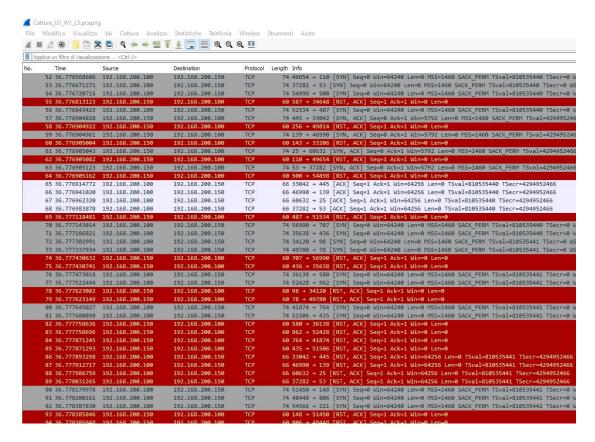
Threat Intelligence & IOC

L'esercizio di oggi consiste nell'analizzare una cattura attraverso Wireshark e rispondere a questi 3 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

Per IOC, Indicatori di Compromissione, dall'inglese "Indicators of Compromise", sono tracce o indicatori che suggeriscono la presenza di una violazione della sicurezza o di un compromesso nei sistemi informatici.

Qui sotto allego lo screen che andremmo ad analizzare:



Come possiamo vedere dall'immagine Wireshark ha registrato un gran numero di pacchetti TCP (SYN) in entrata e diretti a porte diverse, questo potrebbe essere dovuto a due fattori: il prima è che ci sia una scansione, ad esempio tramite nmap, in corso; oppure potrebbe essere in atto un attacco SYN Flood.

Nel primo caso se la scansione la stiamo facendo noi per motivi di test e sicurezza possiamo stare tranquilli altrimenti se l'IP che è segnato è a noi sconosciuto vuol dire che un malvivente sta scansionando la nostra rete per cercare un "entrata" per

l'attacco.

Nel secondo caso, l'attacco SYN Flood, l'attaccante invia un grande numero di richieste SYN al server senza completare l'handshake. Questo può esaurire le risorse del server, come le entrate nella tabella delle connessioni TCP, impedendo la ricezione di nuove connessioni legittime.

Per mitigare ciò che sta succedendo, in caso di scansione possiamo fare una scansione meno invasiva.

Invece in caso di attacco possiamo agire principalmente su 2 cose:

- 1. Firewall: Configura un firewall per filtrare o limitare il traffico di SYN in arrivo. Alcuni firewall possono essere configurati per riconoscere e mitigare gli attacchi SYN flood.
- 2.Rilevamento Intrusione: Utilizza sistemi di rilevamento delle intrusioni (IDS) o sistemi di prevenzione delle intrusioni (IPS) per identificare e rispondere automaticamente agli attacchi SYN flood.