DDOS on google(dns)

Method of DDOS is ping flood

A screenshot of a computer

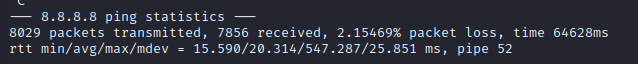
Description automatically generated

As you can see here, the sign of Ping flood is high amount of ICMP traffic. Here the icmp request come from my device to google dns IP. As you can see, ping flood will succeed if the target cant respond all icmp request in time. Unfortunately due to restriction in kali linux I can only send 1 packets per 2ms or 500 packets per 1 seconds. As you can see, some of the request are not replied until the next request came in.

Command used   
A computer code with numbers and symbols

Description automatically generated with medium confidence

2ms = 0.002 second



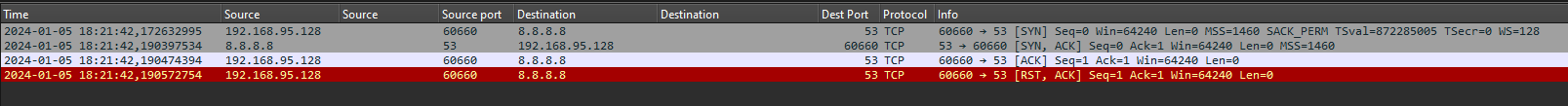
2% packet loss seems like it will take more to cripple google dns

Nmap on google (dns)

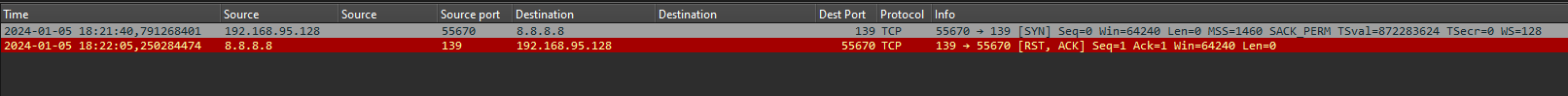
A screen shot of a computer

Description automatically generated

First sign of nmap is a lot of incoming syn packets all designated from same source and target different ports form the IP. Above is the screenshot of nmap to google dns 8.8.8.8.



If the port is opened, you will receive syn ack from the target. Your machine then will send ack and send rst ack. Rst technically will end the connection so that the device can send syn packets to other port.



If the port is closed, you will receive rst ack instead of syn ack from the target.

Unfortunately, I didn’t get non-existent port but I believed that it will timeout because not receiving reply.