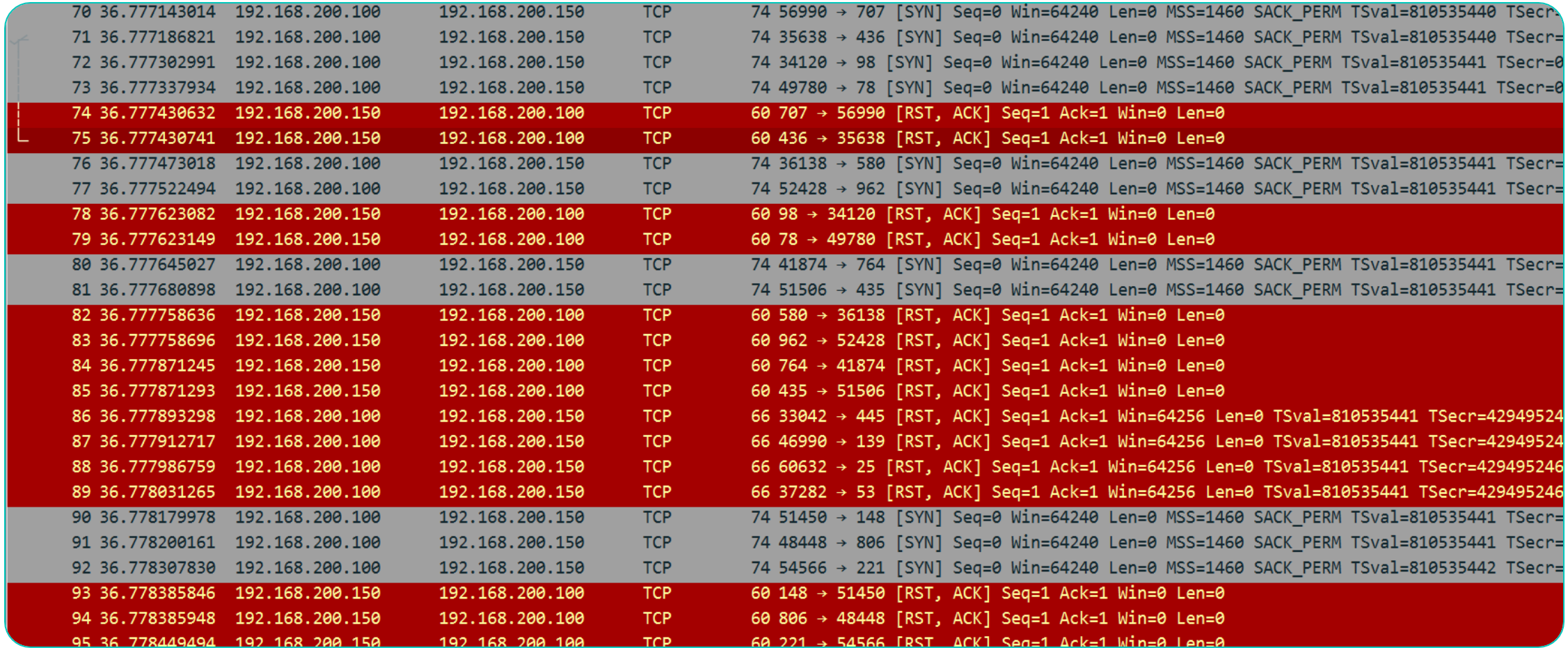
Esercizio S9/L3

Analisi con wireshark



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 TSval=810535440 TSecr=
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 TSval=810535440 TSecr=
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 TSval=810535441 TSecr=0
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 TSval=810535441 TSecr=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
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 TSval=810535441 TSecr=
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 TSval=810535441 TSecr=
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
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 TSval=810535441 TSecr=
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 TSval=810535441 TSecr=
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=42949524
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=42949524
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=429495246
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=429495246
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 TSval=810535441 TSecr=
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 TSval=810535441 TSecr=
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 TSval=810535442 TSecr=
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

Notiamo…

- Come si nota dalle immagini visualizzate in precedenza, notiamo delle richieste SYN da parte dello scanner.
- Ci sono dalla parte evidenziata in rosso le risposte negative alla richiesta perché le porte sono chiuse.

Domande

- 1 Identificare eventuali IOC, ovvero evidenze di attacchi in corso.
- 2 In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati.
- 3 Consigliate un'azione per ridurre gli impatti dell'attacco.

Azioni Consigliate

- Bisognerebbe implementare un firewall che rileva quando esiste una quantità elevata di richieste TCP , bloccando la connessione della macchina che invia la richiesta.
- Trasferire i servizi su porte non note , notando lo scan effettuato si è limitato a scansionare le prima 1024 porte , se i servizi fossero spostati su porte dal range 30.000-50.000 non sarebbero stati trovati dallo scan
- Realizzare un port scan interno per essere sempre al corrente dello stato delle porte aperte.
- Chiudere le porte che non vengono utilizzate.