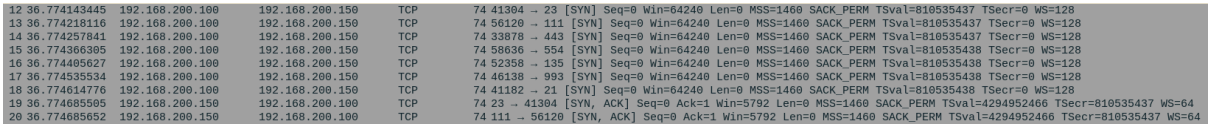
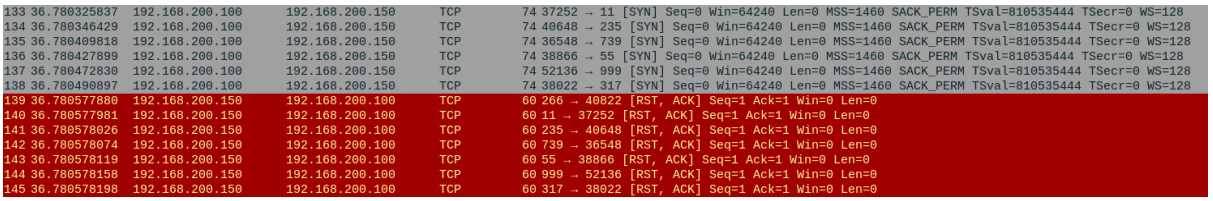
Nell’esercizio di oggi dobbiamo individuare gli indicatori di compromissione (IOC) in un file di wireshark. Gli indicatori di compromissione sono delle prove, osservabili all’interno di una rete o sistema, che possono indicare un’intrusione. Indicatori tipici possono essere firme antivirali, connessioni TCP/UDP elevate o provenienti dallo stesso mittente e diretti su porte diverse, indirizzi IP o URL sospetti, ecc.
Nel file si possono identificare connessioni TCP multiple:



Come possiamo osservare nella figura sopra ci sono molte richieste TCP che partono dallo stesso mittente e vanno ognuna su una porta diversa. Stessa cosa per l’immagine sotto:



Questi sono IOC che possono indicare che qualcuno sta eseguendo una scansione dei servizi sull’indirizzo 192.168.200.150 usando la modalità SYN scan che non completa il three way handshake. Infatti le porte chiuse rispondono con un pacchetto reset (RST), mentre quelle aperte che rispondono con un SYN/ACK non ricevono in risposta il pacchetto ACK che completa il three way handshake.
Ci sono diverse azioni che si possono implementare per mitigare il rischio, come impostare una regola su un firewall per bloccare l’indirizzo IP sospetto, oppure implementare un IPS.
L’identificazione degli IOC è fondamentale per poter valutare le proporzioni dell’incidente e per poter attivare le procedure di incident response.