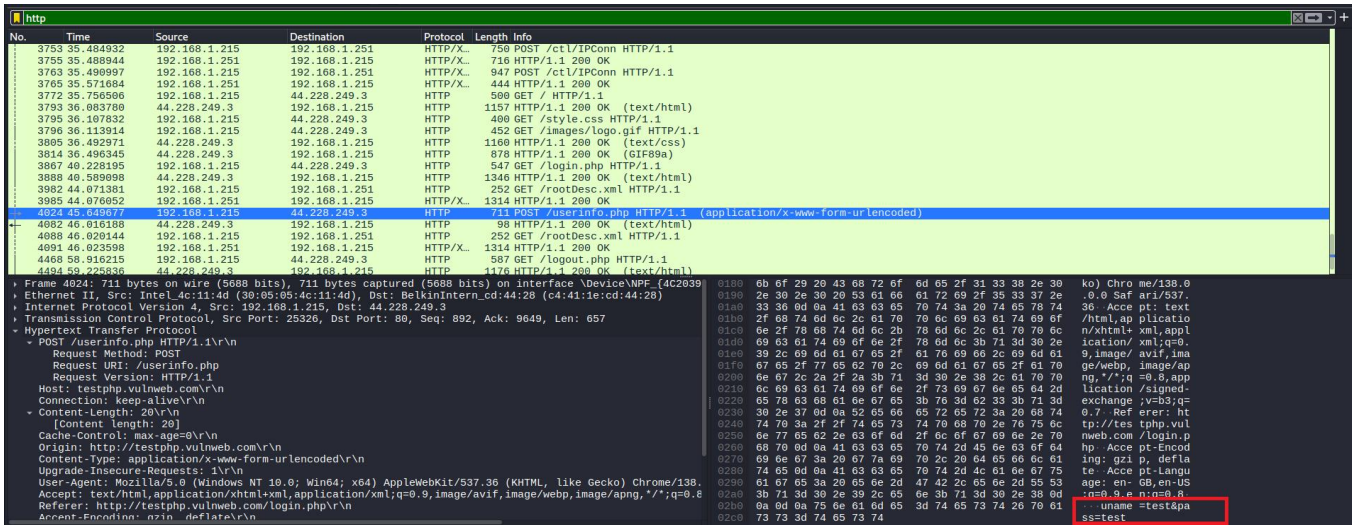
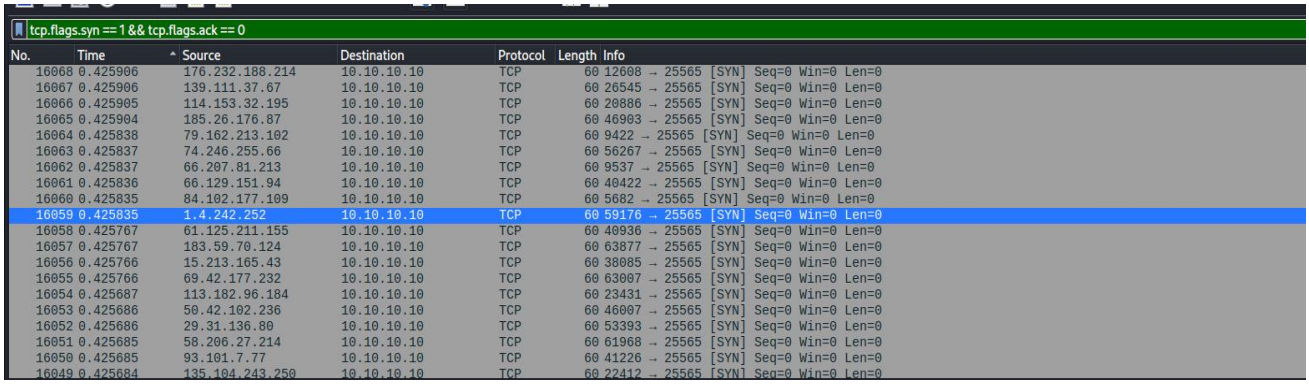
TASK-1



TASK-2

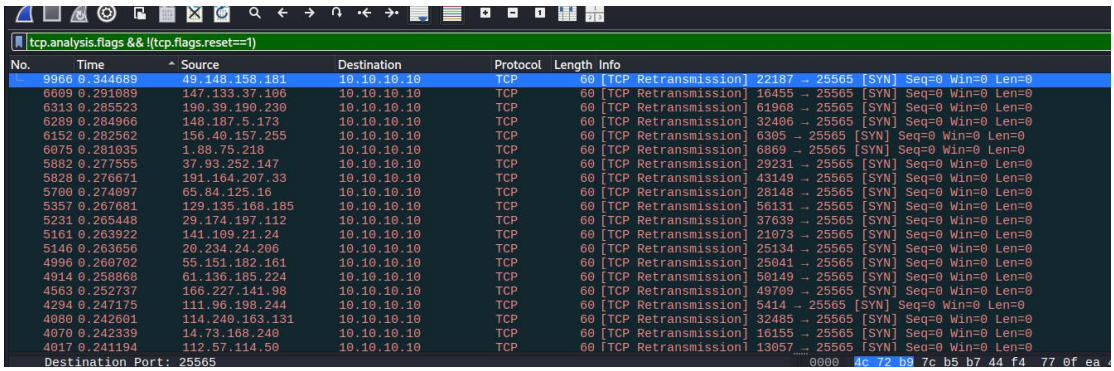
Large numbers of SYN packets were detected from different IP addresses without corresponding SYN+ACK replies.

Filter: tcp.flags.syn == 1 && tcp.flags.ack == 0



TCP anomalies- TCP Retransmission

Filter: tcp.analysis.flags && !(tcp.flags.reset==1)



CONCLUSION: Detected possible all the SYN packets are from **different source IPs**, so it’s a **distributed SYN flood** (DDoS) or scanning activity using spoofed source addresses.