

## PROGETTO S9

Durante la lezione teorica, abbiamo visto la **Threat Intelligence** e gli indicatori di compromissione. Abbiamo visto che gli **IOC** sono evidenze o eventi di un attacco in corso, oppure già avvenuto.

Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con **Wireshark**. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso.
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati.
- Consigliate un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro.

## SOLUZIONE

Nel campo della cybersecurity sicuramente un elemento fondamentale nell'ambito dell'analisi del traffico di rete è **WIRESHARK** questo è un tool che consente di catturare traffico e conseguentemente analizzarlo per evidenziare eventuali anomalie identificando eventuali attacchi.

Dopo aver scaricato il file in questione procedo quindi caricandolo su **Wireshark** per iniziare l'analisi, prendendo in esame il trasferimento dei primi pacchetti, **Figura 1**.

4	23.764777323	192.168.200.150	192.168.200.100	TCP	74 80 → 53860 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
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=810522428 TSecr=4294951165
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=810522428 TSecr=4294951165
8	28.761629461	PCSSystemtec_fd:87:1e	PCSSystemtec_39:7d:fe	ARP	60 Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d:fe	PCSSystemtec_fd:87:1e	ARP	42 192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PCSSystemtec_39:7d:fe	PCSSystemtec_fd:87:1e	ARP	42 Who has 192.168.200.150? Tell 192.168.200.100
11	28.775236099	PCSSystemtec_fd:87:1e	PCSSystemtec_39:7d:fe	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 TSval=810535437 TSecr=0 WS=128
13	36.774216119	192.168.200.100	192.168.200.150	TCP	74 30120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74 58676 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
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=810535438 TSecr=0 WS=128
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=810535438 TSecr=0 WS=128
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=810535438 TSecr=0 WS=128
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=810535438 TSecr=0 WS=128
19	36.774680586	192.168.200.100	192.168.200.150	TCP	74 135 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=810522427 WS=64
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_PERM TSval=4294952466 TSecr=810535437 WS=64
21	36.774685696	192.168.200.100	192.168.200.150	TCP	60 443 → 33876 [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 TSecr=4294952466
25	36.774711872	192.168.200.100	192.168.200.150	TCP	60 30120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
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_PERM TSval=4294952466 TSecr=810535438 WS=64
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=4294952466
29	36.775397800	192.168.200.100	192.168.200.150	TCP	74 59174 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74 56566 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
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 TSval=810535439 TSecr=0 WS=128
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=810535439 TSecr=4294952466
34	36.775652497	192.168.200.150	192.168.200.100	TCP	66 56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35	36.775726033	192.168.200.150	192.168.200.100	TCP	74 21 → 56566 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
36	36.775797004	192.168.200.100	192.168.200.150	TCP	74 80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66 56566 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
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=810535439 TSecr=4294952466
40	36.775975376	192.168.200.100	192.168.200.150	TCP	66 56566 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
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=810535439 TSecr=4294952466

Figura 1.

Considerando la figura in alto posso notare alcune anomalie.

Noto la presenza di un traffico molto elevato di pacchetti inviati dall'host 192.168.200.100 verso 192.168.200.150, in particolare nella sezione evidenziata in verde vi è una sequenza di [RST, ACK] sulle porte 21, 22, 80 rispettivamente **FTP**, **SSH** e **HTTPS** è possibile che l'host sorgente in questo caso stia procedendo con una scansione sul target su delle porte comuni per verificare quale di questi servizi possa essere disponibile/vulnerabile.

Nelle sezioni evidenziate in celeste si fa riferimento al completamento di una **three-way-handshake** su porta 23 (**telnet**), lo stesso avviene per le porte 21, 22 e 80, il tutto si va poi a concludere con una **[RST, ACK]** questo mi fa sospettare di una scansione **nmap -sN** sul target, i servizi elencati in alto sono comunque in ascolto rappresentando una vulnerabilità.

Aldilà di questo noto un numero anomalo di **[RST, ACK]** su porte molto elevate (piu alte della 1024, non comuni) altro elemento che mi fa sospettare che qualcuno stia operando una scansione. **Figura 2**

79	36.777623149	192.168.200.150	192.168.200.100	TCP	60 78 + 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80	36.777645027	192.168.200.100	192.168.200.150	TCP	74 41874 + 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
81	36.777680999	192.168.200.100	192.168.200.150	TCP	74 51906 + 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
82	36.777758636	192.168.200.150	192.168.200.100	TCP	60 580 + 35138 [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 38042 + 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 46990 + 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
88	36.778067950	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=64240 Len=0 MSS=1460 SACK_PERM 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=64240 Len=0 MSS=1460 SACK_PERM 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=64240 Len=0 MSS=1460 SACK_PERM 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	36.778445494	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 42438 + 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM 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=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
98	36.778614095	192.168.200.100	192.168.200.150	TCP	74 54202 + 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM 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=64240 Len=0 MSS=1460 SACK_PERM 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=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
103	36.778820254	192.168.200.100	192.168.200.150	TCP	60 331 + 54202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
104	36.778864493	192.168.200.100	192.168.200.150	TCP	74 39566 + 856 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM 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=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
108	36.779029210	192.168.200.100	192.168.200.150	TCP	60 856 + 39566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
109	36.779055243	192.168.200.150	192.168.200.100	TCP	74 56542 + 807 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
110	36.779122259	192.168.200.150	192.168.200.100	TCP	60 84 + 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111	36.779145094	192.168.200.100	192.168.200.150	TCP	60 939 + 50932 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
112	36.779252884	192.168.200.150	192.168.200.100	TCP	60 807 + 56542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
113	36.779273781	192.168.200.100	192.168.200.150	TCP	74 43140 + 214 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128

Figura 2.

Nella figura sopra è ancora piu presente la risposta di [RST, ACK] ai tentativi di connessione, anche in questo caso come visto prima correlando al resto del traffico catturato mi trovo in presenza di molti **IOC** che mi fanno sospettare di essere in presenza di un attacco dalla macchina **192.168.200.100** verso il target **192.168.200.150**.

Come già detto posso sospettare ti trovarmi di fronte a una scansione **NMAP** sul target nel tentativo di trovare possibili servizi in ascolto, il fatto che il campo WIN sia sempre uguale a 0 puo esserne una conferma visto che mi indica che la finestra tcp sia vuota a questo aggiungo il fatto che posso notare l’ alternanza di richieste **SYN** verso porte diverse seguite sempre da risposte di **reset** da parte del destinatario.

197	36.783426736	192.168.200.100	192.168.200.150	TCP	74 57372 + 333 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535447 TSecr=0 WS=128
198	36.783557923	192.168.200.150	192.168.200.100	TCP	60 964 + 42696 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
199	36.783557992	192.168.200.150	192.168.200.100	TCP	60 333 + 57372 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
200	36.785397588	192.168.200.150	192.168.200.100	TCP	74 52872 + 203 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
201	36.785443154	192.168.200.100	192.168.200.150	TCP	74 37880 + 880 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
202	36.785511331	192.168.200.100	192.168.200.150	TCP	74 50932 + 939 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
203	36.785624918	192.168.200.150	192.168.200.100	TCP	74 47472 + 743 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
204	36.785675017	192.168.200.150	192.168.200.100	TCP	60 283 + 52872 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
205	36.785675093	192.168.200.150	192.168.200.100	TCP	60 880 + 37880 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
206	36.785721042	192.168.200.150	192.168.200.100	TCP	74 41984 + 831 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
207	36.785738953	192.168.200.100	192.168.200.150	TCP	74 57854 + 112 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
208	36.785824156	192.168.200.150	192.168.200.100	TCP	60 939 + 50932 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
209	36.785824723	192.168.200.150	192.168.200.100	TCP	60 743 + 47472 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
210	36.785880968	192.168.200.100	192.168.200.150	TCP	74 57402 + 237 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
211	36.785943368	192.168.200.100	192.168.200.150	TCP	74 33718 + 359 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
212	36.786209855	192.168.200.150	192.168.200.100	TCP	60 831 + 41984 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
213	36.786209978	192.168.200.150	192.168.200.100	TCP	60 122 + 57854 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
214	36.786210010	192.168.200.150	192.168.200.100	TCP	60 237 + 57402 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
215	36.786210059	192.168.200.150	192.168.200.100	TCP	60 359 + 33718 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
216	36.786254145	192.168.200.100	192.168.200.150	TCP	74 35164 + 586 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
217	36.786292426	192.168.200.100	192.168.200.150	TCP	74 59734 + 129 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
218	36.786455822	192.168.200.150	192.168.200.100	TCP	60 586 + 35164 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
219	36.786455938	192.168.200.150	192.168.200.100	TCP	60 129 + 59734 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
220	36.786478004	192.168.200.100	192.168.200.150	TCP	74 45416 + 545 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
221	36.786815129	192.168.200.100	192.168.200.150	TCP	74 45154 + 400 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
222	36.786864504	192.168.200.100	192.168.200.150	TCP	74 38180 + 239 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
223	36.786899954	192.168.200.100	192.168.200.150	TCP	74 37952 + 520 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
224	36.787023089	192.168.200.150	192.168.200.100	TCP	60 545 + 45416 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
225	36.787023165	192.168.200.150	192.168.200.100	TCP	60 400 + 45154 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
226	36.787069390	192.168.200.100	192.168.200.150	TCP	74 43106 + 769 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
227	36.787191686	192.168.200.150	192.168.200.100	TCP	60 239 + 38180 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
228	36.787191781	192.168.200.150	192.168.200.100	TCP	60 520 + 37952 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
229	36.787229817	192.168.200.100	192.168.200.150	TCP	74 42460 + 489 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
230	36.787306501	192.168.200.150	192.168.200.100	TCP	60 769 + 43106 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
231	36.787346317	192.168.200.100	192.168.200.150	TCP	74 49988 + 19 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
232	36.787470904	192.168.200.100	192.168.200.150	TCP	74 44644 + 846 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
233	36.787572344	192.168.200.150	192.168.200.100	TCP	60 489 + 42460 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
234	36.787572497	192.168.200.150	192.168.200.100	TCP	60 19 + 49988 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
235	36.787596289	192.168.200.150	192.168.200.100	TCP	74 51732 + 345 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
236	36.787575289	192.168.200.150	192.168.200.100	TCP	60 846 + 44644 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
237	36.787703316	192.168.200.100	192.168.200.150	TCP	74 55932 + 234 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
238	36.787864391	192.168.200.150	192.168.200.100	TCP	60 345 + 51732 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

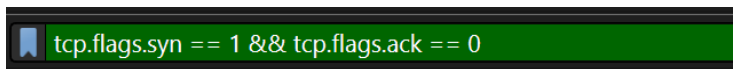
Figura 3.

Andando avanti nell’ analisi nel traffico posso notare come anche in questo caso la situazione sia pressochè analoga alle due figure viste in precedenza, il pattern si mantiene sempre in linea con quanto visto in precedenza.

Sicurametne vi è un’ elevatissima presenza di pacchetti **SYN** alla quale evidentemente non corrisponde un uguale numero di pacchetti **ACK** in risposta, provo quindi a filtrare il traffico in questo modo per accertarmi di non trovarmi di fronte ad un attacco **Syn Flood** o **Dos (Denial of Service)**.

Nella sezione in alto “Apply Filter” vado quindi ad inserire il seguente comando:

`tcp.flags.syn == 1 && tcp.flags.ack == 0`



con l'obiettivo di filtrare solamente i pacchetti SYN che non sono seguiti da pacchetti **ACK** in risposta.

394	36.795527550	192.168.200.100	192.168.200.150	TCP	74	56982 + 683 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535459 TSecr=0 WS=128
396	36.795616489	192.168.200.100	192.168.200.150	TCP	74	55216 + 83 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535459 TSecr=0 WS=128
397	36.795634831	192.168.200.100	192.168.200.150	TCP	74	41520 + 65 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535459 TSecr=0 WS=128
400	36.795726078	192.168.200.100	192.168.200.150	TCP	74	44560 + 731 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535459 TSecr=0 WS=128
401	36.795806610	192.168.200.100	192.168.200.150	TCP	74	39176 + 405 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535459 TSecr=0 WS=128
402	36.795888644	192.168.200.100	192.168.200.150	TCP	74	37760 + 318 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535459 TSecr=0 WS=128
403	36.795966048	192.168.200.100	192.168.200.150	TCP	74	40454 + 321 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535459 TSecr=0 WS=128
404	36.796043782	192.168.200.100	192.168.200.150	TCP	74	54344 + 909 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535459 TSecr=0 WS=128
405	36.796136358	192.168.200.100	192.168.200.150	TCP	74	35948 + 188 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535459 TSecr=0 WS=128
406	36.796199746	192.168.200.100	192.168.200.150	TCP	74	57508 + 310 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535459 TSecr=0 WS=128
407	36.796308835	192.168.200.100	192.168.200.150	TCP	74	33430 + 517 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535460 TSecr=0 WS=128
408	36.796400927	192.168.200.100	192.168.200.150	TCP	74	45276 + 539 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535460 TSecr=0 WS=128
409	36.796479443	192.168.200.100	192.168.200.150	TCP	74	40832 + 1019 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535460 TSecr=0 WS=128
422	36.796640743	192.168.200.100	192.168.200.150	TCP	74	60096 + 549 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535460 TSecr=0 WS=128
423	36.796695404	192.168.200.100	192.168.200.150	TCP	74	57466 + 125 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535460 TSecr=0 WS=128
426	36.796827103	192.168.200.100	192.168.200.150	TCP	74	58382 + 43 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535460 TSecr=0 WS=128
427	36.796919516	192.168.200.100	192.168.200.150	TCP	74	42154 + 695 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535460 TSecr=0 WS=128
430	36.797039374	192.168.200.100	192.168.200.150	TCP	74	38154 + 877 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535460 TSecr=0 WS=128
431	36.797147821	192.168.200.100	192.168.200.150	TCP	74	50578 + 178 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535460 TSecr=0 WS=128
432	36.797266748	192.168.200.100	192.168.200.150	TCP	74	47332 + 991 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535460 TSecr=0 WS=128
436	36.797483249	192.168.200.100	192.168.200.150	TCP	74	34004 + 528 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535461 TSecr=0 WS=128
437	36.797503813	192.168.200.100	192.168.200.150	TCP	74	54360 + 115 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535461 TSecr=0 WS=128
438	36.797565471	192.168.200.100	192.168.200.150	TCP	74	60882 + 442 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535461 TSecr=0 WS=128
439	36.797598149	192.168.200.100	192.168.200.150	TCP	74	49260 + 341 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535461 TSecr=0 WS=128
444	36.797884691	192.168.200.100	192.168.200.150	TCP	74	41054 + 879 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535461 TSecr=0 WS=128
446	36.798363276	192.168.200.100	192.168.200.150	TCP	74	36114 + 837 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535462 TSecr=0 WS=128
447	36.798389913	192.168.200.100	192.168.200.150	TCP	74	49618 + 544 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535462 TSecr=0 WS=128
448	36.798455279	192.168.200.100	192.168.200.150	TCP	74	49448 + 759 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535462 TSecr=0 WS=128
449	36.798475451	192.168.200.100	192.168.200.150	TCP	74	38154 + 797 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535462 TSecr=0 WS=128
454	36.798733073	192.168.200.100	192.168.200.150	TCP	74	40874 + 6 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535462 TSecr=0 WS=128
455	36.798753212	192.168.200.100	192.168.200.150	TCP	74	35932 + 506 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535462 TSecr=0 WS=128
456	36.798829695	192.168.200.100	192.168.200.150	TCP	74	42078 + 900 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535462 TSecr=0 WS=128

Figura 4.

Quello che ottengo come risultato è che praticamente l'intero traffico preso in esame è costituito da pacchetti di questo tipo. Nel caso di **Dos o Syn Flood** l'obiettivo è quello di saturare il server inviando richieste **syn** con frequenza molto elevata, nello specifico caso però queste sono seguite da risposte RST-ACK è quindi molto probabile che si tratti come detto prima di una scansione di porte.

## MITIGAZIONE

Arrivato a questa conclusione sarà necessario prendere in esame delle misure di mitigazione per limitare l'impatto dell'attacco ma anche per prevenire eventuali attacchi futuri.

In primo luogo quello che posso fare è procedere andando a bloccare (magari solo in maniera temporanea) l'IP dell'attaccante 192.168.200.100, magari temporaneamente, mediante un **firewall**, il **firewall** di **windows** o nel caso di **linux** direttamente da IP tables.

Nel caso di **Syn Flood** potrei invece imporre un **rate limiting** andando a limitare il numero di richieste syn che possono essere ricevute dal destinatario.

Fondamentale inoltre chiudere le porte **21, 22, 23** sul target per evitare connessioni **ftp, ssh** e **telnet** evitando vulnerabilità su questi servizi.

## BONUS

Procedo con l'analisi delle **vulnerabilità**, una di queste può essere relativa alla porta di rete che come abbiamo visto è abilitata solo per diagnostica e aggiornamenti, tuttavia potrebbe eventualmente essere sfruttata una debolezza relativa alla configurazione della **vpn** stessa per poter avere traffico malevolo sulla porta. Per quanto riguarda la porta **USB** in questo caso le **Pendrives** sono disabilitate bisognerà comunque assicurarsi che questa limitazione non possa in qualche modo essere aggirata. Bisogna sicuramente tenere in considerazione delle eventuali vulnerabilità del linguaggio con cui è scritto il software che gestisce il tutto. Si tratta di **C99**, una

versione precedente del C, è un linguaggio ad alto livello che presenta alcune vulnerabilità come **buffer overflow** o **sql injection**.

Le eventuali vulnerabilità sono quindi riconducibili a:

- La porta di rete e la configurazione della VPN.
- Il software di gestione del macchinario, linguaggio basso livello.
- Eventuali vulnerabilità su Windows 10, che è comunque un sistema sostanzialmente sicuro.

Proponiamo due soluzioni diverse:

**500 euro:**

La soluzione da 500 euro prende in considerazione un **firewall**, che può essere interposto tra rete aziendale e macchinario, un **HIPS** (Host-based Intrusion Prevention Systems) per limitare eventuali comportamenti malevoli e monitoraggio costante del traffico di rete.

**2500 euro:**

Si può pensare di introdurre in questo caso un sistema **SIEM** (Security information and event management), in maniera tale da analizzare identificare ed eventualmente prevenire le minacce, per esempio **SPLUNK**. Oltre al firewall posso aggiungere un sistema di **IDS/IPS** in maniera tale da identificare comportamenti sospetti garantendo un monitoraggio costante sul traffico di rete. Si può proporre in aggiunta lo svolgimento di **pentest** periodici per assicurarsi che il sistema sia sicuro e aggiornato prevenendo rischi di attacchi futuri.