ESERCIZIO SETTIMANALE S9 L5

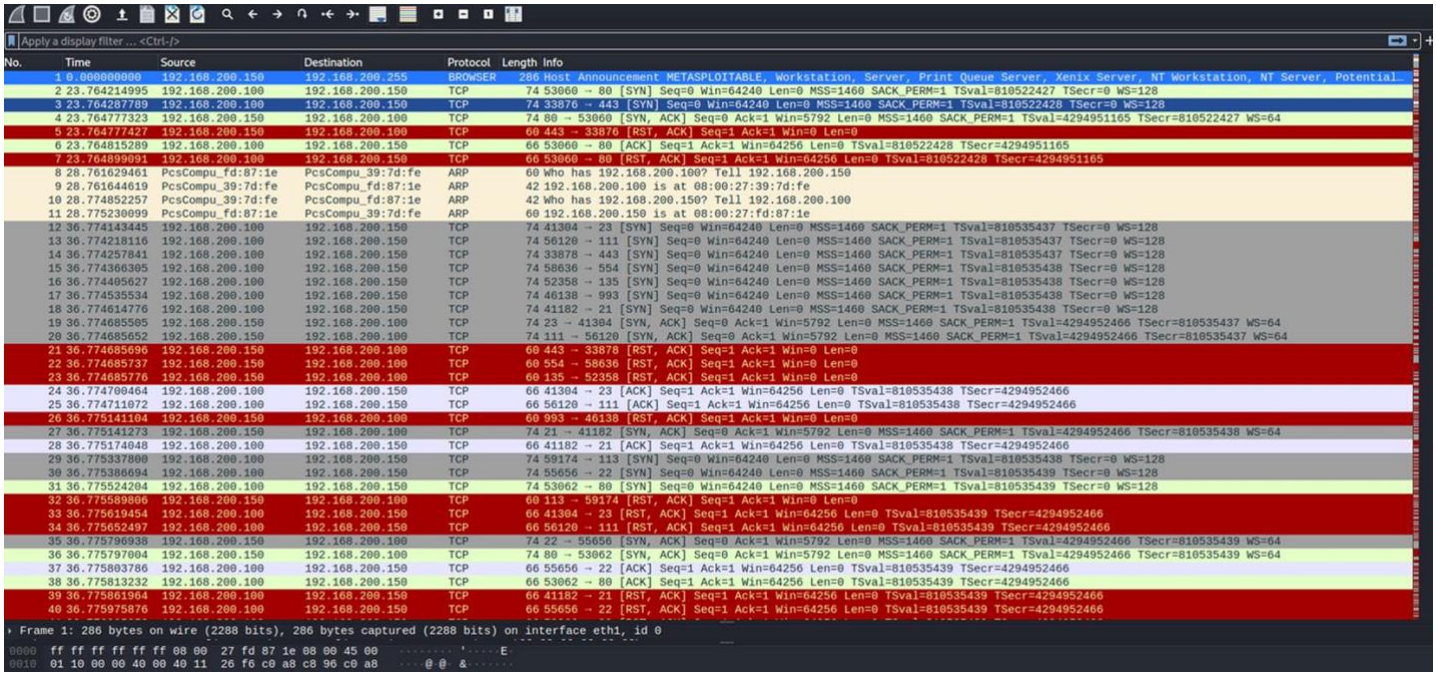
TRACCIA:

Durante la lezione teorica, abbiamo visto la threat intelligence e gli indicatori di compromissione. Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.
Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con wireshark.
Analizzate la cattura attentamente e rispondete ai seguenti quesiti:

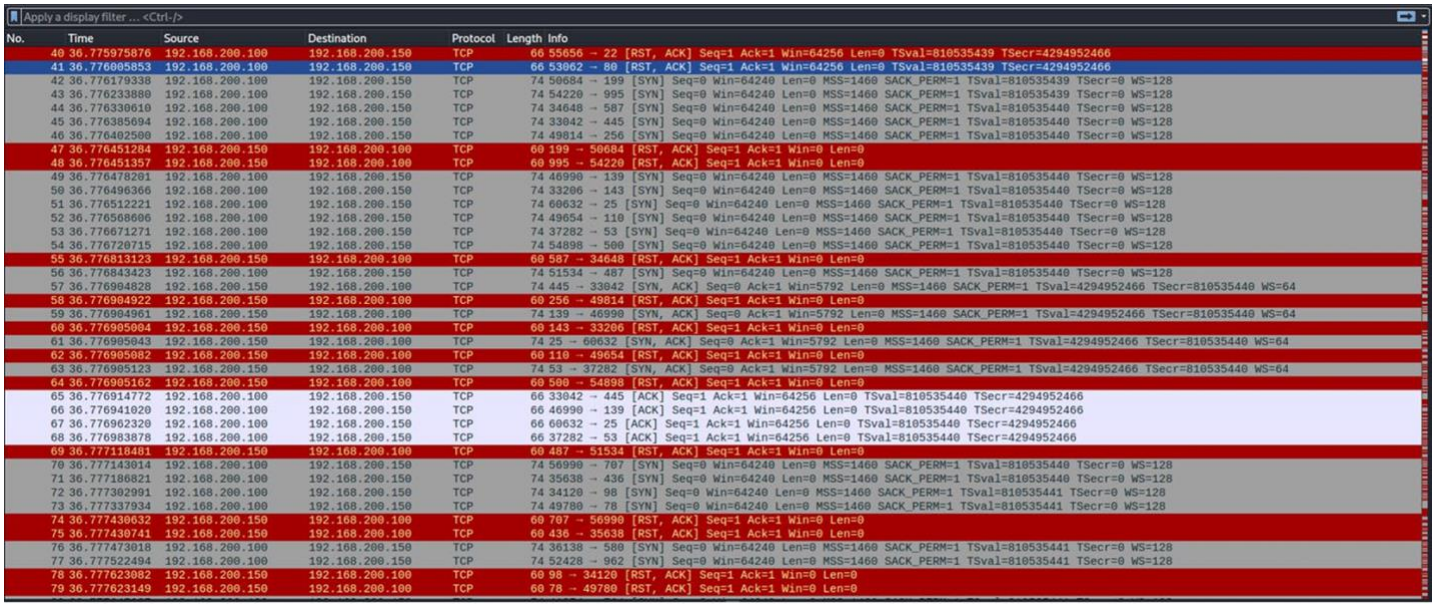
- Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso.
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati.
- Consigliate un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro.

Per analizzare la cattura, spostate il file sulla vostra Kali Linux, e fate doppio-click, vi aprirà la cattura direttamente con Wireshark, dopo aver configurato i permessi per l'utente Kali. Potete spostare il file sulla vostra Kali creando una cartella condivisa tra il vostro host e la Kali come la figura a destra. Vi basterà creare la cartella sul vostro sistema operativo, e configurare la cartella sulla macchina virtuale, specificando il percorso della cartella sul vostro Host ed il nome della cartella. Configurate la cartella con le opzioni in figura.
Da Kali potete accedere alla cartella (ed ai file in essa contenuti) navigando il file system alla directory / media. Il nostro file è nella cartella condivisa. Da qui possiamo spostare il file sul desktop con il comando «mv» specificando il nome del file ed il path di destinazione, come visto nelle lezioni sul file system di Linux. Successivamente assicuratevi che l'utente Kali possa aprire il file assegnando i permessi necessari. A questo punto fate doppio click per analizzare la cattura.
Qualora doveste avere problemi per spostare il file su Kali, trovate una prima parte della cattura negli screenshot di seguito, sufficienti per completare l'esercizio.

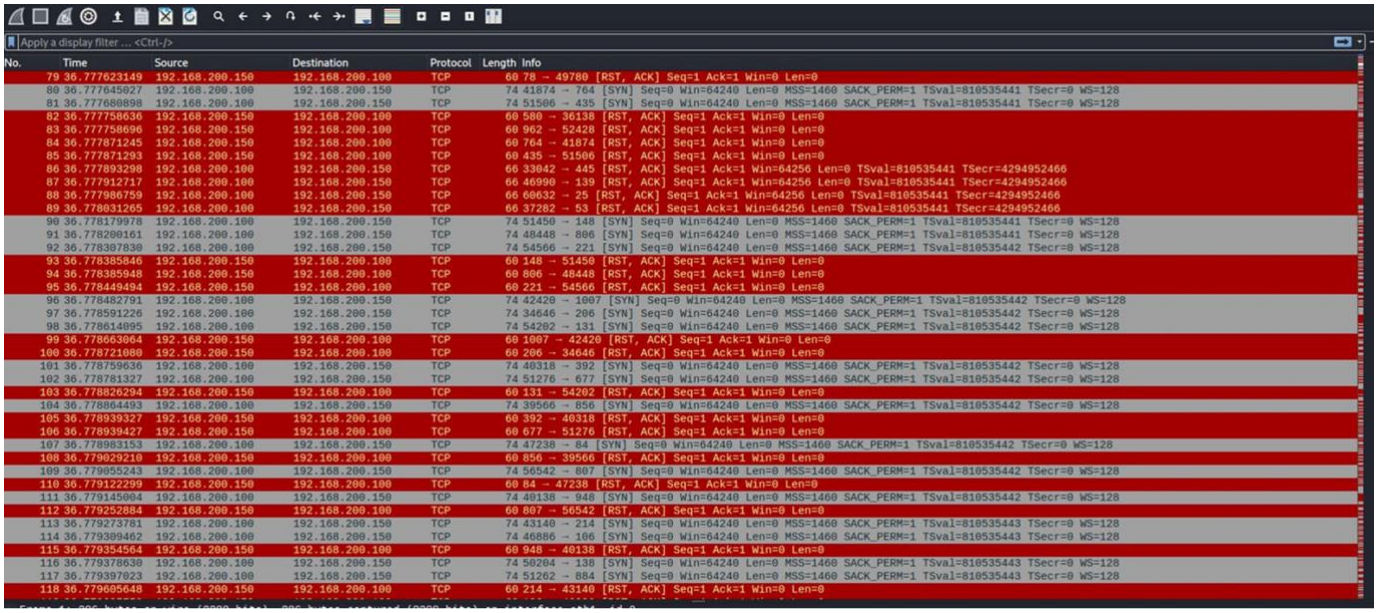
Per completare l’esercizio, ho utilizzato gli screenshot forniti dalla traccia:



```
Apply a display filter ... <Ctrl-/>
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 Server, Potential…
     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=1 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=1 TSval=810522428 TSecr=0 WS=128
     4 23.764777323 192.168.200.150 192.168.200.100  TCP      74 80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294951165 TSecr=810522427 WS=64
     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
     6 23.764815289 192.168.200.100 192.168.200.150  TCP      66 53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
     7 23.764899091 192.168.200.100 192.168.200.150  TCP      66 53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
     8 28.761629461 PcsCompu_fd:87:1e PcsCompu_39:7d:fe ARP    60 Who has 192.168.200.100? Tell 192.168.200.150
     9 28.761644619 PcsCompu_39:7d:fe PcsCompu_fd:87:1e ARP    42 192.168.200.100 is at 08:00:27:39:7d:fe
    10 28.774852257 PcsCompu_39:7d:fe PcsCompu_fd:87:1e ARP    42 Who has 192.168.200.150? Tell 192.168.200.100
    11 28.775230099 PcsCompu_fd:87:1e PcsCompu_39:7d:fe ARP    60 192.168.200.150 is at 08:00:27:fd:87:1e
    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=1 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=1 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=1 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=1 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=1 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=1 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=1 TSval=810535438 TSecr=0 WS=128
    19 36.774685505 192.168.200.150 192.168.200.100  TCP      74 23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535437 WS=64
    20 36.774685652 192.168.200.150 192.168.200.100  TCP      74 111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535437 WS=64
    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
    24 36.774700464 192.168.200.100 192.168.200.150  TCP      66 41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
    25 36.774711072 192.168.200.100 192.168.200.150  TCP      66 56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
    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
    27 36.775141273 192.168.200.150 192.168.200.100  TCP      74 21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535438 WS=64
    28 36.775174048 192.168.200.100 192.168.200.150  TCP      66 41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
    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=1 TSval=810535438 TSecr=0 WS=128
    30 36.775386694 192.168.200.100 192.168.200.150  TCP      74 55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 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=1 TSval=810535439 TSecr=0 WS=128
    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 192.168.200.150 192.168.200.100  TCP      66 56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
    35 36.775796938 192.168.200.150 192.168.200.100  TCP      74 22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535439 WS=64
    36 36.775797004 192.168.200.150 192.168.200.100  TCP      74 80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535439 WS=64
    37 36.775803786 192.168.200.100 192.168.200.150  TCP      66 55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
    38 36.775813232 192.168.200.100 192.168.200.150  TCP      66 53062 → 80 [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
▸ Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0
0000  ff ff ff ff ff ff 08 00  27 fd 87 1e 08 00 45 00   ........ '.....E
0010  01 10 00 00 40 00 40 11  26 f6 c0 a8 c8 96 c0 a8   ....@.@. &.......
```

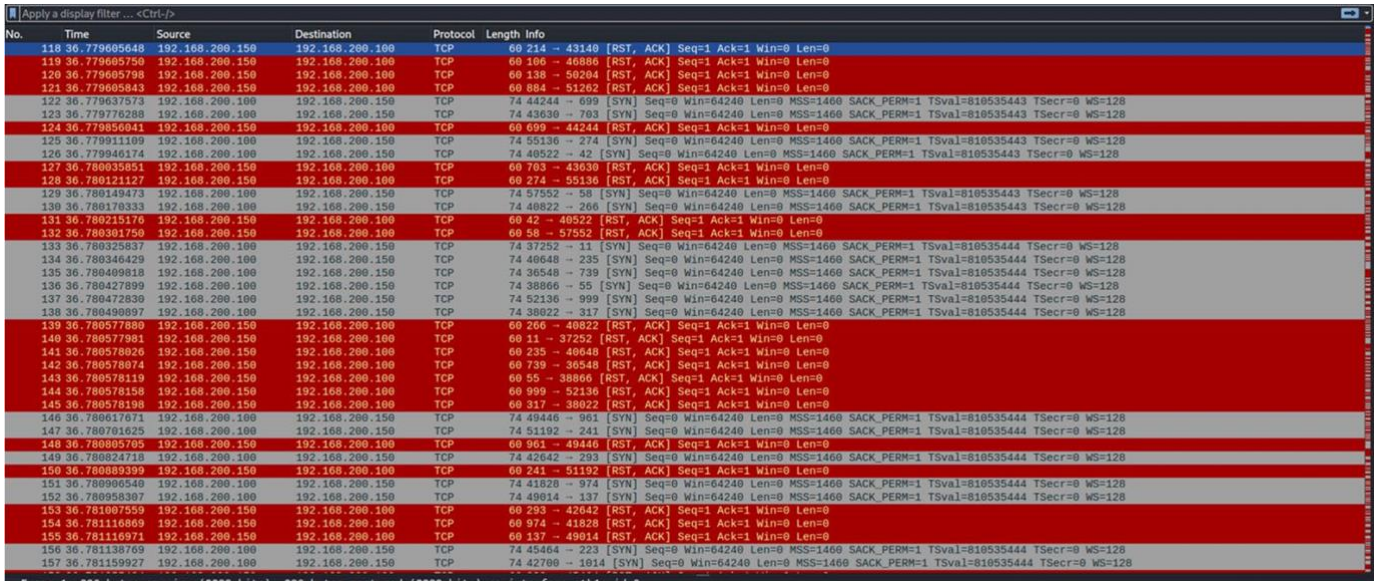


```
Apply a display filter ... <Ctrl-/>
No.  Time          Source           Destination      Protocol Length Info
    40 36.775975876 192.168.200.100 192.168.200.150  TCP      66 55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
    41 36.776005853 192.168.200.100 192.168.200.150  TCP      66 53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
    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=1 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=1 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=1 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=1 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=1 TSval=810535440 TSecr=0 WS=128
    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
    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=1 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=1 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=1 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=1 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=1 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=1 TSval=810535440 TSecr=0 WS=128
    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
    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=1 TSval=810535440 TSecr=0 WS=128
    57 36.776904828 192.168.200.150 192.168.200.100  TCP      74 445 → 33042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64
    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
    59 36.776904961 192.168.200.150 192.168.200.100  TCP      74 139 → 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64
    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
    61 36.776905043 192.168.200.150 192.168.200.100  TCP      74 25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64
    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
    63 36.776905123 192.168.200.150 192.168.200.100  TCP      74 53 → 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64
    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
    65 36.776914772 192.168.200.100 192.168.200.150  TCP      66 33042 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
    66 36.776941020 192.168.200.100 192.168.200.150  TCP      66 46990 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
    67 36.776962320 192.168.200.100 192.168.200.150  TCP      66 60632 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
    68 36.776983878 192.168.200.100 192.168.200.150  TCP      66 37282 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
    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
    70 36.777143014 192.168.200.100 192.168.200.150  TCP      74 56990 → 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
    71 36.777186821 192.168.200.100 192.168.200.150  TCP      74 35638 → 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
    72 36.777302991 192.168.200.100 192.168.200.150  TCP      74 34120 → 98 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
    73 36.777337934 192.168.200.100 192.168.200.150  TCP      74 49780 → 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
    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
    76 36.777473018 192.168.200.100 192.168.200.150  TCP      74 36138 → 580 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
    77 36.777522494 192.168.200.100 192.168.200.150  TCP      74 52428 → 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
    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
```



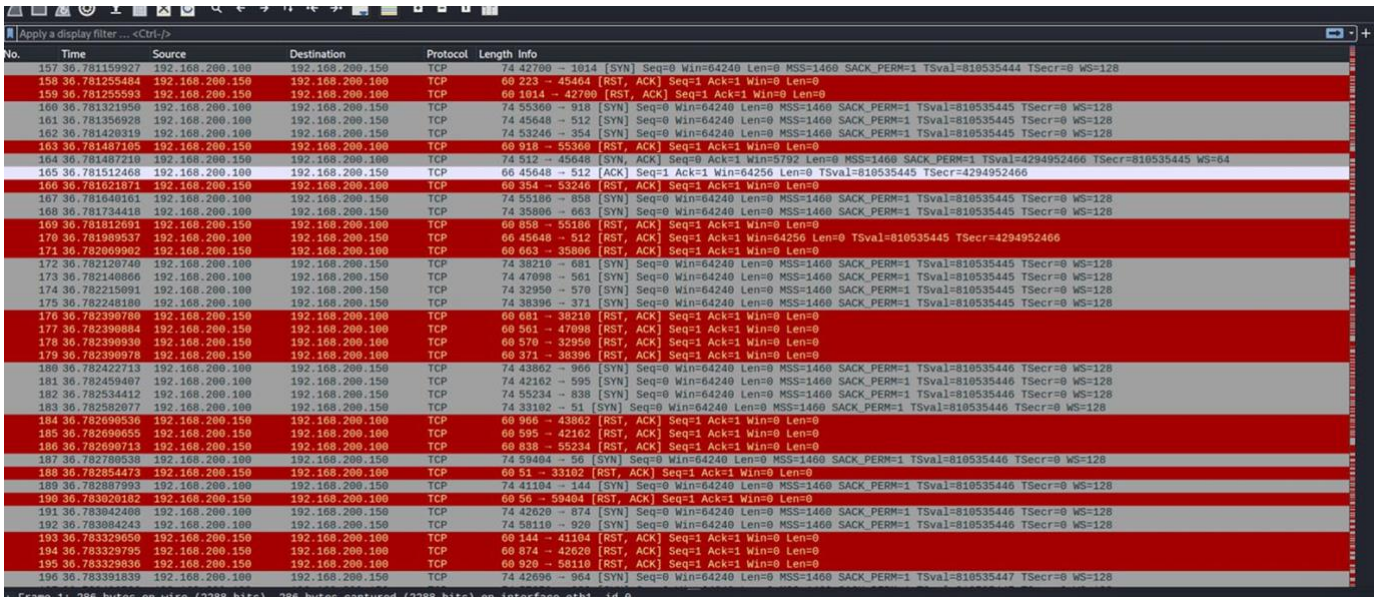
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
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
80	36.777645027	192.168.200.100	192.168.200.150	TCP	74	41874 → 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
81	36.777680898	192.168.200.100	192.168.200.150	TCP	74	51506 → 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
82	36.777758636	192.168.200.150	192.168.200.100	TCP	60	580 → 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83	36.777758696	192.168.200.150	192.168.200.100	TCP	60	962 → 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84	36.777871245	192.168.200.150	192.168.200.100	TCP	60	764 → 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85	36.777871293	192.168.200.150	192.168.200.100	TCP	60	435 → 51506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86	36.777893298	192.168.200.100	192.168.200.150	TCP	66	33042 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
87	36.777912717	192.168.200.100	192.168.200.150	TCP	66	46990 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
88	36.777986759	192.168.200.100	192.168.200.150	TCP	66	60632 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
89	36.778031265	192.168.200.100	192.168.200.150	TCP	66	37282 → 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
90	36.778179978	192.168.200.100	192.168.200.150	TCP	74	51450 → 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
91	36.778200161	192.168.200.100	192.168.200.150	TCP	74	48448 → 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
92	36.778307830	192.168.200.100	192.168.200.150	TCP	74	54566 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
93	36.778385846	192.168.200.150	192.168.200.100	TCP	60	148 → 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94	36.778385948	192.168.200.150	192.168.200.100	TCP	60	806 → 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95	36.778449494	192.168.200.150	192.168.200.100	TCP	60	221 → 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
96	36.778482791	192.168.200.100	192.168.200.150	TCP	74	42420 → 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
97	36.778591226	192.168.200.100	192.168.200.150	TCP	74	34646 → 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
98	36.778614095	192.168.200.100	192.168.200.150	TCP	74	54202 → 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
99	36.778663064	192.168.200.150	192.168.200.100	TCP	60	1007 → 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
100	36.778721080	192.168.200.150	192.168.200.100	TCP	60	206 → 34646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101	36.778759636	192.168.200.100	192.168.200.150	TCP	74	40318 → 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
102	36.778781327	192.168.200.100	192.168.200.150	TCP	74	51276 → 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
103	36.778826294	192.168.200.150	192.168.200.100	TCP	60	131 → 54202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
104	36.778864493	192.168.200.100	192.168.200.150	TCP	74	39566 → 856 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
105	36.778939327	192.168.200.150	192.168.200.100	TCP	60	392 → 40318 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
106	36.778939427	192.168.200.150	192.168.200.100	TCP	60	677 → 51276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
107	36.778983153	192.168.200.100	192.168.200.150	TCP	74	47238 → 84 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
108	36.779029210	192.168.200.150	192.168.200.100	TCP	60	856 → 39566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
109	36.779055243	192.168.200.100	192.168.200.150	TCP	74	56542 → 807 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
110	36.779122299	192.168.200.150	192.168.200.100	TCP	60	84 → 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111	36.779145004	192.168.200.100	192.168.200.150	TCP	74	40138 → 948 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
112	36.779252884	192.168.200.150	192.168.200.100	TCP	60	807 → 56542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
113	36.779273781	192.168.200.100	192.168.200.150	TCP	74	43140 → 214 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
114	36.779309462	192.168.200.100	192.168.200.150	TCP	74	46886 → 106 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
115	36.779354564	192.168.200.150	192.168.200.100	TCP	60	948 → 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
116	36.779378630	192.168.200.100	192.168.200.150	TCP	74	50204 → 138 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
117	36.779397023	192.168.200.100	192.168.200.150	TCP	74	51262 → 884 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
118	36.779605648	192.168.200.150	192.168.200.100	TCP	60	214 → 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0



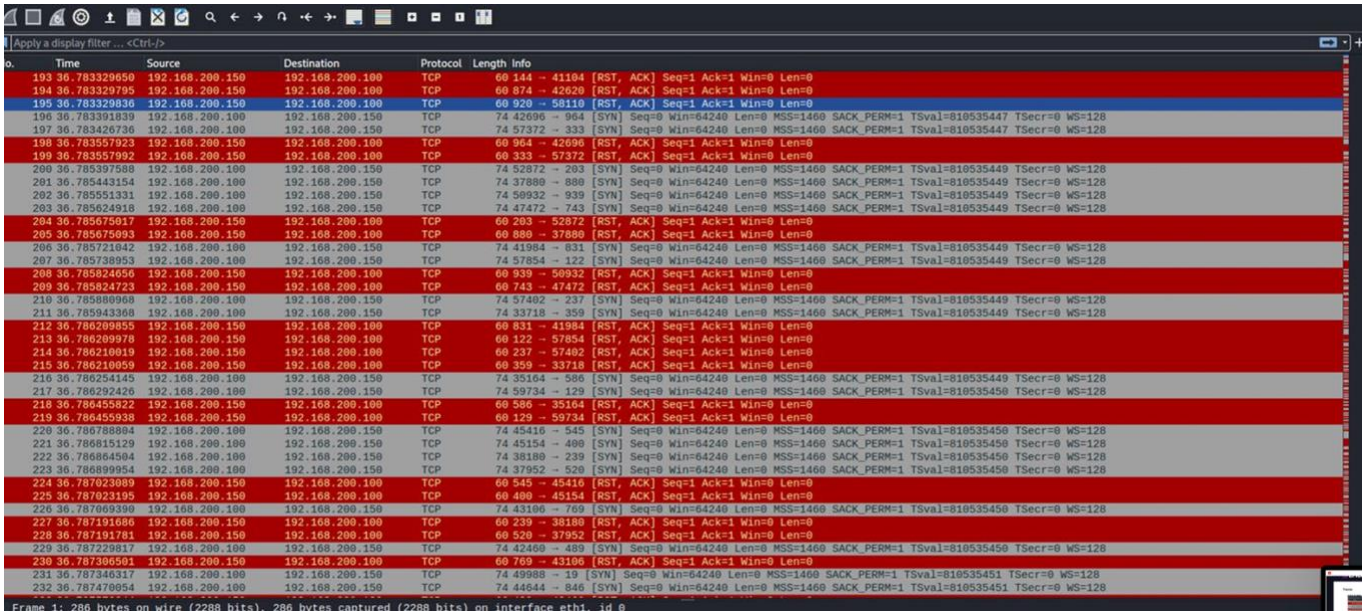
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
118	36.779605648	192.168.200.150	192.168.200.100	TCP	60	214 → 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119	36.779605750	192.168.200.150	192.168.200.100	TCP	60	106 → 46886 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
120	36.779605798	192.168.200.150	192.168.200.100	TCP	60	138 → 50204 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
121	36.779605843	192.168.200.150	192.168.200.100	TCP	60	884 → 51262 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
122	36.779637573	192.168.200.100	192.168.200.150	TCP	74	44244 → 699 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
123	36.779776288	192.168.200.100	192.168.200.150	TCP	74	43630 → 703 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
124	36.779856041	192.168.200.150	192.168.200.100	TCP	60	699 → 44244 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
125	36.779911109	192.168.200.100	192.168.200.150	TCP	74	55136 → 274 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
126	36.779946174	192.168.200.100	192.168.200.150	TCP	74	40522 → 42 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
127	36.780035851	192.168.200.150	192.168.200.100	TCP	60	703 → 43630 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
128	36.780121127	192.168.200.150	192.168.200.100	TCP	60	274 → 55136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
129	36.780149473	192.168.200.100	192.168.200.150	TCP	74	57552 → 58 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
130	36.780170333	192.168.200.100	192.168.200.150	TCP	74	40822 → 266 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
131	36.780215176	192.168.200.150	192.168.200.100	TCP	60	42 → 40522 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
132	36.780301750	192.168.200.150	192.168.200.100	TCP	60	58 → 57552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
133	36.780325837	192.168.200.100	192.168.200.150	TCP	74	37252 → 11 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
134	36.780346429	192.168.200.100	192.168.200.150	TCP	74	40648 → 235 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
135	36.780409818	192.168.200.100	192.168.200.150	TCP	74	36548 → 739 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
136	36.780427899	192.168.200.100	192.168.200.150	TCP	74	38866 → 55 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
137	36.780472830	192.168.200.100	192.168.200.150	TCP	74	52136 → 999 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
138	36.780490897	192.168.200.100	192.168.200.150	TCP	74	38022 → 317 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
139	36.780577880	192.168.200.150	192.168.200.100	TCP	60	266 → 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
140	36.780577981	192.168.200.150	192.168.200.100	TCP	60	11 → 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
141	36.780578026	192.168.200.150	192.168.200.100	TCP	60	235 → 40648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
142	36.780578074	192.168.200.150	192.168.200.100	TCP	60	739 → 36548 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
143	36.780578119	192.168.200.150	192.168.200.100	TCP	60	55 → 38866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
144	36.780578158	192.168.200.150	192.168.200.100	TCP	60	999 → 52136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
145	36.780578198	192.168.200.150	192.168.200.100	TCP	60	317 → 38022 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
146	36.780617671	192.168.200.100	192.168.200.150	TCP	74	49446 → 961 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
147	36.780701625	192.168.200.100	192.168.200.150	TCP	74	51192 → 241 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
148	36.780805705	192.168.200.150	192.168.200.100	TCP	60	961 → 49446 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
149	36.780824718	192.168.200.100	192.168.200.150	TCP	74	42642 → 293 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
150	36.780889399	192.168.200.150	192.168.200.100	TCP	60	241 → 51192 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
151	36.780906540	192.168.200.100	192.168.200.150	TCP	74	41828 → 974 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
152	36.780958307	192.168.200.100	192.168.200.150	TCP	74	49014 → 137 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
153	36.781007559	192.168.200.150	192.168.200.100	TCP	60	293 → 42642 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
154	36.781116869	192.168.200.150	192.168.200.100	TCP	60	974 → 41828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
155	36.781116971	192.168.200.150	192.168.200.100	TCP	60	137 → 49014 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
156	36.781138769	192.168.200.100	192.168.200.150	TCP	74	45464 → 223 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
157	36.781159927	192.168.200.100	192.168.200.150	TCP	74	42700 → 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128



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

No.	Time	Source	Destination	Protocol	Length	Info
157	36.781159927	192.168.200.100	192.168.200.150	TCP	74	42700 → 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
158	36.781255484	192.168.200.150	192.168.200.100	TCP	60	223 → 45464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
159	36.781255593	192.168.200.150	192.168.200.100	TCP	60	1014 → 42700 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
160	36.781321950	192.168.200.100	192.168.200.150	TCP	74	55360 → 918 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
161	36.781356928	192.168.200.100	192.168.200.150	TCP	74	45648 → 512 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
162	36.781420319	192.168.200.100	192.168.200.150	TCP	74	53246 → 354 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
163	36.781487105	192.168.200.150	192.168.200.100	TCP	60	918 → 55360 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
164	36.781487210	192.168.200.150	192.168.200.100	TCP	74	512 → 45648 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535445 WS=64
165	36.781512468	192.168.200.100	192.168.200.150	TCP	66	45648 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
166	36.781621071	192.168.200.150	192.168.200.100	TCP	60	354 → 53246 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
167	36.781640161	192.168.200.100	192.168.200.150	TCP	74	55186 → 858 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
168	36.781734418	192.168.200.100	192.168.200.150	TCP	74	35806 → 663 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
169	36.781812691	192.168.200.150	192.168.200.100	TCP	60	858 → 55186 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
170	36.781989537	192.168.200.100	192.168.200.150	TCP	66	45648 → 512 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
171	36.782069902	192.168.200.150	192.168.200.100	TCP	60	663 → 35806 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
172	36.782120740	192.168.200.100	192.168.200.150	TCP	74	38210 → 681 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
173	36.782140866	192.168.200.100	192.168.200.150	TCP	74	47098 → 561 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
174	36.782215091	192.168.200.100	192.168.200.150	TCP	74	32950 → 570 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
175	36.782248180	192.168.200.100	192.168.200.150	TCP	74	38396 → 371 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
176	36.782390780	192.168.200.150	192.168.200.100	TCP	60	681 → 38210 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
177	36.782390884	192.168.200.150	192.168.200.100	TCP	60	561 → 47098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
178	36.782390930	192.168.200.150	192.168.200.100	TCP	60	570 → 32950 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
179	36.782390978	192.168.200.150	192.168.200.100	TCP	60	371 → 38396 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
180	36.782422713	192.168.200.100	192.168.200.150	TCP	74	43862 → 966 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
181	36.782459407	192.168.200.100	192.168.200.150	TCP	74	42162 → 595 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
182	36.782534412	192.168.200.100	192.168.200.150	TCP	74	55234 → 838 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
183	36.782582077	192.168.200.100	192.168.200.150	TCP	74	33102 → 51 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
184	36.782690536	192.168.200.150	192.168.200.100	TCP	60	966 → 43862 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
185	36.782690655	192.168.200.150	192.168.200.100	TCP	60	595 → 42162 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
186	36.782690713	192.168.200.150	192.168.200.100	TCP	60	838 → 55234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
187	36.782780538	192.168.200.100	192.168.200.150	TCP	74	59404 → 56 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
188	36.782854473	192.168.200.150	192.168.200.100	TCP	60	51 → 33102 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
189	36.782887993	192.168.200.100	192.168.200.150	TCP	74	41104 → 144 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
190	36.783020182	192.168.200.150	192.168.200.100	TCP	60	56 → 59404 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
191	36.783042408	192.168.200.100	192.168.200.150	TCP	74	42620 → 874 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
192	36.783084243	192.168.200.100	192.168.200.150	TCP	74	58110 → 920 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
193	36.783329650	192.168.200.150	192.168.200.100	TCP	60	144 → 41104 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
194	36.783329795	192.168.200.150	192.168.200.100	TCP	60	874 → 42620 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
195	36.783329836	192.168.200.150	192.168.200.100	TCP	60	920 → 58110 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
196	36.783391839	192.168.200.100	192.168.200.150	TCP	74	42696 → 964 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535447 TSecr=0 WS=128



ANALISI:

Dall'analisi delle immagini caricate, vediamo che i pacchetti catturati contengono diverse anomalie, tra cui un numero significativo di pacchetti TCP con flag RST, ACK e SYN inviati in rapida successione. Questa configurazione suggerisce una possibile attività malevola.
Di seguito rispondo ai quesiti richiesti:

1. Identificazione ed analisi degli IOC (Indicator of Compromise)

Gli Indicatori di Compromissione (IOC) identificati nei pacchetti catturati includono:

- Eccessivo numero di pacchetti TCP RST, ACK:

L'host 192.168.200.150 sta inviando numerosi pacchetti RST, ACK al destinatario 192.168.200.100.
Questo potrebbe indicare che il sistema sta cercando di terminare connessioni sospette o sta rispondendo a tentativi di connessione non autorizzati.

- Numerosi pacchetti TCP SYN senza completamento della connessione (SYN flood):
  Si osservano molte richieste TCP SYN senza un completamento del three-way handshake (assenza di pacchetti SYN-ACK seguiti da un ACK).
  Questo è un chiaro sintomo di un attacco SYN flood, che mira a esaurire le risorse del server prendendo di mira la tabella delle connessioni incomplete.

- Frequenza temporale anomala tra i pacchetti
  I pacchetti sono inviati a intervalli estremamente brevi (millisecondi), il che è insolito per una normale comunicazione TCP.
  Questo può indicare uno script automatizzato o un tool di attacco.

Conclusione sugli IOC:

Gli indicatori suggeriscono un attacco di tipo Denial of Service (DoS), molto probabilmente SYN Flood, in corso sulla rete interna tra i due host. L'attaccante potrebbe essere 192.168.200.150, mentre il bersaglio è 192.168.200.100.

2. Ipotesi sui vettori di attacco utilizzati:

Dato il comportamento dei pacchetti osservati, è possibile ipotizzare i seguenti scenari di attacco:

A. SYN Flood Attack:

- L'attaccante inonda il server con pacchetti SYN, senza completare il three-way handshake.
- Questo porta a un esaurimento delle connessioni disponibili sul server, impedendo ad altri utenti legittimi di accedere.

- Questo tipo di attacco è spesso realizzato con botnet, script Python o strumenti come Scapy.

B. Spoofing IP per amplificare l'attacco:

- L'host che sta inviando i pacchetti potrebbe non essere il vero attaccante, ma piuttosto un host compromesso o un IP falsificato.
- Gli attacchi SYN Flood spesso usano IP spoofing per evitare di essere rilevati e per rendere più difficile il blocco a livello firewall.

C. Test di vulnerabilità o attività di scansione malevola:

- Se questi pacchetti non fossero parte di un attacco DoS, potrebbe trattarsi di una scansione aggressiva (es. con Nmap) per cercare porte aperte e servizi vulnerabili.
- Tuttavia, la quantità di pacchetti suggerisce più probabilmente un attacco DoS.

3. Azioni consigliate per mitigare l'attacco e prevenire futuri attacchi:

Per mitigare l'attacco in corso e prevenire futuri attacchi, si consigliano le seguenti azioni:

A. Mitigazione immediata dell'attacco in corso:

- Bloccare l'IP sospetto a livello di firewall
- Se 192.168.200.150 è confermato come attaccante, aggiungere una regola di drop nel firewall per bloccare tutto il traffico in ingresso da quell'IP.

2. Abilitare SYN Cookies:

- SYN Cookies aiutano a prevenire SYN Flood mantenendo le connessioni sotto controllo.

3. Limitare il numero di connessioni per IP:

- Configurare il firewall per limitare il numero di connessioni TCP simultanee dallo stesso IP, ad esempio:

iptables -A INPUT -p tcp --syn -m limit --limit 10/second -j ACCEPT
iptables -A INPUT -p tcp --syn -j DROP

B. Prevenzione di attacchi futuri:

1. Implementare un sistema di rilevamento delle intrusioni (IDS/IPS):

- Strumenti come Suricata o Snort possono rilevare e bloccare attacchi SYN Flood in tempo reale.

2. Analisi forense dell'host attaccante:

- Se l'IP 192.168.200.150 appartiene alla rete interna, potrebbe essere compromesso da malware o controllato da un attaccante.

3. Monitorare i log di sistema e della rete:

- Utilizzare SIEM (Security Information and Event Management) come Splunk, per monitorare traffico sospetto.

Conclusione:

L’analisi dei pacchetti mostra un attacco SYN Flood in corso da 192.168.200.150 verso 192.168.200.100. Questo può portare a disservizi di rete e impatto sulle prestazioni del server.

Per mitigarlo, si consiglia di bloccare l’IP attaccante, abilitare SYN cookies, limitare le connessioni per IP, e implementare un IDS/IPS per rilevare attacchi futuri. Se l’host attaccante fa parte della rete interna, è necessario investigare ulteriormente per verificare una compromissione.