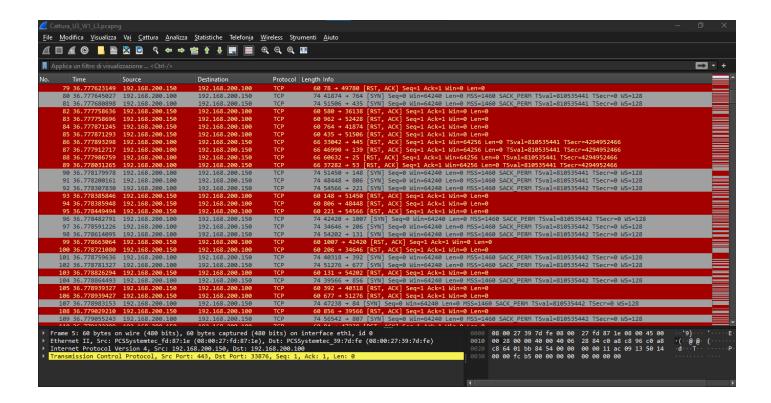
Analizzare la cattura di rete effettuata con Wireshark attentamente e rispondere ai seguenti quesiti:

- Identificare 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



Analisi del file:

- Richieste eccessive TCP su porte differenti;
- Possibile controllo/scansione sul l'indirizzo IP 192.168.200.150 (target) da parte dell'indirizzo 192.168.200.100 (possibile attaccante);
- Applicare delle regole/policy sul Firewall per evitare che un malintenzionato possa utilizzarle a suo vantaggio.

29 36.775337800 1	192.168.200.100	192.168.200.150	TCP	74 59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30 36.775386694 1	92.168.200.100	192.168.200.150	TCP	74 55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31 36.775524204 1	92.168.200.100	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 1	92.168.200.150	192.168.200.100	TCP	60 113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33 36.775619454 1	92.168.200.100	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 1	92.168.200.100	192.168.200.150	TCP	66 56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

Vediamo che ci sono molte richiesta a parte dell'IP 192.168.200.100 verso l'IP 192.168.200.150. Infatti, vi sono delle righe dove le risposte sono positive (SYN, ACK) sulle porte aperte ed altre negative (RST, ACK) indicando le porte non risponde, pertanto chiusa.

Applicando delle regole sul Firewall possiamo impedire che l'Host 192.168.200.100 possa accedere.