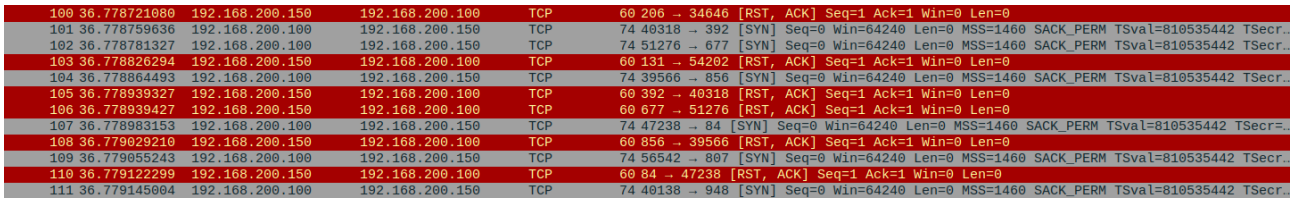
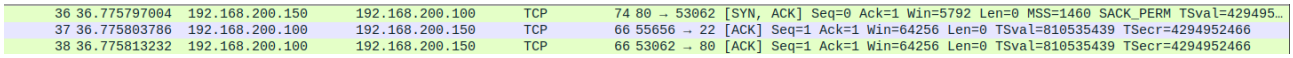
ESERCIZIO 3 SETTIMANA 9



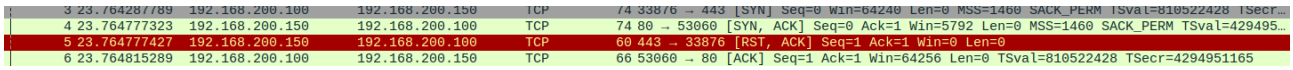
100	36.778721080	192.168.200.150	192.168.200.100	TCP	60 206 → 34646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101	36.778759636	192.168.200.100	192.168.200.150	TCP	74 40318 → 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr…
102	36.778781327	192.168.200.100	192.168.200.150	TCP	74 51276 → 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr…
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 TSval=810535442 TSecr…
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 TSval=810535442 TSecr=…
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 TSval=810535442 TSecr…
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 TSval=810535442 TSecr…

Analizzando questo frame su wireshark possiamo notare una gran quantità di richieste TCP (SYN) da parte dell'attaccante (in grigio) con IP 192.168.200.100 che vengono rifiutate dall'host (in rosso) con IP 192.168.200.150.

Tutte le richieste TCP (SYN) che vengono fatte vengono rifiutate infatti come risposta l'host invia un pacchetto RST-ACK il che indica che la porta è chiusa.



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 TSval=429495…
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



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…
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 TSval=429495…
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

Alcune porte come la 80, la 53062 e la 53060 rispondono con un SYN-ACK, ciò vuol dire che quelle porte sono aperte.

Si può notare che a ogni richiesta viene provata una porta diversa n elevato numero di richieste TCP su un elevato range di porte, può significare che l'attaccante stia facendo una scansione con nmap per esempio.

Come soluzione proporrei di inserire nel firewall delle regole che bloccano l'accesso a quelle porte da parte dell'IP 192.168.200.100, in questo modo l'attaccante non potrà più sfruttare quelle porte per i suoi scopi.