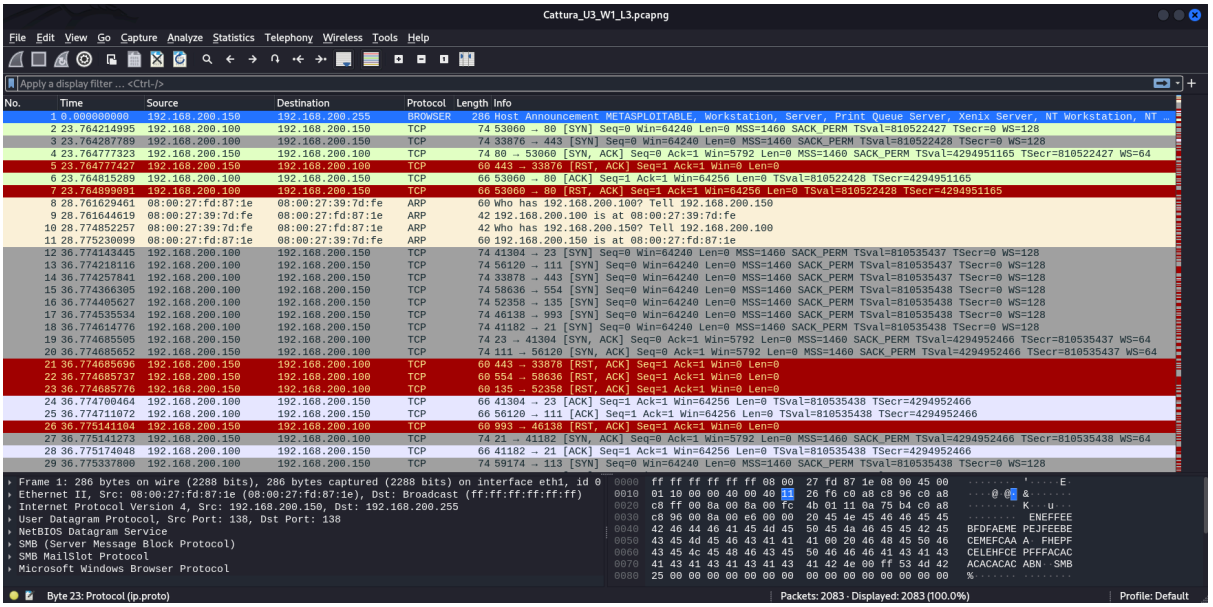
CONSEGNA S9/L3

Per l’esercizio pratico di oggi, troviamo in allegato una cattura di rete effettuata con Wireshark.
Analizzare la cattura attentamente e rispondere ai seguenti quesiti:

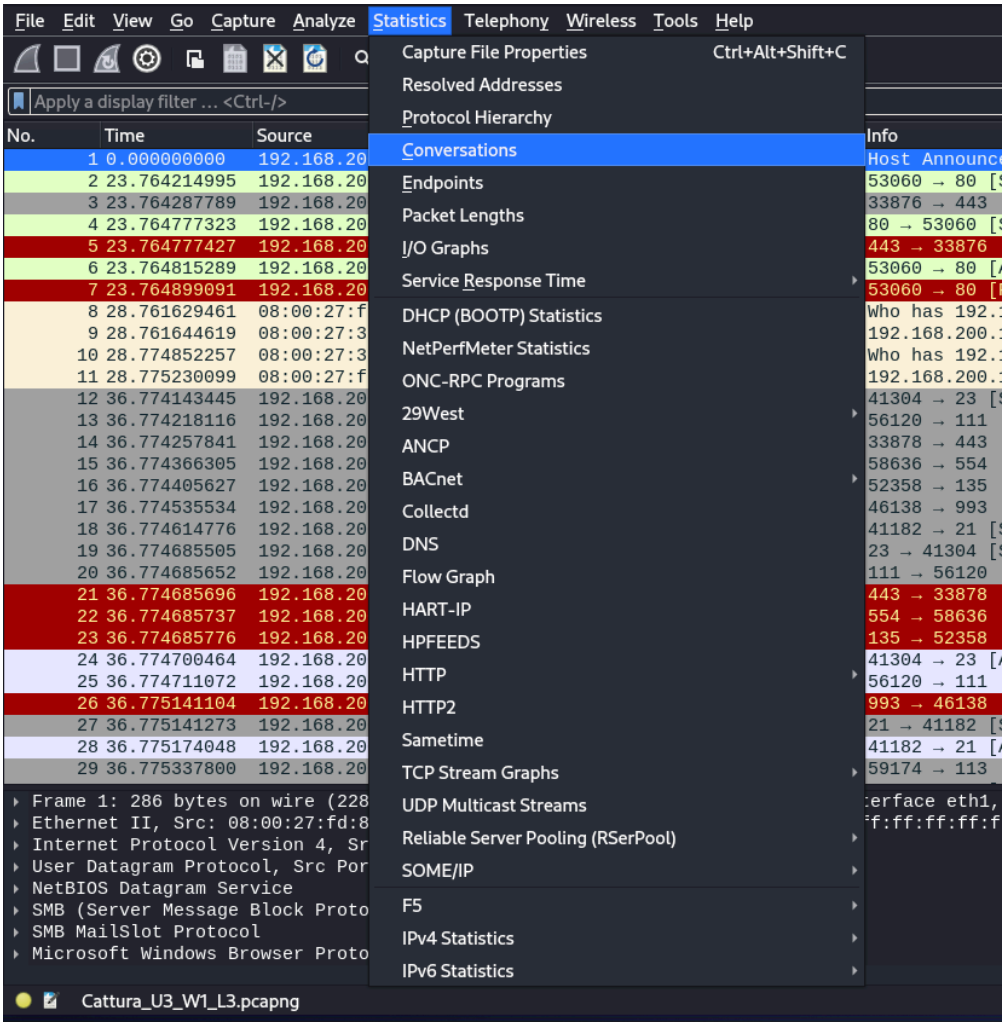
- Identificare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un’azione per ridurre gli impatti dell’attacco

SCANSIONE

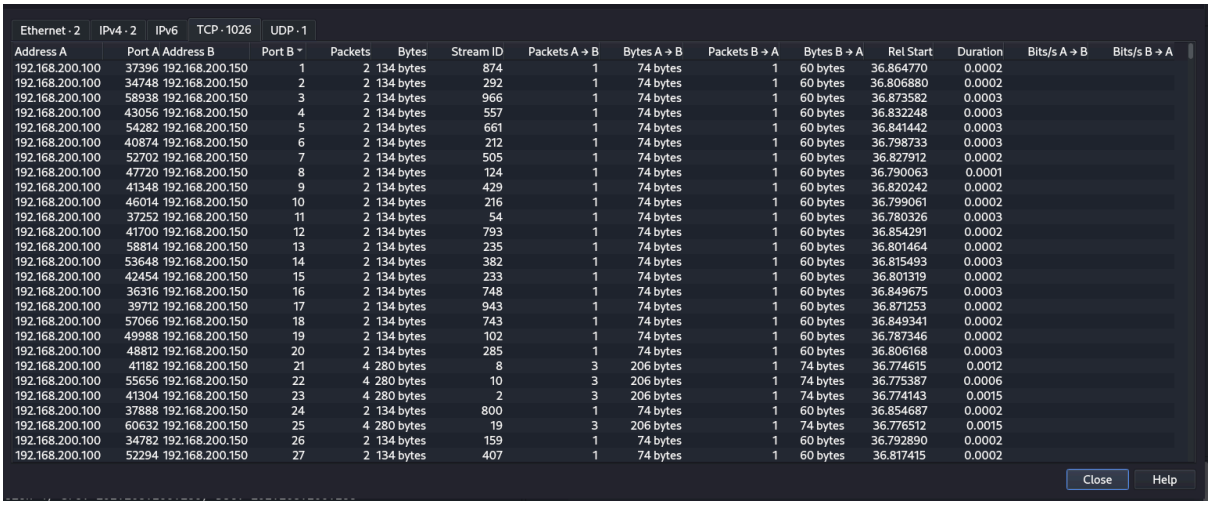


Notiamo come appaiono molti protocolli TCP verso le porte della macchina con ip 192.168.200.150 da una macchina sorgente con ip 192.168.200.100.

Andiamo ad evidenziare le conversazioni:



Quello che vediamo in atto è palesemente un port scanning:



Come misure di prevenzione suggeriamo di chiudere le porte non utilizzate e filtrare le altre, impostare il firewall in modo tale che le porte comunichino solo con ip e protocolli prestabiliti.