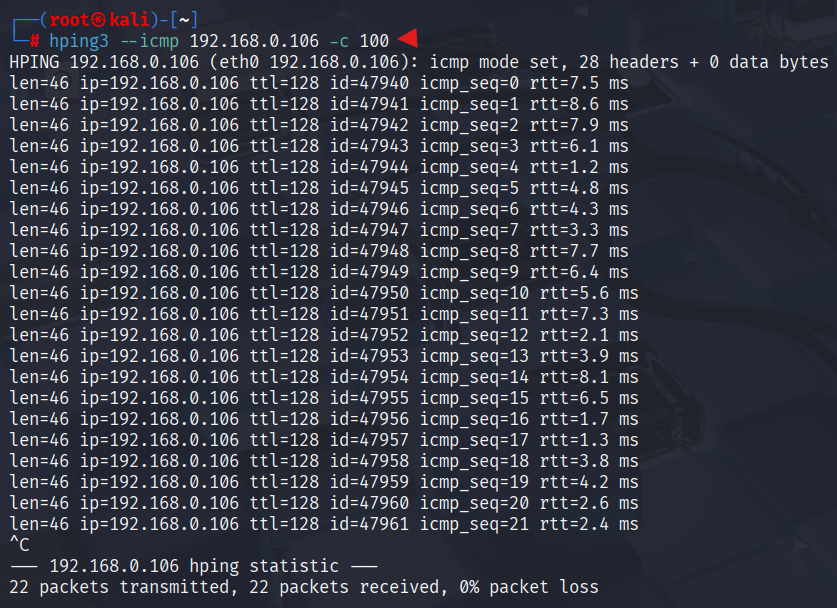
**Denial Of Service (DOS) :** It is a cyberattack where a malicious actor aims to make a computer or network resource unavailable to its intended users by disrupting its normal functioning. This is typically achieved by overwhelming the target with a flood of traffic or requests, making it unable to process legitimate requests. DoS attacks can disrupt services like websites, online accounts, or other network resources.

**Distributed Denial of Service (DDOS) :** It is a malicious cyberattack that overwhelms a target server, website, or network with a flood of traffic, making it unavailable to legitimate users. This attack involves multiple compromised systems, often a botnet, sending a massive amount of requests to overwhelm the target's resources.

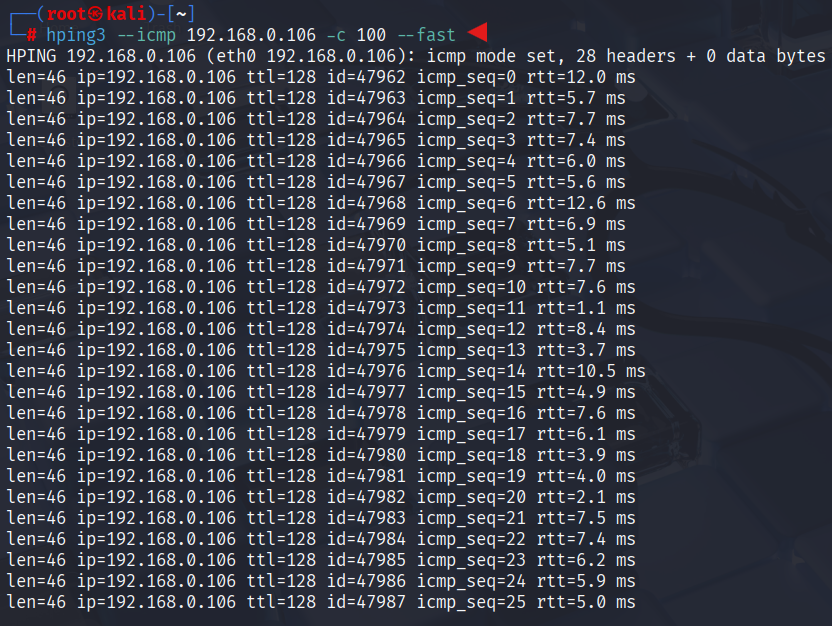
**DOS attack on Virtual Machine :** Using hping3 tool

Before performing an dos attack we need to know the ip address of the system that your trying to attack on the we will use the hping tool along with a protocol to attack on specific port and how many request do you wish to send per/second.

Eample : hping3 --icmp 192.168.0.106 -c 100 here



Now we will send more traffic to the target system by using --flood, --faster command in hping tool as shown in the snapshot below.



As soon as we run the command the hping sent 90 packets in 17.1 ms, we can see the traffic in the traget system as shown in snap shot. We are using more than 50% of cpu usage and 1.2mbps of speed were both the resources are increasing the utilization as we send the traffic, as a result at the end. user who is on windows 10 find it difficult for usage of system/ In some cases the system may crash completely making it unavailable.

