- Identificare eventuali IOC, ovvero evidenze di attacchi in corso → **Richieste TCP ripetute**
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati → **Molto probabilmente è in corso una scansione sul target 192.168.200.150 dall'attaccante 192.168.200.100**
- Consigliate un'azione per ridurre gli impatti dell'attacco → **potremmo configurare delle policy firewall per bloccare accesso a tutte le porta da parte di quel determinato attaccante, in modo tale da evitare che informazioni circa porta / servizi in ascolto finiscano nella mani dell'attaccante.**

Dalla cattura notiamo che ci sono un numero elevato di richieste TCP (SYN) su porte sempre diverse in destinazione → questo ci fa pensare ad una potenziale scansione in corso da parte dell'host 192.168.200.100 verso l'host target 192.168.200.150. Questa ipotesi è supportata dal fatto che per alcune righe della cattura vediamo risposte positive del target [SYN+ACK] ad indicare che la porta è aperta. Per altre, invece, notiamo la risposta [RST+ACK] ad indicare che la porta è chiusa. Lato target, si potrebbero configurare delle regole firewall per respingere le richieste in entrata dall'host 192.168.200.100.

Richiesta SYN da parte dello scanner

Risposte negative da parte dell'host. La porta è chiusa