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

Abbiamo osservato un elevato numero di richieste TCP ripetute, con pacchetti SYN inviati a porte diverse. Questo comportamento suggerisce che potrebbe essere in corso una scansione delle porte da parte dell'host 192.168.200.100 verso il target 192.168.200.150. Le risposte ricevute dal target confermano questa ipotesi:

Alcuni pacchetti hanno ricevuto una risposta [SYN+ACK], indicando che le porte sono aperte.

Altri pacchetti hanno ricevuto una risposta [RST+ACK], segnalando che le porte sono chiuse.

È probabile che l'attaccante stia eseguendo una scansione delle porte per identificare quali servizi sono in ascolto sul target 192.168.200.150. La scansione delle porte è un metodo comune utilizzato per raccogliere informazioni sui servizi attivi e potenzialmente vulnerabili.

Per mitigare l'impatto di questo attacco, si consiglia di configurare il firewall del target per bloccare tutte le richieste provenienti dall'IP dell'attaccante, ovvero 192.168.200.100. Questo impedirebbe all'attaccante di ottenere informazioni sulle porte e sui servizi in ascolto. In particolare, si potrebbero impostare regole firewall per:

Bloccare tutto il traffico TCP in entrata da 192.168.200.100.

Monitorare e registrare gli accessi per identificare e rispondere tempestivamente a future attività sospette.

Implementando queste misure, si contribuirà a proteggere l'asset target da ulteriori ricognizioni e potenziali attacchi.