Hping3

hping3 is a command-line utility for crafting and sending custom TCP/IP packets. It is a versatile tool that allows you to perform various tasks, such as network scanning, fingerprinting, and testing network security. With hping3, you can simulate different types of network traffic, making it a valuable tool for network testing and troubleshooting.

Usecase: -

1. Network Scanning and Discovery: - To discover active hosts and open ports on a network

2. Firewall Testing: - To test the effectiveness of firewall rules and configurations.

3. Denial of Service (DoS) Testing: - To simulate DoS attacks to test the resilience of systems and networks under stress.

4. Network Performance Testing: - Can measure round-trip time (RTT) and packet loss by sending custom packets and analyzing the responses, useful for diagnosing network performance issues.

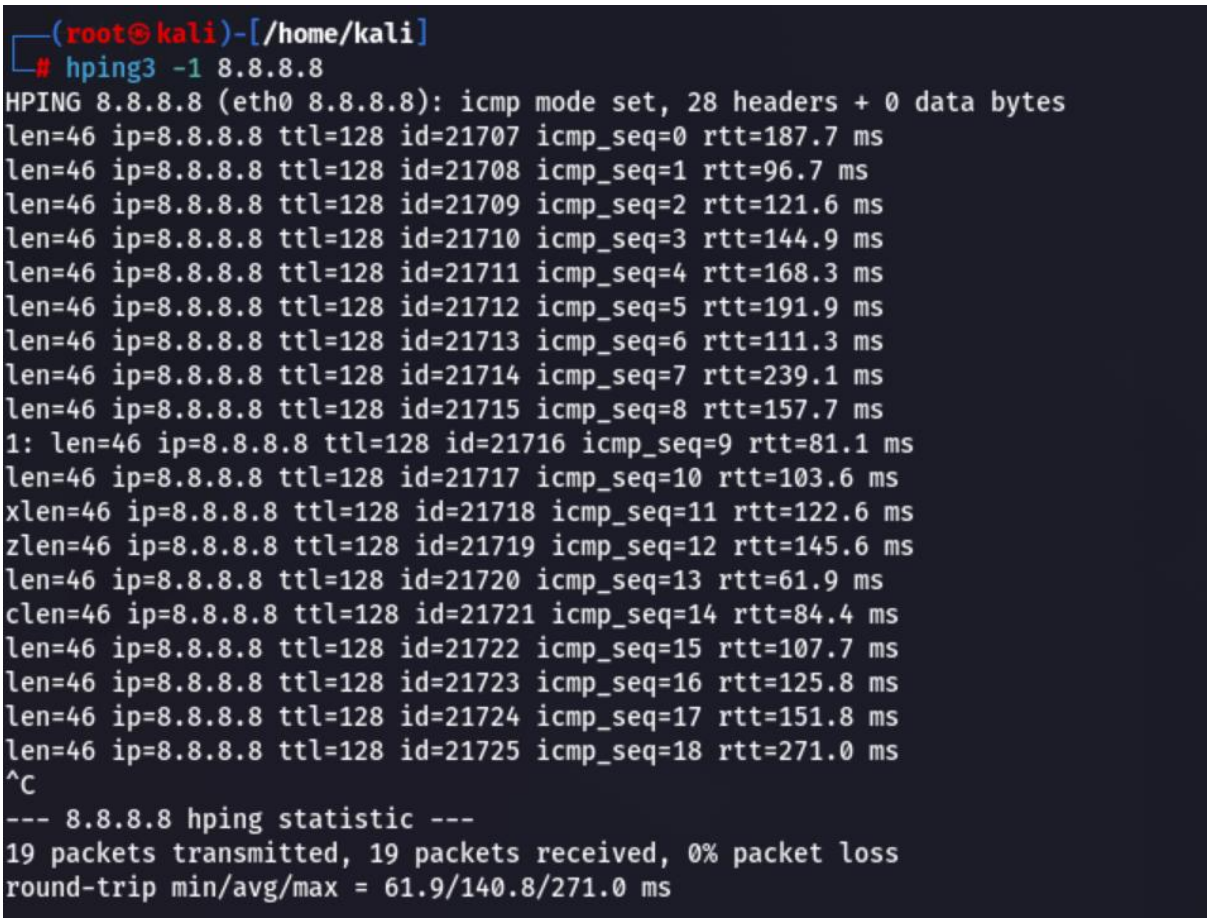
5. Traceroute: - Can perform traceroute-like operations to trace the path packets take to reach a destination, using various protocols.

6. Advanced Network Testing: - Users can create highly specific test scenarios by customizing packet headers, payloads, and other parameters.

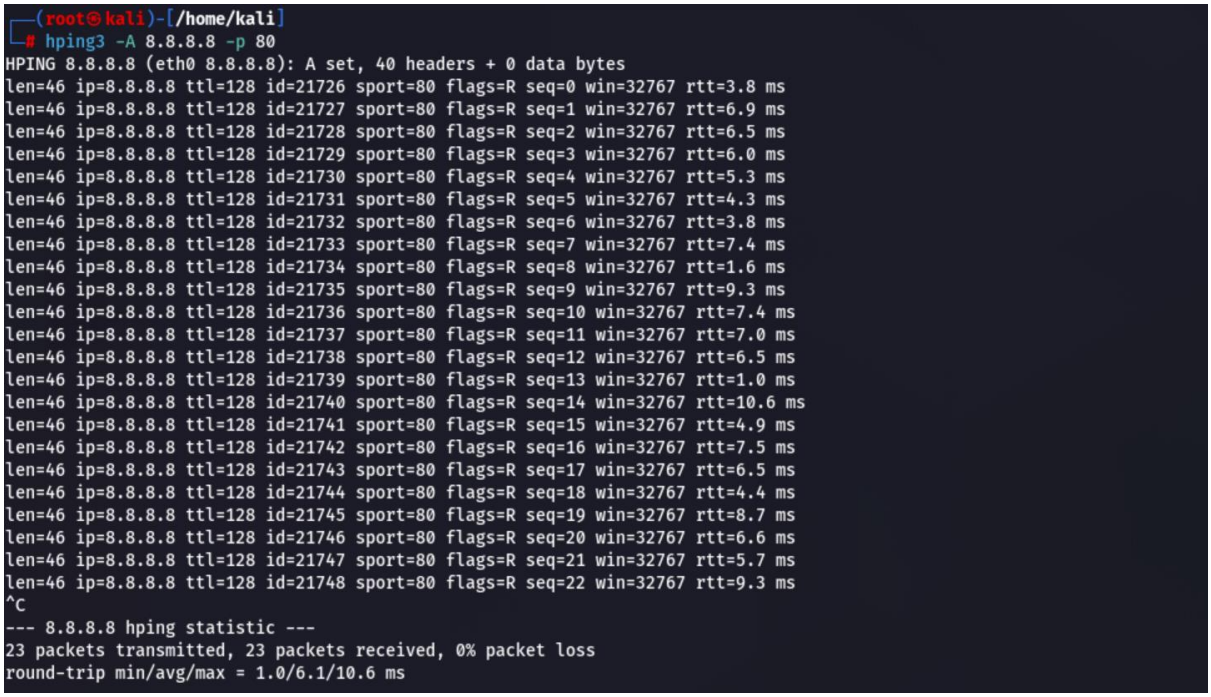
7. OS Fingerprinting: - Can help identify the operating system of a remote host.

Example: -

1. By issuing the -1 , hping sends an ICMP-echo request to 10.0.0.25 and receives ICMP-reply, the same as with a ping utility.



2. By issuing -A command, Hping checks if a host is alive on a network. If it finds a live host and an open port, it returns an RST response.



3. Using the argument -2 in the command line specifies that Hping operates in UDP mode. We can use either `--udp` of `-2` arguments in the command line. By issuing the above command, Hping sends UDP packets to port 80 on the host (10.0.0.25). It returns an ICMP port unreachable message if it finds the port closed, and does not respond with a message if the port is open.