

Dalla cattura notiamo che ci sono un numero elevato di richieste TCP (SYN) su porte sempre diverse il che potrebbe significare un attacco in corso da 192.168.200.100 verso l'host target 192.168.200.150.

118	36.779605648	192.168.200.150	192.168.200.100	TCP	60 214 → 43140	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119	36.779605750	192.168.200.150	192.168.200.100	TCP	60 106 → 46886	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
120	36.779605798	192.168.200.150	192.168.200.100	TCP	60 138 → 50204	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
121	36.779605843	192.168.200.150	192.168.200.100	TCP	60 884 → 51262	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
122	36.779637573	192.168.200.100	192.168.200.150	TCP	74 44244 → 699	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F
123	36.779776288	192.168.200.100	192.168.200.150	TCP	74 43630 → 703	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F
124	36.779856041	192.168.200.150	192.168.200.100	TCP	60 699 → 44244	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
125	36.779911109	192.168.200.100	192.168.200.150	TCP	74 55136 → 274	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F
126	36.779946174	192.168.200.100	192.168.200.150	TCP	74 40522 → 42	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F
127	36.780035851	192.168.200.150	192.168.200.100	TCP	60 703 → 43630	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
128	36.780121127	192.168.200.150	192.168.200.100	TCP	60 274 → 55136	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
129	36.780149473	192.168.200.100	192.168.200.150	TCP	74 57552 → 58	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F
130	36.780170333	192.168.200.100	192.168.200.150	TCP	74 40822 → 266	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F
131	36.780215176	192.168.200.150	192.168.200.100	TCP	60 42 → 40522	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
132	36.780301750	192.168.200.150	192.168.200.100	TCP	60 58 → 57552	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
133	36.780325837	192.168.200.100	192.168.200.150	TCP	74 37252 → 11	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F
134	36.780346429	192.168.200.100	192.168.200.150	TCP	74 40648 → 235	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F
135	36.780409818	192.168.200.100	192.168.200.150	TCP	74 36548 → 739	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F
136	36.780427899	192.168.200.100	192.168.200.150	TCP	74 38866 → 55	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F
137	36.780472830	192.168.200.100	192.168.200.150	TCP	74 52136 → 999	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F
138	36.780490897	192.168.200.100	192.168.200.150	TCP	74 38022 → 317	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F
139	36.780577880	192.168.200.150	192.168.200.100	TCP	60 266 → 40822	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
140	36.780577981	192.168.200.150	192.168.200.100	TCP	60 11 → 37252	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
141	36.780578026	192.168.200.150	192.168.200.100	TCP	60 235 → 40648	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
142	36.780578074	192.168.200.150	192.168.200.100	TCP	60 739 → 36548	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
143	36.780578119	192.168.200.150	192.168.200.100	TCP	60 55 → 38866	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
144	36.780578158	192.168.200.150	192.168.200.100	TCP	60 999 → 52136	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
145	36.780578198	192.168.200.150	192.168.200.100	TCP	60 317 → 38022	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
146	36.780617671	192.168.200.100	192.168.200.150	TCP	74 49446 → 961	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F
147	36.780701625	192.168.200.100	192.168.200.150	TCP	74 51192 → 241	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F
148	36.780805705	192.168.200.150	192.168.200.100	TCP	60 961 → 49446	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
149	36.780824718	192.168.200.100	192.168.200.150	TCP	74 42642 → 293	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F
150	36.780889399	192.168.200.150	192.168.200.100	TCP	60 241 → 51192	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
151	36.780906540	192.168.200.100	192.168.200.150	TCP	74 41828 → 974	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F
152	36.780958307	192.168.200.100	192.168.200.150	TCP	74 49014 → 137	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F
153	36.781007559	192.168.200.150	192.168.200.100	TCP	60 293 → 42642	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
154	36.781116869	192.168.200.150	192.168.200.100	TCP	60 974 → 41828	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
155	36.781116971	192.168.200.150	192.168.200.100	TCP	60 137 → 49014	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
156	36.781138769	192.168.200.100	192.168.200.150	TCP	74 45464 → 223	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F
157	36.781159927	192.168.200.100	192.168.200.150	TCP	74 42700 → 1014	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F

Questa ipotesi è supportata dal fatto che per alcune righe della cattura vediamo 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. Lato target, si potrebbero configurare delle regole firewall per respingere le richieste in entrata dall'host 192.168.200.100.

Potremmo configurare delle policy firewall per bloccare accesso a tutte le porta da parte di quel determinato attaccante, in modo tale da evitare che informazioni circa porta / servizi in ascolto finiscano nella mani dell'attaccante.