S9L5 Luca Calvigioni

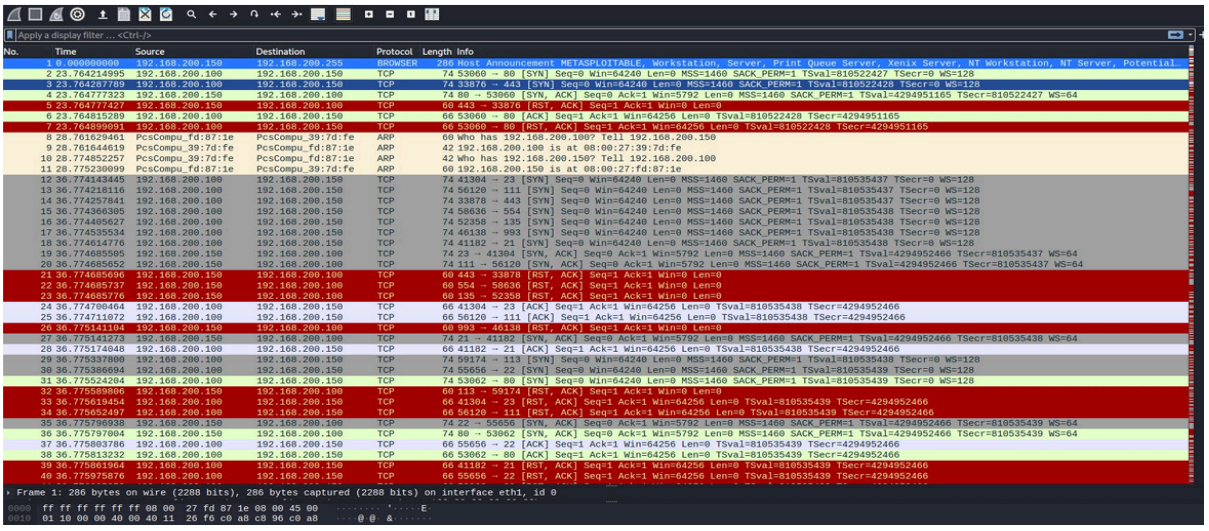
THREAT INTELLIGENCE E IOC

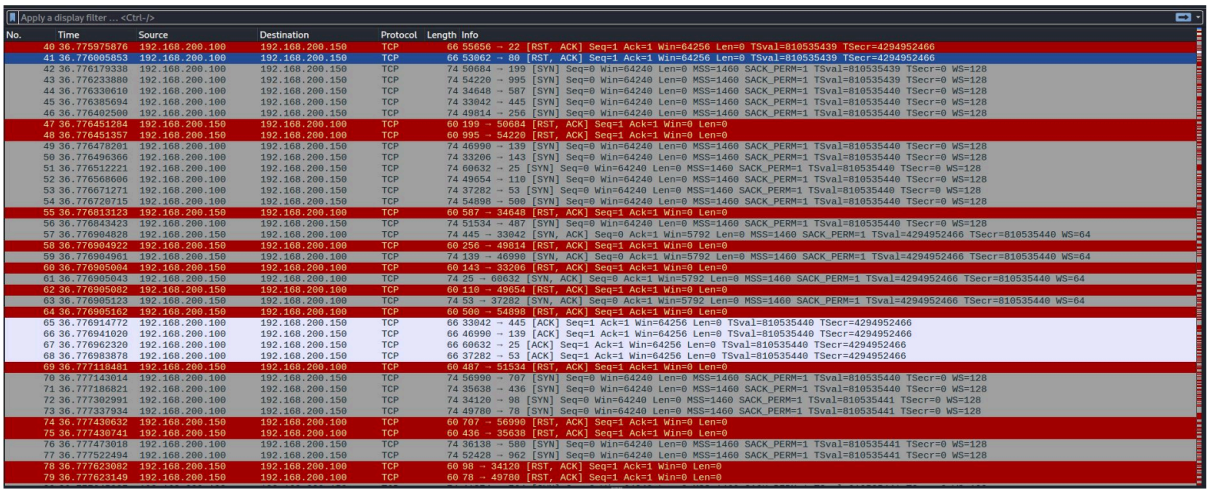
Per Threat Intelligence si intende la raccolta, l'analisi e la condivisione di informazioni su minacce attuali e potenziali alla sicurezza informatica. Queste informazioni includono dettagli sui cyber attacchi, sulle vulnerabilità dei sistemi, sulle tattiche degli attaccanti e sugli indicatori di compromissione IoC. Gli IoC sono evidenze o eventi di un attacco in corso, oppure già avvenuto, elenchiamone alcuni:

- Indirizzi IP sospetti
- Hash di file
- Url o domini malevoli
- Pacchetti syn senza completamento della stretta di mano a 3 vie
- Processi anomali ecc

Oggi andremo ad analizzare una cattura di rete effettuata con Wireshark e risponderemo ai seguenti quesiti:

- Identificare ed analizzare eventuali IOC.
- Fare delle ipotesi sui potenziali vettori di attacco utilizzati.
- Consigliare un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro.





Identificazione IOC

- L’Indirizzo IP del presunto attaccante è privato, ciò vuol dire che l’ attaccante si trova nella nostra stessa rete locale (LAN)

- Ripetuti pacchetti SYN provenienti dall’indirizzo IP 192.168.200.100 senza concludere la stretta di mano a 3 vie tipica del protocollo TCP (SYN, SYN/ACK, ACK) quindi al posto di ACK l’attaccante invierà un RST per interrompere la connessione, questo può essere un segno di un port scanning.

- Risposta RST da parte del server 192.168.200.150 sta ad indicare una sorta di protezione e quindi interrompe la connessione o semplicemente potrebbe essere che la porta è chiusa.

- Traffico elevato di pacchetti SYN (SYN FLOOD) provenienti dalla stessa sorgente in modo ripetitivo può essere un chiaro segno di attacco DoS.

Ipotesi

In base agli IOC identificati possiamo fare le seguenti ipotesi sui vettori di attacco:

- SYN FLOOD (Denial of Service): L'attaccante invia pacchetti SYN per aprire connessioni TCP senza completare il processo di handshake. Ciò può esaurire le risorse del server, rendendolo indisponibile per altri utenti a causa del numero elevato di richieste da gestire. Questo prende il nome di attacco DoS

- PORT SCANNING: È probabile che l’attaccante stia utilizzando uno strumento di scanning come ad esempio NMAP per verificare la presenza di servizi attivi sulle porte aperte e di conseguenza prepararsi per ulteriori exploit.
  Ipotizzando un comando nmap che l’attaccante può aver lanciato

  nmap -sT -p- -Pn 192.168.200.150

  -sT permette di completare la connessione e subito dopo chiuderla con RST,ACK
  -p- scansiona tutte e 65535 le porte logiche.
  -Pn omette la fase di invio del ping, per bypassare firewall o comunque eludere sistemi di rilevamento di intrusione.

Consigli e misure preventive

Per ridurre l’impatto dell’attacco attuale e prevenire futuri attacchi simili, è necessario adottare un approccio che combini misure immediate, configurazioni preventive e strategie a lungo termine.

- Bloccare o comunque limitare l’indirizzo IP sospetto impostando una regola del firewall, questo impedirà ulteriori tentativi di connessione dall'attaccante

- Analizzare in tempo reale il traffico di rete per individuare eventuali attività sospette non provenienti dall’IP bloccato. Questo permette di identificare altri potenziali attaccanti o variazioni dell’attacco, questo vale anche per prevenire futuri attacchi.

- Se sono presenti porte aperte che non ospitano servizi attivi, chiuderle immediatamente. Questo riduce la superficie di attacco e limita l’efficacia di scansioni multi-porta.

- Utilizzare sistemi di rilevamento e prevenzione delle intrusioni come IDS/IPS per identificare e bloccare attacchi DoS automaticamente.

- Imporre limiti sulle connessioni TCP, ovvero regole che limitino il numero di connessioni incomplete per ogni IP sorgente, ad esempio un SYN FLOOD protection.

- Aggiornamento costante di dispositivi e software per chiudere vulnerabilità note.

- Ultimo ma non per importanza è il sensibilizzare gli utenti ad adottare buone pratiche di sicurezza informatica.

Conclusioni

Tirando le Somme si tratta di una Scansione Nmap perchè viene generato un traffico limitato e sequenziale con l'obiettivo è raccogliere informazioni sulle porte aperte e non sovraccaricare il sistema, al contrario di un attacco Dos che punta ad esaurire la capacità del server con l’invio di migliaia o milioni di pacchetti.

Per concludere possiamo dire che adottare misure immediate per contenere l’attacco corrente è cruciale, ma prevenire attacchi futuri richiede una combinazione di configurazioni preventive, monitoraggio continuo e buone pratiche di sicurezza. Il rafforzamento della rete e dei server riduce la superficie di attacco e migliora la prevenzione da attacchi sempre più sofisticati.