.220	202.173.28.250	TCP	Host
38	0.967351	24.6.173.220	216.115.212.254	TCP	Host
44	0.158701	24.6.173.220	67.217.65.244	TCP	Host
45	0.014867	24.6.173.220	64.74.80.187	TCP	Host
56	0.212343	24.6.173.220	202.173.28.250	TCP	Host
65	0.000240	24.6.173.220	216.115.212.254	TCP	Host
81	0.234611	24.6.173.220	67.217.65.244	TCP	Host
82	0.016919	24.6.173.220	64.74.80.187	TCP	Host
93	0.359137	24.6.173.220	202.173.28.250	TCP	Host
140	0.000781	24.6.169.43	199.47.217.177	TCP	Host
162	0.004660	24.6.173.220	199.47.216.174	TCP	Host

Aplicaremos ese filtro y le agregamos **&& ip.dst==24.6.0.0/16** y podremos ver 5 paquetes

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main display area is divided into three panes. The top pane shows a list of captured packets, filtered by the expression `tcp.flags == 0x002 && ip.dst == 24.6.0.0/16`. This filter results in 5 packets being displayed. The middle pane shows the details of the selected packet (No. 551), including the TCP header fields: Sequence number, Acknowledgment number, and Flags (SYN). The bottom pane shows the raw packet data in hexadecimal and ASCII. The status bar at the bottom indicates that 575 packets were captured and 5 are currently displayed (0.9%).

No.	Time	Source	Destination	Protocol	Host	Info
352	0.142873	121.125.72.180	24.6.169.43	TCP		57003 → 8880 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
353	0.256469	121.125.72.180	24.6.173.220	TCP		57003 → 8880 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
535	1.008432	24.6.169.43	24.6.173.220	TCP		54708 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
537	2.420274	24.6.169.43	24.6.173.220	TCP		[TCP Retransmission] 54708 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
551	1.971118	24.6.169.43	24.6.173.220	TCP		[TCP Retransmission] 54708 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460

[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Sequence number (raw): 195426019
[Next sequence number: 1 (relative sequence number)]
> Acknowledgment number: 34203886
Acknowledgment number (raw): 34203886
0111 = Header Length: 28 bytes (7)
> Flags: 0x002 (SYN)
Window size value: 65535

0000 c8 60 00 19 9e 19 00 01 5c 31 bb c1 08 00 45 20 .^.....\1...E
0010 00 30 aa dd 00 00 73 06 19 68 79 7d 48 b4 18 06 .0....s..hy)H..
0020 a9 2b de ab 22 b0 0b a5 f6 e3 02 09 e8 ee 70 02 .+..\".....p..
0030 ff ff 10 e0 00 00 02 04 05 b4 01 01 04 02

Flags (12 bits) (tcp.flags), 2 byte(s) | Packets: 575 · Displayed: 5 (0.9%) | Profile: wireshark101