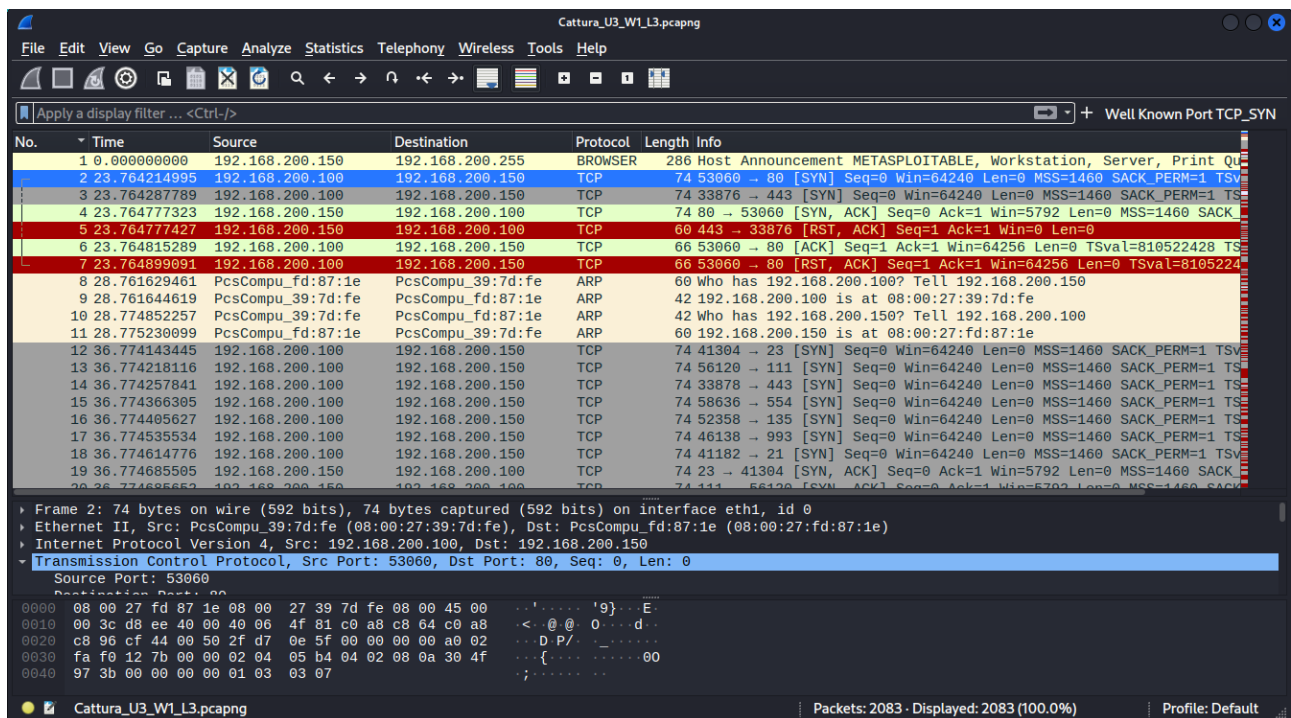


# Threat Intelligence & IoC

Per l'esercizio pratico di oggi analizzeremo la cattura di una comunicazione con Wireshark

## FASE 1

Iniziamo ad analizzare il file rilasciato dalla traccia. Una volta portato il file all'interno dell'ambiente Kali, tramite la cartella condivisa, lo carichiamo all'interno di **Wireshark**



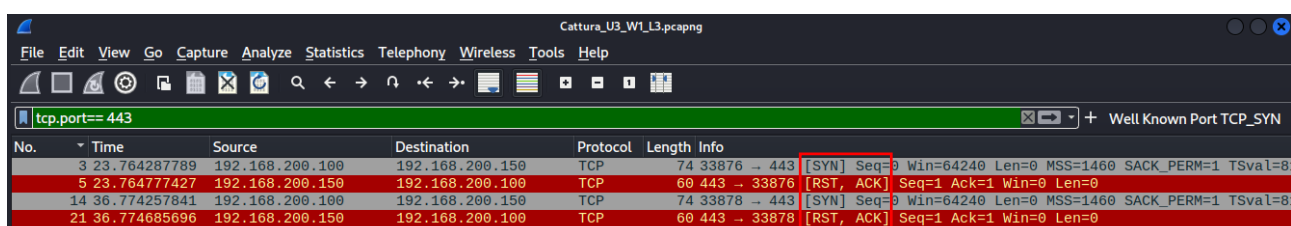
## FASE 2

La prima cosa che notiamo è la presenza dello stesso IP attaccante “**192.168.200.150**”.

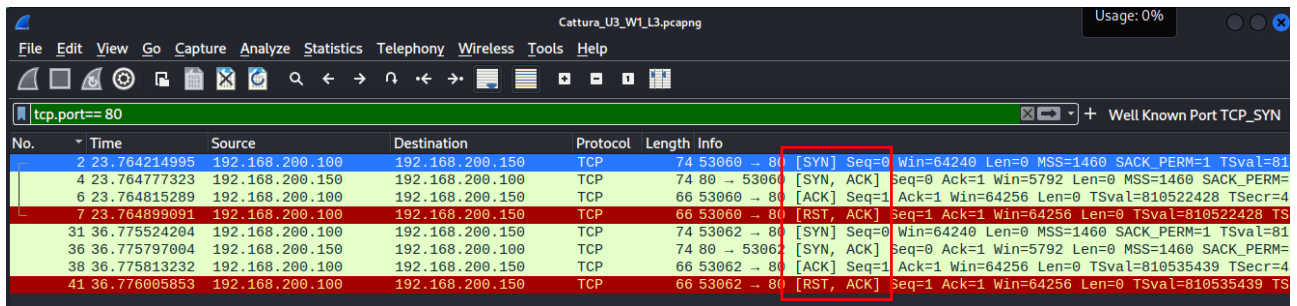
La continua presenza di questo IP e la presenza di una comunicazione andata a buon fine su molte porte, ci conferma che si tratta di una scansione. Il RST inviato dalla macchina attaccante ci conferma ulteriormente una scansione di tipo -sT o -sV. Il che significa che qualcuno vuole sapere i servizi attivi sulle porte e forse anche le versioni. Perché ?

Qui sotto si riporta un esempio di porta aperta e di una porta “chiusa”.

Sulla porta attaccata il nostro attaccante non è riuscito a completare la connessione quindi gli risulterà chiusa/filtrata



Invece sulla porta 80 avendo completato la connessione ha sottratto informazioni che potrebbero essere pericolose per noi.



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 TSval=810522428 TSecr=0
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=1460 SACK_PERM=1 TSval=810522428 TSecr=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=810522428 TSecr=4
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=810522428 TSecr=4
31	36.775524284	192.168.200.100	192.168.200.150	TCP	74	53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810522428 TSecr=0
36	36.775797004	192.168.200.150	192.168.200.100	TCP	74	80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=810522428 TSecr=0
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4
41	36.776095853	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4

## FASE 3

Dopo questa analisi possiamo dire con certezza di essere nel mirino di qualcuno. Essendo gli IP nella stessa rete forse un tecnico potrebbe aver effettuato una scansione di controllo, oppure nel peggiore dei casi un Dipendente Fenomeno sta tramando qualcosa.

Un vettore di attacco possibile sulla porta 80 (HTTP) potrebbe essere un SQLi sul nostro database. Il che (come ben sappiamo) può portare ad una fuga di dati molto importante. (Pablo Picasso)

Come soluzione si potrebbe inizialmente inserire IP attaccante in una blacklist, in modo da bloccare le comunicazioni e giocare di anticipo. Se invece fosse un tecnico, anche esterno, incaricato dalla azienda allora li si può riportare tutto allo stato originale.

Se il nostro utente interno è in possesso di queste informazioni potremmo anche solo bloccare l'ingresso alle porte dove il servizio potrebbe recare danni, come ad esempio la porta 80