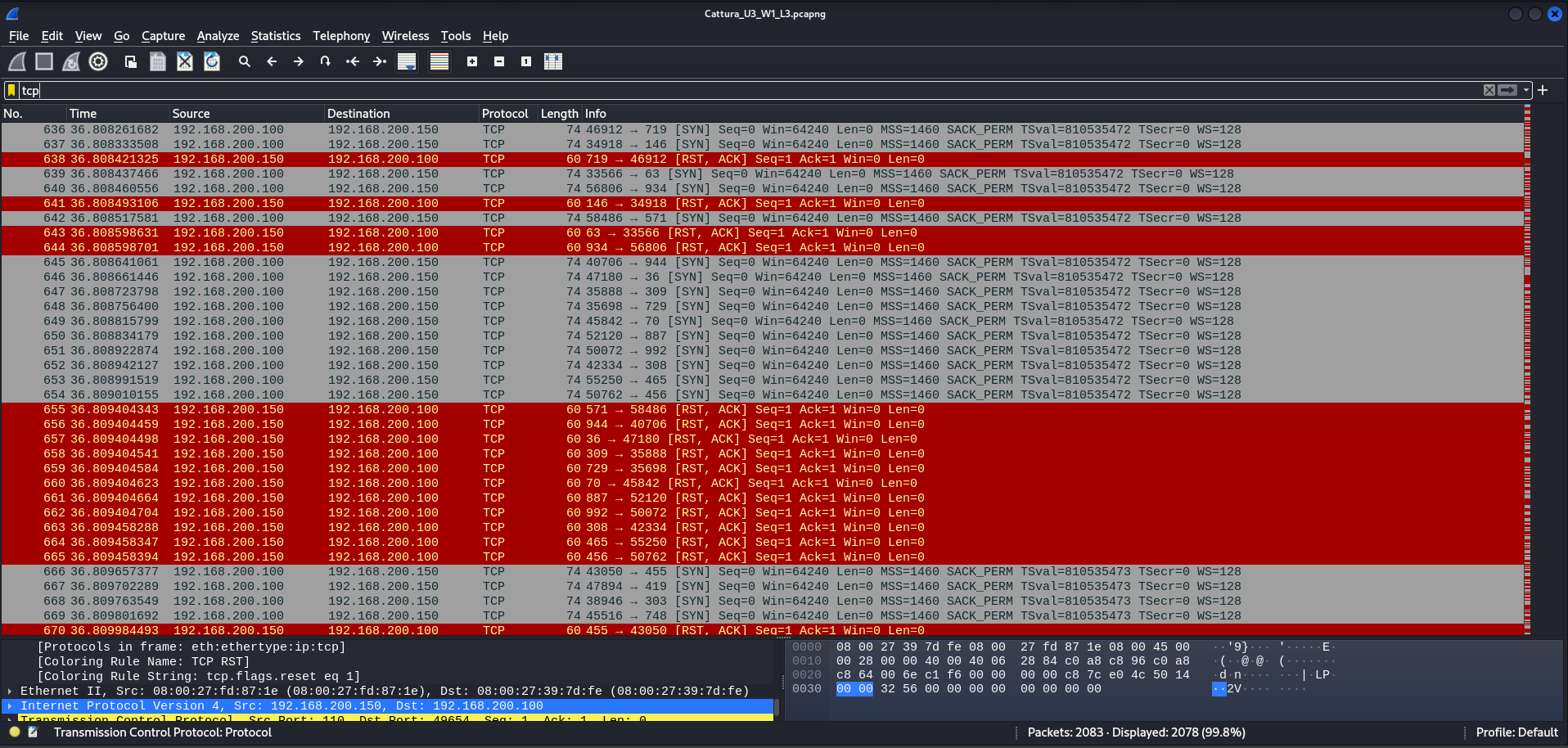
**Threat Intelligence & IOC**

**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

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

L'analisi del traffico di rete rivela un'intensa attività di tentativi di connessione TCP utilizzando il flag SYN, mirati a porte di destinazione variabili sull'host 192.168.200.150. Tale schema di comportamento è tipicamente indicativo di una scansione delle porte, condotta dall'host con indirizzo IP 192.168.200.100. Tale attività suggerisce un tentativo di identificare servizi attivi e potenzialmente vulnerabili sull'host target. La conferma di porte aperte è data dall'osservazione di pacchetti [SYN+ACK], mentre la segnalazione di porte chiuse è evidenziata da risposte [RST+ACK].

Questo tipo di attività di scansione può essere un precursore di tentativi di intrusione o di altre forme di attacco informatico, poiché l'attaccante cerca di mappare la superficie di attacco dell'host target.

Per mitigare il rischio associato a queste scansioni e potenziali attacchi successivi, l'host destinatario dovrebbe considerare l'implementazione di misure di sicurezza quali:

* Configurazione di firewall per bloccare esplicitamente connessioni in ingresso non sollecitate, in particolare da indirizzi IP sospetti come il 192.168.200.100.
* Utilizzo di sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS) per identificare e bloccare attività sospette in tempo reale.
* Regolare aggiornamento e patching dei servizi esposti per mitigare vulnerabilità note che potrebbero essere sfruttate.
* Implementazione di tecniche di oscuramento delle porte, come il cambiamento delle porte di servizio standard su numeri non convenzionali, riducendo così la superficie di attacco visibile durante una scansione casuale.

Adottando queste strategie, l'host destinatario può aumentare significativamente la propria resilienza contro scansioni malevole e tentativi di intrusione, proteggendo le proprie risorse e dati da accessi non autorizzati.