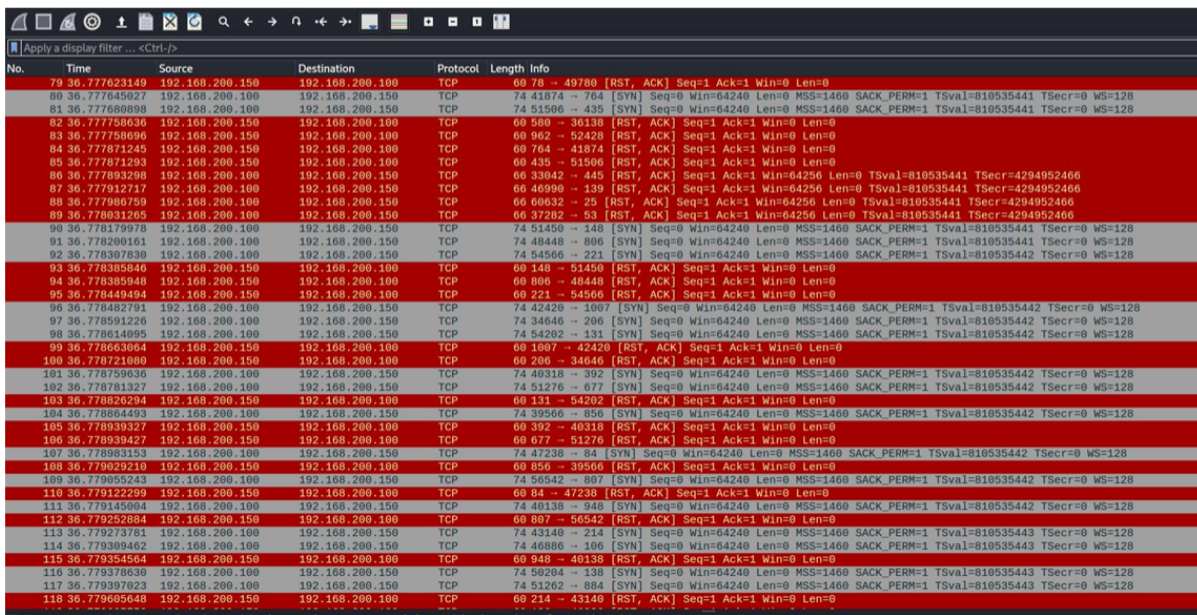


# PRATICA S9/L3

**SCOPO:** Analizzare la cattura di rete effettuate con wireshark e: Indentificare eventuali IOC,ovvero evidenziare gli attacchi in corso. Fare delle ipotesi sui potenziali vettori di attacco utilizzati in base agli IOC trovati. Consigliare un'azione per ridurre gli impatti dell'attacco.

## RISOLUZIONE.



No.	Time	Source	Destination	Protocol	Length	Info
79	36.777023149	192.168.200.150	192.168.200.100	TCP	60	78 → 49760 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80	36.777045027	192.168.200.100	192.168.200.150	TCP	74	41874 → 704 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
81	36.777068938	192.168.200.100	192.168.200.150	TCP	74	51506 → 435 [SYN] Seq=0 Win=0 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	46998 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
88	36.777980759	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=0 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=0 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=0 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=0 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=0 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	54292 → 131 [SYN] Seq=0 Win=0 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=0 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=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
103	36.778839274	192.168.200.150	192.168.200.100	TCP	60	151 → 51276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
104	36.778864493	192.168.200.100	192.168.200.150	TCP	74	39566 → 656 [SYN] Seq=0 Win=0 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=0 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	656 → 39566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
109	36.779055213	192.168.200.100	192.168.200.150	TCP	74	50542 → 897 [SYN] Seq=0 Win=0 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	36.779145084	192.168.200.100	192.168.200.150	TCP	74	40138 → 948 [SYN] Seq=0 Win=0 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	897 → 50542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
113	36.779273781	192.168.200.100	192.168.200.150	TCP	74	43148 → 214 [SYN] Seq=0 Win=0 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	40896 → 106 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
115	36.779354504	192.168.200.150	192.168.200.100	TCP	60	948 → 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
116	36.779378638	192.168.200.100	192.168.200.150	TCP	74	50284 → 138 [SYN] Seq=0 Win=0 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=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
118	36.779685648	192.168.200.150	192.168.200.100	TCP	60	214 → 43148 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Analizzando le schermate della pratica,possiamo vedere che ci da tante informazione come: Tempo ; sorgente ; indirizzo IP dell'attaccante(192.168.200.100); indirizzo IP del target(192.168.200.150) ; protocollo e molte altre informazioni.

## 1-indentificazione eventuali IOC

Come indentificazione IOC possiamo notare sulla schermata sopra un numero elevato di richieste TCP su porte sempre diverse in destinazione.

## PRATICA S9/L3

### 2-)ipotesi su eventuali vettori di attacchi utilizzati

Le richieste TCP ripetute possono essere dovuti a una scansione sul target **192.168.200.150** dall'attaccante **192.168.200.100** ,visto che per alcune righe del target abbiamo risposte positive del target[SYN + ACK] ad indicare che la porta è aperta, per altre ,invece notiamo la risposta [RST + ACK] ad indicare che la porta è chiusa.

### 3-)Azione per ridurre gli impatti dell'attacco

- configurare le policy firewall per bloccare accesso a tutte le porte da parte di quel determinato attaccante.
- impostare un IPS e un IDS per alertare il target se c'è troppe richieste.
- stabilire un honey pot a monte per attirare e inganare l'attaccante.