

## Threat Intelligence & IOC

Data la traccia dell'esercizio ho analizzato la cattura di rete con WireShark e possiamo denotare diverse curiosità.

Ci sono due indirizzi ip **192.168.200.100** e **192.168.200.150** che si scambiano pacchetti nella rete, tutti TCP.

No.	Time	Source	Destination	Protocol	Length	Info
79	0.77722140	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
80	0.77722552	192.168.200.100	192.168.200.150	TCP	74	74 [SYN] 40700 (SYN) Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM TSval=181035441 Tsecr=0 WS=128
81	0.77722600	192.168.200.150	192.168.200.100	TCP	74	74 [ACK] 40700 (ACK) Seq=1 Win=0 Len=0 MSS=1460 SACK_PERM TSval=181035441 Tsecr=0 WS=128
82	0.77722650	192.168.200.100	192.168.200.150	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
83	0.77722680	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
84	0.77722710	192.168.200.100	192.168.200.150	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
85	0.77722740	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
86	0.77722770	192.168.200.100	192.168.200.150	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
87	0.77722800	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
88	0.77722830	192.168.200.100	192.168.200.150	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
89	0.77722860	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
90	0.77722890	192.168.200.100	192.168.200.150	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
91	0.77722920	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
92	0.77722950	192.168.200.100	192.168.200.150	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
93	0.77722980	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
94	0.77723010	192.168.200.100	192.168.200.150	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
95	0.77723040	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
96	0.77723070	192.168.200.100	192.168.200.150	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
97	0.77723100	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
98	0.77723130	192.168.200.100	192.168.200.150	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
99	0.77723160	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
100	0.77723190	192.168.200.100	192.168.200.150	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
101	0.77723220	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
102	0.77723250	192.168.200.100	192.168.200.150	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
103	0.77723280	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
104	0.77723310	192.168.200.100	192.168.200.150	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
105	0.77723340	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
106	0.77723370	192.168.200.100	192.168.200.150	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
107	0.77723400	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
108	0.77723430	192.168.200.100	192.168.200.150	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
109	0.77723460	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
110	0.77723490	192.168.200.100	192.168.200.150	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
111	0.77723520	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
112	0.77723550	192.168.200.100	192.168.200.150	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
113	0.77723580	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
114	0.77723610	192.168.200.100	192.168.200.150	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
115	0.77723640	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
116	0.77723670	192.168.200.100	192.168.200.150	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
117	0.77723700	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
118	0.77723730	192.168.200.100	192.168.200.150	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
119	0.77723760	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
120	0.77723790	192.168.200.100	192.168.200.150	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
121	0.77723820	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
122	0.77723850	192.168.200.100	192.168.200.150	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0
123	0.77723880	192.168.200.150	192.168.200.100	TCP	60	60 [RST] 40700 (RST, ACK) Seq=1 ACK=1 Win=0 Len=0

Secondo il protocollo TCP per far sì che ci sia una connessione vera e propria bisogna completare il 3 way handshake (SYN, ACK, SYN-ACK). In questo caso il 3 way handshake non viene completato mai, c'è invio SYN da parte di 200.100 e risposta ACK ed RST da parte di 200.150 ma nessun completamento. Il tutto si ripete per innumerevoli volte, le righe colorate di rosso segnalano questo problema.

Tutto ciò denota un probabile invio massivo dalla macchina 192.168.200.100 di pacchetti SYN, questo tipo di traffico potrebbe essere un attacco **SYN Flood** dove la macchina attaccante riempie di connessioni la macchina vittima per far sì che causi un blocco nell'utilizzo della stessa (un Denial of Service - DoS). Altra ipotesi plausibile potrebbe essere una ricognizione molto aggressiva, ovvero un **port scanning intenso**.

E' importante notare che la macchina attaccata è una Metasploitable, quindi molto vulnerabile non essendo di ultima generazione.

```

Packet offset: 0 bytes
Source name: METASPLOITABLE<00> (Workstation/Redirector)
Destination name: WORKGROUP<id> (Local Master Browser)

```

Di conseguenza possiamo affermare che:

- L'elevato numero di pacchetti SYN e l'assenza di pacchetti che completano il handshake (ACK) sono segnali di un comportamento malevolo da parte della macchina **192.168.200.100**
- Non ci sono prove che **192.168.200.150** stia inviando traffico simile verso 192.168.200.100, anzi sembra reagire in modo difensivo cercando di chiudere connessioni utili con RST (Reset Connection).

**Cosa fare per mitigare attacchi di questo tipo?**

In questo caso la cosa migliore da fare sarebbe bloccare l'ip sorgente dell'attacco (200.100) tramite il firewall o IDS/IPS.

Per evitare attacchi di questo tipo in futuro è sempre meglio aggiornare i dispositivi, mantenere la rete controllata ed impostare limitazioni di richieste SYN da un singolo indirizzo IP.