PROGETTO S9

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 ed analizzare 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 attuale ed eventualmente un simile attacco futuro.

SOLUZIONE

Nel campo della cybersecurity sicuramente un elemento fondamentale nell' ambito dell' analisi del traffico di rete è ***WIRESHARK*** questo è un tool che consente di catturare traffico e conseguentemente analizzarlo per evidenziare eventuali anomalie identificando eventuali attacchi.

Dopo aver scaricato il file in questione procedo quindi caricandolo su ***Wireshark*** per iniziare l' analisi, prendendo in esame il trasferimento dei primi pacchetti, ***Figura 1.***

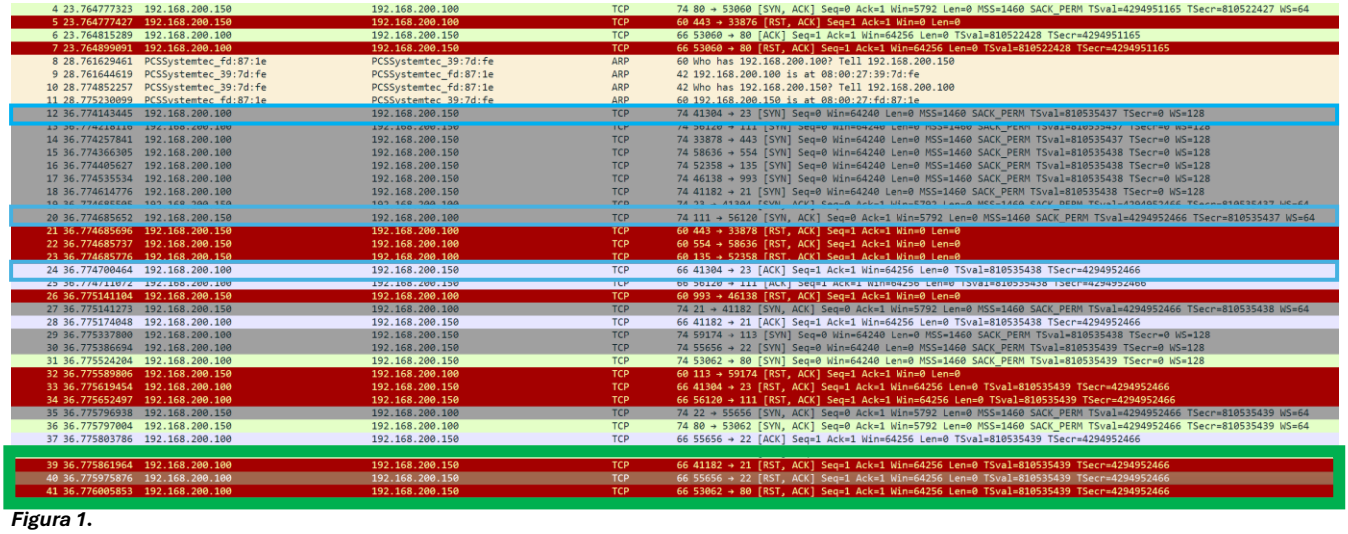

Figura 1.

Considerando la figura in alto posso notare alcune anomalie.

Noto la presenza di un traffico molto elevato di pacchetti inviati dall' host 192.168.200.100 verso 192.168.200.150, in particolare nella sezione evidenziata in verde vi è una sequenza di [RST, ACK] sulle porte 21, 22, 80 rispettivamente ***FTP***, ***SSH*** e ***HTTPS*** è possibile che l' host sorgente in questo caso stia procedendo con una scansione sul target su delle porte comuni per verificare quale di questi servizi possa essere disponibile/vulnerabile.

Nelle sezioni evidenziate in celeste si fa riferimento al completamento di una ***three-way-handshack*** su porta ***23*** (***telnet***), lo stesso avviene per le porte ***21***, ***22*** e ***80***, il tutto si va poi a conludere con una ***[RST, ACK]*** questo mi fa sospettare di una scansione **nmap -sN** sul target, i servizi elencati in alto sono comunque in ascolto rappresentando una vulnerabilità.

Aldilà di questo noto un numero anomalo di ***[RST, ACK]*** su porte molto elevate (piu alte della 1024, non comuni) altro elemento che mi fa sospettare che qualcuno stia operando una scansione. ***Figura 2***

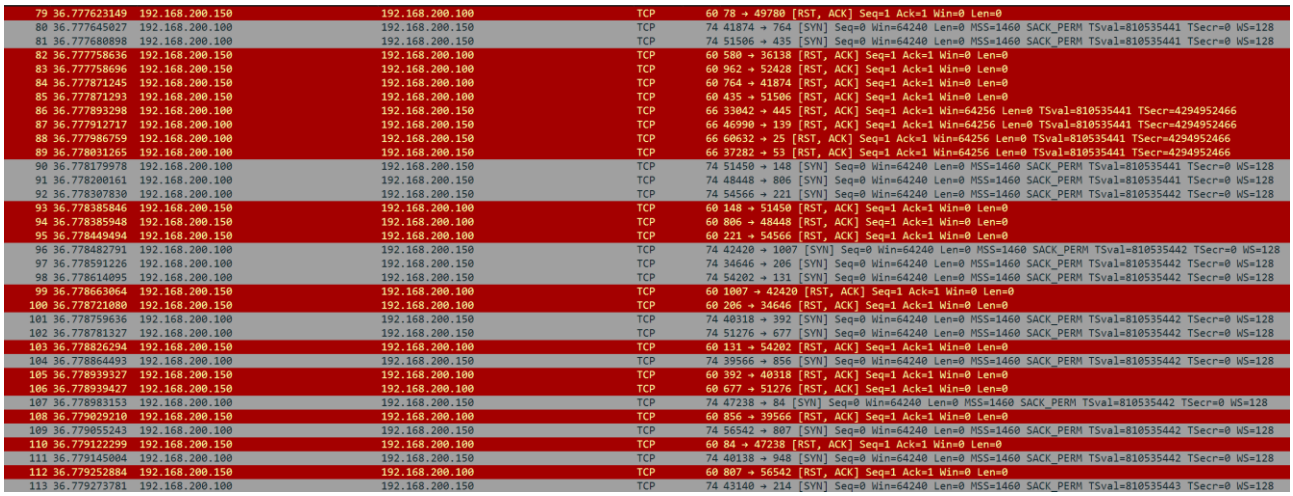

Figura 2.

Nella figura sopra è ancora piu presente la risposta di [RST, ACK] ai tentativi di connessione, anche in questo caso come visto prima correlando al resto del traffico catturato mi trovo in presenza di molti ***IOC*** che mi fanno sospettare di essere in presenza di un attacco dalla macchina ***192.168.200.100*** verso il target ***192.168.200.150***.

Come già detto posso sospettare ti trovarmi di fronte a una scansione ***NMAP*** sul target nel tentativo di trovare possibili servizi in ascolto, il fatto che il campo WIN sia sempre uguale a 0 puo esserne una conferma visto che mi indica che la finestra tcp sia vuota a questo aggiungo il fatto che posso notare l' alternanza di richieste ***SYN*** verso porte diverse seguite sempre da risposte di ***reset*** da parte del destinatario.

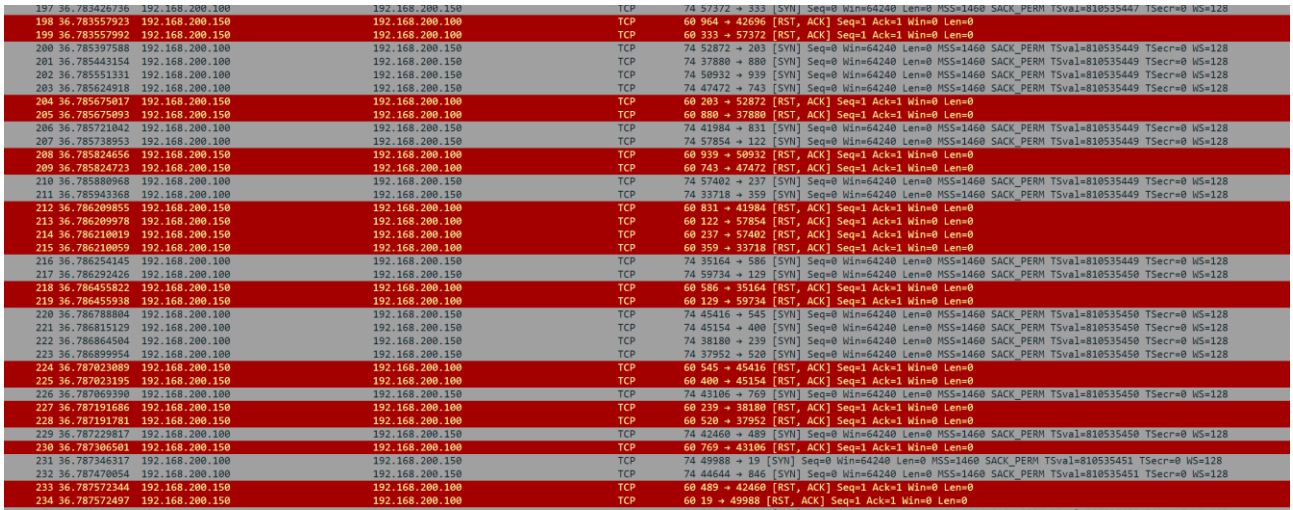

Figura 3.

Andando avanti nell' analisi nel traffico posso notare come anche in questo caso la situazione sia pressochè analoga alle due figure viste in precedenza, il pattern si mantiene sempre in linea con quanto visto in precedenza.

Sicurametne vi è un' elevatissima presenza di pacchetti ***SYN*** alla quale evidentemente non corrisponde un uguale numero di pacchetti ***ACK*** in risposta, provo quindi a filtrare il traffico in questo modo per accertarmi di non trovarmi di fronte ad un attacco ***Syn Flood*** o ***Dos*** (***Denial of Service***).

Nella sezione in alto "Apply Filter" vado quindi ad inserire il seguente comando:

tcp.flags.syn == 1 && tcp.flags.ack == 0

con l' obbiettivo di filtrare solamente i pacchetti SYN che non sono seguiti da pacchetti ***ACK*** in risposta.

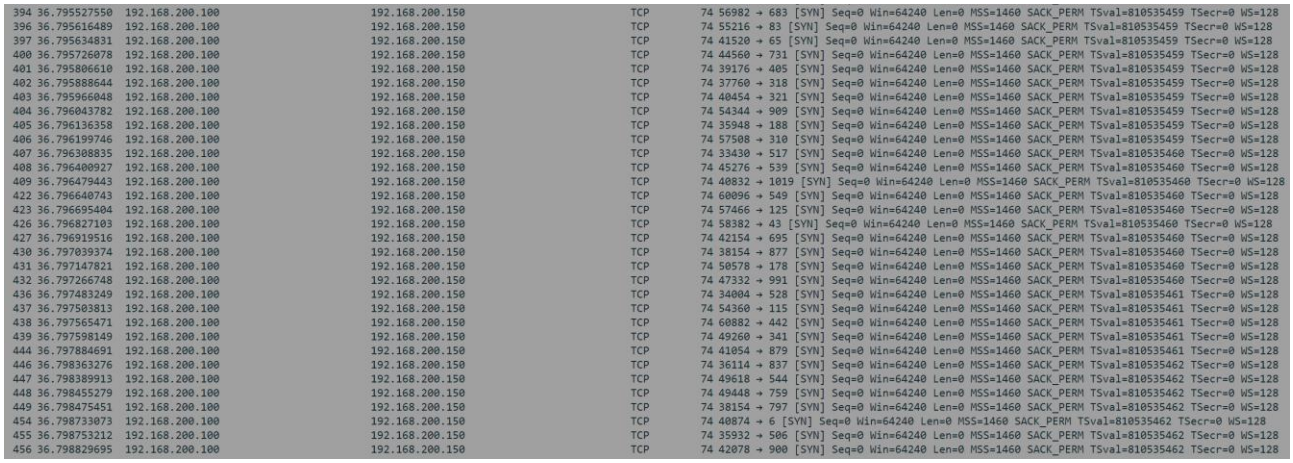

Figura 4.

Quello che ottengo come risulato è che praticamente l' intero traffico preso in esame è costituito da pacchetti di questo tipo. Nel caso di ***Dos*** o ***Syn Flood*** l' obbiettivo è quello di saturare il server inviando richieste ***syn*** con frequenza molto elevata, nello specifico caso però queste sono seguite da risposte RST-ACK è quindi molto probabile che si tratti come detto prima di una scansione di porte.

MITIGAZIONE

Arrivato a questa conclusione sarà necessario prendere in esame delle misure di mitigazione per limitare l' impatto dell' attacco ma anche per prevenire eventuali attacchi futuri.

In primo luogo quello che posso fare è procedere andando a bloccare (magari solo in maniera temporanea) l' IP dell' attaccante 192.168.200.100, magari temporaneamente, mediante un ***firewall***, il ***firewall*** di ***windows*** o nel caso di ***linux*** direttamente da IP tables.

Nel caso di ***Syn Flood*** potrei invece imporre un ***rate limiting*** andando a limitare il numero di richieste syn che possono essere ricevute dal destinatario.

Fondamentale inoltre chiudere le porte ***21***, ***22***, ***23*** sul target per evitare connessioni ***ftp***, ***ssh*** e ***telnet*** evitando vulnerabilità su questi servizi.

BONUS

Procedo con l' analisi delle ***vulnerabilità***, una di queste puo essere relativa alla porta di rete che come abbiamo visto è abilitata solo per diagnostica e aggiornamenti, tuttavia potrebbe eventualmente essere sfruttata una debolezza relativa alla configurazione della ***vpn*** stessa per poter avere traffico malevolo sulla porta. Per quanto riguarda la porta ***USB*** in questo caso le **Pendrive** sono disabilitate bisognerà comunque assicurarsi che questa limitazione non possa in qualche modo essere agirata. Bisogna sicuramente tenere in considerazione delle eventuali vulnerabilità del linguaggio con cui è scritto il software che gestisce il tutto. Si tratta di ***C99***, una versione precedente del C, è un linguaggio a basso livello che presenta alcune vulnerabilità come **buffer**

overflow o **sql injection**. Altro elemento che bisogna tenere in considerazione riguarda sicuramente i permessi di accesso degli utenti.

Le eventuali vulnerabilità sono quindi riconducibili a:

- La porta di rete e la configurazione della VPN.
- Il software di gestione del macchinario, linguaggio basso livello.
- Eventuali vulnerabilità su Windows 10, che è comunque un sistema sostanzialmente sicuro.

Proponiamo due soluzione diverse:

500 euro:

La soluzioe da 500 euro prende in considerazione un **firewall**, che puo essere interposto tra rete aziendale e macchinario, un ***HIPS*** (Host-based Intrusion Prevention Systems) per limtare eventuali comportamenti malevoli. e monitoraggio costante del traffico di rete.

2500 euro:

Si puo pensare di introdurre in questo caso un sistema ***SIEM*** (Security information and event management), in maniera tale da analizzare identificare ed eventualmente prevenire le minacce, per esempio ***SPLUNK***. Oltre al firewall posso aggiungere un sistema di ***IDS/IPS*** in maniera tale da identificare comportamenti sospetti garantendo un monitoraggio costante sul traffico di rete. Si puo proporre in aggiunta lo svolgimento di ***pentest*** periodici per assicurarsi che il sistema sia sicuro e aggiornato prevenendo rischi di attacchi futuri.