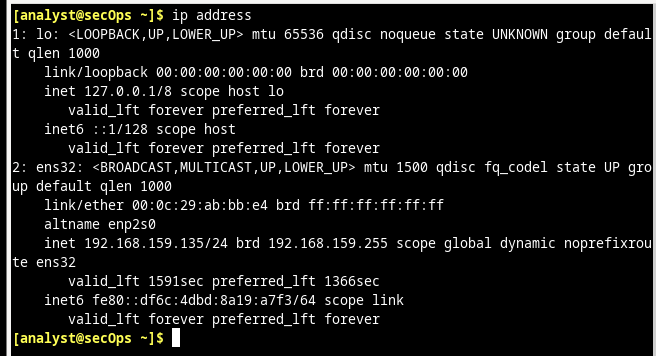
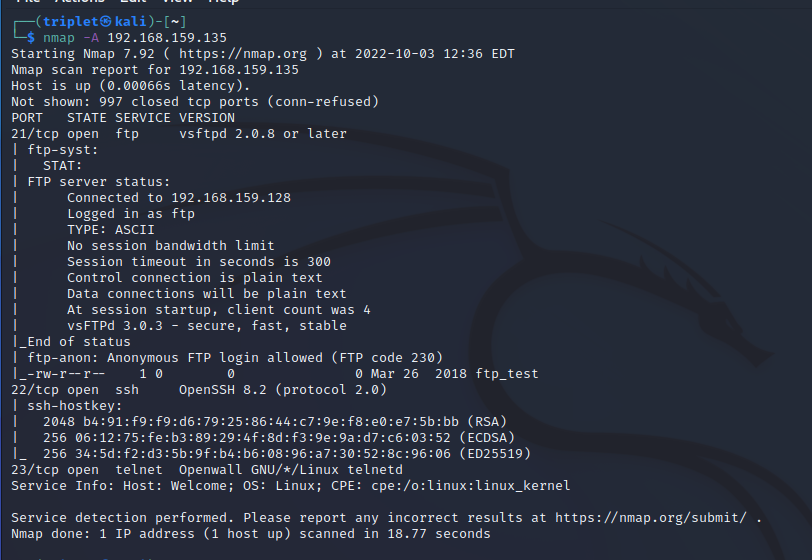
First I will use nmap to scan the victim





As we can see about the nmap result. The victim has 3 opened ports, which has number 21, 22, 23 that serves ftp, ssh, telnet services as well as lots of valuable information.

Then I wil open wireshark to view more clearly about the process of hping3

First I will run a command: sudo hping3 -1 -a 10.10.10.10 192.168.159.135 –flood

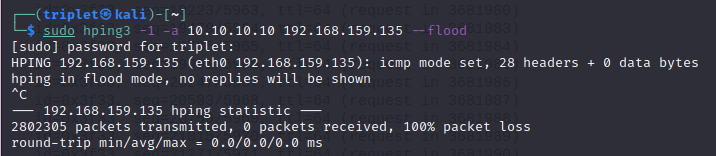
Breakdown:

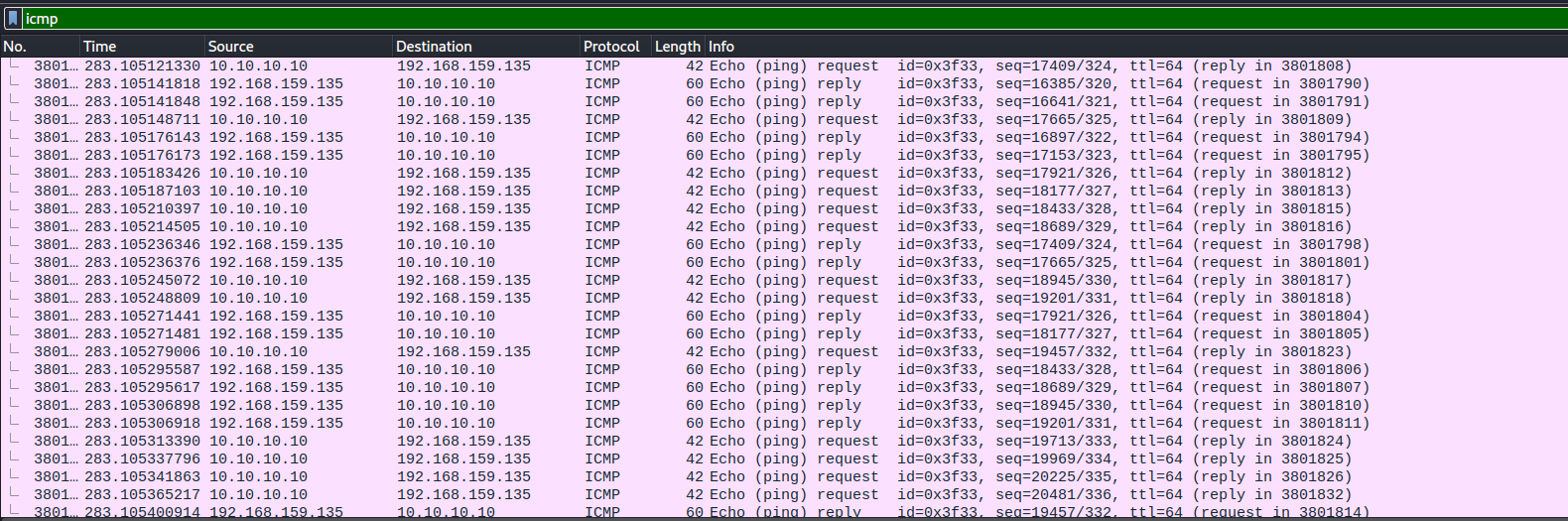
-1: specified the icmp attack

-a: spoofed the source ip address to some not real address follow by the victim address

--flood: ping to death overflow the service

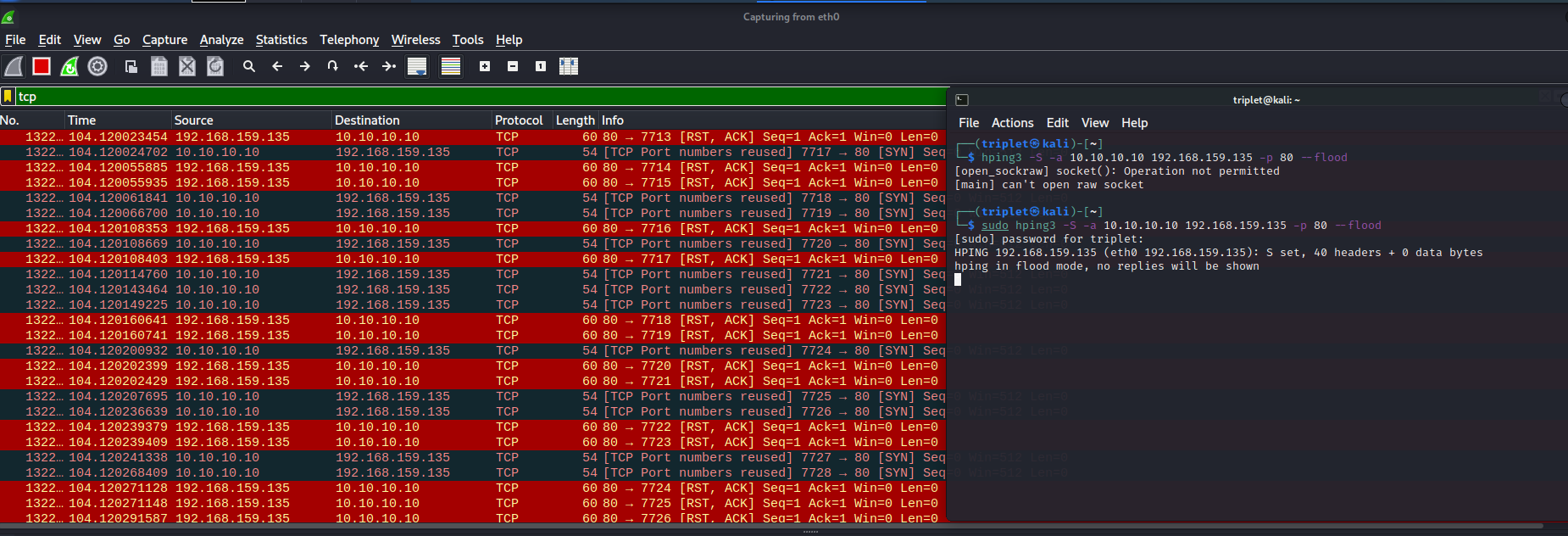
This will generate a ping of death technique that send massive number of icmp pakets to the victim to overload its service.





As we can see there are amount of 3 millions packets send to the victim, but it is still alive.

Then I will use SYN flooding attack and see what will happen



I use the command: sudo hping3 -S -a 10.10.10.10 192.168.159.135 -p 80 –flood

Breakdown:

-S: specified the SYN flag of the packet leading to the SYN flooding attack

-a: spoofed the source ip address to the not real ip follow by the victim ip address

-p: specified the port that the attack cause on is port 80

--flood: overflow the services.