



REPORT S9/L5

Threat Intelligence & IOC

Luca Tavani

Applichiamo il filtro giusto per trovare i SYN (scansione)

Step 1

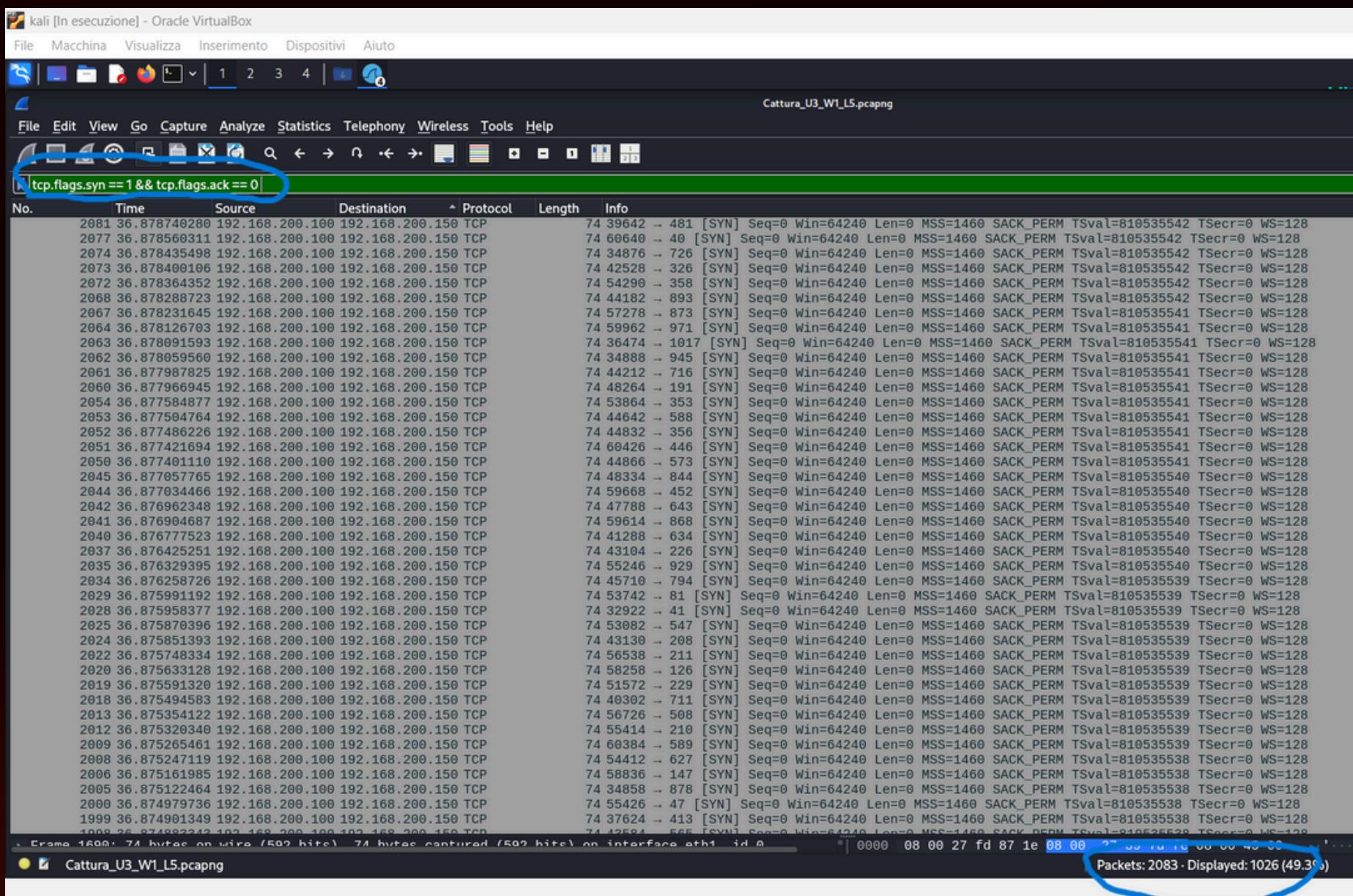
su Wireshark e nella barra filtri:

tcp.flags.syn == 1 && tcp.flags.ack == 0

Questo ci mostra:

Solo i pacchetti SYN puri

Quindi tutti i tentativi di connessione fatti dall'attaccante



Sono stati rilevati **1026** indicatori di compromissione (IOC) associati a un'attività di port scanning da parte dell'host. 192.168.200.100, che ha effettuato tentativi di connessione (flag SYN) verso numerose porte sul target 192.168.200.150. Tali attività sono tipiche di una fase di ricognizione iniziale da parte di un attaccante. Presumibilmente sta usando uno strumento di scansione nmap per iniziare con syn il three-way handshake su molte porte.

Prima analisi IOC completata.

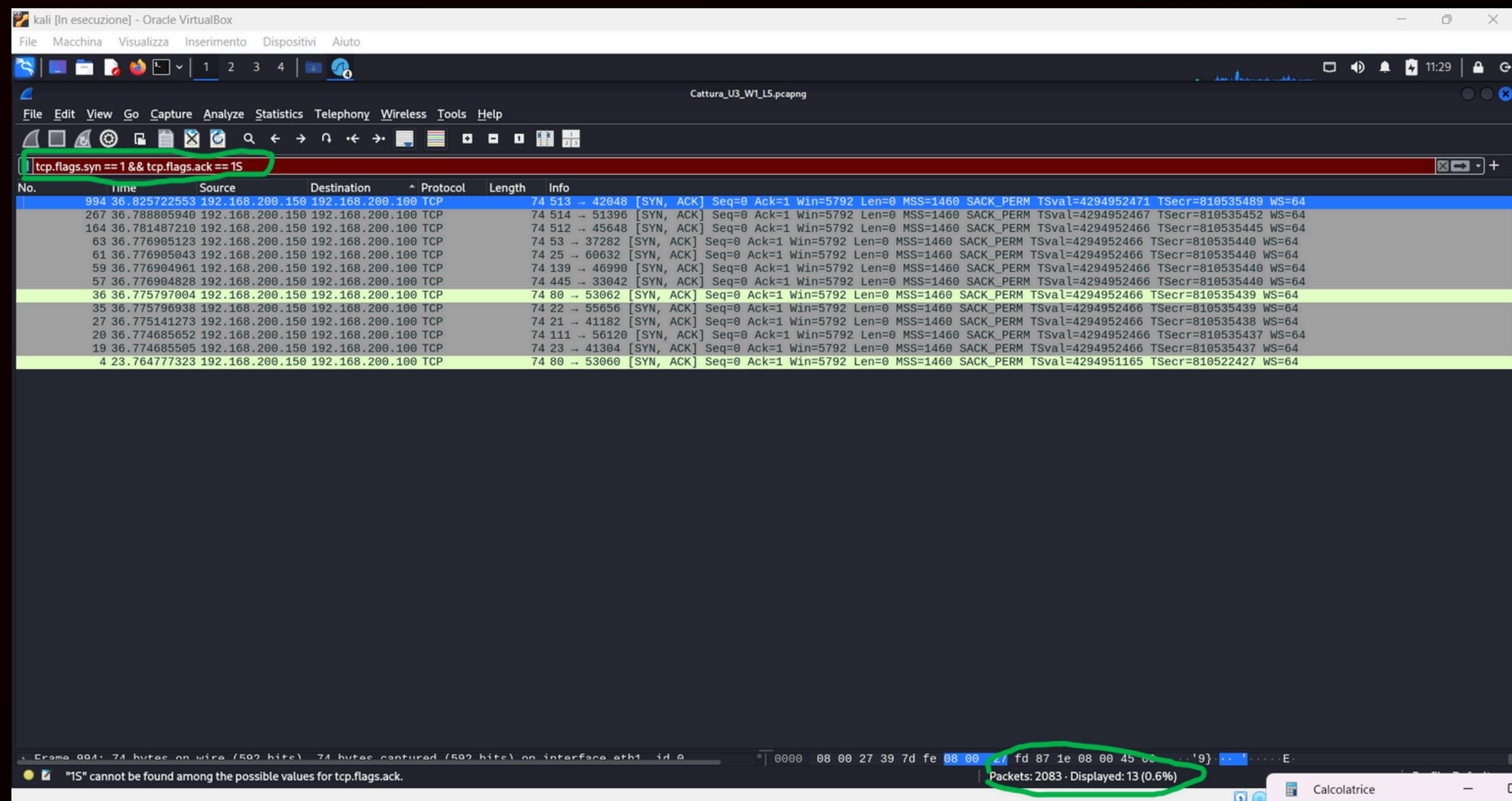
Step 2

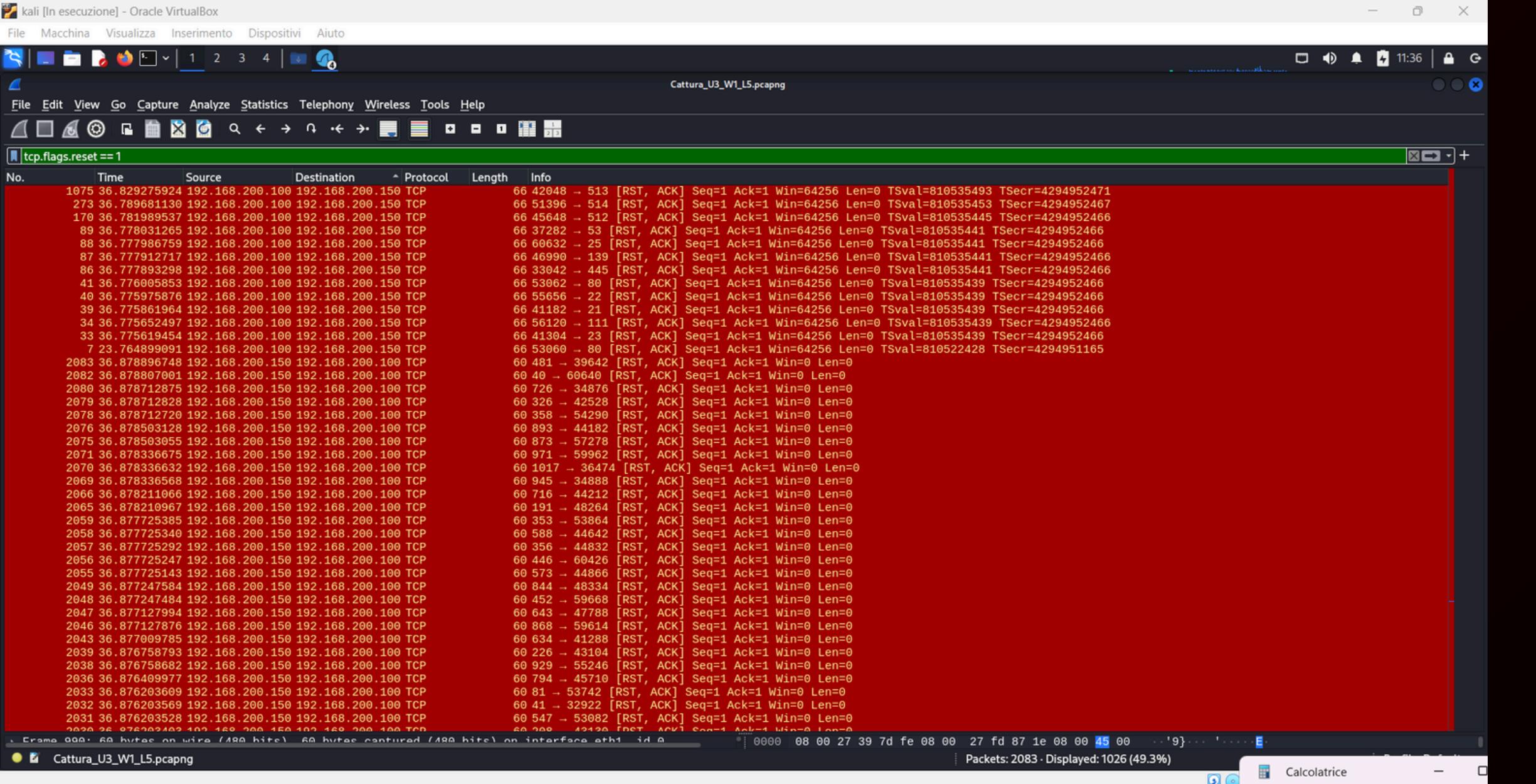
`tcp.flags.syn == 1 && tcp.flags.ack == 1`

Questo comando mostra solo SYN/ACK, cioè porte che hanno risposto positivamente

come possiamo osservare ci sono 13 risposte al Syn, la vittima ha risposto con ack mostrando dunque le porte vulnerabili.

Seconda analisi
ioc completata





Step 3



terza analisi ioc
completata

Grazie al filtro

`tcp.flags.reset == 1`

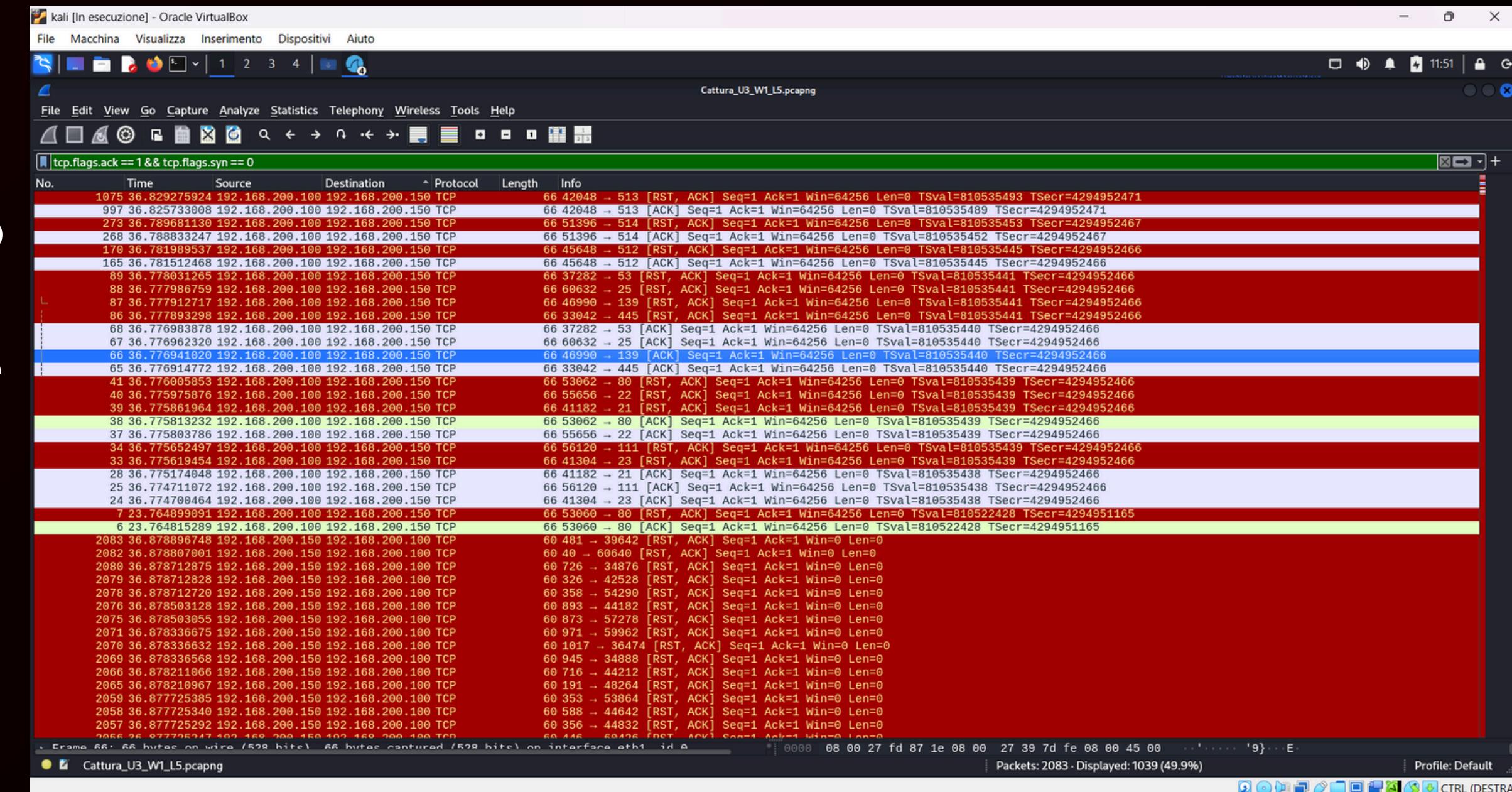
Possiamo notare senza farci ingannare dal colore che non è una criticità, anzi, i numerosi RST che vediamo servono per dimostrare che il target ha respinto l'attacco.

Step 4

Alcuni pacchetti con flag ACK non hanno ricevuto risposta visibile oppure sono stati ignorati dal target, e sono visualizzati in grigio nella cattura. Questo comportamento può indicare che il sistema difensivo ha effettuato un drop silenzioso oppure che la scansione era strutturata per evitare risposte esplicite. Tali pacchetti, sebbene non generino errori evidenti, fanno parte del comportamento malevolo dell'attaccante e vanno considerati **IOC a bassa criticità**.

Ora per valutare se l'attaccante dopo il syn synack abbia completato o tentato di fare ack usiamo il filtro:

tcp.flags.ack == 1 && tcp.flags.syn == 0



Conclusione di criticità:

L'attaccante ha inviato pacchetti SYN alle varie porte, ha ricevuto 13 risposte SYN/ACK e ha risposto con pacchetti ACK (come previsto nel three-way handshake). Tuttavia, non ha proseguito con alcun trasferimento dati, e la maggior parte delle connessioni sono state interrotte immediatamente, spesso con pacchetti RST inviati dalla vittima. Questo comportamento è indicativo di una scansione stealth effettuata probabilmente tramite Nmap in modalità TCP SYN o TCP Connect Scan, con l'obiettivo di identificare porte aperte senza stabilire una sessione attiva."

L'analisi evidenzia un attacco in corso nella sua fase preliminare di ricognizione. Tuttavia, non è stato effettuato alcun trasferimento dati successivo né si è stabilita una sessione TCP completa.

L'analisi ha incluso il controllo del campo `tcp.len`, che indica la presenza di dati nel pacchetto TCP. L'assenza di pacchetti con `tcp.len > 0` conferma che non è avvenuto alcun trasferimento di dati, e che l'attacco è rimasto confinato alla fase di ricognizione, senza svilupparsi in una compromissione attiva del sistema.

Questo conferma che l'attacco è stato intercettato e contenuto prima di un eventuale exploit, e rientra pienamente nella definizione di "attacco in corso" come indicato dalla traccia.



Azioni per ridurre attacchi futuri, si consiglia di:

- Abilitare un sistema IDS/IPS (Intrusion Detection/Prevention System) come Suricata o Snort per rilevare automaticamente scansioni e pattern sospetti.
- Implementare il port knocking o il firewall con regole più restrittive, evitando l'esposizione diretta di porte non necessarie.
- Limitare la visibilità dei servizi tramite firewall perimetrale e segmentazione della rete, in modo che i servizi sensibili siano accessibili solo da indirizzi IP autorizzati.
- Applicare il rate limiting per evitare che un host possa effettuare troppi tentativi in poco tempo.
- Effettuare un hardening dei servizi attivi sulle 13 porte che hanno risposto al SYN/ACK, verificando che siano protette da autenticazione forte e aggiornate.
- Monitorare i log di sistema in tempo reale, integrando strumenti come Zeek, ELK stack o Security Onion per un'analisi continua e visiva del traffico.

Grazie per l'attenzione

Luca Javani

