Report di Analisi della Cattura Wireshark

1. Identificazione degli Indicatori di Compromissione (IOC)

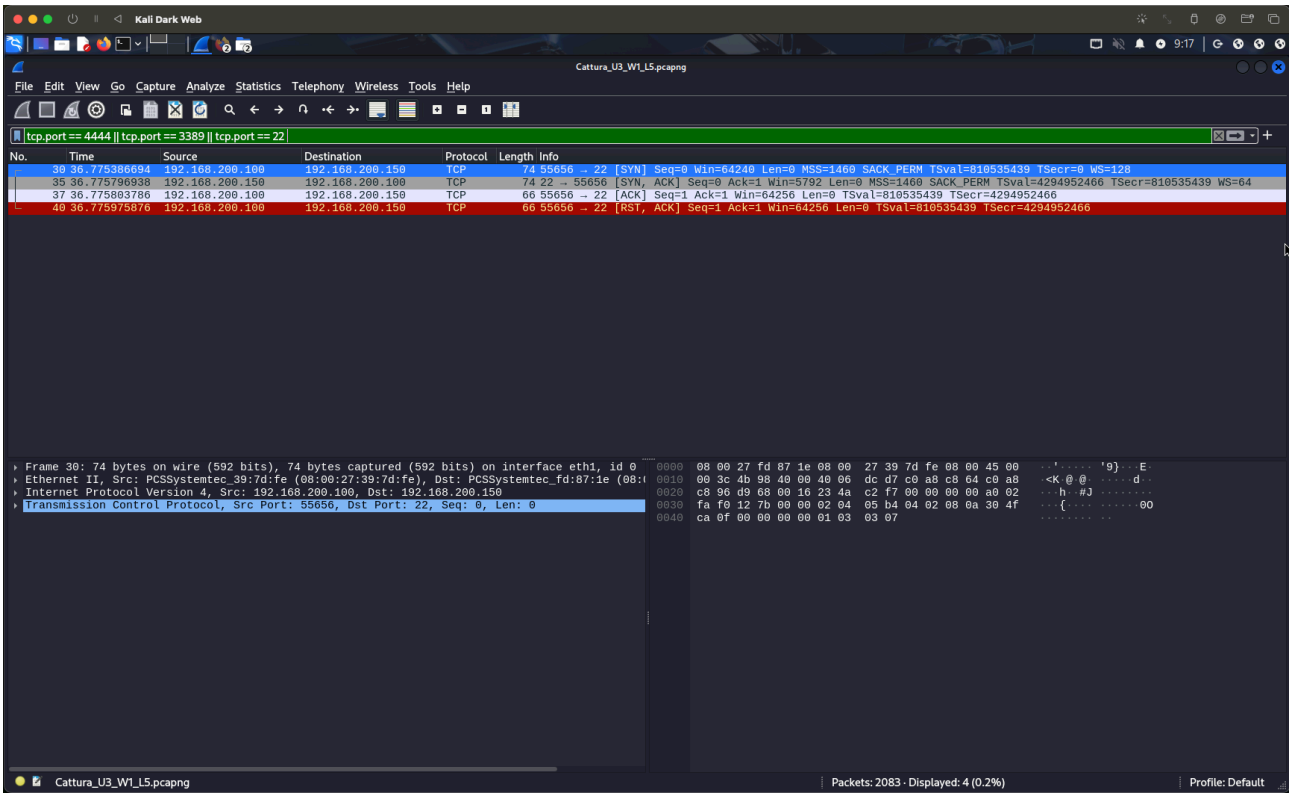
Durante l'analisi del traffico di rete, sono stati individuati diversi elementi sospetti:

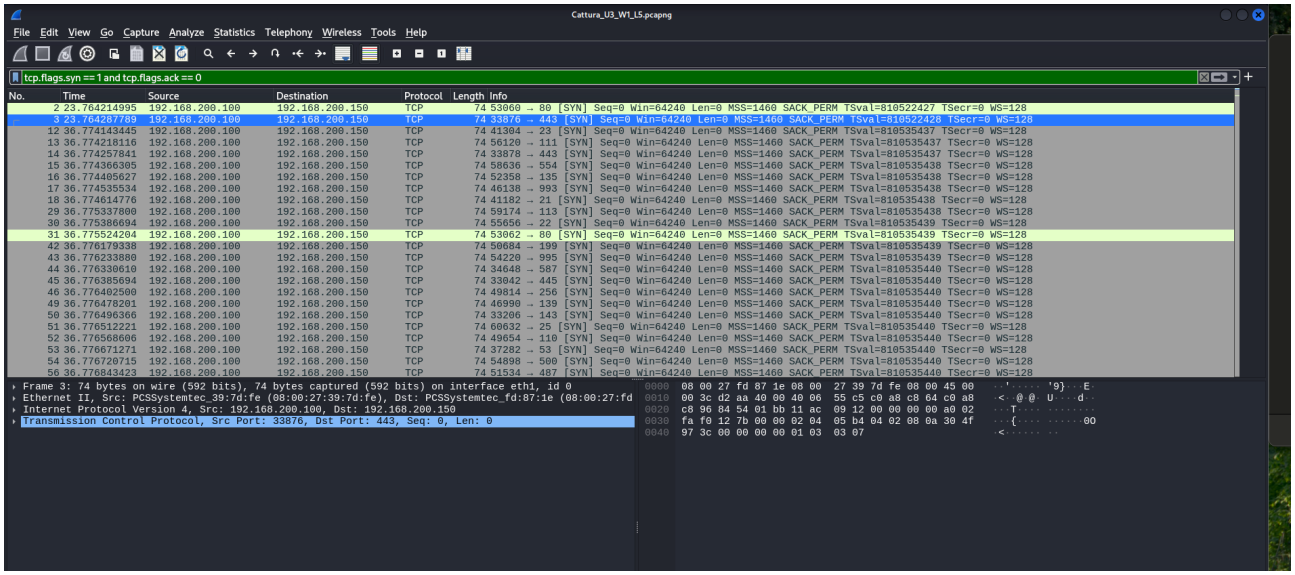
- **Host sospetto**: è stata rilevata una macchina identificata come "METASPLOITABLE"
- **Pacchetti di reset anomali (RST)**: sono stati registrati 1026 pacchetti con flag RST, suggerendo possibili scansioni aggressive o interruzioni forzate delle connessioni.
- **Attività su porte alte**: sono stati osservati 2078 pacchetti con traffico su porte non standard, un comportamento spesso associato a comunicazioni malevole o strumenti di attacco.

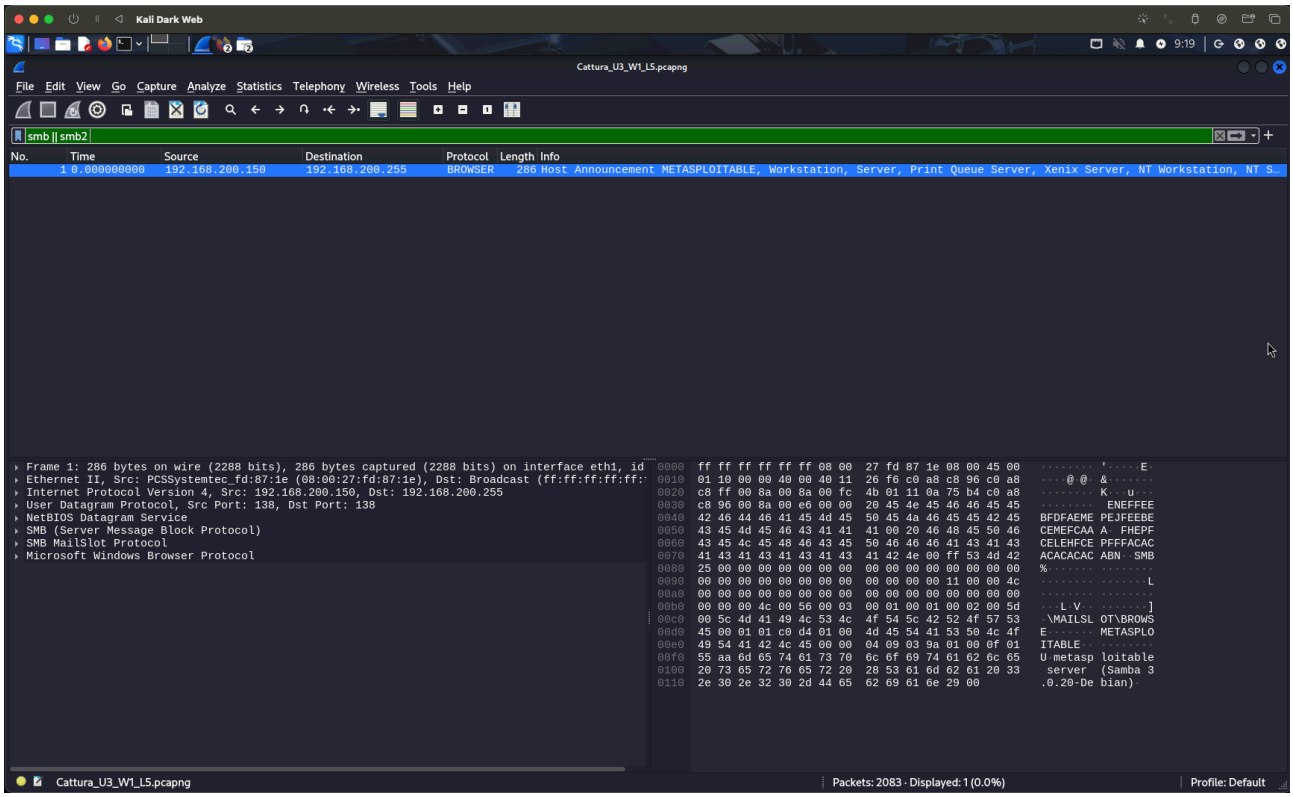
2. Ipotesi sui vettori di attacco

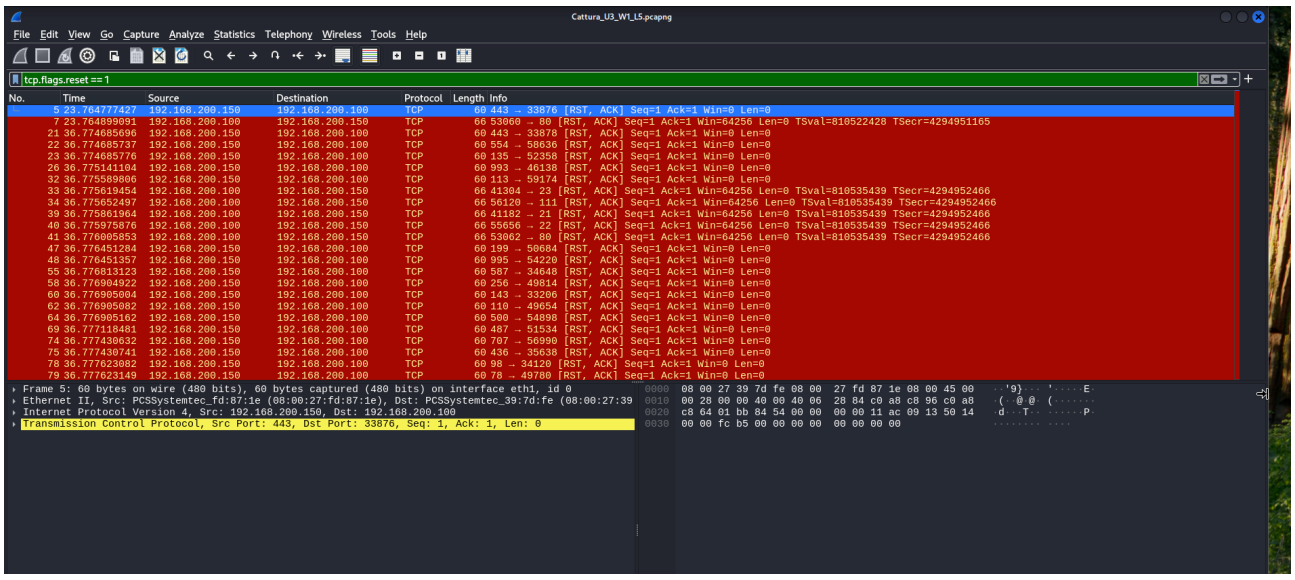
Sulla base degli IOC identificati, si possono ipotizzare i seguenti vettori di attacco:

- **Scansioni di rete attive**: il numero elevato di pacchetti RST potrebbe indicare un tentativo di mappatura della rete da parte di un attaccante.
- **Tentativi di exploit**: la presenza di un host "METASPLOITABLE" suggerisce che siano stati eseguiti tentativi di exploit.




Cattura_U3_W1_L5.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn == 1 and tcp.flags.ack == 0
No. Time Source Destination Protocol Length Info
2 23.764214995 192.168.200.100 192.168.200.150 TCP 74 53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
3 23.764287789 192.168.200.100 192.168.200.150 TCP 74 33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
12 36.774143445 192.168.200.100 192.168.200.150 TCP 74 41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13 36.774218116 192.168.200.100 192.168.200.150 TCP 74 56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
14 36.774257841 192.168.200.100 192.168.200.150 TCP 74 33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15 36.774366305 192.168.200.100 192.168.200.150 TCP 74 58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16 36.774405627 192.168.200.100 192.168.200.150 TCP 74 52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
17 36.774535534 192.168.200.100 192.168.200.150 TCP 74 46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
18 36.774614776 192.168.200.100 192.168.200.150 TCP 74 41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
29 36.775337800 192.168.200.100 192.168.200.150 TCP 74 59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30 36.775386604 192.168.200.100 192.168.200.150 TCP 74 55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31 36.775524204 192.168.200.100 192.168.200.150 TCP 74 53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
42 36.776179338 192.168.200.100 192.168.200.150 TCP 74 50684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
43 36.776233880 192.168.200.100 192.168.200.150 TCP 74 54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
44 36.776330610 192.168.200.100 192.168.200.150 TCP 74 34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
45 36.776385694 192.168.200.100 192.168.200.150 TCP 74 33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
46 36.776402500 192.168.200.100 192.168.200.150 TCP 74 49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
49 36.776478201 192.168.200.100 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
50 36.776496366 192.168.200.100 192.168.200.150 TCP 74 33206 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
51 36.776512221 192.168.200.100 192.168.200.150 TCP 74 60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
52 36.776568606 192.168.200.100 192.168.200.150 TCP 74 49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
54 36.776720715 192.168.200.100 192.168.200.150 TCP 74 54898 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
56 36.776843423 192.168.200.100 192.168.200.150 TCP 74 51534 → 487 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth1, id 0
Ethernet II, Src: PCSSystemtec_39:7d:fe (08:00:27:39:7d:fe), Dst: PCSSystemtec_fd:87:1e (08:00:27:fd
Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200.150
Transmission Control Protocol, Src Port: 33876, Dst Port: 443, Seq: 0, Len: 0
0000 08 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45 00
0010 00 3c d2 aa 40 00 40 06 55 c5 c0 a8 c8 64 c0 a8
0020 c8 96 84 54 01 bb 11 ac 09 12 00 00 00 00 a0 02
0030 fa f0 12 7b 00 00 02 04 05 b4 04 02 08 0a 30 4f
0040 97 3c 00 00 00 00 01 03 03 07


Kali Dark Web
Cattura_U3_W1_L5.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
smb || smb2
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.200.150 192.168.200.255 BROWSER 286 Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT S…
Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id
Ethernet II, Src: PCSSystemtec_fd:87:1e (08:00:27:fd:87:1e), Dst: Broadcast (ff:ff:ff:ff:ff:
Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.255
User Datagram Protocol, Src Port: 138, Dst Port: 138
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
Microsoft Windows Browser Protocol
0000 ff ff ff ff ff ff 08 00 27 fd 87 1e 08 00 45 00
0010 01 10 00 00 40 00 40 11 26 f6 c0 a8 c8 96 c0 a8
0020 c8 ff 00 8a 00 8a 00 fc 4b 01 11 0a 75 b4 c0 a8
0030 c8 96 00 8a 00 e6 00 00 20 45 4e 45 46 46 45 45
0040 42 46 44 46 41 45 4d 45 50 45 4a 46 45 45 42 45
0050 43 45 4d 45 46 43 41 41 41 00 20 46 48 45 50 46
0060 43 45 4c 45 48 46 43 45 50 46 46 46 41 43 41 43
0070 41 43 41 43 41 43 41 43 41 42 4e 00 ff 53 4d 42
0080 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 00 11 00 00 4c
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0 00 00 00 4c 00 56 00 03 00 01 00 01 00 02 00 5d
00c0 00 5c 4d 41 49 4c 53 4c 4f 54 5c 42 52 4f 57 53
00d0 45 00 01 01 c0 d4 01 00 4d 45 54 41 53 50 4c 4f
00e0 49 54 41 42 4c 45 00 00 04 09 03 9a 01 00 0f 01
00f0 55 aa 6d 65 74 61 73 70 6c 6f 69 74 61 62 6c 65
0100 20 73 65 72 76 65 72 20 28 53 61 6d 62 61 20 33
0110 2e 30 2e 32 30 2d 44 65 62 69 61 6e 29 00
Cattura_U3_W1_L5.pcapng
Packets: 2083 · Displayed: 1 (0.0%)
Profile: Default


Cattura_U3_W1_L5.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.reset == 1
No. Time Source Destination Protocol Length Info
5 23.764777427 192.168.200.150 192.168.200.100 TCP 60 443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7 23.764899091 192.168.200.150 192.168.200.100 TCP 66 53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
21 36.774685696 192.168.200.150 192.168.200.100 TCP 60 443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22 36.774685737 192.168.200.150 192.168.200.100 TCP 60 554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23 36.774685776 192.168.200.150 192.168.200.100 TCP 60 135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26 36.775141104 192.168.200.150 192.168.200.100 TCP 60 993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
32 36.775589806 192.168.200.150 192.168.200.100 TCP 60 113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33 36.775619454 192.168.200.100 192.168.200.150 TCP 66 41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34 36.775652497 192.168.200.100 192.168.200.150 TCP 66 56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39 36.775861964 192.168.200.100 192.168.200.150 TCP 66 41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40 36.775975876 192.168.200.100 192.168.200.150 TCP 66 55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41 36.776005853 192.168.200.100 192.168.200.150 TCP 66 53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
47 36.776451284 192.168.200.150 192.168.200.100 TCP 60 199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48 36.776451357 192.168.200.150 192.168.200.100 TCP 60 995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
55 36.776813123 192.168.200.150 192.168.200.100 TCP 60 587 → 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58 36.776904922 192.168.200.150 192.168.200.100 TCP 60 256 → 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
60 36.776905004 192.168.200.150 192.168.200.100 TCP 60 143 → 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
62 36.776905082 192.168.200.150 192.168.200.100 TCP 60 110 → 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
64 36.776905162 192.168.200.150 192.168.200.100 TCP 60 500 → 54898 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
69 36.777118481 192.168.200.150 192.168.200.100 TCP 60 487 → 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
74 36.777430632 192.168.200.150 192.168.200.100 TCP 60 707 → 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75 36.777430741 192.168.200.150 192.168.200.100 TCP 60 436 → 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
78 36.777623082 192.168.200.150 192.168.200.100 TCP 60 98 → 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79 36.777623149 192.168.200.150 192.168.200.100 TCP 60 78 → 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth1, id 0
Ethernet II, Src: PCSSystemtec_fd:87:1e (08:00:27:fd:87:1e), Dst: PCSSystemtec_39:7d:fe (08:00:27:39
Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.100
Transmission Control Protocol, Src Port: 443, Dst Port: 33876, Seq: 1, Ack: 1, Len: 0
0000 08 00 27 39 7d fe 08 00 27 fd 87 1e 08 00 45 00
0010 00 28 00 00 40 00 40 06 28 84 c0 a8 c8 96 c0 a8
0020 c8 64 01 bb 84 54 00 00 00 00 11 ac 09 13 50 14
0030 00 00 fc b5 00 00 00 00 00 00 00 00