

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.

```
Kali Linux
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)~$ cd /home/kali/Desktop
(kali@kali)~/Desktop$ ls
Cattura_U3_W1_L5.pcapng
(kali@kali)~/Desktop$ ls -la
total 216
drwxr-xr-x  2 kali kali   4096 May 30 04:32 .
drwxr-xr-x 23 kali kali   4096 May 30 04:33 ..
-rw-rw-r--  1 kali kali 209024 May 30 04:31 Cattura_U3_W1_L5.pcapng
(kali@kali)~/Desktop$ chmod ugo+rw Cattura_U3_W1_L5.pcapng
(kali@kali)~/Desktop$ chown kali Cattura_U3_W1_L5.pcapng
(kali@kali)~/Desktop$ ls -la
total 216
drwxr-xr-x  2 kali kali   4096 May 30 04:32 .
drwxr-xr-x 23 kali kali   4096 May 30 05:03 ..
-rw-rw-rw-  1 kali kali 209024 May 30 04:31 Cattura_U3_W1_L5.pcapng
(kali@kali)~/Desktop$
```

- 2.3 Apertura con Wireshark

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

Wireshark interface showing a packet capture of a Metasploit session. The packet list shows a SYN flood attack from 192.168.200.150 to 192.168.200.255. The packet details pane shows the Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and NetBIOS Datagram Service layers. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, P...
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER...
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER...
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=146...
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=81052...
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=...
8	28.761629461	PCSSystemtec_fd:87:...	PCSSystemtec_39:7d:...	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d:...	PCSSystemtec_fd:87:...	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PCSSystemtec_39:7d:...	PCSSystemtec_fd:87:...	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PCSSystemtec_fd:87:...	PCSSystemtec_39:7d:...	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER...
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER...
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER...
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER...
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER...

Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bi...
Ethernet II, Src: PCSSystemtec_fd:87:1e (08:00:27:fd:87:1e), Dst: Br...
Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200...
User Datagram Protocol, Src Port: 138, Dst Port: 138
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
Microsoft Windows Browser Protocol

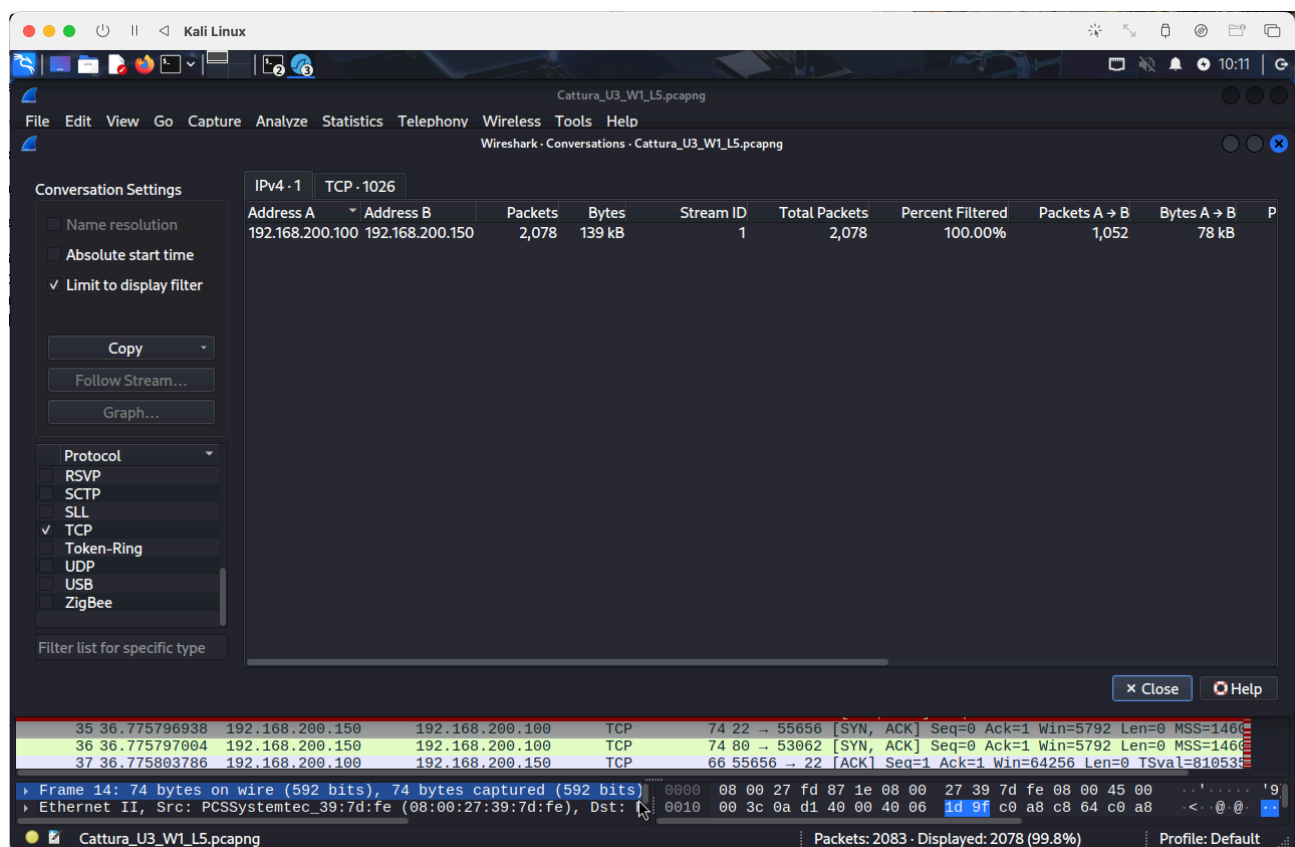
Bytes 40-41: Checksum (udp.checksum) Packets: 2083 Profile: Default

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:

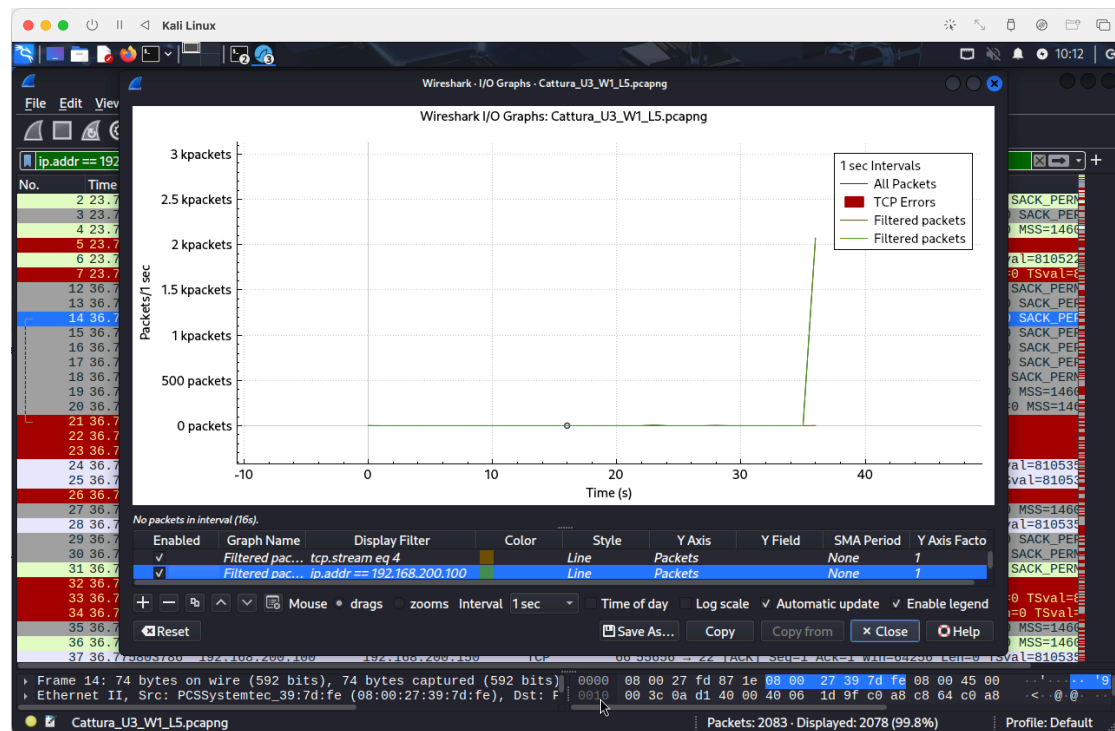
3.1 Analisi delle conversazioni TCP

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).

The image shows the Wireshark packet list window for the file 'Cattura_U3_W1_L5.pcapng'. The list displays network traffic filtered by the filter 'ip.addr == 192.168.200.100'. The list shows a series of TCP SYN packets (Seq=0, Win=64240, Len=0, MSS=1460) sent from 192.168.200.100 to 192.168.200.150, and corresponding RST/ACK packets (Seq=1, Ack=1, Win=64256, Len=0, TSval=81053) sent from 192.168.200.150 back to 192.168.200.100. The list also shows other TCP packets (Seq=0, Win=64240, Len=0, MSS=1460) sent from 192.168.200.100 to 192.168.200.150. The list is sorted by time, showing the sequence of events. The bottom of the window displays the packet details for the selected packet (Frame 14), showing the Ethernet II header and the IP header.

No.	Time	Source	Destination	Protocol	Length	Info
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 33876 [RST, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
5	23.764777427	192.168.200.150	192.168.200.100	TCP	68	443 → 33876 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=81052
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=81052
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
15	36.774360305	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
19	36.774685595	192.168.200.100	192.168.200.150	TCP	74	23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
20	36.774695652	192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
21	36.774685606	192.168.200.150	192.168.200.100	TCP	68	443 → 33878 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	68	554 → 58636 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	68	135 → 52358 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
24	36.774709404	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=81053
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=81053
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=81053
29	36.775337800	192.168.200.100	192.168.200.150	TCP	74	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74	55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
32	36.775589806	192.168.200.150	192.168.200.100	TCP	68	113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775610454	192.168.200.150	192.168.200.100	TCP	68	41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=81053
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=81053
35	36.775799938	192.168.200.150	192.168.200.100	TCP	74	22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
36	36.775797094	192.168.200.150	192.168.200.100	TCP	74	80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=81053

4. Identificazione degli Indicatori di Compromissione (IOC)

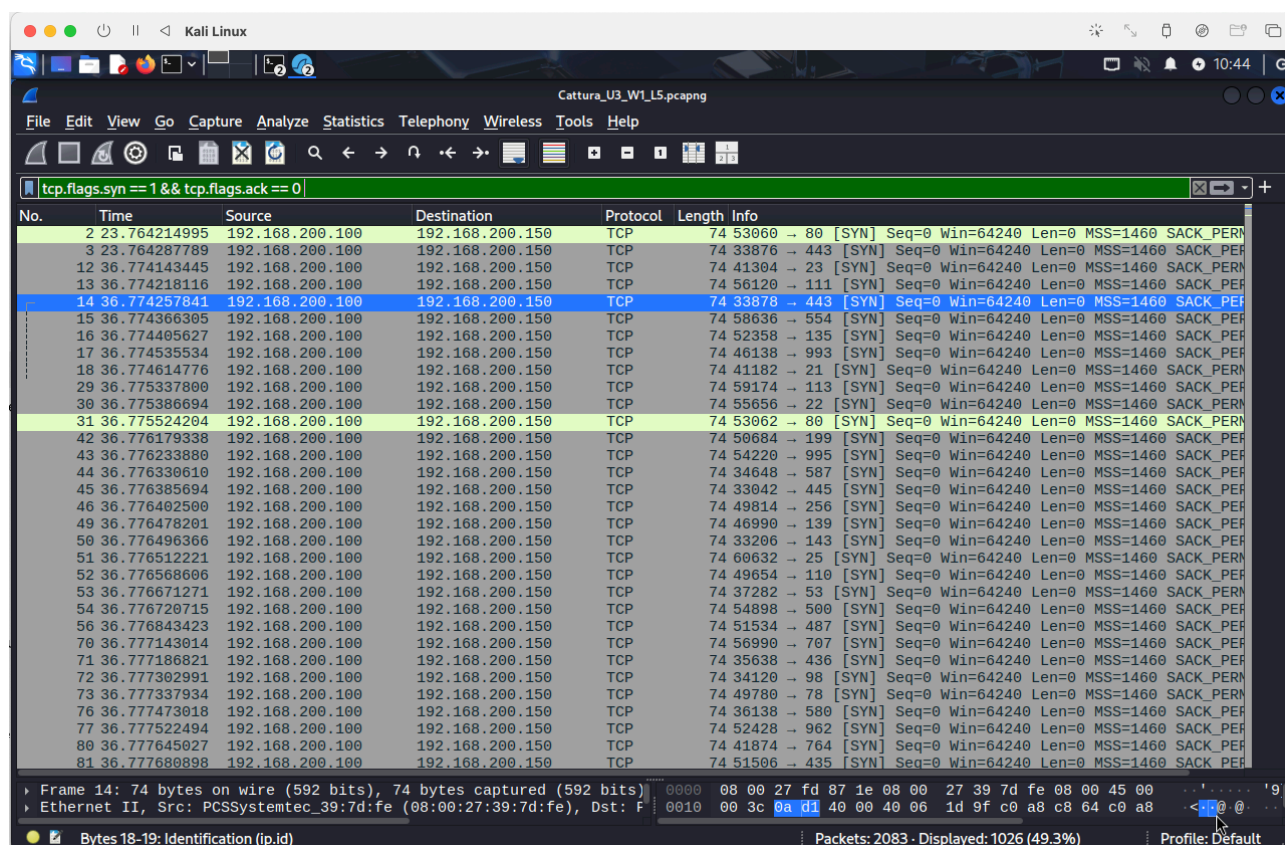
Dall'analisi approfondita del traffico catturato, emergono con chiarezza diversi **indicatori di compromissione**, associati a una fase di **ricognizione attiva** condotta dall'host 192.168.200.100. Questa attività è stata isolata attraverso filtri specifici su Wireshark, con evidenze tecniche puntuali.

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.

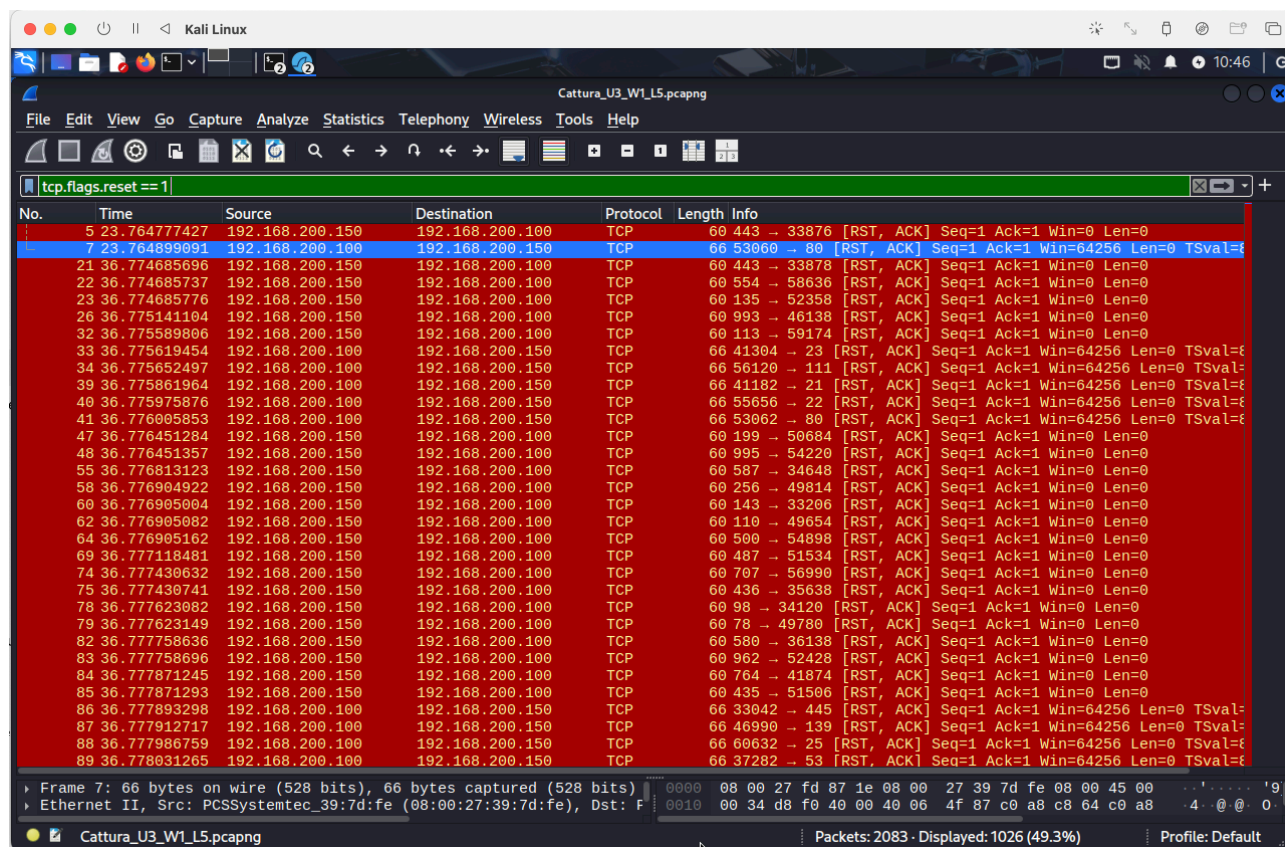


4.2 Filtro RST – Rifiuto sistematico delle connessioni

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.