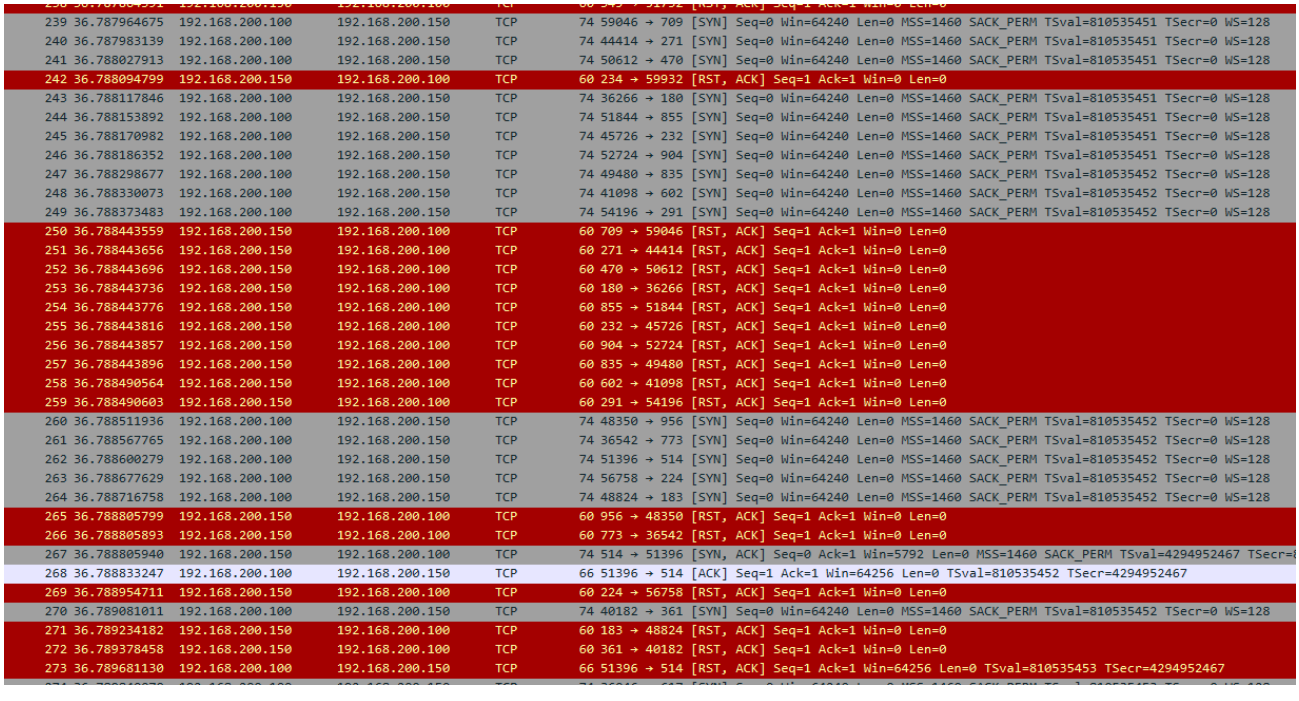
Threat Intelligence & IOC

Ci è stata consegnata una cattura di rete effettuata con Wireshark e ci è stato chiesto di analizzarla attentamente per rispondere ai seguenti quesiti:

- **1)** Identificare eventuali IOC, ovvero evidenze di attacchi in corso;
- **2)** In base agli IOC trovati, fare delle ipotesi sui potenziali vettori di attacco utilizzati;
- **3)** Consigliare un’azione per ridurre gli impatti dell’attacco.

Una volta analizzato il file ho effettuato uno screenshot su di un punto importante (essendo troppo lungo) che andrò quindi a commentare.

1) Gli **IOC** identificati:



239	36.787964675	192.168.200.100	192.168.200.150	TCP	74 59046 → 709 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
240	36.787983139	192.168.200.100	192.168.200.150	TCP	74 44414 → 271 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
241	36.788027913	192.168.200.100	192.168.200.150	TCP	74 50612 → 470 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
242	36.788094799	192.168.200.150	192.168.200.100	TCP	60 234 → 59932 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
243	36.788117846	192.168.200.100	192.168.200.150	TCP	74 36266 → 180 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
244	36.788153892	192.168.200.100	192.168.200.150	TCP	74 51844 → 855 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
245	36.788170982	192.168.200.100	192.168.200.150	TCP	74 45726 → 232 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
246	36.788186352	192.168.200.100	192.168.200.150	TCP	74 52724 → 904 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
247	36.788298677	192.168.200.100	192.168.200.150	TCP	74 49480 → 835 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535452 TSecr=0 WS=128
248	36.788330073	192.168.200.100	192.168.200.150	TCP	74 41098 → 602 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535452 TSecr=0 WS=128
249	36.788373483	192.168.200.100	192.168.200.150	TCP	74 54196 → 291 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535452 TSecr=0 WS=128
250	36.788443559	192.168.200.150	192.168.200.100	TCP	60 709 → 59046 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
251	36.788443656	192.168.200.150	192.168.200.100	TCP	60 271 → 44414 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
252	36.788443696	192.168.200.150	192.168.200.100	TCP	60 470 → 50612 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
253	36.788443736	192.168.200.150	192.168.200.100	TCP	60 180 → 36266 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
254	36.788443776	192.168.200.150	192.168.200.100	TCP	60 855 → 51844 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
255	36.788443816	192.168.200.150	192.168.200.100	TCP	60 232 → 45726 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
256	36.788443857	192.168.200.150	192.168.200.100	TCP	60 904 → 52724 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
257	36.788443896	192.168.200.150	192.168.200.100	TCP	60 835 → 49480 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
258	36.788490564	192.168.200.150	192.168.200.100	TCP	60 602 → 41098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
259	36.788490603	192.168.200.150	192.168.200.100	TCP	60 291 → 54196 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
260	36.788511936	192.168.200.100	192.168.200.150	TCP	74 48350 → 956 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535452 TSecr=0 WS=128
261	36.788567765	192.168.200.100	192.168.200.150	TCP	74 36542 → 773 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535452 TSecr=0 WS=128
262	36.788600279	192.168.200.100	192.168.200.150	TCP	74 51396 → 514 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535452 TSecr=0 WS=128
263	36.788677629	192.168.200.100	192.168.200.150	TCP	74 56758 → 224 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535452 TSecr=0 WS=128
264	36.788716758	192.168.200.100	192.168.200.150	TCP	74 48824 → 183 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535452 TSecr=0 WS=128
265	36.788805799	192.168.200.150	192.168.200.100	TCP	60 956 → 48350 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
266	36.788805893	192.168.200.150	192.168.200.100	TCP	60 773 → 36542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
267	36.788805940	192.168.200.150	192.168.200.100	TCP	74 514 → 51396 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952467 TSecr=
268	36.788833247	192.168.200.100	192.168.200.150	TCP	66 51396 → 514 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535452 TSecr=4294952467
269	36.788954711	192.168.200.150	192.168.200.100	TCP	60 224 → 56758 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
270	36.789081011	192.168.200.100	192.168.200.150	TCP	74 40182 → 361 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535452 TSecr=0 WS=128
271	36.789234182	192.168.200.150	192.168.200.100	TCP	60 183 → 48824 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
272	36.789378458	192.168.200.150	192.168.200.100	TCP	60 361 → 40182 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
273	36.789681130	192.168.200.100	192.168.200.150	TCP	66 51396 → 514 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535453 TSecr=4294952467

Si possono vedere continue richieste di connessioni TCP in arrivo dall’IP 192.168.200.100 verso il nostro IP 192.168.200.150, richieste che ci arrivano su moltissime nostre porte, che essendo chiuse, inviano un messaggio di RST, ACK evidenziato in rosso.

2) In base agli **IOC** trovati posso ipotizzare che si tratta si una scansione di rete, nello specifico di molte delle porte del nostro dispositivo.

3) Per ridurre gli impatti dell'attacco, in questo specifico caso trattandosi di un singolo indirizzo, andrei a bloccare l'indirizzo IP che sta scansionando tramite regola sul mio firewall, così da rendere impossibile inviare ulteriori richieste.