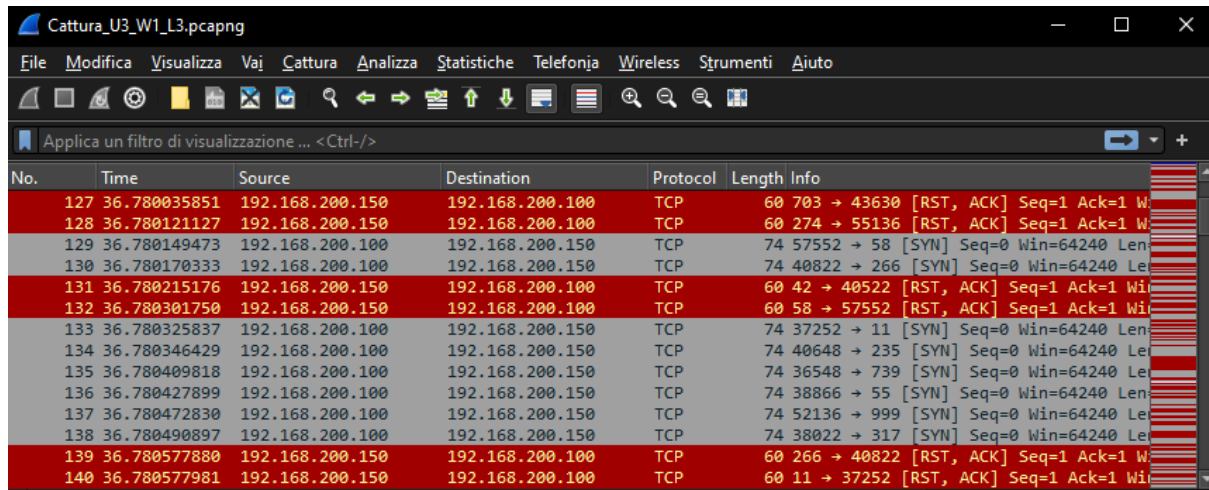


Andando ad analizzare la cattura su wireshark, dobbiamo:

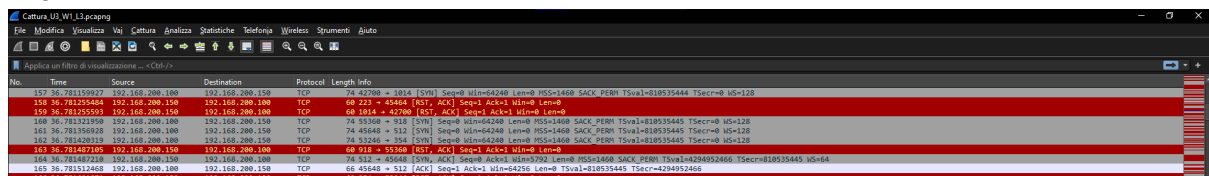
- Identificare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fare delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliare un'azione per ridurre gli impatti dell'attacco



No.	Time	Source	Destination	Protocol	Length	Info
127	36.780035851	192.168.200.150	192.168.200.100	TCP	60	703 → 43630 [RST, ACK] Seq=1 Ack=1 W
128	36.780121127	192.168.200.150	192.168.200.100	TCP	60	274 → 55136 [RST, ACK] Seq=1 Ack=1 W
129	36.780149473	192.168.200.100	192.168.200.150	TCP	74	57552 → 58 [SYN] Seq=0 Win=64240 Len
130	36.780170333	192.168.200.100	192.168.200.150	TCP	74	40822 → 266 [SYN] Seq=0 Win=64240 Le
131	36.780215176	192.168.200.150	192.168.200.100	TCP	60	42 → 40522 [RST, ACK] Seq=1 Ack=1 Wi
132	36.780301750	192.168.200.150	192.168.200.100	TCP	60	58 → 57552 [RST, ACK] Seq=1 Ack=1 Wi
133	36.780325837	192.168.200.100	192.168.200.150	TCP	74	37252 → 11 [SYN] Seq=0 Win=64240 Len
134	36.780346429	192.168.200.100	192.168.200.150	TCP	74	40648 → 235 [SYN] Seq=0 Win=64240 Le
135	36.780409818	192.168.200.100	192.168.200.150	TCP	74	36548 → 739 [SYN] Seq=0 Win=64240 Le
136	36.780427899	192.168.200.100	192.168.200.150	TCP	74	38866 → 55 [SYN] Seq=0 Win=64240 Len
137	36.780472830	192.168.200.100	192.168.200.150	TCP	74	52136 → 999 [SYN] Seq=0 Win=64240 Le
138	36.780490897	192.168.200.100	192.168.200.150	TCP	74	38022 → 317 [SYN] Seq=0 Win=64240 Le
139	36.780577880	192.168.200.150	192.168.200.100	TCP	60	266 → 40822 [RST, ACK] Seq=1 Ack=1 W
140	36.780577981	192.168.200.150	192.168.200.100	TCP	60	11 → 37252 [RST, ACK] Seq=1 Ack=1 Wi

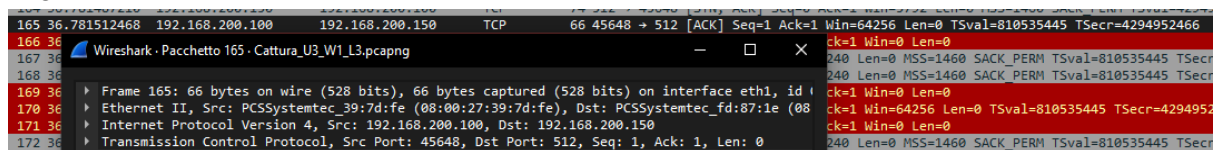
Come possiamo vedere da queste richieste su wireshark notiamo che vengono mandate tante richieste SYN all'ip 192.168.200.150 dall'ip 192.168.200.100, che vengono a loro volta bloccate da una porta chiusa RST, ACK.

Da queste richieste ripetute possiamo ipotizzare che l'ip 192.168.200.100 stia facendo una scansione dell'ip 192.168.200.150 cercando delle possibili vie di entrata nella macchina target. Quindi l'utilizzo di nmap o qualche altro tipo di scannerizzazione.



No.	Time	Source	Destination	Protocol	Length	Info
157	36.781155927	192.168.200.150	192.168.200.100	TCP	74	42008 → 512 [SYN] Seq=0 Win=0 Len=0
158	36.781254404	192.168.200.150	192.168.200.100	TCP	60	223 → 45648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
159	36.781255593	192.168.200.150	192.168.200.100	TCP	60	1014 → 42700 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
160	36.781259598	192.168.200.100	192.168.200.150	TCP	74	55308 → 512 [SYN] Seq=0 Win=0 Len=0
161	36.781359028	192.168.200.100	192.168.200.150	TCP	74	45648 → 512 [SYN] Seq=0 Win=0 Len=0
162	36.781403119	192.168.200.100	192.168.200.150	TCP	74	51248 → 512 [SYN] Seq=0 Win=0 Len=0
163	36.781497105	192.168.200.150	192.168.200.100	TCP	60	512 → 55308 [ACK] Seq=1 Ack=1 Win=0 Len=0
164	36.781497218	192.168.200.150	192.168.200.100	TCP	74	512 → 45648 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
165	36.781512468	192.168.200.100	192.168.200.150	TCP	60	45648 → 512 [ACK] Seq=1 Ack=1 Win=0 Len=0
166	36.781512468	192.168.200.100	192.168.200.150	TCP	60	512 → 55308 [ACK] Seq=1 Ack=1 Win=0 Len=0

Da questo screenshot vediamo anche che ci sono risposte di ACK da parte della macchina target, questo perchè c'è una porta aperta, come in questo caso la porta 512.



No.	Time	Source	Destination	Protocol	Length	Info
165	36.781512468	192.168.200.100	192.168.200.150	TCP	66	45648 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
166	36.781512468	192.168.200.100	192.168.200.150	TCP	66	45648 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
167	36.781512468	192.168.200.100	192.168.200.150	TCP	66	45648 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
168	36.781512468	192.168.200.100	192.168.200.150	TCP	66	45648 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
169	36.781512468	192.168.200.100	192.168.200.150	TCP	66	45648 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
170	36.781512468	192.168.200.100	192.168.200.150	TCP	66	45648 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
171	36.781512468	192.168.200.100	192.168.200.150	TCP	66	45648 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
172	36.781512468	192.168.200.100	192.168.200.150	TCP	66	45648 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466

Per ridurre le azioni possibili dell'attaccante possiamo configurare un firewall in modo tale da bloccare completamente l'accesso a qualsiasi porta della macchina target da parte dell'indirizzo ip 192.168.200.100 dell'attaccante..