ANALISI WIRESHARK

1. **Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso:**

La prima cosa che possiamo osservare è che abbiamo un iniziale tentativo di connessione TCP seguito solo successivamente da una chiamata ARP. Questo potrebbe avvenire o per verificare che gli host siano raggiungibili o per cercare di reperire ulteriori informazioni sugli stessi.

1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Pri
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74 ✓	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74 ✓	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74 ✓	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60 ✓	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66 ✓	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=8105224
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66 ✓	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=81
8	28.761629461	PCSSystemtec_fd:87:…	PCSSystemtec_39:7d:…	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d:…	PCSSystemtec_fd:87:…	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PCSSystemtec_39:7d:…	PCSSystemtec_fd:87:…	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PCSSystemtec_fd:87:…	PCSSystemtec_39:7d:…	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74 ✓	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74 ✓	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM

8	28.761629461	PCSSystemtec_fd:87:…	PCSSystemtec_39:7d:…	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d:…	PCSSystemtec_fd:87:…	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PCSSystemtec_39:7d:…	PCSSystemtec_fd:87:…	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PCSSystemtec_fd:87:…	PCSSystemtec_39:7d:…	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e

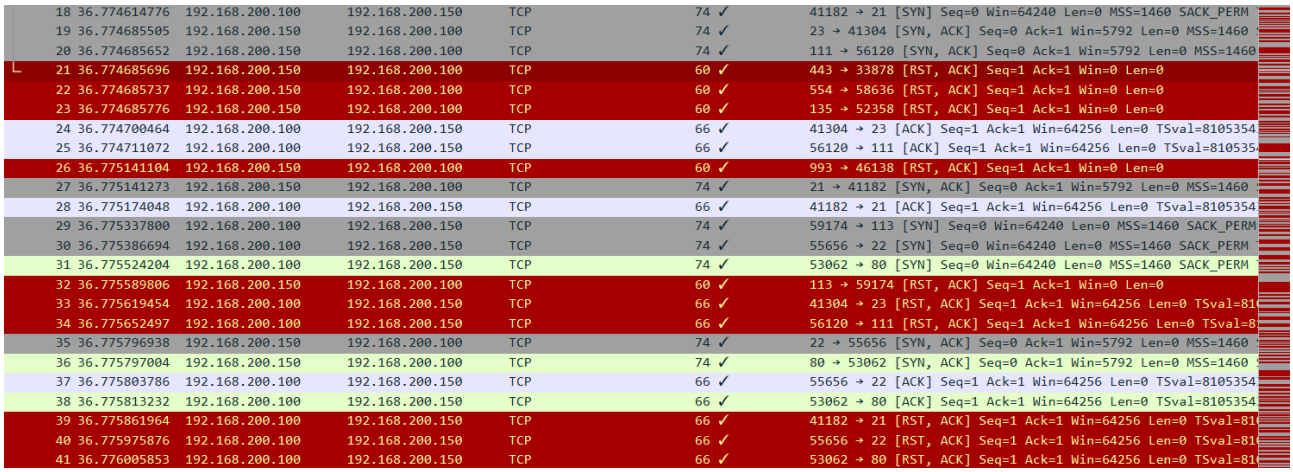
Dopo la chiamata ARP si tenta nuovamente di dare avvio ad una connessione TCP:

12	36.774143445	192.168.200.100	192.168.200.150	TCP	74 ✓	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74 ✓	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74 ✓	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74 ✓	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74 ✓	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74 ✓	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74 ✓	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74 ✓	23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PE
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74 ✓	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_P
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60 ✓	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60 ✓	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60 ✓	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66 ✓	41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSec
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66 ✓	56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSe
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60 ✓	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74 ✓	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PE
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66 ✓	41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr
29	36.775337800	192.168.200.100	192.168.200.150	TCP	74 ✓	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74 ✓	55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8

TCP è un protocollo orientato alla connessione, il che significa che stabilisce una connessione affidabile tra due host prima che i dati possano essere scambiati; tale processo è conosciuto come “three-way handshake”:

SYN -->
<-- SYN/ACK
ACK -->

Osserviamo come in questo caso non sia possibile portare a termine la connessione TCP in quanto interviene una risposta RST. Quando una connessione TCP deve essere interrotta bruscamente, il flag RST viene utilizzato per chiudere immediatamente la connessione senza terminare la stessa.



18	36.774614776	192.168.200.100	192.168.200.150	TCP	74 ✓	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74 ✓	23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74 ✓	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60 ✓	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60 ✓	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60 ✓	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66 ✓	41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=8105354
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66 ✓	56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60 ✓	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74 ✓	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66 ✓	41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=8105354
29	36.775337800	192.168.200.100	192.168.200.150	TCP	74 ✓	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74 ✓	55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74 ✓	53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
32	36.775589806	192.168.200.150	192.168.200.100	TCP	60 ✓	113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66 ✓	41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=81
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66 ✓	56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=8
35	36.775796938	192.168.200.150	192.168.200.100	TCP	74 ✓	22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
36	36.775797004	192.168.200.150	192.168.200.100	TCP	74 ✓	80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66 ✓	55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=8105354
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66 ✓	53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=8105354
39	36.775861964	192.168.200.100	192.168.200.150	TCP	66 ✓	41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=81
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66 ✓	55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=81
41	36.776005853	192.168.200.100	192.168.200.150	TCP	66 ✓	53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=81

Osservando attentamente possiamo notare che non sono stati traferiti dati in quanto sia Seq che Ack sono pari a 1, oltremodo il Len=0 ci sta ad indicare che nel segmento TCP non ci sono dati da trasmettere. Il pacchetto è utilizzato solo per il controllo della connessione e non porta alcun payload di dati.

```
[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

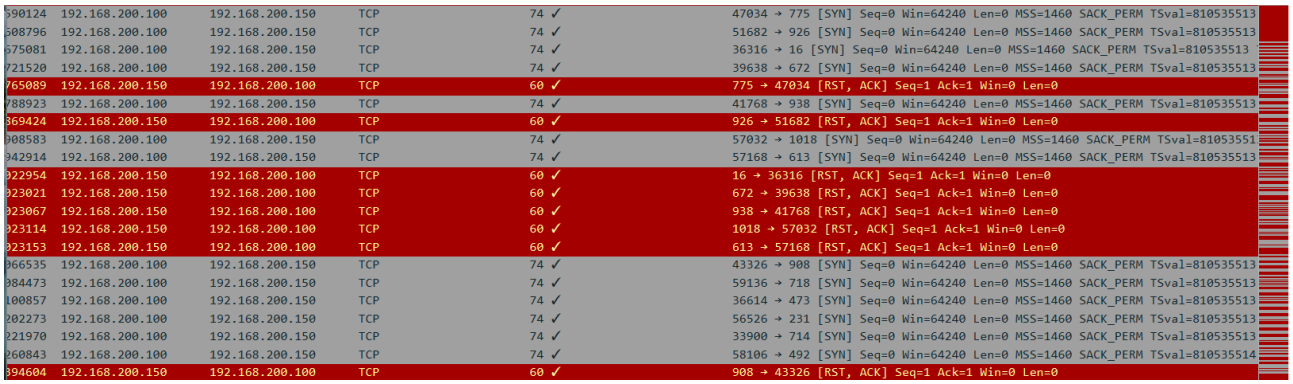
2. **In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati**

Quanto sopra individuato potrebbe essere associato ad un comportamento malevolo in quanto un aggressore potrebbe inviare pacchetti RST per identificare quali porte sono aperte o chiuse su un sistema e ricevendo un RST in risposta comprendere che la porta è chiusa o potrebbe oltremodo essere indicativo di un attaccante che sta tentando di interrompere una connessione legittima tra due parti.

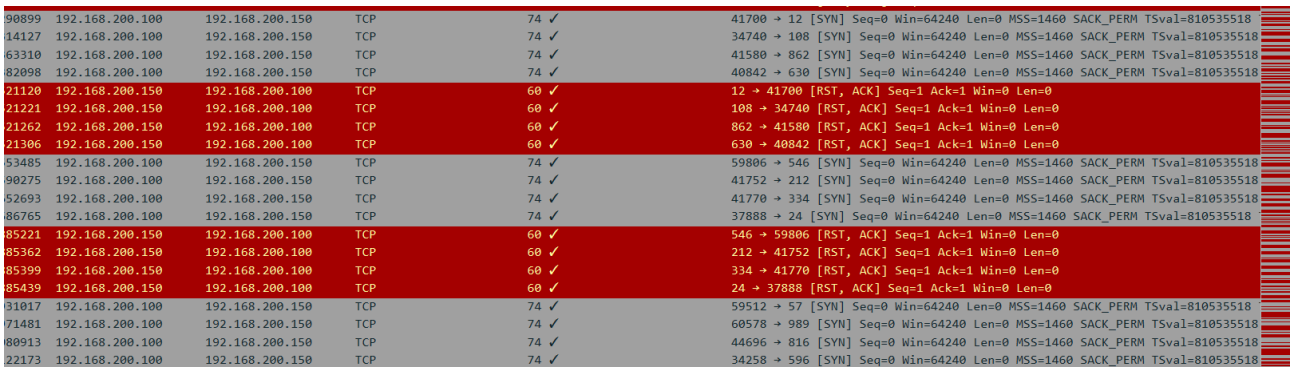
Da un ulteriore analisi possiamo osservare un tentativo di connessione su porte diverse, il che potrebbe essere ulteriormente indicativo di un tentativo di scansione delle porte stesse.

Risulta poi evidente dagli screen riportati di seguito come i tentativi di connessione provengano da un solo indirizzo ip (192.168.200.100) e come lo stesso tenti di inviare una grande quantità di pacchetti in un breve periodo di tempo. Ciò potrebbe essere indicativo di un attacco brute-force o di un attacco SYN Flood. In questo caso si tratta di un comune attacco Dos/DDoS in cui un gran numero di pacchetti **SYN** viene inviato senza mai ricevere ACK e quindi senza mai completare la connessione. Un attacco del genere potrebbe saturare le risorse del server rendendolo, quindi, incapace di gestire nuove connessioni legittime.

Non ritengo però di tratti di un SYN flood in quanto continuiamo ad avere flag RST che chiudono la connessione senza terminarla. In un di attacco SYN flood l'aggressore sfrutta il fatto che, dopo aver ricevuto un primo pacchetto SYN, il server attaccato risponderà con uno o più pacchetti SYN/ACK attendendo poi la fase finale dell'handshake. Il server attaccato rimarrà quindi in attesa di una risposta che però non arriverà mai mentre l'aggressore continuerà ad inviare pacchetti SYN costringendo così il server attaccato a mantenere contemporaneamente più connessioni aperte comportando ciò che ad un certo punto il server sarà sovraccaricato e non sarà più in grado di funzionare normalmente.



590124	192.168.200.100	192.168.200.150	TCP	74 ✓	47034 → 775 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535513
508796	192.168.200.100	192.168.200.150	TCP	74 ✓	51682 → 926 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535513
575081	192.168.200.100	192.168.200.150	TCP	74 ✓	36316 → 16 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535513
721520	192.168.200.100	192.168.200.150	TCP	74 ✓	39638 → 672 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535513
765089	192.168.200.150	192.168.200.100	TCP	60 ✓	775 → 47034 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
788923	192.168.200.100	192.168.200.150	TCP	74 ✓	41768 → 938 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535513
369424	192.168.200.150	192.168.200.100	TCP	60 ✓	926 → 51682 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
908583	192.168.200.100	192.168.200.150	TCP	74 ✓	57032 → 1018 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=81053551
942914	192.168.200.100	192.168.200.150	TCP	74 ✓	57168 → 613 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535513
922954	192.168.200.150	192.168.200.100	TCP	60 ✓	16 → 36316 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
923021	192.168.200.150	192.168.200.100	TCP	60 ✓	672 → 39638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
923067	192.168.200.150	192.168.200.100	TCP	60 ✓	938 → 41768 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
923114	192.168.200.150	192.168.200.100	TCP	60 ✓	1018 → 57032 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
923153	192.168.200.150	192.168.200.100	TCP	60 ✓	613 → 57168 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
966535	192.168.200.100	192.168.200.150	TCP	74 ✓	43326 → 908 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535513
984473	192.168.200.100	192.168.200.150	TCP	74 ✓	59136 → 718 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535513
100857	192.168.200.100	192.168.200.150	TCP	74 ✓	36614 → 473 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535513
202273	192.168.200.100	192.168.200.150	TCP	74 ✓	56526 → 231 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535513
221970	192.168.200.100	192.168.200.150	TCP	74 ✓	33900 → 714 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535513
260843	192.168.200.100	192.168.200.150	TCP	74 ✓	58106 → 492 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535514
394604	192.168.200.150	192.168.200.100	TCP	60 ✓	908 → 43326 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0



90899	192.168.200.100	192.168.200.150	TCP	74 ✓	41700 → 12 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535518
14127	192.168.200.100	192.168.200.150	TCP	74 ✓	34740 → 108 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535518
63310	192.168.200.100	192.168.200.150	TCP	74 ✓	41580 → 862 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535518
82098	192.168.200.100	192.168.200.150	TCP	74 ✓	40842 → 630 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535518
21120	192.168.200.150	192.168.200.100	TCP	60 ✓	12 → 41700 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21221	192.168.200.150	192.168.200.100	TCP	60 ✓	108 → 34740 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21262	192.168.200.150	192.168.200.100	TCP	60 ✓	862 → 41580 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21306	192.168.200.150	192.168.200.100	TCP	60 ✓	630 → 40842 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
53485	192.168.200.100	192.168.200.150	TCP	74 ✓	59806 → 546 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535518
90275	192.168.200.100	192.168.200.150	TCP	74 ✓	41752 → 212 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535518
52693	192.168.200.100	192.168.200.150	TCP	74 ✓	41770 → 334 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535518
86765	192.168.200.100	192.168.200.150	TCP	74 ✓	37888 → 24 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535518
85221	192.168.200.150	192.168.200.100	TCP	60 ✓	546 → 59806 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85362	192.168.200.150	192.168.200.100	TCP	60 ✓	212 → 41752 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85399	192.168.200.150	192.168.200.100	TCP	60 ✓	334 → 41770 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85439	192.168.200.150	192.168.200.100	TCP	60 ✓	24 → 37888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31017	192.168.200.100	192.168.200.150	TCP	74 ✓	59512 → 57 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535518
71481	192.168.200.100	192.168.200.150	TCP	74 ✓	60578 → 989 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535518
80913	192.168.200.100	192.168.200.150	TCP	74 ✓	44696 → 816 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535518
22173	192.168.200.100	192.168.200.150	TCP	74 ✓	34258 → 596 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535518

513998	192.168.200.100	192.168.200.150	TCP	74 ✓	47188 → 236 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535524
563144	192.168.200.100	192.168.200.150	TCP	74 ✓	35644 → 770 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535524
644281	192.168.200.100	192.168.200.150	TCP	74 ✓	41840 → 171 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535524
665202	192.168.200.100	192.168.200.150	TCP	74 ✓	47626 → 156 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535524
704199	192.168.200.100	192.168.200.150	TCP	74 ✓	35530 → 182 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535524
775150	192.168.200.150	192.168.200.100	TCP	60 ✓	236 → 47188 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

3. **Consigliate un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro**

Per ridurre l'impatto dei possibili attacchi che sono stati configurati si potrebbero innanzitutto implementare le configurazioni dei firewall al fine di bloccare o limitare il traffico non autorizzato o comunque sospetto. Si potrebbero quindi filtrare i pacchetti provenienti da indirizzi IP non autorizzati o da porte non utilizzate.

È oltretutto consigliabile un monitoraggio continuo del traffico mediante strumenti come Wireshark che possano aiutarci a rilevare attività sospette.

Sarebbe poi consigliabile assicurarsi che i servizi esposti (es. http) siano aggiornati alle ultime patch di sicurezza, oltremodo sarebbe necessario disabilitare o rimuovere quei servizi non necessari che espongono però la rete a dei rischi. È poi necessario assicurarsi che i servizi che utilizzano TLS/SSL abbiano certificati aggiornati e non siano vulnerabili ad eventuali exploit.

Nel caso in cui si trattasse di un attacco SYN Flood sarebbe necessario prevenirlo mediante l'abilitazione di SYN cookies sul server modificando così la gestione delle connessioni TCP al fine di impedire di allocare risorse fino a quando la connessione non sia stata completata.

Infine, è necessario implementare un sistema di backup regolare di tutti i dati e servizi critici così da permetterci un ripristino rapido del servizio nel caso in cui l'attacco avesse successo.

È importante poi assicurarsi di testare regolarmente i piani di disaster recovery così che possano essere rapidamente implementati in caso di necessità.