S9-L3

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:

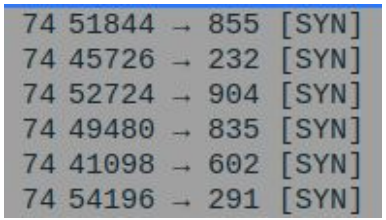
- Identificare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco

Esercizio

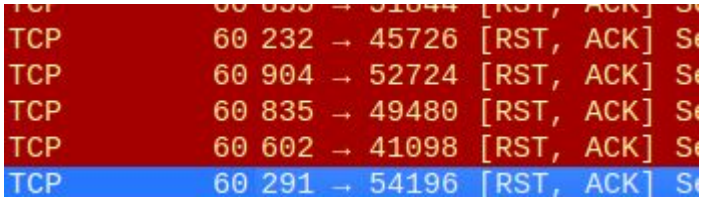
290	36.790558570	192.168.200.100	192.168.200.150	TCP	74	49498 → 395 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
291	36.790591103	192.168.200.100	192.168.200.150	TCP	74	41388 → 152 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
292	36.790673451	192.168.200.150	192.168.200.100	TCP	60	168 → 59258 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
293	36.790673508	192.168.200.150	192.168.200.100	TCP	60	416 → 44832 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
294	36.790712367	192.168.200.100	192.168.200.150	TCP	74	39996 → 459 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
295	36.790770268	192.168.200.100	192.168.200.150	TCP	74	38366 → 975 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
296	36.790854525	192.168.200.150	192.168.200.100	TCP	60	395 → 49498 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
297	36.790854622	192.168.200.150	192.168.200.100	TCP	60	152 → 41388 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
298	36.790854667	192.168.200.150	192.168.200.100	TCP	60	459 → 39996 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
299	36.790913868	192.168.200.100	192.168.200.150	TCP	74	40562 → 314 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
300	36.790933139	192.168.200.100	192.168.200.150	TCP	74	59320 → 430 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
301	36.791024940	192.168.200.100	192.168.200.150	TCP	74	54254 → 601 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
302	36.791072636	192.168.200.100	192.168.200.150	TCP	74	38236 → 384 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
303	36.791117030	192.168.200.150	192.168.200.100	TCP	60	975 → 38366 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
304	36.791117089	192.168.200.150	192.168.200.100	TCP	60	314 → 40562 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
305	36.791117128	192.168.200.150	192.168.200.100	TCP	60	430 → 59320 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
306	36.791214816	192.168.200.150	192.168.200.100	TCP	60	601 → 54254 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
307	36.791214891	192.168.200.150	192.168.200.100	TCP	60	384 → 38236 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
308	36.791257634	192.168.200.100	192.168.200.150	TCP	74	54406 → 761 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
309	36.791277803	192.168.200.100	192.168.200.150	TCP	74	53624 → 535 [SYN] Seq=0 Win=64240 Len=0 MSS=1460

Esercizio

Abbiamo notato molte richieste SYN su diverse porte.



In alcune delle richieste, abbiamo notato che la porta è contrassegnata in rosso, indicando che è chiusa.



Esercizio

Sulla base delle analisi effettuate, sembra che l'attaccante stia eseguendo una scansione del target. Ciò è evidenziato dalle risposte positive [SYN+ACK] per le porte aperte e [RST+ACK] per quelle chiuse.
Propongo le seguenti soluzioni:

- Configura un firewall per filtrare e bloccare il traffico sospetto dall'host 192.168.200.100. Puoi limitare le connessioni SYN in arrivo o bloccare completamente l'accesso da quell'indirizzo IP.
- Implementa regole di blocco a livello di sistema o di rete per ridurre la probabilità di successo di un attacco di scansione SYN. Ad esempio, potresti bloccare gli indirizzi IP che effettuano un numero elevato di connessioni SYN senza completare la procedura di handshake.