S9-L3

Preparazione

Importiamo il file sulla nostra Kali ed apriamolo (tramite GUI doppio clic, se da terminale dai prima tutti i permessi user)

Per aprire il file utilizzeremo Wireshark, un tool GUI che ci permette di analizzare e monitorare i flussi di rete sniffando le comunicazioni su una rete, permettendoci di identificare potenziali compromissioni.

Considerando gli indicatori di compromissione (IOC) rilevabili a livello di rete, nel file corrente potremmo apprezzare richieste TCP multiple su ampi intervalli di porte; questo è indicativo di una scansione in corso.

Filtri

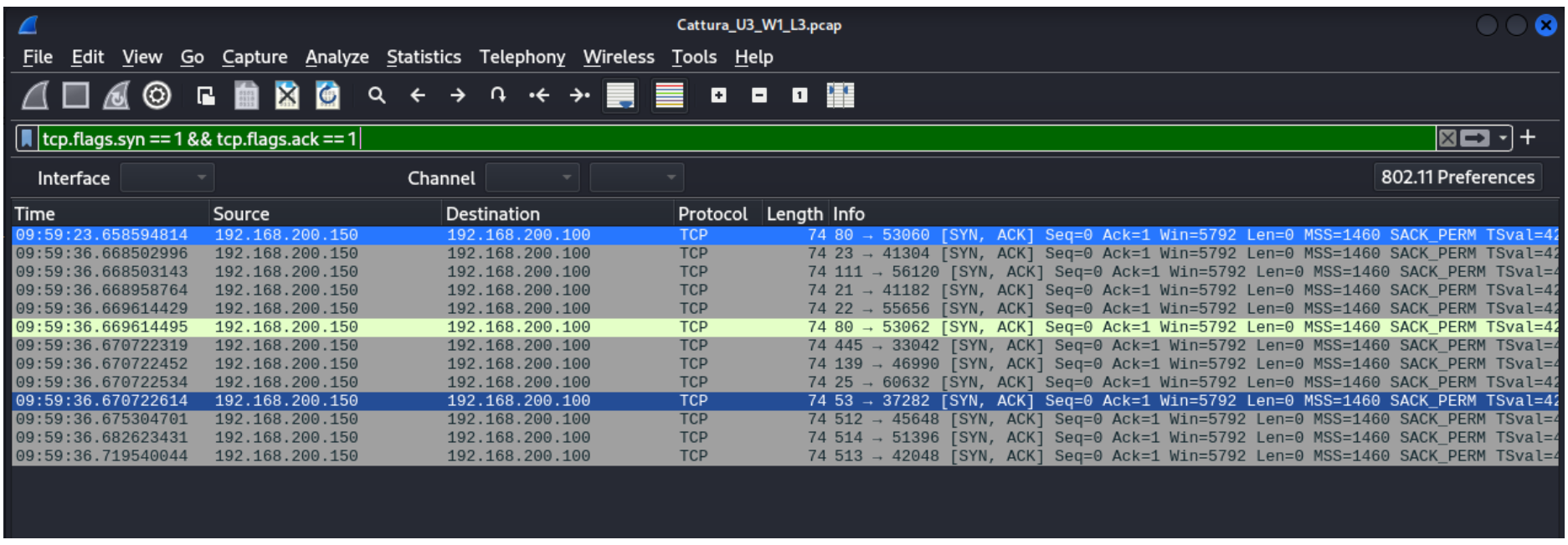
Per muoverci meglio all'interno di questo file possiamo applicare dei filtri.

Il primo filtro da utilizzare lo applicheremo per prendere coscienza del numero di pacchetti (o frames) catturati dalla rete che siano arrivati al secondo passaggio del three hands shake (SYN-ACK).

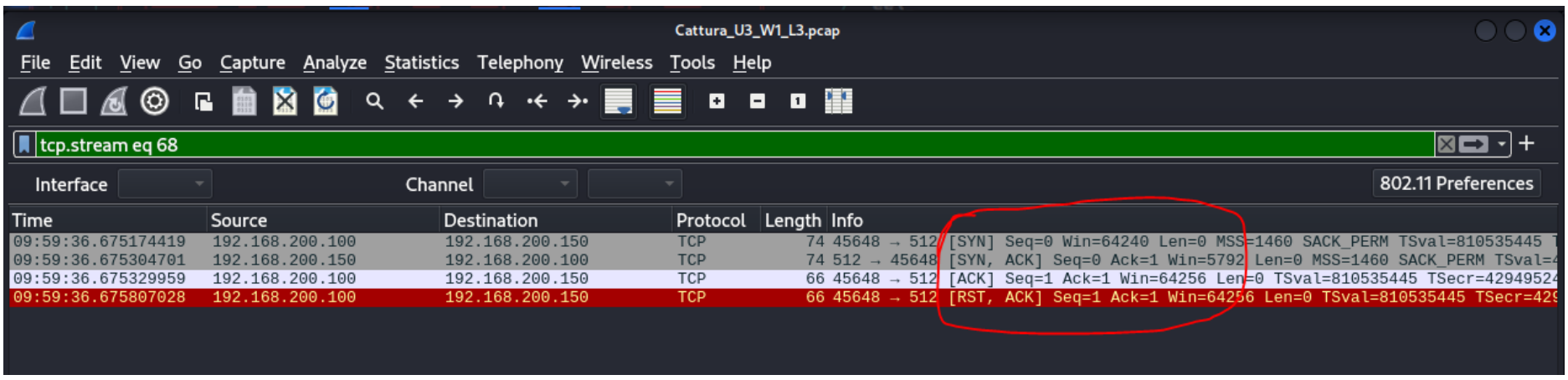
Il comando utilizzato è il seguente:

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

Ecco l'output:



Se clicchiamo con il tasto destro su un frame, come quello evidenziato in blu nell'immagine soprastante, e andando su Follow TCP, allora potremmo visionare come output l'immagine sottostante.



Tutte le porte della prima immagine ci daranno un output articolato in quattro frame come il sovrastante.
In questo screen possiamo apprezzare:

- Primo frame, questo è il primo pacchetto inviato dal client al server per iniziare una connessione TCP. Nel pacchetto SYN, il client invia un numero di sequenza iniziale (ISN) e chiede di stabilire una connessione.
- Secondo frame, questo è il secondo pacchetto, inviato dal server in risposta al pacchetto SYN del client. Il server risponde con un proprio numero di sequenza e un numero di acknowledgment (ACK) che conferma la ricezione del SYN dal client.
- Terzo frame, questo è il terzo pacchetto, inviato dal client per confermare la ricezione del SYN-ACK del server. Con questo pacchetto, il client invia un acknowledgment per il numero di sequenza del server, completando così il handshake.

Il pacchetto in rosso visualizzato nello screenshot di Wireshark indica un pacchetto TCP con i flag "RST" e "ACK" attivi. Questo tipo di pacchetto è comunemente utilizzato per terminare una connessione TCP o per segnalare che un pacchetto è stato ricevuto in un contesto inaspettato.

Nello specifico, il flag **RST (Reset)** viene usato per interrompere una connessione, ad esempio se un host riceve un pacchetto per una connessione che non riconosce o non vuole mantenere attiva. Il flag **ACK (Acknowledge)** conferma che il pacchetto è stato ricevuto.