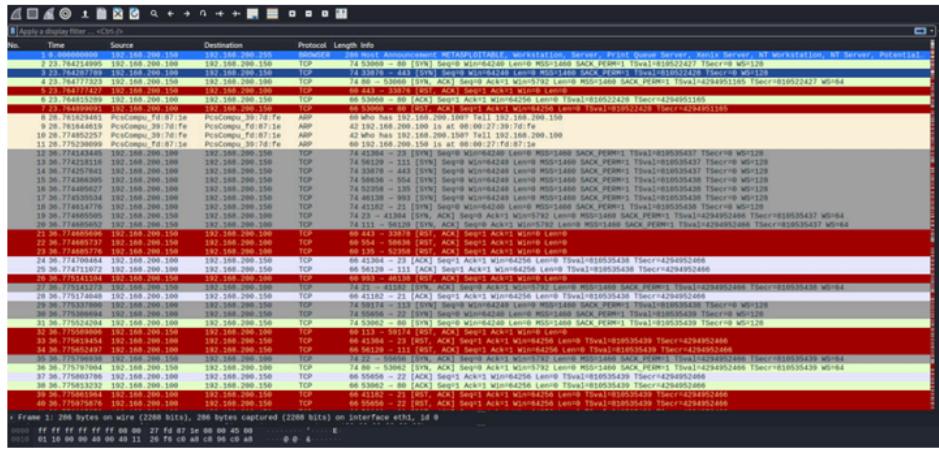


S9L5

Introduzione

Durante l'esercizio pratico sono stati analizzati i dati di una cattura di rete al fine di identificare Indicatori di Compromissione (IOC), formulare ipotesi sui potenziali vettori di attacco e consigliare azioni per mitigare gli impatti dell'attacco attuale ed eventuali futuri. La cattura di rete è stata esaminata tramite una serie di screenshot che mostrano traffico anomalo. L'obiettivo è fornire una spiegazione chiara e semplice di ogni osservazione rilevata.

Svolgimento



6

Pagina 1

Dalla prima serie di screenshot emerge un pattern ricorrente di pacchetti TCP tra gli indirizzi IP 192.168.200.150 (sorgente) e 192.168.200.100 (destinazione).

- **Tipologia di traffico:**
 - Numerosi pacchetti con flag **RST/ACK** (Reset/Acknowledge).
 - Sequenze SYN ripetute con alcune risposte SYN-ACK. Tuttavia, molte connessioni non vengono completate, suggerendo un problema di saturazione o gestione del traffico.
 - Righe in giallo (8-20): Questi pacchetti rappresentano richieste TCP SYN. La colorazione gialla evidenzia che il server non sta rispondendo correttamente alle richieste, forse a causa della saturazione. Questo comportamento è tipico di un attacco SYN Flood, dove molte richieste SYN vengono inviate senza completare le connessioni.
- **Indicazioni preliminari:** L'elevata frequenza dei pacchetti SYN suggerisce un tentativo deliberato di sovraccaricare il server, bloccandone il normale funzionamento.

No.	Time	Source	Destination	Protocol	Length	Info
40	36.775975076	192.168.200.100	192.168.200.150	TCP	66 5565 - 22 [RST, ACK] Seq=1 Ack=1 Win=64250 Len=0 Tsvl=810535439 Tscr=8294952466	
41	36.776005853	192.168.200.100	192.168.200.150	TCP	66 5565 - 23 [SYN, ACK] Seq=1 Ack=1 Win=64250 Len=0 Tsvl=810535439 Tscr=8294952466	
42	36.776037839	192.168.200.100	192.168.200.150	TCP	74 50561 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535437 Tscr=80 WS=128	
43	36.776233880	192.168.200.100	192.168.200.150	TCP	74 54220 - 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535439 Tscr=80 WS=128	
44	36.776330610	192.168.200.100	192.168.200.150	TCP	74 34649 - 597 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=80 WS=128	
45	36.776427059	192.168.200.100	192.168.200.150	TCP	74 50561 - 200 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=80 WS=128	
46	36.776429590	192.168.200.100	192.168.200.150	TCP	74 49814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=80 WS=128	
47	36.776451284	192.168.200.150	192.168.200.100	TCP	60 199 - 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
48	36.776451357	192.168.200.150	192.168.200.100	TCP	60 995 - 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
49	36.776478201	192.168.200.100	192.168.200.150	TCP	74 50561 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535437 Tscr=80 WS=128	
50	36.776500000	192.168.200.100	192.168.200.150	TCP	74 34649 - 597 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=80 WS=128	
51	36.776512221	192.168.200.100	192.168.200.150	TCP	74 60632 - 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=80 WS=128	
52	36.776568606	192.168.200.100	192.168.200.150	TCP	74 49654 - 118 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=80 WS=128	
53	36.776617271	192.168.200.100	192.168.200.150	TCP	74 37282 - 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=80 WS=128	
54	36.776620000	192.168.200.100	192.168.200.150	TCP	74 50561 - 200 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=80 WS=128	
55	36.776813123	192.168.200.150	192.168.200.100	TCP	60 597 - 34649 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
56	36.776843423	192.168.200.100	192.168.200.150	TCP	74 51534 - 487 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=80 WS=128	
57	36.776904828	192.168.200.100	192.168.200.150	TCP	74 445 - 33842 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=80 WS=128	
58	36.776904922	192.168.200.150	192.168.200.100	TCP	60 256 - 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
59	36.776905043	192.168.200.100	192.168.200.150	TCP	74 50561 - 200 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=80 WS=128	
60	36.776905084	192.168.200.100	192.168.200.150	TCP	60 143 - 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
61	36.776905083	192.168.200.100	192.168.200.150	TCP	74 459 - 60633 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=82494952466 Tscr=810535440 WS=64	
62	36.776905082	192.168.200.100	192.168.200.150	TCP	60 110 - 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
63	36.776905107	192.168.200.100	192.168.200.150	TCP	74 459 - 60633 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0	
64	36.776905107	192.168.200.150	192.168.200.100	TCP	60 500 - 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
65	36.776914772	192.168.200.100	192.168.200.150	TCP	60 33842 - 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535440 Tscr=82494952466	
66	36.776914820	192.168.200.100	192.168.200.150	TCP	66 46990 - 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535440 Tscr=82494952466	
67	36.776914820	192.168.200.100	192.168.200.150	TCP	66 60632 - 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535440 Tscr=82494952466	
68	36.776914820	192.168.200.100	192.168.200.150	TCP	66 60632 - 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535440 Tscr=82494952466	
69	36.777118081	192.168.200.150	192.168.200.100	TCP	60 487 - 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
70	36.777143014	192.168.200.100	192.168.200.150	TCP	74 50990 - 56990 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=82494952466	
71	36.777186621	192.168.200.100	192.168.200.150	TCP	74 35635 - 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=80 WS=128	
72	36.777186621	192.168.200.100	192.168.200.150	TCP	74 459 - 60633 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0	
73	36.777186621	192.168.200.100	192.168.200.150	TCP	74 459 - 60633 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=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	36.777436318	192.168.200.100	192.168.200.150	TCP	74 36135 - 50638 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535441 Tscr=80 WS=128	
77	36.777436318	192.168.200.100	192.168.200.150	TCP	74 36135 - 50638 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0	
78	36.777623982	192.168.200.100	192.168.200.150	TCP	60 99 - 34129 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
79	36.777623149	192.168.200.100	192.168.200.150	TCP	60 78 - 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	

7

Pagina 2

La seconda schermata mostra un incremento del numero di connessioni TCP che non riescono a completarsi. Questo rafforza l'ipotesi di un attacco in corso.

- **Osservazioni principali:**
 - L'indirizzo IP 192.168.200.150 continua a inviare richieste SYN ripetute al server.
 - Non vi è alcuna risposta SYN-ACK da parte del server, il che implica che la connessione non viene mai stabilita.
 - Il traffico appare automatizzato, con richieste regolari e uniformi, il che suggerisce l'uso di uno script o di un tool per generare l'attacco.
- **Possibili effetti:** Questo comportamento può portare a un esaurimento delle risorse del server, rendendolo incapace di rispondere a richieste legittime.

No.	Time	Source	Destination	Protocol	Length	Info
79	36.777022949	192.168.200.150	192.168.200.100	TCP	60 78 - 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
80	36.777022949	192.168.200.100	192.168.200.150	TCP	74 51508 - 439 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535441 Tscr=80 WS=128	
82	36.777058630	192.168.200.150	192.168.200.100	TCP	60 588 - 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
83	36.777058696	192.168.200.100	192.168.200.150	TCP	60 962 - 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
84	36.777071245	192.168.200.150	192.168.200.100	TCP	60 46990 - 41566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
85	36.777071245	192.168.200.100	192.168.200.150	TCP	60 456 - 41566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
86	36.777093293	192.168.200.150	192.168.200.100	TCP	66 33942 - 44 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535441 Tscr=82494952466	
87	36.777192171	192.168.200.100	192.168.200.150	TCP	60 110 - 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
88	36.777192171	192.168.200.150	192.168.200.100	TCP	66 60632 - 29 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535441 Tscr=82494952466	
89	36.777192171	192.168.200.100	192.168.200.150	TCP	66 60632 - 29 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535441 Tscr=82494952466	
90	36.777192171	192.168.200.150	192.168.200.100	TCP	66 60632 - 29 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535441 Tscr=82494952466	
91	36.777206161	192.168.200.100	192.168.200.150	TCP	74 48448 - 880 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=80 WS=128	
92	36.777206161	192.168.200.100	192.168.200.150	TCP	74 54202 - 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=80 WS=128	
93	36.777206161	192.168.200.150	192.168.200.100	TCP	60 51458 - 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
94	36.777385940	192.168.200.150	192.168.200.100	TCP	68 886 - 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
95	36.777385940	192.168.200.100	192.168.200.150	TCP	68 221 - 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
96	36.777428731	192.168.200.100	192.168.200.150	TCP	74 42420 - 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535442 Tscr=80 WS=128	
97	36.777428731	192.168.200.150	192.168.200.100	TCP	74 34649 - 880 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535442 Tscr=80 WS=128	
98	36.777428731	192.168.200.100	192.168.200.150	TCP	74 54202 - 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535442 Tscr=80 WS=128	
99	36.778658664	192.168.200.150	192.168.200.100	TCP	60 1607 - 42428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
100	36.778658664	192.168.200.100	192.168.200.150	TCP	60 208 - 34649 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
101	36.778658664	192.168.200.150	192.168.200.100	TCP	74 48448 - 880 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535442 Tscr=80 WS=128	
102	36.778813272	192.168.200.100	192.168.200.150	TCP	74 51276 - 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535442 Tscr=80 WS=128	
103	36.778813272	192.168.200.150	192.168.200.100	TCP	60 131 - 54262 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
104	36.778844973	192.168.200.100	192.168.200.150	TCP	74 35956 - 850 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535442 Tscr=80 WS=128	
105	36.778844973	192.168.200.150	192.168.200.100	TCP	60 1607 - 42428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
106	36.778839427	192.168.200.100	192.168.200.150	TCP	68 677 - 51767 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
107	36.778839427	192.168.200.150	192.168.200.100	TCP	74 47238 - 84 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535442 Tscr=80 WS=128	
108	36.778922109	192.168.200.100	192.168.200.150	TCP	68 856 - 39566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
109	36.779122299	192.168.200.150	192.168.200.100	TCP	60 84 - 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
110	36.779145904	192.168.200.100	192.168.200.150	TCP	74 49138 - 948 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535442 Tscr=80 WS=128	
112	36.779252884	192.168.200.150	192.168.200.100	TCP	60 887 - 56542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
113	36.779252884	192.168.200.100	192.168.200.150	TCP	74 48448 - 880 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535443 Tscr=80 WS=128	
114	36.779386462	192.168.200.100	192.168.200.150	TCP	74 46889 - 1000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535443 Tscr=80 WS=128	
115	36.779385564	192.168.200.150	192.168.200.100	TCP	68 948 - 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
116	36.779386393	192.168.200.100	192.168.200.150	TCP	74 56204 - 130 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535443 Tscr=80 WS=128	
117	36.779397023	192.168.200.100	192.168.200.150	TCP	74 51262 - 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535443 Tscr=80 WS=128	
118	36.779685640	192.168.200.150	192.168.200.100	TCP	68 214 - 43148 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	

8

Pagina 3

Nel terzo screenshot si osserva che il traffico anomalo persiste, con una quantità significativa di pacchetti TCP caratterizzati da flag **RST/ACK**

- **Ulteriori dettagli:**
 - La destinazione (192.168.200.100) continua a rispondere con pacchetti RST/ACK, ma non riesce a gestire efficacemente le richieste SYN provenienti dal client.
 - La ripetizione del pattern suggerisce che il server è sotto pressione costante, il che potrebbe comportare rallentamenti o blocchi completi del servizio.
- **Indicazioni:** Questo tipo di comportamento è un chiaro segnale di attacco, confermando la presenza di un tentativo di saturazione delle risorse del server.

Apply a display filter ... <Ctrl+>/						
No.	Time	Sources	Destination	Protocol	Length	Info
118	36.779865448	192.168.200.159	192.168.200.100	TCP	69 314 - 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
119	36.779865750	192.168.200.158	192.168.200.100	TCP	69 106 - 46886 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
120	36.779865798	192.168.200.158	192.168.200.100	TCP	69 138 - 50284 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
121	36.779865843	192.168.200.158	192.168.200.100	TCP	69 884 - 51260 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
122	36.779865793	192.168.200.100	192.168.200.159	TCP	74 439644 - 689 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM=1 TSval=810535443 TSerr=0 WS=128	
123	36.779865794	192.168.200.158	192.168.200.100	TCP	74 439644 - 689 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM=1 TSval=810535443 TSerr=0 WS=128	
124	36.779865641	192.168.200.158	192.168.200.100	TCP	69 699 - 44244 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
125	36.779911109	192.168.200.100	192.168.200.158	TCP	74 55136 - 274 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM=1 TSval=810535443 TSerr=0 WS=128	
126	36.779946174	192.168.200.100	192.168.200.158	TCP	74 489522 - 42 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM=1 TSval=810535443 TSerr=0 WS=128	
127	36.780021159	192.168.200.158	192.168.200.100	TCP	69 106 - 45216 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
128	36.780021177	192.168.200.158	192.168.200.100	TCP	69 274 - 55136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
129	36.780149473	192.168.200.100	192.168.200.158	TCP	74 57582 - 58 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM=1 TSval=810535443 TSerr=0 WS=128	
130	36.780178333	192.168.200.100	192.168.200.158	TCP	74 48822 - 57524 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
131	36.780215176	192.168.200.158	192.168.200.100	TCP	74 48822 - 40522 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
132	36.780215177	192.168.200.158	192.168.200.100	TCP	69 42 - 40522 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
133	36.780215178	192.168.200.158	192.168.200.100	TCP	69 59 - 40522 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
134	36.780346423	192.168.200.158	192.168.200.158	TCP	74 37252 - 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM=1 TSval=810535444 TSerr=0 WS=128	
134	36.780346429	192.168.200.158	192.168.200.158	TCP	74 48648 - 235 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM=1 TSval=810535444 TSerr=0 WS=128	
135	36.780499818	192.168.200.100	192.168.200.158	TCP	74 36548 - 739 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM=1 TSval=810535444 TSerr=0 WS=128	
136	36.780499899	192.168.200.100	192.168.200.158	TCP	74 38948 - 55 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM=1 TSval=810535444 TSerr=0 WS=128	
136	36.780572309	192.168.200.100	192.168.200.158	TCP	74 38948 - 55 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM=1 TSval=810535444 TSerr=0 WS=128	
138	36.780499897	192.168.200.100	192.168.200.158	TCP	74 38922 - 317 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM=1 TSval=810535444 TSerr=0 WS=128	
139	36.780577888	192.168.200.158	192.168.200.100	TCP	69 266 - 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
140	36.780577981	192.168.200.158	192.168.200.100	TCP	60 11 - 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
141	36.780577982	192.168.200.158	192.168.200.100	TCP	60 285 - 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
142	36.780577984	192.168.200.158	192.168.200.100	TCP	69 69 - 36540 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
143	36.780578119	192.168.200.158	192.168.200.100	TCP	69 55 - 38866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
144	36.780578158	192.168.200.158	192.168.200.100	TCP	69 999 - 52130 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
145	36.780578198	192.168.200.158	192.168.200.100	TCP	69 317 - 38022 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
145	36.780578199	192.168.200.158	192.168.200.100	TCP	74 48646 - 902 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM=1 TSval=810535444 TSerr=0 WS=128	
147	36.780751626	192.168.200.100	192.168.200.158	TCP	74 51197 - 236 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM=1 TSval=810535444 TSerr=0 WS=128	
148	36.780885795	192.168.200.158	192.168.200.100	TCP	69 961 - 49440 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
149	36.780824718	192.168.200.100	192.168.200.158	TCP	74 42642 - 293 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM=1 TSval=810535444 TSerr=0 WS=128	
150	36.780885999	192.168.200.158	192.168.200.100	TCP	69 241 - 51199 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
150	36.780885999	192.168.200.158	192.168.200.100	TCP	69 241 - 51199 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
152	36.780958397	192.168.200.100	192.168.200.158	TCP	74 48914 - 236 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM=1 TSval=810535444 TSerr=0 WS=128	
153	36.781007559	192.168.200.158	192.168.200.100	TCP	69 293 - 42642 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
154	36.781116869	192.168.200.158	192.168.200.100	TCP	69 974 - 41828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
155	36.781116971	192.168.200.158	192.168.200.100	TCP	69 137 - 49014 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
156	36.781138769	192.168.200.100	192.168.200.158	TCP	74 45464 - 223 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM=1 TSval=810535444 TSerr=0 WS=128	
157	36.781139027	192.168.200.100	192.168.200.158	TCP	74 42798 - 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM=1 TSval=810535444 TSerr=0 WS=128	

9

Pagina 4

La quarta schermata mostra che il pattern di traffico anomalo continua senza variazioni significative. Questo indica che l'attacco è persistente e mirato.

- **Osservazioni chiave:**
 - Lo stesso indirizzo IP sorgente (192.168.200.150) è responsabile di tutto il traffico anomalo.
 - Non vi sono segni di traffico legittimo tra le richieste SYN.
- **Impatto sul server:**
 - Il server non è in grado di elaborare traffico legittimo, poiché tutte le sue risorse sono impegnate a gestire richieste maliziose.
 - Questo potrebbe causare un blocco completo del servizio per gli utenti legittimi.

No	Time	Source	Destination	Protocol	Length	Info
157	30.7.8115927	192.168.200.160	192.168.200.150	TCP	74	1814 - 1814 [SYN] Seq=0 Win=4240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535444 Tsecr=0 WS=128
158	30.7.812155484	192.168.200.150	192.168.200.100	TCP	69	223 - 45464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
159	30.7.812155500	192.168.200.100	192.168.200.150	TCP	69	223 - 45464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
160	30.7.812155500	192.168.200.100	192.168.200.150	TCP	74	53508 - 5181 [SYN] Seq=0 Win=4240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535445 Tsecr=0 WS=128
161	30.7.81356528	192.168.200.160	192.168.200.150	TCP	74	45468 - 512 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535445 Tsecr=0 WS=128
162	30.7.81420319	192.168.200.160	192.168.200.150	TCP	74	53246 - 354 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535445 Tsecr=0 WS=128
163	30.7.81420319	192.168.200.160	192.168.200.150	TCP	74	53246 - 354 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535445 Tsecr=0 WS=128
164	30.7.81420319	192.168.200.160	192.168.200.150	TCP	74	5312 - 45648 [SYN] Seq=1 Ack=1 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535445 Tsecr=0 WS=64
165	30.7.81420319	192.168.200.160	192.168.200.150	TCP	66	45468 - 512 [ACK] Seq=1 Ack=1 Win=0 Len=0 Tsvl=810535445 Tsecr=4294952466 Tsvl=810535445 WS=64
166	30.7.81621971	192.168.200.150	192.168.200.100	TCP	69	354 - 53246 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
167	30.7.81734418	192.168.200.160	192.168.200.150	TCP	74	53596 - 563 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535445 Tsecr=0 WS=128
168	30.7.81712691	192.168.200.160	192.168.200.150	TCP	68	858 - 55186 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
169	30.7.81889537	192.168.200.160	192.168.200.150	TCP	68	45468 - 512 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 Tsvl=810535445 Tsecr=4294952466
170	30.7.81889537	192.168.200.160	192.168.200.150	TCP	69	45468 - 512 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535445 Tsecr=0 WS=128
171	30.7.81927476	192.168.200.150	192.168.200.100	TCP	74	38218 - 581 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535445 Tsecr=0 WS=128
172	30.7.81927476	192.168.200.150	192.168.200.100	TCP	74	47698 - 561 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535445 Tsecr=0 WS=128
173	30.7.82140866	192.168.200.160	192.168.200.150	TCP	74	47698 - 561 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535445 Tsecr=0 WS=128
174	30.7.82215091	192.168.200.160	192.168.200.150	TCP	74	47698 - 561 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535445 Tsecr=0 WS=128
175	30.7.82215091	192.168.200.160	192.168.200.150	TCP	74	47698 - 561 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535445 Tsecr=0 WS=128
176	30.7.82359780	192.168.200.150	192.168.200.100	TCP	68	681 - 38210 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
177	30.7.82359780	192.168.200.160	192.168.200.100	TCP	68	561 - 47988 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
178	30.7.82359939	192.168.200.160	192.168.200.100	TCP	68	578 - 32956 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
179	30.7.82359939	192.168.200.160	192.168.200.100	TCP	68	45468 - 512 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
180	30.7.82359939	192.168.200.160	192.168.200.150	TCP	74	45502 - 565 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535446 Tsecr=0 WS=128
181	30.7.82459407	192.168.200.160	192.168.200.150	TCP	74	42162 - 595 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535446 Tsecr=0 WS=128
182	30.7.82521012	192.168.200.160	192.168.200.150	TCP	74	55234 - 838 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535446 Tsecr=0 WS=128
183	30.7.82521012	192.168.200.160	192.168.200.150	TCP	74	55234 - 838 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535446 Tsecr=0 WS=128
184	30.7.82699536	192.168.200.150	192.168.200.100	TCP	68	966 - 43862 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
185	30.7.82699555	192.168.200.160	192.168.200.100	TCP	68	595 - 42162 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
186	30.7.82699713	192.168.200.160	192.168.200.100	TCP	68	838 - 55234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
187	30.7.82699713	192.168.200.160	192.168.200.150	TCP	68	45468 - 512 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
188	30.7.82699713	192.168.200.160	192.168.200.150	TCP	68	51 - 33102 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
189	30.7.82687993	192.168.200.160	192.168.200.150	TCP	74	41104 - 144 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535446 Tsecr=0 WS=128
190	30.7.82687993	192.168.200.160	192.168.200.100	TCP	68	56 - 39494 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
191	30.7.82687993	192.168.200.160	192.168.200.150	TCP	74	45502 - 565 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535446 Tsecr=0 WS=128
192	30.7.83884243	192.168.200.160	192.168.200.150	TCP	74	58110 - 920 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535446 Tsecr=0 WS=128
193	30.7.83884243	192.168.200.160	192.168.200.150	TCP	68	928 - 41104 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
194	30.7.83329795	192.168.200.160	192.168.200.150	TCP	68	874 - 42626 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
195	30.7.83329795	192.168.200.160	192.168.200.150	TCP	68	874 - 42626 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
196	30.7.83331339	192.168.200.160	192.168.200.150	TCP	74	42696 - 364 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535446 Tsecr=0 WS=128

10

Pagina 5

Le ultime schermate confermano che l'attacco è consistente e che l'obiettivo è saturare il server con un attacco **TCP SYN Flood**.

No	Time	Source	Destination	Protocol	Length	Info
189	30.7.83326750	192.168.200.160	192.168.200.150	TCP	68	19 - 41184 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
190	30.7.83326750	192.168.200.160	192.168.200.150	TCP	68	674 - 42208 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
191	30.7.83326750	192.168.200.160	192.168.200.150	TCP	68	928 - 58110 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192	30.7.83326750	192.168.200.160	192.168.200.150	TCP	74	42696 - 364 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535447 Tsecr=0 WS=128
193	30.7.83357992	192.168.200.160	192.168.200.150	TCP	68	333 - 57372 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
194	30.7.83357992	192.168.200.160	192.168.200.150	TCP	74	42696 - 364 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535447 Tsecr=0 WS=128
195	30.7.83357992	192.168.200.160	192.168.200.150	TCP	74	42696 - 364 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535447 Tsecr=0 WS=128
196	30.7.83357992	192.168.200.160	192.168.200.150	TCP	74	42696 - 364 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535447 Tsecr=0 WS=128
197	30.7.83357992	192.168.200.160	192.168.200.150	TCP	74	42696 - 364 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535447 Tsecr=0 WS=128
198	30.7.83357992	192.168.200.160	192.168.200.150	TCP	74	42696 - 364 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535447 Tsecr=0 WS=128
199	30.7.83357992	192.168.200.160	192.168.200.150	TCP	74	42696 - 364 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535447 Tsecr=0 WS=128
200	30.7.83537888	192.168.200.160	192.168.200.150	TCP	74	52872 - 293 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535448 Tsecr=0 WS=128
201	30.7.83543154	192.168.200.160	192.168.200.150	TCP	74	37880 - 889 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535448 Tsecr=0 WS=128
202	30.7.83543154	192.168.200.160	192.168.200.150	TCP	74	37880 - 889 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535448 Tsecr=0 WS=128
203	30.7.83543154	192.168.200.160	192.168.200.150	TCP	74	37880 - 889 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535448 Tsecr=0 WS=128
204	30.7.835675617	192.168.200.160	192.168.200.150	TCP	68	203 - 52872 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
205	30.7.835675617	192.168.200.160	192.168.200.150	TCP	68	899 - 37889 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
206	30.7.835675617	192.168.200.160	192.168.200.150	TCP	68	899 - 37889 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
207	30.7.83573853	192.168.200.160	192.168.200.150	TCP	74	57854 - 122 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535448 Tsecr=0 WS=128
208	30.7.83573853	192.168.200.160	192.168.200.150	TCP	74	57854 - 122 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535448 Tsecr=0 WS=128
209	30.7.83672473	192.168.200.160	192.168.200.150	TCP	68	743 - 47472 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
210	30.7.83672473	192.168.200.160	192.168.200.150	TCP	74	45416 - 545 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535448 Tsecr=0 WS=128
211	30.7.83678894	192.168.200.160	192.168.200.150	TCP	74	37318 - 359 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535448 Tsecr=0 WS=128
212	30.7.83629955	192.168.200.160	192.168.200.150	TCP	68	831 - 41984 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
213	30.7.83629976	192.168.200.160	192.168.200.150	TCP	68	122 - 57854 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
214	30.7.83629976	192.168.200.160	192.168.200.150	TCP	68	122 - 57854 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
215	30.7.83629976	192.168.200.160	192.168.200.150	TCP	68	122 - 57854 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
216	30.7.83629445	192.168.200.160	192.168.200.150	TCP	74	35164 - 586 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535448 Tsecr=0 WS=128
217	30.7.836232426	192.168.200.160	192.168.200.150	TCP	74	57374 - 129 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535449 Tsecr=0 WS=128
218	30.7.836232426	192.168.200.160	192.168.200.150	TCP	74	57374 - 129 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535449 Tsecr=0 WS=128
219	30.7.836232426	192.168.200.160	192.168.200.150	TCP	68	129 - 59734 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
220	30.7.83678894	192.168.200.160	192.168.200.150	TCP	74	45416 - 545 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535450 Tsecr=0 WS=128
221	30.7.836881529	192.168.200.160	192.168.200.150	TCP	74	45154 - 408 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535450 Tsecr=0 WS=128
222	30.7.836881529	192.168.200.160	192.168.200.150	TCP	74	45154 - 408 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535450 Tsecr=0 WS=128
223	30.7.836889954	192.168.200.160	192.168.200.150	TCP	74	37892 - 528 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 SACK_PERM=1 Tsvl=810535450 Tsecr=0 WS=128
224	30.7.836720899	192.168.200.160	192.168.200.150	TCP	68	545 - 45416 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
225	30.7.836720899	192.168.200.160	19			

1. **Abilitare il TCP SYN Cookie:** Questa tecnica aiuta a proteggere il server gestendo le richieste SYN in modo più efficiente e riducendo il rischio di saturazione.
2. **Implementare un firewall:** Configurare il firewall per bloccare l'IP sorgente
3. **Utilizzare un sistema IDS/IPS:** Strumenti come Suricata possono rilevare e bloccare automaticamente pattern di traffico sospetti.
4. **Monitorare i log del server:** Analizzare i log per raccogliere ulteriori informazioni sull'attacco e identificare eventuali altre vulnerabilità.

Conclusioni

L'analisi della cattura di rete ha rivelato un attacco mirato al server 192.168.200.100, caratterizzato da un comportamento tipico di un attacco TCP SYN Flood. Sono state proposte azioni concrete per mitigare l'impatto dell'attacco e proteggere il sistema da futuri eventi simili. L'esercizio dimostra l'importanza della Threat Intelligence e della capacità di identificare tempestivamente gli Indicatori di Compromissione.