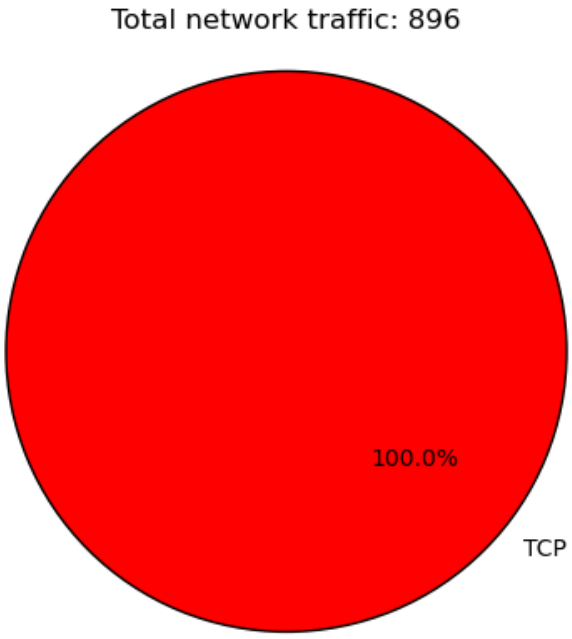
PCAP Analysis report

This report analyzes the PCAP file: amp.TCP.syn.optionallyACK.optionallysamePort.pcapng. It will determine whether a DDoS attack is detected. Some types of attacks we will search for include: SYN flooding, UDP flooding, ICMP flooding, and HTTP-GET flooding.



TCP: 892 TCP packets with a AVG packet size of: 64.39, packet rat
1.09

TCP SYN Flood: [DDoS ALERT] High volume of suspicious traffic detected!
- Target IP: 10.10.10.10
- Number of Attacker IPs: 51
- Target Port: 43136
- Packet Rate: 0.42 packets/sec
- 38.34% of the TCP traffic is detected as TCP SYN Flood attack
- Below is a list of IP addresses suspected to be the source of the attack.

IP	Total Packets Sent	Total Bytes Sent	Packet Rate
136.243.174.154	164	12136	1718.43
163.158.248.5	82	6068	865.14
178.238.236.27	16	1024	10825.76
45.146.165.209	8	480	101.03
83.83.223.119	5	310	5951.06
185.65.202.93	4	296	55.95
185.214.127.100	3	222	41.92
87.211.83.72	3	186	9739.1

165.227.47.247	3	180	493.1
91.121.144.97	2	120	188.37
62.109.17.7	2	148	47.53
187.188.161.233	2	132	5011.12
54.82.2.136	2	148	27.95
103.54.248.234	2	120	71.97
50.116.54.77	2	148	44.5
189.223.253.1	2	132	20610.83
37.29.119.34	2	132	20610.83
103.109.56.161	2	132	9903.91
106.51.114.109	2	132	9950.9
179.50.170.176	2	132	6447.82
103.80.210.150	2	132	20610.83
42.51.60.58	1	60	1
134.122.48.60	1	60	1
74.120.14.89	1	60	1
192.99.132.24	1	66	1
104.248.48.77	1	60	1
193.27.228.64	1	60	1
45.143.203.12	1	60	1
193.27.228.61	1	60	1
193.27.228.65	1	60	1
51.178.221.14	1	66	1
193.27.228.63	1	60	1
217.73.164.210	1	60	1
162.142.125.65	1	60	1
45.229.55.127	1	60	1
161.97.166.249	1	60	1
45.146.165.19	1	60	1
23.148.145.7	1	60	1
189.149.180.153	1	60	1
193.118.55.165	1	60	1
139.59.122.100	1	60	1
193.118.53.212	1	60	1
45.155.205.247	1	60	1
193.118.53.210	1	74	1
89.248.168.112	1	60	1
45.146.164.214	1	60	1

134.209.66.174	1	60	1
45.135.232.119	1	60	1
42.117.213.47	1	60	1
194.165.16.22	1	60	1
45.146.165.149	1	60	1

Results of the PCAP analysis:

- SYN flood has been detected.
- No evidence of a UDP flood attack has been detected.
- No evidence of an ICMP flood attack has been detected.