Report: Analisi Threat Intelligence e Indicatori di Compromissione

1. Obiettivo dell'analisi

L'obiettivo dell'esercitazione è identificare eventuali **Indicatori di Compromissione (IOC)** all'interno di una **cattura di rete** (.pcapng) ottenuta tramite Wireshark, riconducibili ad **attacchi informatici in corso o già avvenuti**.
Successivamente, sarà necessario ipotizzare il **vettore di attacco** e suggerire delle **contromisure** tecniche per limitare gli impatti futuri.

2. Preparazione e set-up

- 2.1 Acquisizione del file

È stato fornito il file Cattura_U3_W1_L5.pcapng contenente la cattura di rete da analizzare.

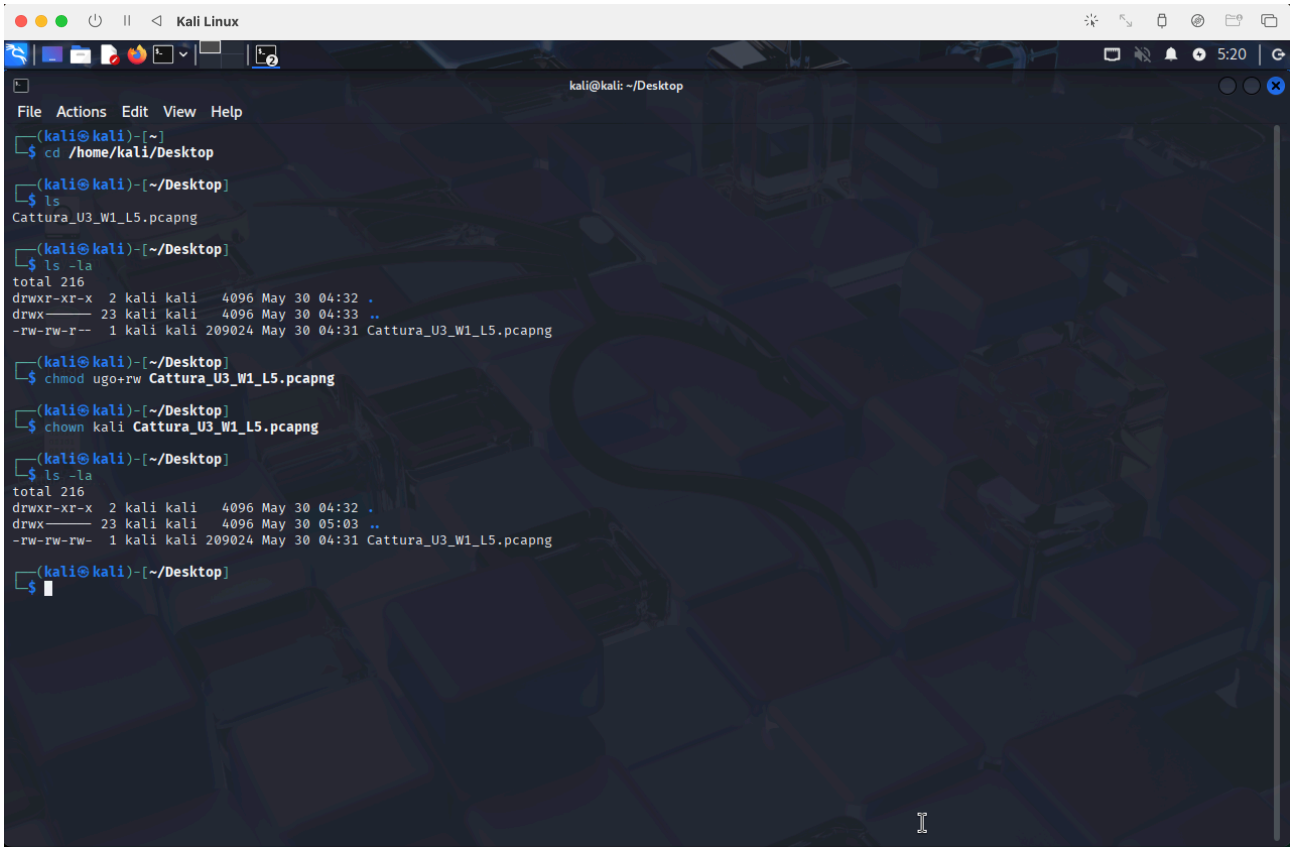
- 2.2 Importazione su Kali Linux

Il file è stato spostato nella directory del Desktop dell'utente Kali e sono stati verificati e assegnati correttamente i permessi per consentirne la lettura e l'apertura da parte di Wireshark.

Nota: I permessi del file risultavano già corretti (rw-rw-r--, owner: kali), tuttavia, per sicurezza e in linea con la procedura illustrata nella traccia, sono stati riconfermati manualmente tramite chmod e chown.
Quindi non erano strettamente necessarie né la chmod né la chown, **ma** eseguirle **non ha creato alcun problema**: è stato solo un passaggio **ridondante ma prudente**, utile se ci fossero state incertezze o se il file fosse stato copiato da root o con permessi errati.

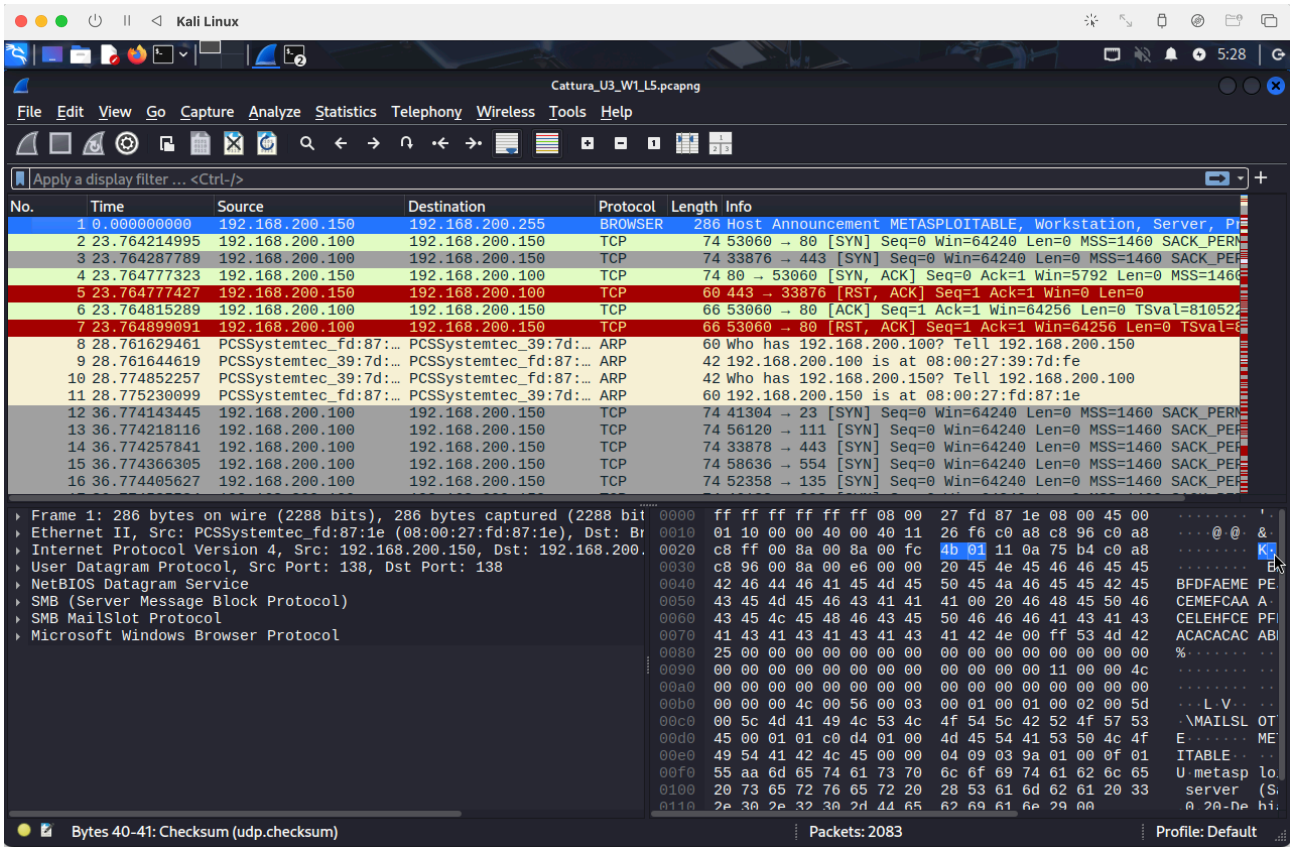
- chmod ugo+rw: garantisce che tutti gli utenti (user, group, others) abbiano **permessi di lettura e scrittura** sul file.
- chown kali: assegna la **proprietà del file** all'utente kali.

Questi passaggi sono **fondamentali** per evitare errori di accesso durante l'analisi in Wireshark.



- 2.3 Apertura con Wireshark

Il file è stato infine aperto correttamente, pronto per l'analisi.

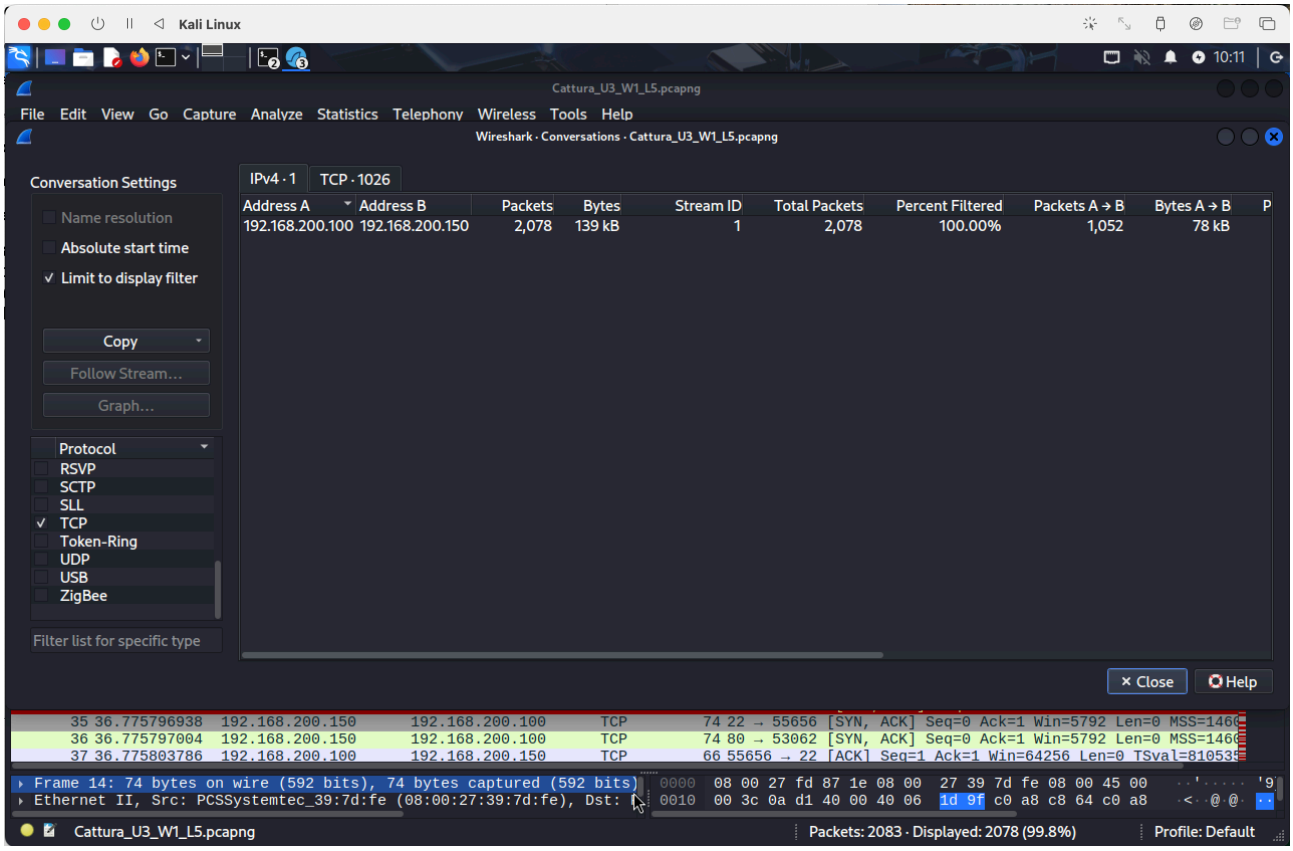


3. Analisi delle conversazioni, grafici I/O e tracciamento dell'attaccante

Per rafforzare l'analisi e identificare con precisione l'host responsabile dell'attività malevola (attaccante), sono stati effettuati i seguenti approfondimenti su Wireshark:

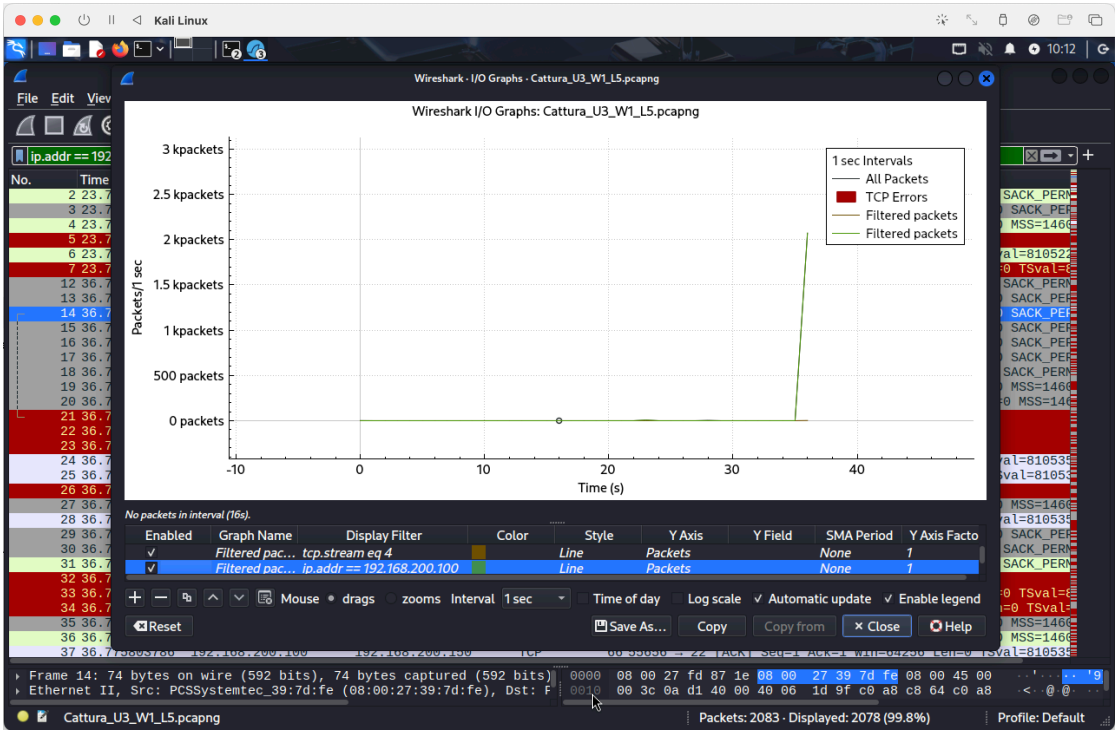
3.1 Analisi delle conversazioni TCP

Attraverso il menu Statistics > Conversations, scheda **TCP**, è stato possibile osservare che l'indirizzo IP 192.168.200.100 ha instaurato **una sola conversazione TCP molto intensa** con 192.168.200.150, per un totale di **2078 pacchetti** e **139 kB** scambiati. Questo dato è coerente con un comportamento aggressivo e automatizzato, come quello osservabile in un attacco di scansione o forza bruta.



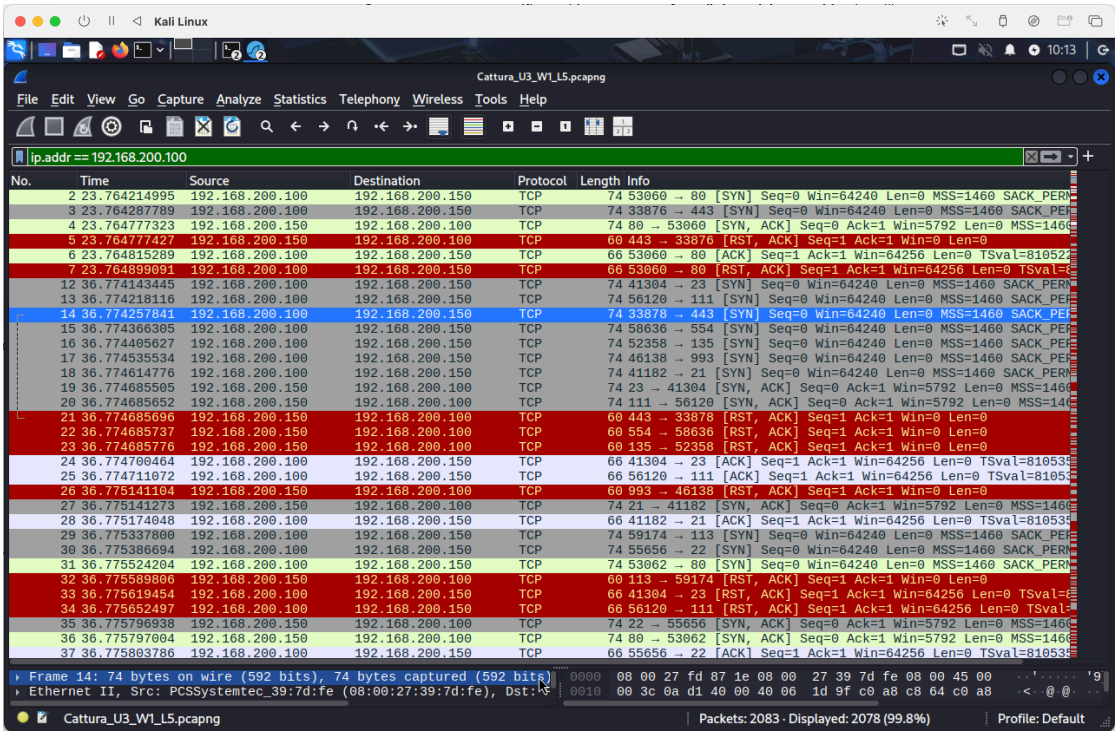
3.2 Analisi del traffico nel tempo (I/O Graphs)

Dal grafico generato in Statistics > I/O Graphs, applicando il filtro ip.addr == 192.168.200.100, si osserva un **picco improvviso di traffico**, concentrato in una finestra temporale ristretta (tra il secondo 36 e 38). Questo comportamento è tipico di un attacco automatizzato, come un TCP scan o un tentativo di brute-force, che genera un numero elevato di connessioni in pochissimo tempo.



3.3 Tracciamento dell'attaccante

Applicando il filtro ip.addr == 192.168.200.100, abbiamo isolato tutto il traffico associato all'host sospetto. I risultati confermano che l'host 192.168.200.100 ha avviato **centinaia di richieste TCP SYN** verso l'host bersaglio 192.168.200.150, su più porte (80, 443, 21, 111, ecc.), ricevendo **pacchetti RST/ACK** in risposta. Questo conferma che l'host bersaglio stava **rifiutando connessioni**, probabilmente a causa di un tentativo di connessione anomala (es. tentativo di scansione porte).



4. Identificazione degli Indicatori di Compromissione (IOC)

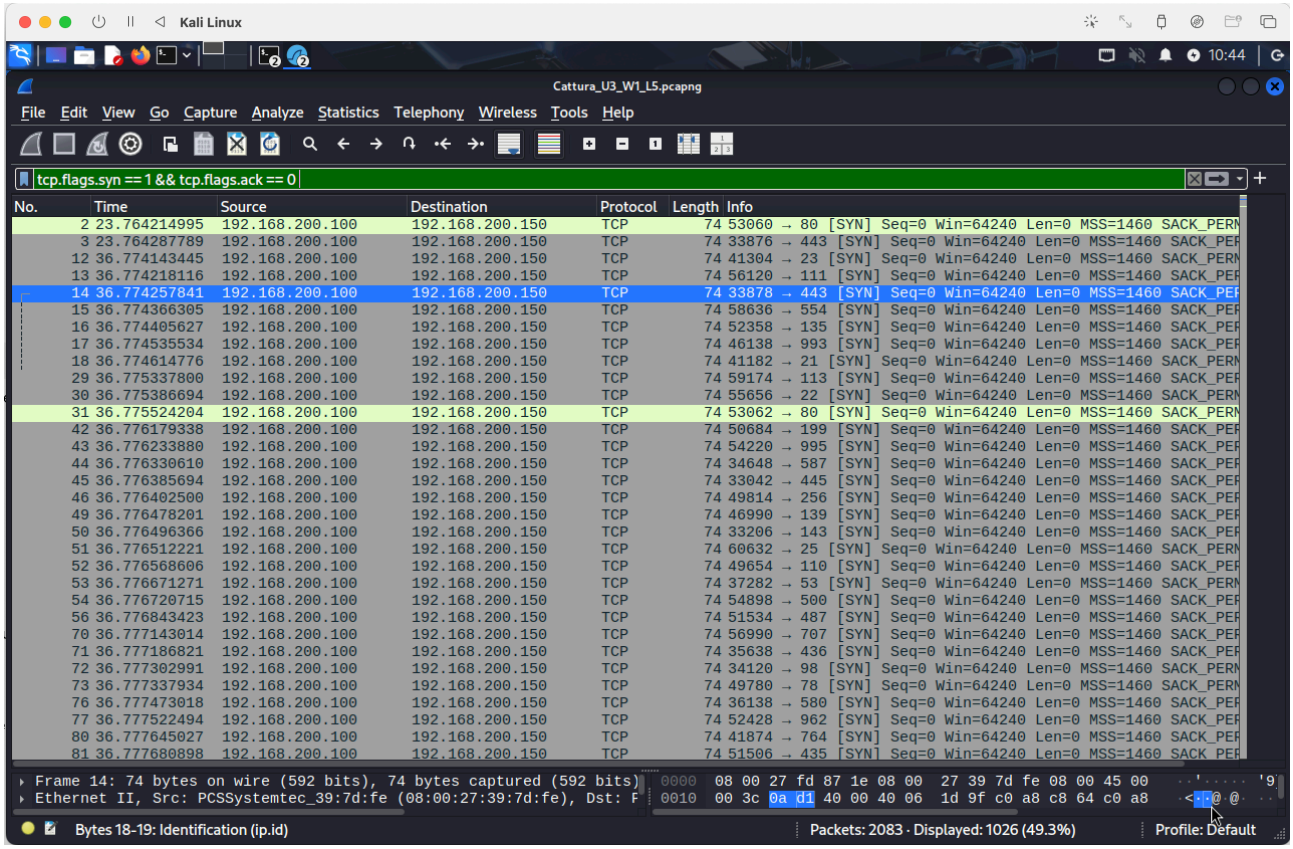
Dall'analisi approfondita del traffico catturato, emergono con chiarezza diversi **indicatori di compromissione**, associati a una fase di **ricognizione attiva** condotta dall'host 192.168.200.100. Questa attività è stata isolata attraverso filtri specifici su Wireshark, con evidenze tecniche puntuali.

4.1 Filtro SYN – TCP Port Scanning

Filtro utilizzato: tcp.flags.syn == 1 && tcp.flags.ack == 0

Osservazioni:

- L'attaccante ha inviato richieste TCP SYN verso il target 192.168.200.150 su numerose porte (21, 22, 80, 443, 445, 3389…).
- L'assenza di flag ACK indica che l'obiettivo era identificare **porte aperte**, senza stabilire connessioni complete.

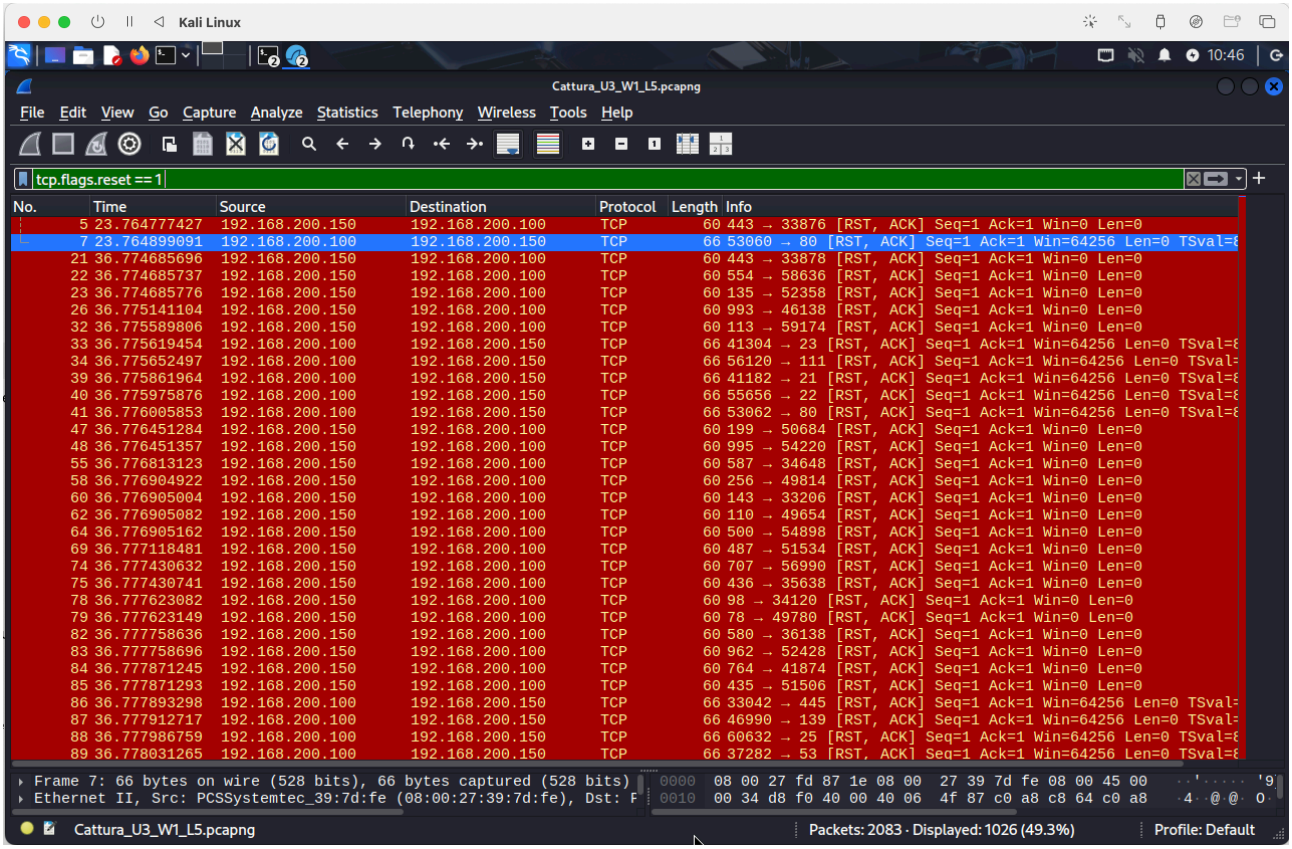


4.2 Filtro RST – Rifiuto sistematico delle connessioni

Filtro utilizzato: tcp.flags.reset == 1

Osservazioni:

- Le risposte del target 192.168.200.150 sono **pacchetti RST/ACK**, che indicano il rifiuto attivo delle connessioni.
- Questo comportamento è **tipico di un sistema che non ha i servizi attivi sulle porte target**, o che blocca le connessioni indesiderate.



4.3 TCP Streams – Nessun payload

Procedura:

- Tasto destro su un pacchetto TCP SYN verso porta 80 o 443 > Follow > TCP Stream.

Risultato:

- I flussi risultano **vuoti** (nessun dato HTTP/HTTPS trasmesso), confermando che le connessioni **non sono mai state completate**.

4.4 IO Graph – Picco di traffico

Filtro usato: ip.addr == 192.168.200.100

Osservazioni:

- L’host attaccante ha generato **un picco improvviso e concentrato di pacchetti** in una finestra temporale molto breve (tra secondo 36 e 38).
- Questo pattern è tipico di uno **scan automatizzato** (es. Nmap, masscan).

4.5 Tabella riepilogativa degli IOC

Tipo IOC	Dettaglio	Evidenza tecnica
IP attaccante	192.168.200.100	Tutto il traffico malevolo proviene da qui
Port Scanning	SYN verso porte comuni	Filtro: tcp.flags.syn == 1 && tcp.flags.ack == 0
Blocco delle porte	Risposte RST/ACK dal target	Filtro: tcp.flags.reset == 1
Nessun payload	TCP Stream vuoti (no GET, POST, SSL handshake)	Follow TCP Stream
Traffico anomalo	Picco nel grafico I/O	Finestra temporale limitata

5. Ipotesi vettore d’attacco e contromisure

Obiettivo: Fornire una spiegazione plausibile dell'attacco e proporre difese concrete per prevenirlo.

Ipotesi sull’attacco

Dall’analisi delle trame e dei flag TCP risulta evidente un attacco in corso da parte dell’host **192.168.200.100** verso **192.168.200.150**. I pacchetti in sequenza mostrano:

- Numerose richieste **TCP SYN** verso molte porte.
- Risposte **RST/ACK** che indicano che le porte sono chiuse o bloccate.
- Tentativi su porte 80, 443, 111, 22 ecc. => indica **scansione attiva delle porte (port scan)**.

Tecnica individuata: TCP SYN Scan

Strumento plausibile: Nmap

Vettore d'attacco: Ricognizione per rilevamento servizi attivi, primo passo di una possibile intrusione.

Contromisure consigliate:

- **Configurazione firewall**
  - Bloccare attivamente gli IP sospetti (es. 192.168.200.100).
  - Abilitare regole IDS/IPS per identificare scansioni di rete.
- **Port Knocking / Port Filtering**
  - Utilizzare tecniche di offuscamento delle porte (nascondere SSH, HTTP non pubblici).
- **Rate limiting**
  - Limitare il numero di connessioni TCP al secondo per proteggere i servizi esposti.
- **Threat Intelligence attiva**
  - Integrare con strumenti SIEM per correlare eventi e bloccare in tempo reale.

6. Conclusioni finali e osservazioni

L'analisi del file Cattura_U3_W1_L5.pcapng ha permesso di ricostruire con precisione una fase iniziale di attacco, riconducibile a una **ricognizione tecnica tramite TCP SYN Scan**, condotta dall'host 192.168.200.100 contro il target 192.168.200.150.

I dati raccolti sono coerenti con un attacco automatizzato, caratterizzato da:

- Elevato numero di pacchetti SYN inviati in breve tempo;
- Risposte RST/ACK da parte del target, che rifiuta le connessioni;
- Assenza di payload nei flussi TCP (connessioni non completate);
- Picco di traffico nel grafico I/O, compatibile con scansioni rapide (es. Nmap).

Non si rilevano evidenze di accesso riuscito o di esfiltrazione dati, pertanto l'attività è da classificarsi come **tentativo di enumerazione dei servizi esposti** (ricognizione). Tuttavia, trattandosi della **prima fase della cyber kill chain**, l'attività può evolvere rapidamente in un attacco completo se non contenuta.

Valutazione complessiva

L'host attaccante ha agito in modo sistematico, testando porte e protocolli noti per scoprire vulnerabilità sfruttabili. L'assenza di risposta concreta da parte del target (nessun handshake completo, né contenuti HTTP visibili) dimostra che il bersaglio ha respinto i tentativi, ma evidenzia comunque un'esposizione di superficie potenzialmente attaccabile.

L'analisi effettuata ha permesso di identificare:

- L'origine dell'attacco;
- Il metodo e la tecnica impiegata;
- Il comportamento difensivo del sistema;
- Le principali contromisure da implementare per rafforzare la sicurezza.

Sintesi finale

L'analisi del file Cattura_U3_W1_L5.pcapng ha evidenziato un'attività di ricognizione in corso da parte dell'host 192.168.200.100, che ha eseguito un TCP SYN scan sul target 192.168.200.150. I numerosi tentativi di connessione su porte comuni, la risposta sistematica con pacchetti RST/ACK e l'assenza di payload nei flussi TCP confermano che si tratta di una scansione non autorizzata in fase iniziale.

Il picco di traffico concentrato in pochi secondi e il volume elevato di pacchetti generati rafforzano l'ipotesi di un attacco automatizzato, probabilmente con strumenti come Nmap. Sebbene l'attacco non sia andato a segno, rappresenta un chiaro indicatore di compromissione.

La rete ha reagito correttamente bloccando le connessioni, ma il comportamento osservato giustifica l'adozione di contromisure preventive, come firewall, IDS/IPS e segmentazione. L'intervento tempestivo e l'analisi accurata permettono di mitigare il rischio e prevenire escalation future.

Spinazzola (BT) 30/05/2025