

Creación manual de paquete TCP/IP

Contenido De La Memoria

1. Crea un pantallazo de lo mostrado en Wireshark	2
2. ¿Qué flags tiene "encendidos" tu paquete?, ¿y el de vuelta?	2
3. Pon mal el checksum y observa qué pasa	3
4. Pon un TTL=2 y observa qué pasa	3

Crea un paquete TCP SYN que vaya a 91.142.214.181 , escucha con Wireshark y observa si obtienes la respuesta.

1. Crea un pantallazo de lo mostrado en Wireshark

Capturing from enp0s3						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	91.142.214.181	TCP	54	12345 → 80 [SYN] Seq=0 Win=28944 Len=0
2	0.056036362	91.142.214.181	10.0.2.15	TCP	60	80 → 12345 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
3	0.000031276	10.0.2.15	91.142.214.181	TCP	54	12345 → 80 [RST] Seq=1 Win=0 Len=0

2. ¿Qué flags tiene "encendidos" tu paquete?, ¿y el de vuelta?

- Paquete de IDA

0101 = Header Length: 20 bytes (5)	
Flags: 0x002 (SYN)	
Window size value: 28944	
[Calculated window size: 28944]	
Checksum: 0xcff6 [correct]	
[Checksum Status: Good]	
[Calculated Checksum: 0xcff6]	
0000	52 54 00 12 35 00 08 00 27 cc 63 3f 08 00 45 00 RT..5...'.c?..E.
0010	00 28 ab cd 00 00 40 06 90 b0 0a 00 02 0f 5b 8e .(....@.....[.
0020	d6 b5 30 39 00 50 00 00 00 00 00 00 00 00 50 02 ..09.P.....P.
0030	71 10 cf f6 00 00 q.....

- Paquete de VUELTA

0110 = Header Length: 24 bytes (6)	
Flags: 0x012 (SYN, ACK)	
Window size value: 32768	
[Calculated window size: 32768]	
Checksum: 0x8f20 [correct]	
[Checksum Status: Good]	
[Calculated Checksum: 0x8f20]	
Unreset sequence: 0	
0000	08 00 27 cc 63 3f 52 54 00 12 35 00 08 00 45 00 ..'.c?RT..5...E.
0010	00 2c 00 c7 00 00 ff 06 7c b2 5b 8e d6 b5 0a 00 .,..... .[.....
0020	02 0f 00 50 30 39 00 00 1a 19 00 00 00 01 60 12 ...P09.....`.
0030	80 00 8f 20 00 00 02 04 05 b4 00 00

3. Pon mal el checksum y observa qué pasa

Lo que pasa es que te salta un error de Checksum y Wireshark te da el correcto para que lo corrijas en el paquete.

4	0.011034106	172.23.130.5	10.0.2.15	DNS	161 Standard query response 0x1ab1 AAAA connectivity-check.ubuntu...
5	0.859792000	10.0.2.15	91.142.214.181	TCP	54 12345 → 80 [SYN] Seq=0 Win=28944 [TCP CHECKSUM INCORRECT] Len...
6	4.146970354	PcsCompu_cc:63:3f	RealtekU_12:35:00	ARP	42 Who has 10.0.2.1? Tell 10.0.2.15
7	0.000444056	RealtekU_12:35:00	PcsCompu_cc:63:3f	ARP	60 10.0.2.1 is at 52:54:00:12:35:00

Flags:	0x002 (SYN)
Window size value:	28944
[Calculated window size:	28944]
Checksum:	0xffff6 incorrect, should be 0xcff6(maybe caused by "TCP checksum offload"?)
[Checksum Status:	Bad]
[Calculated Checksum:	0xcff6]
Urgent pointer:	0
[Timestamps]	

4. Pon un TTL=2 y observa qué pasa

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	91.142.214.181	TCP	54	12345 → 80 [SYN] Seq=0 Win=28944 Len=0
2	0.038812633	91.142.214.181	10.0.2.15	TCP	60	80 → 12345 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
3	0.00029264	10.0.2.15	91.142.214.181	TCP	54	12345 → 80 [RST] Seq=1 Win=0 Len=0

Flags:	0x0000
Fragment offset:	0
Time to live:	2
Protocol:	TCP (6)