PRATICA S9L3 – Giorgio Trovesi

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

Dalla cattura visibile nell'immagine sottostante possiamo notare un elevato numero di richieste TCP-SYN su porte sempre diverse, questo ci fa dedurre che vi è in corso una possibile scansione da parte dell'host 192.168.200.100 verso il 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 è chiusa.

Per ovviare a ciò è consigliabile configurare le policy del firewall per bloccare l'accesso a tutte le porte da parte di quel determinato attaccante in modo tale da evitare che prenda informazioni o che possa utilizzare servizi in ascolto.