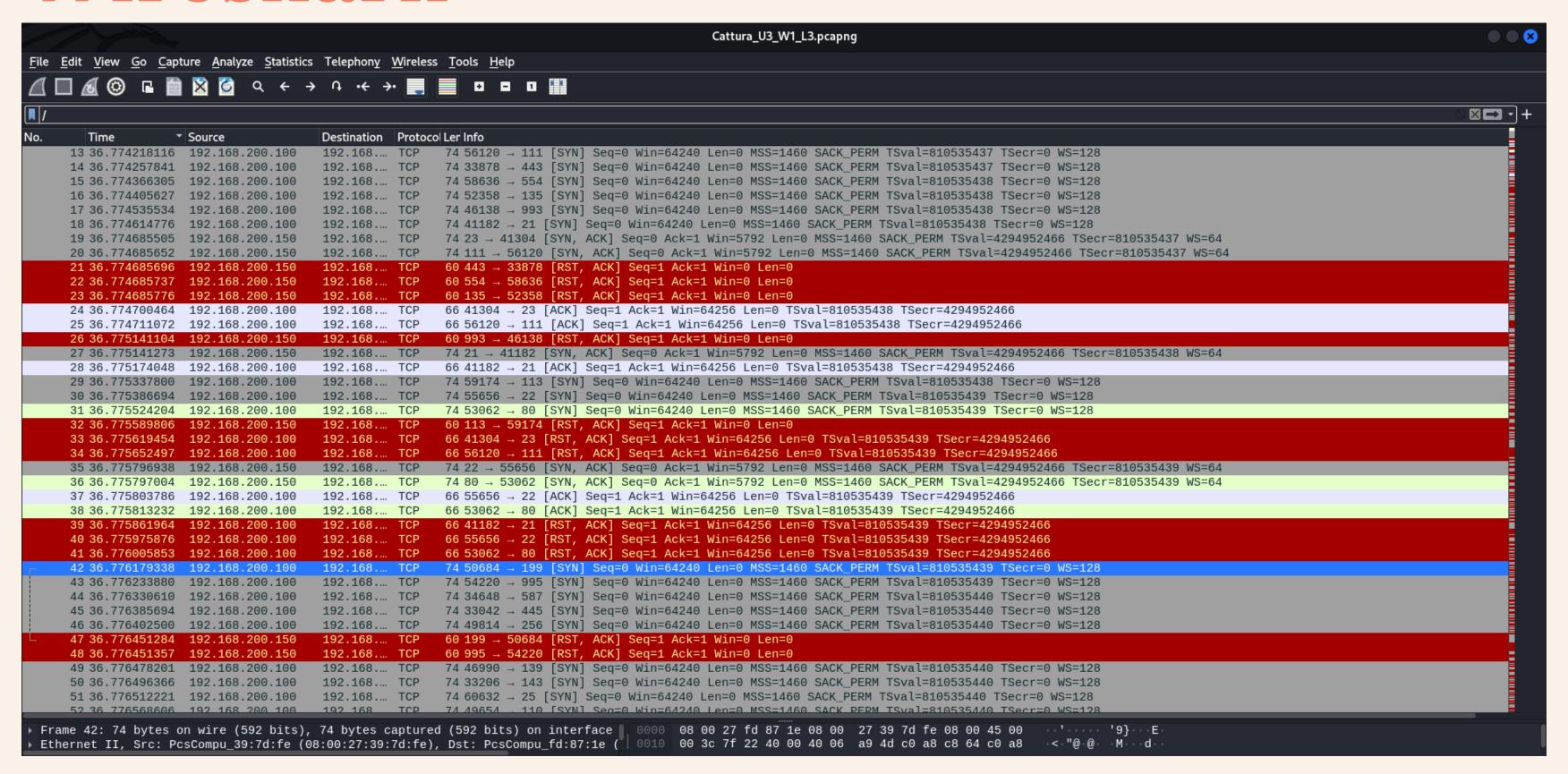
Cattura Wireshark

L'esercizio di oggi consiste nella lettura e comprensione di una cattura effettuata su wireshark, tentando di capire che tipo di attacco sia stato effettuato.



Lettura

La cattura mostra un gran numero di pacchetti SYN inviati dalla macchina 192.168.200.100 verso la macchina 192.168.200.150, tutti con lo stesso contenuto e indirizzati a porte sempre diverse.

A sua volta la macchina ".150" risponde con dei pacchetti ACK ad alcune di queste richieste.

Conclusioni

Con tutta probabilità si tratta di una scansione dei servizi attivi sulla macchina 192.168.200.150, che invia risposte ACK quando una sua porta aperta viene richiesta.

Per ridurre l'impatto di questo attacco sarebbe utile un firewall o l'utilizzo di un reverse proxy