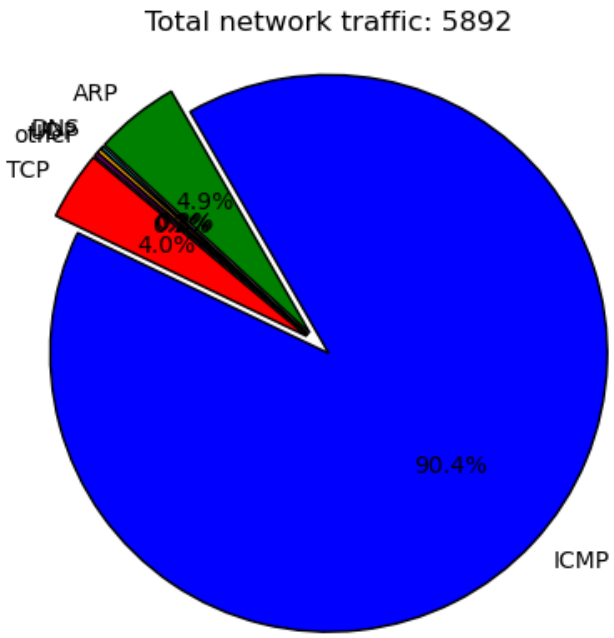
PCAP Analysis report

This report analyzes the PCAP file: ICMP_DDOS.pcap. 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.This file contains 92.36% (Total of 5442) IPv4 packets and 2.73% (Total of 161) IPv6 packets



TCP: 235 TCP packets. AVG packet size of: 165.46

packet rate: 7.03

ICMP: 5327 ICMP packets. AVG packet size of: 42.54

packet rate: 167.04

ARP: 289 ARP packets. AVG packet size of: 59.56

packet rate: 8.99

DNS: 11 DNS packets. AVG packet size of: 240.27

packet rate: 1.92

UDP: 16 UDP packets. AVG packet size of: 344.56

packet rate: 0.78

Other: 14 Other packets. AVG packet size of: 86.86

packet rate: 0.93

UDP Flood: [DDoS ALERT] High volume of suspicious traffic detected!
- Target IP: 192.168.1.254
- Number of Attacker IPs: 1
- Average Packet Rate: 166666.67
- Attack Duration: 0.00/secs
- Below is a list of IP addresses suspected to be the source of the attack.

IP	Total Packets Sent	Total Bytes Sent	Packet Rate
192.168.1.33	2	675	166666.67

ICMP Flood: [DDoS ALERT] High volume of suspicious traffic detected!
- Target IP: 192.168.1.254
- Average Packet Rate: 162.03
- Attack Duration: 31.89/secs
- Below is a list of IP addresses suspected to be the source of the attack.

IP	Total Packets Sent	Total Bytes Sent	Packet Rate
192.168.1.186	5167	217014	162.03

Results of the PCAP analysis:

- No evidence of a SYN flood attack has been detected. Only 0.00% of TCP handshakes remain incomplete, which is within the expected threshold for normal network fluctuations. Additionally, there are no abnormal spikes in SYN packet rates or signs of bursty traffic behavior that would indicate a volumetric attack.
- UDP flood has been detected.
- ICMP flood has been detected.
- No evidence of an HTTP-GET flood attack has been detected.