Threat Intelligence & IOC

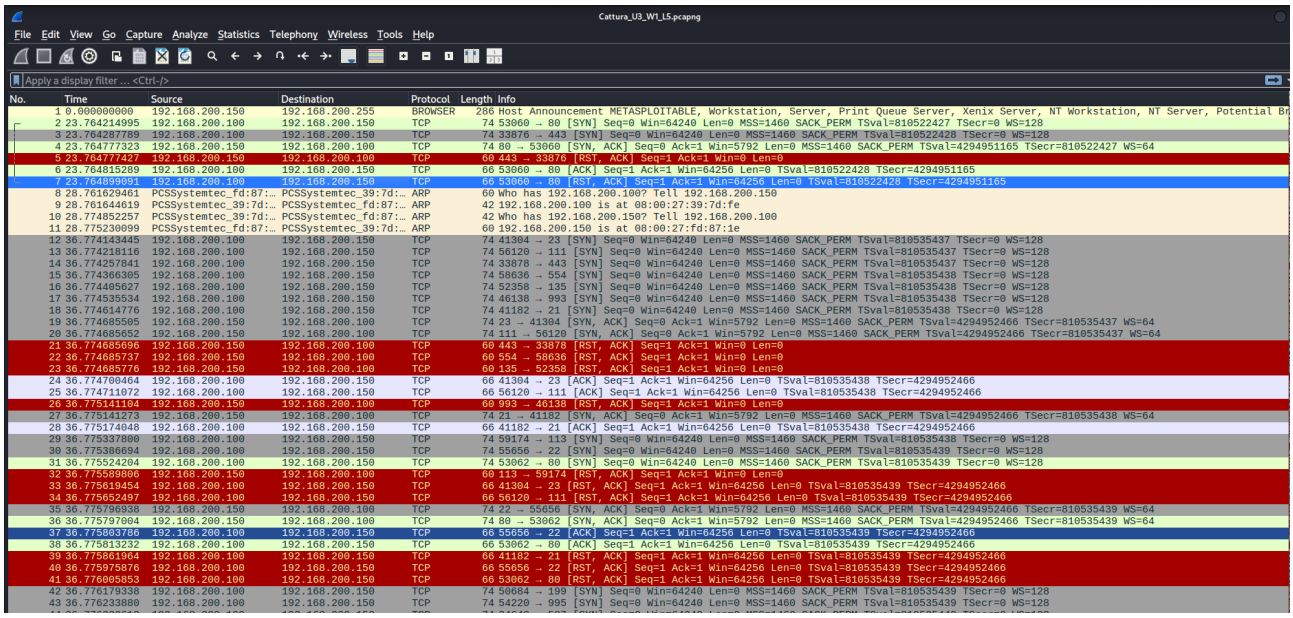
Per l’esercizio pratico di oggi, troviamo in allegato una cattura di rete effettuata con Wireshark. Dovremmo analizzare la cattura attentamente e rispondere ai seguenti quesiti:

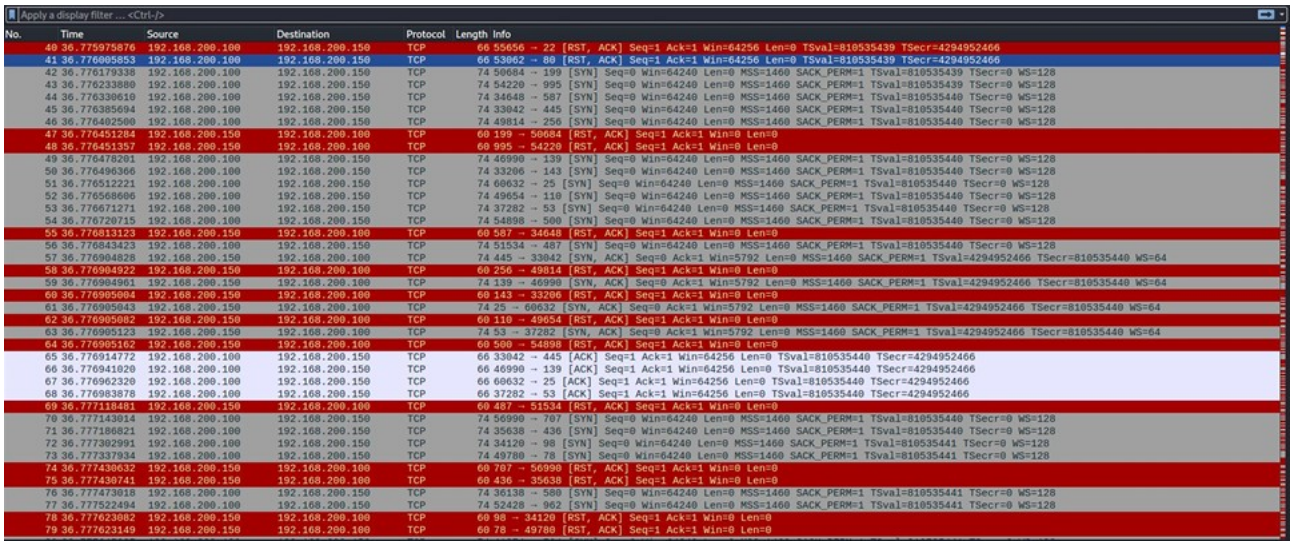
1 Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso

2 In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati

3 Consigliate un’azione per ridurre gli impatti dell’attacco attuale ed eventualmente un simile attacco futuro

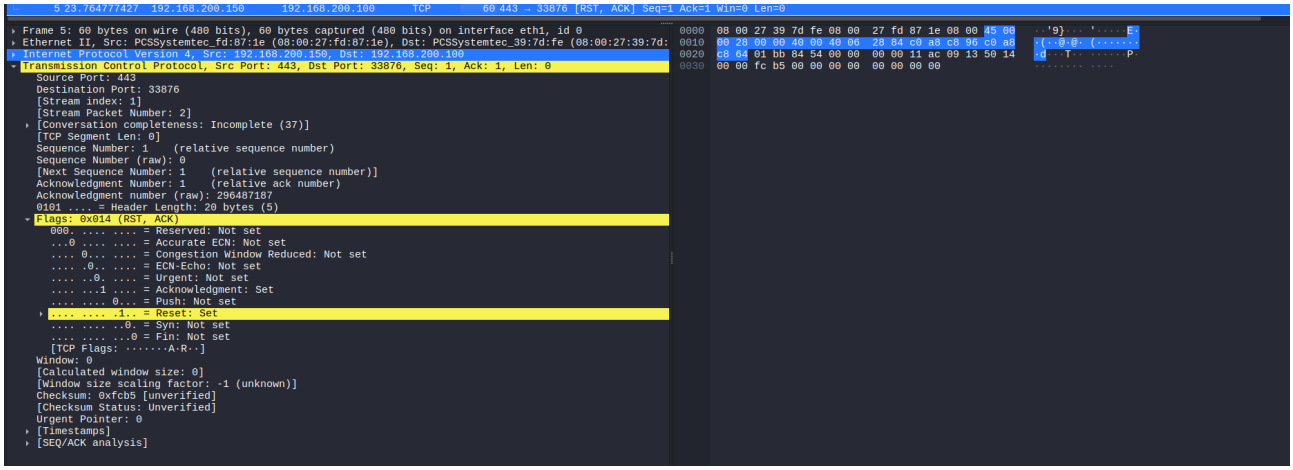
Apriamo il file sulla nostra macchina virtuale Kali con **Wireshark** per poterlo analizzare. Vediamo come ci sia un intenso traffico di pacchetti TCP tra due IP: **192.168.200.150** e **192.168.200.100** (possibile target)



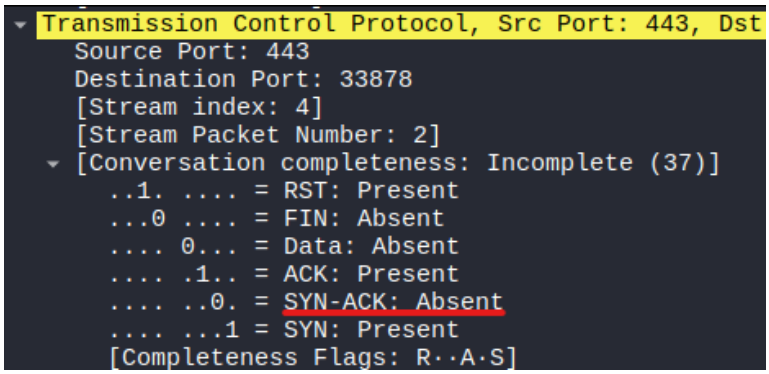


1.Analisi IOC

Da una prima analisi si nota un elevato numero di connessioni **TCP**. Le porte colpite sono oltre la numero 60000, inoltre le connessioni terminano bruscamente con il flag **“RST, ACK”.** Queste informazioni potrebbero segnalarci un **Port scanning**, con tentativi continui di connessione falliti.



Tutto ci viene ancor di più confermato dal fatto che non sono presenti le risposte **SYN-ACK**, quindi **l’handshake** non viene concluso.



2.Ipotesi sui vettori utilizzati

1 Port Scanning: l'host invia vari pacchetti di dati a diverse porte dell'IP del target per determinare quali servizi sono accessibili e in esecuzione. Tra i vari vettori che possono essere utilizzatiti abbiamo: **nmap**, **netcat metasploitable**

2 DoS (Denial of Service): l'host tenta di sovraccaricare la rete del target tramite un traffico eccessivo di dati in entrata. Questo può rendere il sistema lento e malfunzionante. Qui un potenziale vettore che può essere utilizzato è **Nping**

3 Brute Force: l'host tenta sistematicamente di forzare credenziali sui servizi esposti (come ad esempio SSH o Telnet) Tra i vari vettori che possono essere utilizzatiti abbiamo **Hydra** o **Medusa**

L'ipotesi, in teoria, più corretta dovrebbe essere il **port scanner,** questo perché:

1 Ogni volta che non avviene la risposta **SYN-ACK** l'invio di pacchetti si indirizza verso una porta diversa

2 Le porte attaccate arrivano, e addirittura, superano la 60000

3 I pacchetti sono inviati in ordine e le tempistiche indicano un possibile **nmap**

3. Azioni consigliate

Le precauzioni che si possono prendere per evitare questo tipo attacco possono essere:

1 Bloccare il traffico da 192.168.200.150 tramite firewall

2 Isolare 192.168.200.100 per verificarne l'integrità

3 Implementare un **IDS/IPS**

4 Limitare l'accesso ai servizi essenziali

5 Applicare regole di **firewall interne** per ridurre l'esposizione dei sistemi

6 Mantenere i sistemi aggiornati e chiudere porte non necessarie

4 Conclusione

L’analisi della cattura, evidenzia un comportamento di **ricognizione di rete ostile**, finalizzato all’identificazione dei servizi attivi su una possibile macchina vulnerabile. E’ cruciale in questi casi intervenire, isolando il servizio attaccato e attuare delle misure di sicurezza preventive per evitare ulteriori prove di intrusioni da parte di utenti malevoli.