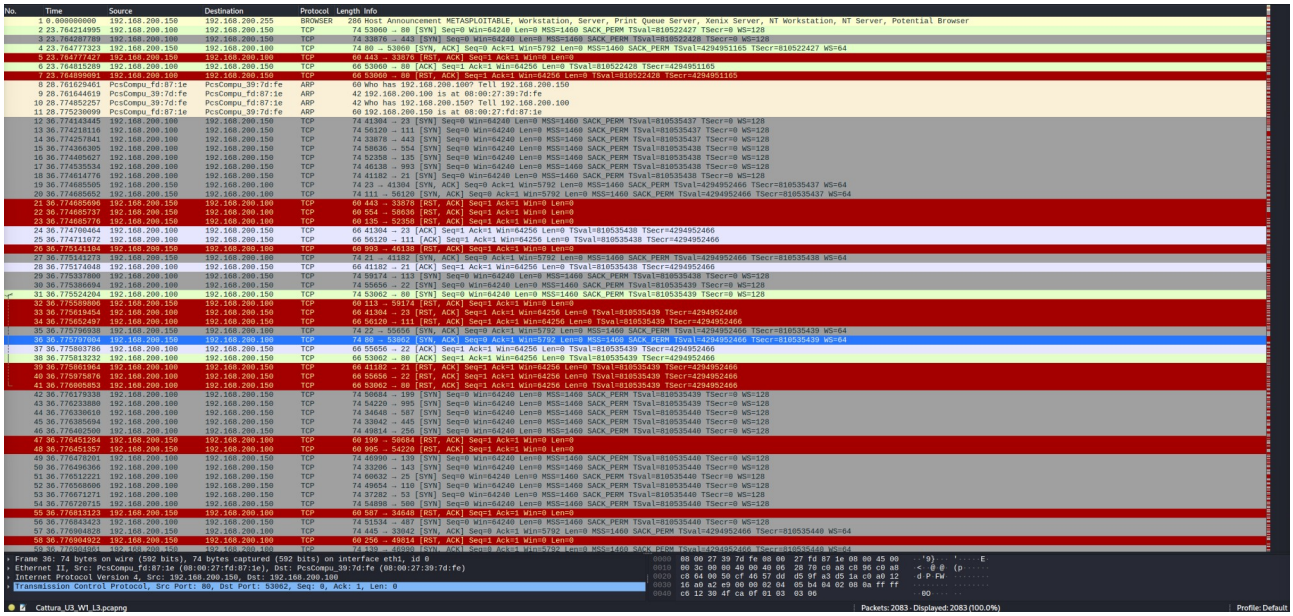
S9 LEZIONE 3

Traccia:
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 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 iniziare vediamo che la macchina con IP 192.168.200.100 è la macchina attaccante mentre la macchina è 192.168.200.150 ed è una macchina Metasploitable.

La macchina attaccante invia un grande numero di pacchetti SYN su protocollo TCP alla macchina Metasploitable.

Queste potrebbero essere alcune spiegazioni:

- **Attacco DDoS (Distributed Denial of Service):** Un elevato numero di pacchetti TCP inviati potrebbe essere parte di un attacco DDoS, in cui numerosi dispositivi compromessi vengono utilizzati per sovraccaricare la capacità di risposta del sistema di destinazione, impedendone il normale funzionamento.

- **Scansione di Porte (Port Scanning):** Potrebbe essere un tentativo di individuare porte aperte su un sistema al fine di identificare servizi in esecuzione e possibili vulnerabilità. Questo potrebbe essere parte di un'attività di hacking o ricognizione.

- **Flusso di Dati Legittimo:** In alcuni casi, un elevato traffico TCP potrebbe essere normale, ad esempio durante l'invio o la ricezione di grandi quantità di dati legittimi. Ad esempio, il

trasferimento di file, lo streaming video o altre attività che richiedono un elevato utilizzo di connessioni TCP.

- **Problemi di Rete:** Potrebbe anche essere il risultato di problemi di configurazione di rete o errori, come loop di rete o configurazioni non ottimali.

Quindi probabilmente l'attaccante sta facendo una scansione per vedere quali porte della macchina Metasploitable sono aperte per identificare servizi in esecuzione e potenziali vulnerabilità. In poche parole vengono inviati pacchetti SYN a diverse porte le quali potrebbero rispondere con SYN-ACK.

Oppure la macchina attaccante sta eseguendo un attacco DdoS.

Possibili soluzioni:

- **Filtraggio del traffico:** implementare dei filtri di rete o firewall per limitare il numero di connessioni provenienti dal singolo IP
- **Rilevamento e risposta alle scansioni di porte:** utilizzare sistemi di rilevamento delle intrusioni o prevenzione intrusioni (IDS e IPS)
- **Aggiornamenti e patch:** assicurarsi che il sistema operativo e le applicazioni siano aggiornate alle ultime patch di sicurezza.