Progetto Settimanale 17/01/2025

Osservazioni generali:
Dalla scansione Wireshark possiamo evidenziare che l'***host-1*** - ***192.168.200.100*** tenta di connettersi (invio di pacchetti TCP *SYN*) a diverse porte dell'***host-2*** - ***192.168.200.150*** tramite l'invio di pacchetti SYN.
L'host-2 accetta *temporaneamente* la connessione solo su alcune porte, inviando pacchetti SYN,ACK; mentre rifiuta la connessione su tutte le altre, inviando pacchetti di tipo RST,ACK.
Tuttavia anche sulle porte in cui è stata accettata precedentemente la connessione non avviene nessuno scambio di pacchetti o richiesta di nessun tipo, quindi la connessione viene chiusa dall'host-2 inviando pacchetti RST,ACK.
Questo ***flusso 'strano' di pacchetti*** suggerisce uno dei due scenari:

- sta avvenendo un semplice ***port-scanning*** da parte dell'host-1 '*potenziale attaccante*' verso l'host-2 che ha rivelato diverse porte aperte: 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514. Questo spiegherebbe l'assenza di dati scambiati successivamente alla connessione.
- ***Sistemi di difesa*** lato host-2 *(IDS/IPS o Firewall)* hanno prontamente chiuso le connessioni avvenute riconoscendo il traffico di rete sospetto.

La presenza di una ***richiesta ARP*** da parte dell'host-1 indirizzata all'host-2, *nonostante conoscesse già* il suo IP, lascia pensare ad una prima fase di ricognizione (scanning) in cui l'host-1 volesse conferma dell'esistenza e dello stato dell'host-2. *(ho escluso problemi o scadenza dell'ARP-Table)*.

Tracce:

1. **Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso.**
   Il ***particolare flusso di pacchetti*** suggerirebbe che 192.168.200.100 sia un ***IP sospetto.***
   Entrambi i fattori potrebbero rappresentare ***Indici di Compromissione*** di un potenziale attacco informatico o almeno di un port-scanning di ricognizione iniziale.

2. **In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati.**
   - **Ipotesi 1 (più probabile)**
     L'host-1 (192.168.200.100) è un dispositivo sconosciuto sulla rete!
     In tal caso potrebbe trattarsi di un'intrusione nella rete 192.168.200.0/24 da parte di un attaccante nel tentativo di accedere ad altri host in modo non autorizzato, iniziando con un port-scanning nel tentativo di sfruttare vulnerabilità di servizi attivi su eventuali porte aperte.

   - **Ipotesi 2 (meno probabile)**
     L'host-1 (192.168.200.100) è già conosciuto e fidato!
     In tal caso potrebbe trattarsi di un malware che ha infettato l'host-1 e sta procedendo ad un attacco informatico nel tentativo di accedere ad altri host presenti sulla rete per propagarsi e accedere a informazioni sensibili.
     **La presenza della ARP-Request mi farebbe escludere questa ipotesi!*

3. **Consigliate un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro.**
   Nel nostro caso non sembra sia avvenuto un vero e proprio attacco ma solo un port-scanning, tuttavia è possibile migliorare ulteriormente le difese dell'host-2:
   - Installando e configurando un ***Firewall*** che blocchi subito IP sospetti e che limiti l'accesso solo a indirizzi specifici o sub-net fidate.
   - Implementando ***IDS/IPS*** che rileverebbero subito un port-scanning e bloccherebbero l'IP sospetto.
   - Abilitare il ***Rate Limiting*** che limita il numero di connessioni di un server.
   - Disabilitare porte e servizi inutilizzati.