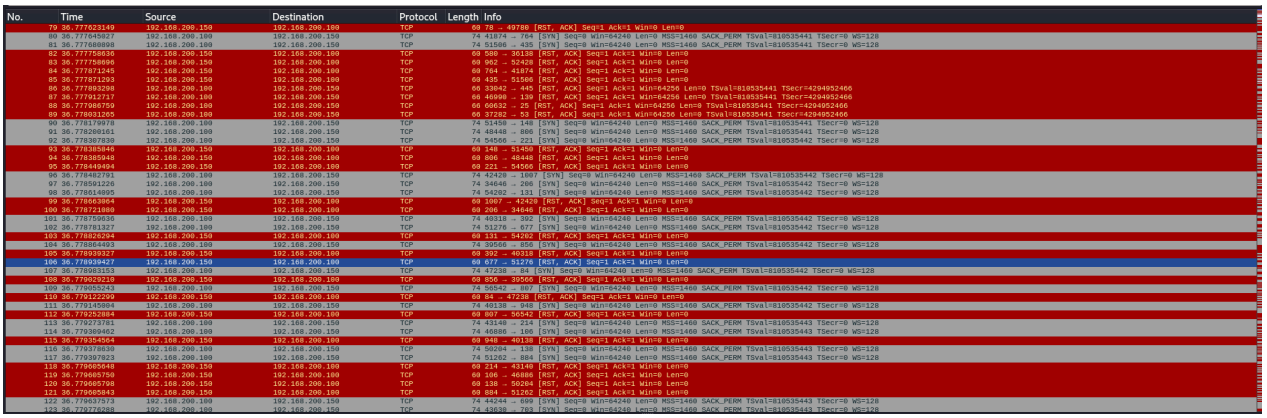
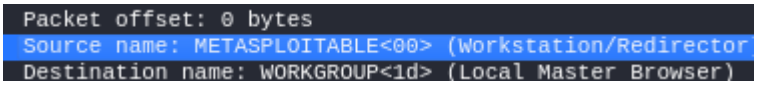
Threat Intelligence & IOC

Data la traccia dell'esercizio ho analizzato la cattura di rete con WireShark e possiamo denotare diverse curiosità.
Ci sono due indirizzi ip **192.168.200.100** e **192.168.200.150** che si scambiano pacchetti nella rete, tutti TCP.



Secondo il protocollo TCP per far si che ci sia una connessione vera e propria bisogna completare il 3 way handshake (SYN, ACK, SYN-ACK). In questo caso il 3 way handshake non viene completato mai, c'è invio SYN da parte di 200.100 e risposta ACK ed RST da parte di 200.150 ma nessun completamento. Il tutto si ripete per innumerevoli volte, le righe colorate di rosso segnalano questo problema.
Tutto ciò denota un probabile invio massivo dalla macchina 192.168.200.100 di pacchetti SYN, questo tipo di traffico potrebbe essere un attacco **SYN Flood** dove la macchina attaccante riempie di connessioni la macchina vittima per far si che causi un blocco nell'utilizzo della stessa (un Denial of Service - DoS). Altra ipotesi plausibile potrebbe essere una ricognizione molto aggressiva, ovvero un **port scanning intenso**.
E' importante notare che la macchina attaccata è una Metasploitable, quindi molto vulnerabile non essendo di ultima generazione.



Di conseguenza possiamo affermare che:
- L'elevato numero di pacchetti SYN e l'assenza di pacchetti che completano il handshake (ACK) sono segnali di un comportamento malevolo da parte della macchina **192.168.200.100**
- Non ci sono prove che **192.168.200.150** stia inviando traffico simile verso 192.168.200.100, anzi sembra reagire in modo difensivo cercando di chiudere connessioni utili con RST (Reset Connection).

Cosa fare per mitigare attacchi di questo tipo?
In questo caso la cosa migliore da fare sarebbe bloccare l'ip sorgente dell'attacco (200.100) tramite il firewall o IDS/IPS.
Per evitare attacchi di questo tipo in futuro è sempre meglio aggiornare i dispositivi, mantenere la rete controllata ed impostare limitazioni di richieste SYN da un singolo indirizzo IP.