EPICODE

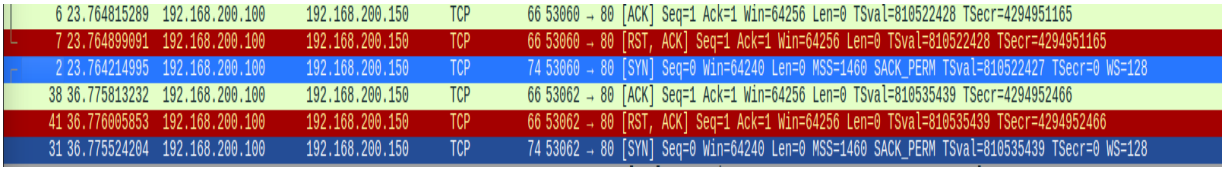
INTRODUZIONE

Durante l’esercitazione è stata analizzata una cattura di rete con Wireshark per identificare possibili Indicatori di Compromissione (IOC), applicando i concetti di Threat Intelligence studiati nella lezione teorica. L’obiettivo era riconoscere eventuali segni di attività malevola, ipotizzare il vettore d’attacco utilizzato e proporre contromisure per limitare l’impatto e prevenire attacchi simili in futuro.

---

1) Identificazione degli IOC

Analizzando il traffico TCP presente nella cattura, è stato individuato un comportamento sospetto proveniente dall’host `192.168.200.100`, che tentava ripetute connessioni verso l’host `192.168.200.150` su numerose porte, tra cui la porta 80. La presenza di numerosi pacchetti con flag `SYN` e risposte `RST` è un chiaro segnale di **port scanning**, attività tipicamente riconosciuta come un IOC. Il traffico verso porte elevate e l’assenza di risposta positiva da parte della macchina destinataria rafforzano l’ipotesi di una ricognizione automatica.



6	23.764815289	192.168.200.100	192.168.200.150	TCP	66 53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66 53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74 53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66 53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41	36.776005853	192.168.200.100	192.168.200.150	TCP	66 53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74 53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128

(Perché ci siamo concentrati sulla porta **80**?

1. La porta 80 è ben riconoscibile e comune

- È la **porta standard del protocollo HTTP**, quindi sappiamo che serve per il **traffico web**.
- Se un attaccante sta cercando vulnerabilità, proverà sicuramente anche la 80 perché:
    - Potrebbe esserci un **web server vulnerabile** (Apache, nginx, IIS...).
    - È facile da raggiungere e analizzare (con curl, browser, nmap, gobuster…))

2) Ipotesi sul vettore di attacco

Il comportamento osservato suggerisce che l'host `192.168.200.100` stia eseguendo una scansione attiva della rete per individuare servizi vulnerabili. Questo tipo di attività rappresenta la **fase iniziale di un attacco informatico**, nota come "ricognizione". L'attaccante, una volta identificate le porte aperte e i servizi esposti, potrebbe sfruttare eventuali vulnerabilità note per compromettere il sistema di destinazione.

3) Azioni correttive e preventive

Per contenere l’attacco in corso:

- Isolare immediatamente l’host sospetto `192.168.200.100` dalla rete.
- Analizzare il dispositivo con strumenti antimalware per verificare un’eventuale compromissione.
  Per prevenire attacchi futuri:
- Configurare un sistema di **Intrusion Detection (IDS)** per rilevare scansioni di porte e altri comportamenti anomali.
- Applicare regole firewall interne per limitare l’accesso ai soli servizi necessari.
- Segmentare la rete per ridurre il rischio di compromissione laterale.
- Monitorare costantemente il traffico e i log di rete.

4) CONCLUSIONI

L’analisi della cattura di rete ha permesso di individuare un IOC chiaro, riconducibile a una scansione di rete. L'applicazione dei concetti di Threat Intelligence ha reso possibile interpretare correttamente l’evento, formulare un’ipotesi realistica e suggerire azioni concrete per mitigare il rischio e rafforzare la sicurezza dell’infrastruttura.