CISCO CYBER OPS GIORNO 2

S11-L3:

Laboratorio: Utilizzo di Wireshark per Osservare la Stretta di Mano TCP a 3 Vie.

In questo laboratorio, completa i seguenti obiettivi:

- **Parte 1:** Preparare gli host per catturare il traffico
- **Parte 2**: Analizzare i pacchetti utilizzando Wireshark
- **Parte 3:** Visualizzare i pacchetti utilizzando tcpdump

https://itexamanswers.net/9-2-6-lab-using-wireshark-to-observe-the-tcp-3-way-handshake-answers.html

S11-L3:

PASSO 1: AVVIAMO KALI ED APRIAMO WIRESHARK E UNA PAGINA BROWSER

PASSO 2: SU WIRESHARK APPLICHIAMO UN FILTRO TCP E PRENDIAMO IN CONSIDERAZIONE LE PRIME TRE CONNESSIONI CHE CORRISPONDONO ALLA STRETTA DI MANO A TRE VIE SYN, SYN ACK, ACK.

S11-L3:

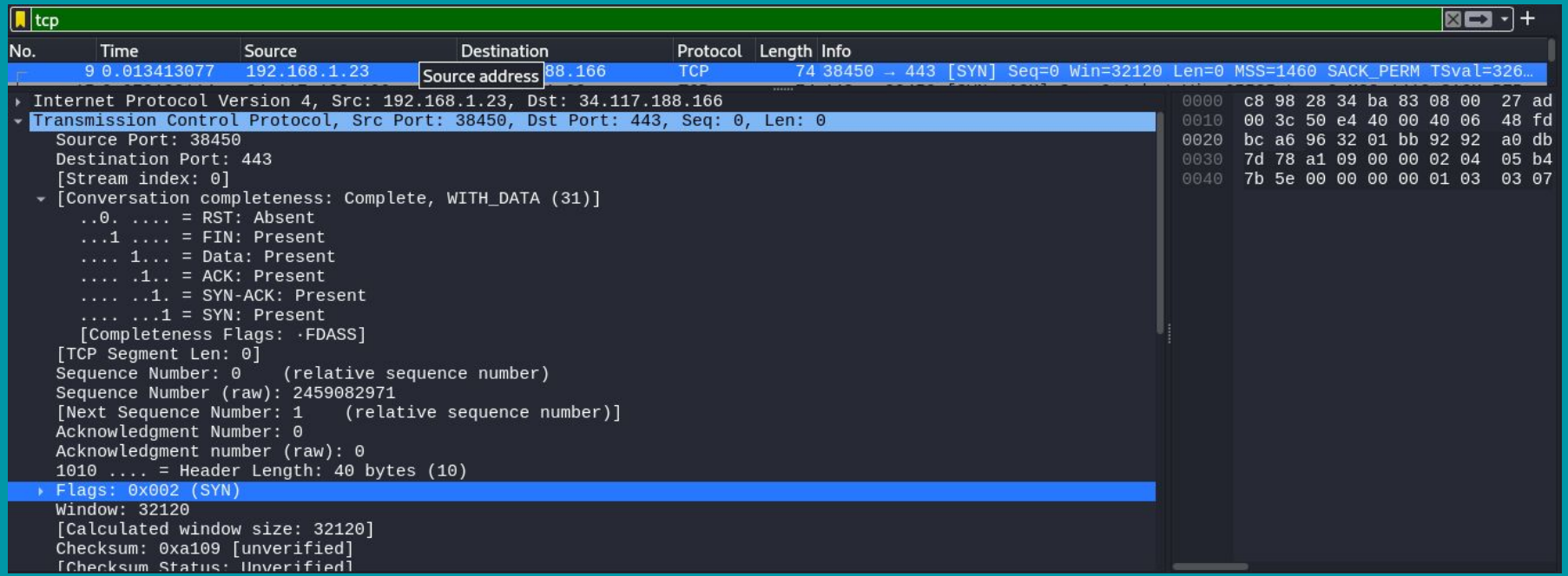
Passaggio 2: esaminare le informazioni contenute nei pacchetti, inclusi indirizzi IP, numeri di porta TCP e flag di controllo TCP.

a. In questo esempio, il frame 9 è l'inizio dell'handshake a tre vie tra il PC e il server. Nel riquadro dell'elenco dei pacchetti (sezione superiore della finestra principale), seleziona il primo pacchetto, se necessario.

b. Fare clic sulla **freccia** a sinistra del Transmission Control Protocol nel riquadro dei dettagli del pacchetto per espanderlo ed esaminare le informazioni TCP. Individuare le informazioni sulla porta di origine e di destinazione.

c. Fai clic sulla **freccia** a sinistra di Flags. Un valore di 1 significa che il flag è impostato. Individua il flag impostato in questo pacchetto.

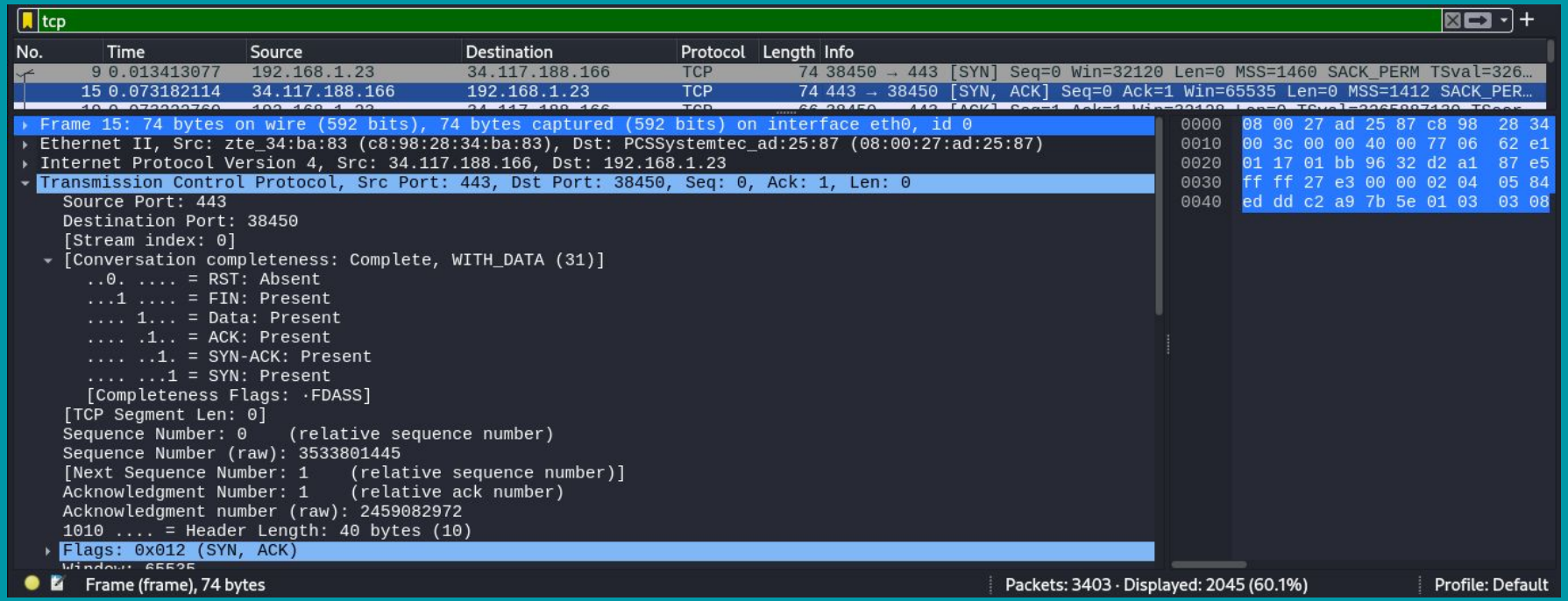
S11-L3:


tcp
No. Time Source Destination Protocol Length Info
9 0.013413077 192.168.1.23 Source address 88.166 TCP 74 38450 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=326…
Internet Protocol Version 4, Src: 192.168.1.23, Dst: 34.117.188.166
Transmission Control Protocol, Src Port: 38450, Dst Port: 443, Seq: 0, Len: 0
Source Port: 38450
Destination Port: 443
[Stream index: 0]
[Conversation completeness: Complete, WITH_DATA (31)]
..0. .... = RST: Absent
...1 .... = FIN: Present
.... 1... = Data: Present
.... .1.. = ACK: Present
.... ..1. = SYN-ACK: Present
....1 = SYN: Present
[Completeness Flags: ·FDASS]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2459082971
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1010 .... = Header Length: 40 bytes (10)
Flags: 0x002 (SYN)
Window: 32120
[Calculated window size: 32120]
Checksum: 0xa109 [unverified]
[Checksum Status: Unverified]
0000 c8 98 28 34 ba 83 08 00 27 ad
0010 00 3c 50 e4 40 00 40 06 48 fd
0020 bc a6 96 32 01 bb 92 92 a0 db
0030 7d 78 a1 09 00 00 02 04 05 b4
0040 7b 5e 00 00 00 00 01 03 03 07

S11-L3:

Seleziona il pacchetto successivo nell'handshake a tre vie. In questo esempio, questo è il frame 15. Questo è il server web che risponde alla richiesta iniziale di avviare una sessione.

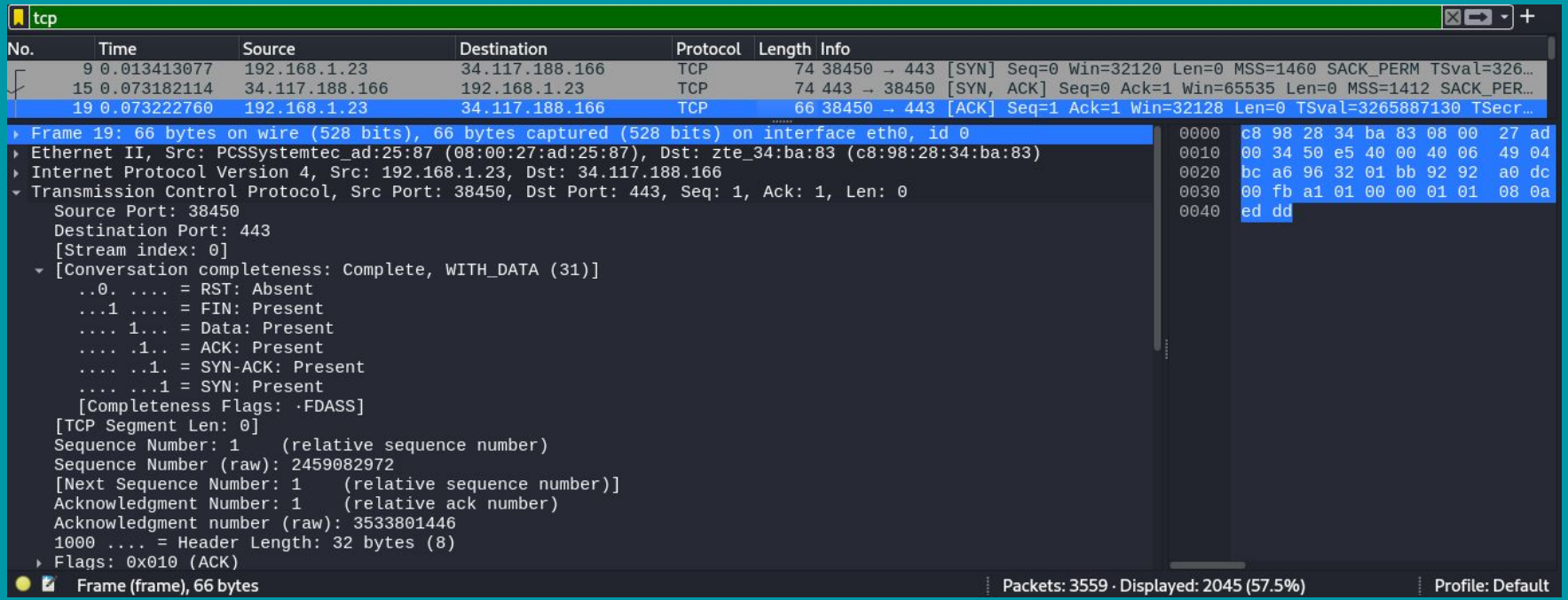
S11-L3:


tcp
No. Time Source Destination Protocol Length Info
9 0.013413077 192.168.1.23 34.117.188.166 TCP 74 38450 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=326…
15 0.073182114 34.117.188.166 192.168.1.23 TCP 74 443 → 38450 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PER…
Frame 15: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
Ethernet II, Src: zte_34:ba:83 (c8:98:28:34:ba:83), Dst: PCSSystemtec_ad:25:87 (08:00:27:ad:25:87)
Internet Protocol Version 4, Src: 34.117.188.166, Dst: 192.168.1.23
Transmission Control Protocol, Src Port: 443, Dst Port: 38450, Seq: 0, Ack: 1, Len: 0
Source Port: 443
Destination Port: 38450
[Stream index: 0]
[Conversation completeness: Complete, WITH_DATA (31)]
..0. .... = RST: Absent
...1 .... = FIN: Present
.... 1... = Data: Present
.... .1.. = ACK: Present
.... ..1. = SYN-ACK: Present
....1 = SYN: Present
[Completeness Flags: ·FDASS]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 3533801445
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2459082972
1010 .... = Header Length: 40 bytes (10)
Flags: 0x012 (SYN, ACK)
0000 08 00 27 ad 25 87 c8 98 28 34
0010 00 3c 00 00 40 00 77 06 62 e1
0020 01 17 01 bb 96 32 d2 a1 87 e5
0030 ff ff 27 e3 00 00 02 04 05 84
0040 ed dd c2 a9 7b 5e 01 03 03 08
Frame (frame), 74 bytes
Packets: 3403 · Displayed: 2045 (60.1%)
Profile: Default

S11-L3:

Infine, seleziona il terzo pacchetto nell'handshake a tre vie.

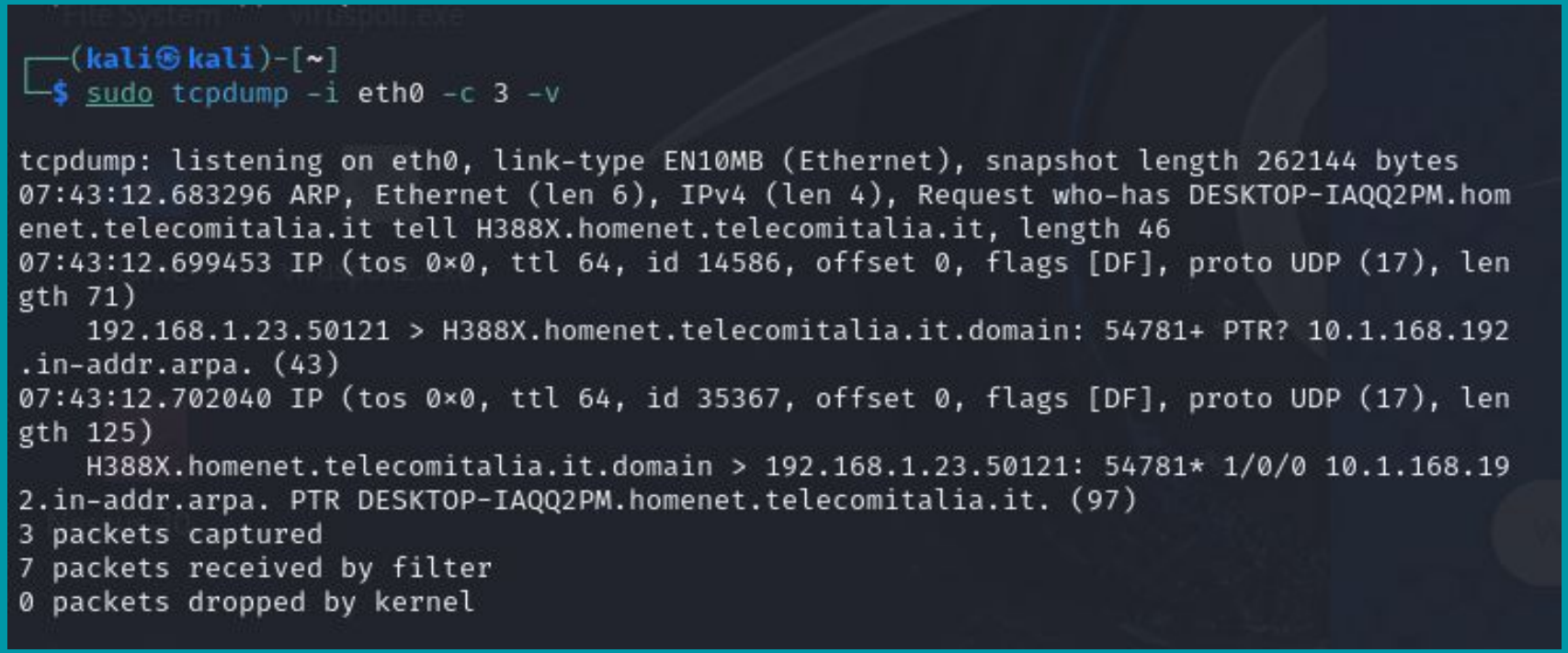
S11-L3:


tcp
No. Time Source Destination Protocol Length Info
9 0.013413077 192.168.1.23 34.117.188.166 TCP 74 38450 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=326…
15 0.073182114 34.117.188.166 192.168.1.23 TCP 74 443 → 38450 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PER…
19 0.073222760 192.168.1.23 34.117.188.166 TCP 66 38450 → 443 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3265887130 TSecr…
Frame 19: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_ad:25:87 (08:00:27:ad:25:87), Dst: zte_34:ba:83 (c8:98:28:34:ba:83)
Internet Protocol Version 4, Src: 192.168.1.23, Dst: 34.117.188.166
Transmission Control Protocol, Src Port: 38450, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
Source Port: 38450
Destination Port: 443
[Stream index: 0]
[Conversation completeness: Complete, WITH_DATA (31)]
..0. .... = RST: Absent
...1 .... = FIN: Present
.... 1... = Data: Present
.... .1.. = ACK: Present
.... ..1. = SYN-ACK: Present
....1 = SYN: Present
[Completeness Flags: ·FDASS]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2459082972
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3533801446
1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
0000 c8 98 28 34 ba 83 08 00 27 ad
0010 00 34 50 e5 40 00 40 06 49 04
0020 bc a6 96 32 01 bb 92 92 a0 dc
0030 00 fb a1 01 00 00 01 01 08 0a
0040 ed dd
Frame (frame), 66 bytes
Packets: 3559 · Displayed: 2045 (57.5%)
Profile: Default

S11-L3:

Possiamo vedere il traffico anche con tcpdump, in questo caso analizzeremo sempre i primi tre pacchetti

S11-L3:


┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -i eth0 -c 3 -v
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
07:43:12.683296 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has DESKTOP-IAQQ2PM.hom
enet.telecomitalia.it tell H388X.homenet.telecomitalia.it, length 46
07:43:12.699453 IP (tos 0×0, ttl 64, id 14586, offset 0, flags [DF], proto UDP (17), len
gth 71)
192.168.1.23.50121 > H388X.homenet.telecomitalia.it.domain: 54781+ PTR? 10.1.168.192
.in-addr.arpa. (43)
07:43:12.702040 IP (tos 0×0, ttl 64, id 35367, offset 0, flags [DF], proto UDP (17), len
gth 125)
H388X.homenet.telecomitalia.it.domain > 192.168.1.23.50121: 54781* 1/0/0 10.1.168.19
2.in-addr.arpa. PTR DESKTOP-IAQQ2PM.homenet.telecomitalia.it. (97)
3 packets captured
7 packets received by filter
0 packets dropped by kernel