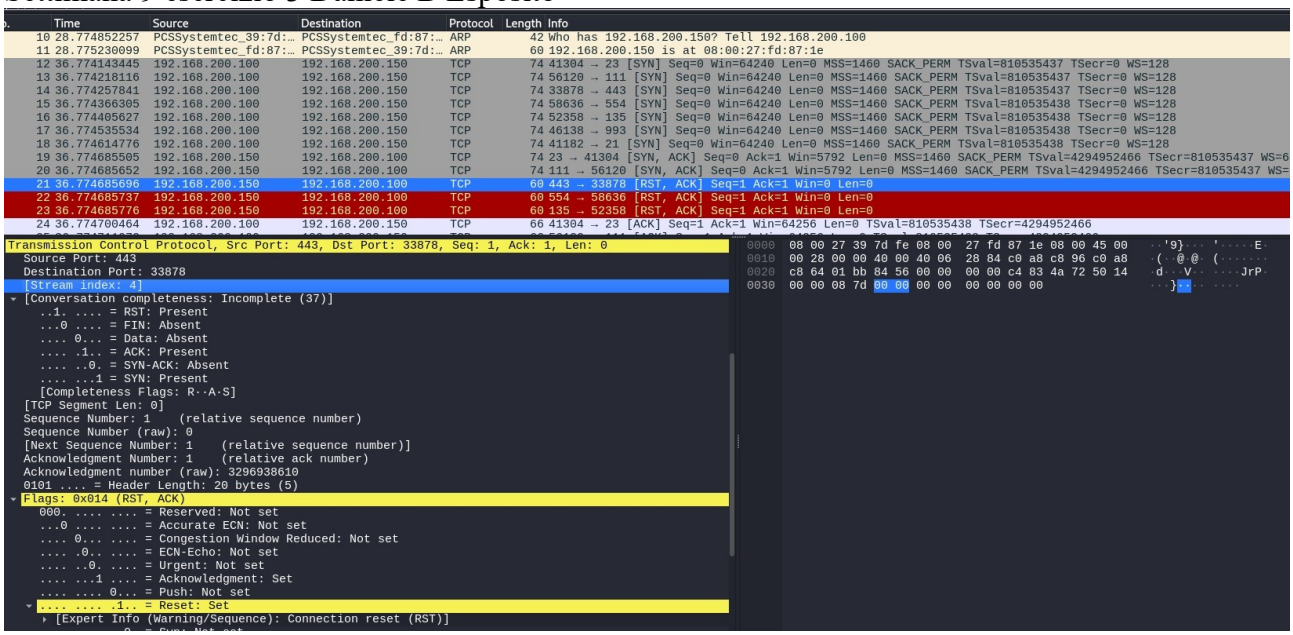
Settimana 9 esercizio 3 Daniele D'Esposito



Aprendo il file fornito dalla traccia, appare una sessione di wireshark che cattura la comunicazione tra gli ip 192.168.200.150(attaccato) e 192.168.200.100(attaccante).
Si puo' notare come l'indirizzo attaccante mandi tante richieste TCP a molte porte. Prendendo in esame la riga 21 si vede che la porta 443 manda alla porta 33878 un segnale di reset(rst) che termina la connessione lasciando incompleto il 3 way handshake iniziato nella riga 14 con un syn. Questo significa che la porta e' chiusa. Se invece la porta risponde con syn/ack allora e' aperta.
E' ragionevole concludere che l'attaccante stia usando strumenti di port scanning, come per esempio nmap.
Per ovviare al problema bisogna utilizzare un firewall che impedisca la comunicazione con l'ip attaccante.