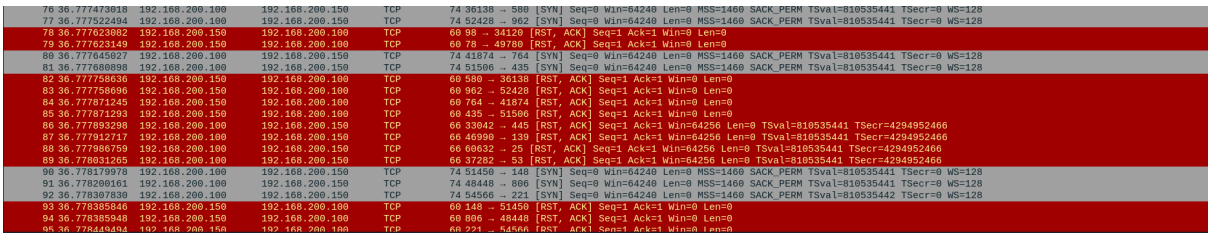
S9L3



```
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=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 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
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=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 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 60032 → 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 36.778170578  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=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 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 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
```

La comunicazione è fra due host con ip 192.168.200.100 e 192.168.200.150

In base ai dati raccolti dalla cattura si può concludere che l'host .100 stia effettuando una scansione
(ad esempio con nmap) per enumerare i servizi attivi sull'host.150

Possiamo arrivare a questa conclusione vedendo come il primo host invii tante richieste SYN su
porte sempre diverse (in rosso vediamo invece le risposte del secondo host)

Oltre a recuperare informazioni che potrebbero essere utili al primo host per lanciare un attacco sul
secondo, questo tipo di traffico potrebbe anche impedire il corretto funzionamento dell'host 2 in
quanto potrebbe congestionare il traffico verso tale macchina da parte di altri utenti legittimi.

Un buon modo per reagire in questo caso sarebbe bloccare l'ip 192.168.200.100 sull'IPS o sul
Firewall (in una situazione aziendale) una volta rilevato il comportamento anomalo. Per evitare casi
simili in futuro sarebbe una buona idea permettere le richieste sulle porte in ascolto della macchina .
150 solo da utenti o ip autorizzati, e negare eventuali altre richieste su altre porte, configurando il
firewall o l'ips di conseguenza.