EPICODE

Esercizio 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.

SOLUZIONE

Dall’analisi effettuata si riscontrano moltissime richieste TCP da parte di un unico indirizzo ip (192.168.200.100) ad un altro indirizzo ip (192.168.200.150). Le molteplici richieste sono indirizzate ad un grande numero di porte, si deduce quindi che con tutta probabilità è in corso una scansione.

Un’azione da intraprendere il prima possibile è mettere una regola firewall che blocca completamente tutte le richieste da parte dell’ip attaccante (192.168.200.100).  
Inoltre, la richiesta viene da un ip privato facente parte della medesima rete, questo significa che l’attaccante è già all’interno della rete LAN. In questa grave situazione bisogna limitare al massimo i danni. Alcune azioni che si possono intraprendere sono:  
- Isolare il dispositivo compromesso, disconnettendolo, per evitare che infetti altri dispositivi.  
- Cercare di capire come l’attaccante è entrato nella rete.  
- Cambiare le password.  
- Controllare i dati ed eventualmente ripristinarli.

Immagine che contiene testo, schermata, software, Parallelo

Descrizione generata automaticamente