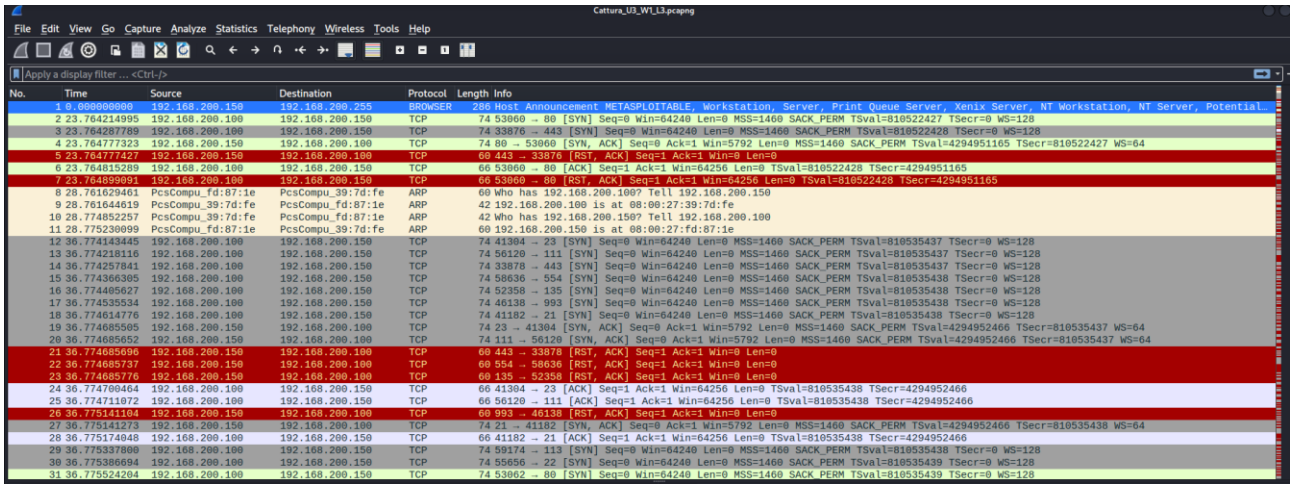

a) Identificare eventuali IOC, ovvero evidenze di attacchi in corso

*Analizzando la cattura di rete effettuata con Wireshark, si può notare come ci siano delle **richieste TCP ripetute**, che rappresentano IOC.*

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

*L'attaccante 102.168.200.100 potrebbe **star scansionando il target** 192.168.200.150, in quanto dalla cattura notiamo che ci sono un numero elevato di richieste TCP (SYN) su porte sempre diverse di destinazione. L' ipotesi dello scansionamento è supportata dal fatto che per alcune righe della cattura si notano risposte positive del target (ovvero [SYN+ACK]) ad indicare che la porta è aperta. Per altre, invece, notiamo che la risposta (ovvero [RST+ACK]) va ad indicare che la porta è chiusa.*

c) Consigliate un'azione per ridurre gli impatti dell'attacco

*Si potrebbero **configurare le regole del firewall** in maniera tale da bloccare l'accesso a tutte le porte all' attaccante 192.168.200.100, in modo tale da evitare che informazioni riguardanti la porta e i servizi in ascolto finiscano nelle mani dell'attaccante.*