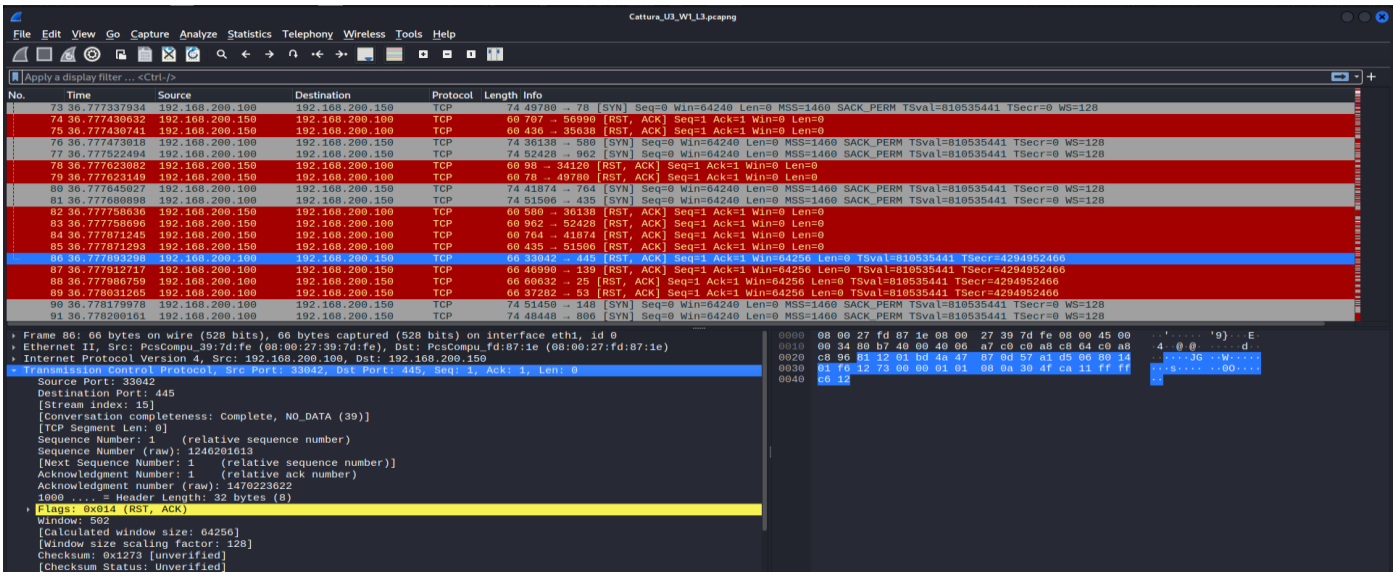
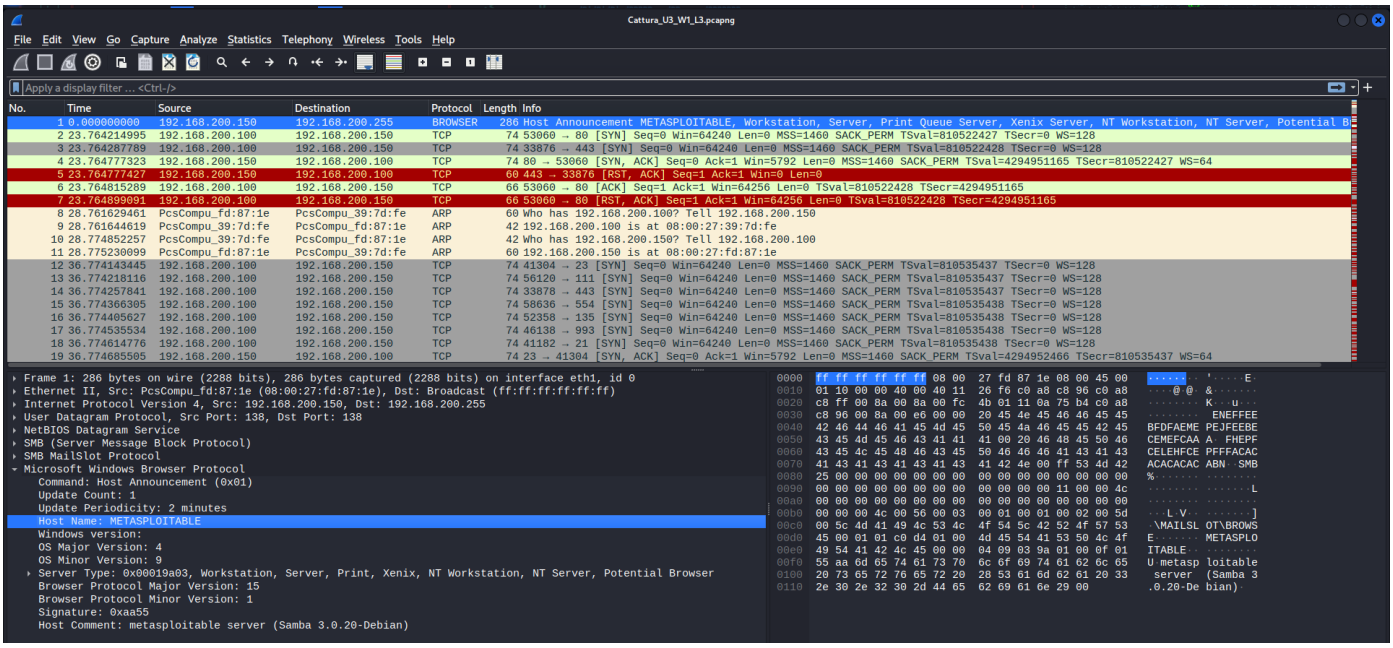
Esercizio epicode 22.11.2023





Identificare eventuali IOC, ovvero evidenze di attacchi in corso

Controllando la prima immagine si possono vedere varie richieste tcp syn, quindi dall'indirizzo IP 192.168.200.150 a varie porte sull'indirizzo 192.168.200.100. Quindi si potrebbe trattare di una scansione di rete.

In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati

Sulla prima riga della seconda immagine di wireshark si riconosce l'host (quindi della potenziale macchina attaccante) che è Metasploitable.

Consigliate un'azione per ridurre gli impatti dell'attacco

Si può utilizzare un firewall per bloccare l'ip dell'attaccante dato che le macchine si trovano sulla stessa rete.