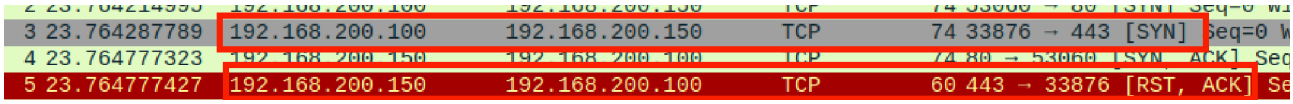
Traccia:
Durante la lezione teorica, abbiamo visto la Threat Intelligence e gli indicatori di compromissione. Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.

Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark.

Analizzate la cattura 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

In base all'evidenze riscontrate nell'allegato possiamo notare che ci potrebbe essere una scansione in corso dall'indirizzo IP 192.168.200.100 verso il target 192.168.200.150 date le varie richieste tcp rilevate. Possiamo infatti notare che dal primo indirizzo IP vi sono diverse richieste di SYN verso il target, alcune seguite da risposta positiva cioè SYN/ACK che vanno ad indicare che la porta è aperta (come nel caso della porta 80), altre invece danno danno come risposta RST+ACK e quindi ci dice che la porta è chiusa. Come metodo di difesa potremmo impostare delle regole sul firewall che impediscono a questo IP di eseguire richieste in entrata, potremmo anche cercare di risalire al computer attaccante dato che si trova sulla nostra rete interna come ci suggerisce il suo indirizzo IP.

Esempio porta chiusa 443



Esempio porta aperta 80