

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.

```
(root@kali)-[/home/kali]
# hping3 -1 8.8.8.8
HPING 8.8.8.8 (eth0 8.8.8.8): icmp mode set, 28 headers + 0 data bytes
len=46 ip=8.8.8.8 ttl=128 id=21707 icmp_seq=0 rtt=187.7 ms
len=46 ip=8.8.8.8 ttl=128 id=21708 icmp_seq=1 rtt=96.7 ms
len=46 ip=8.8.8.8 ttl=128 id=21709 icmp_seq=2 rtt=121.6 ms
len=46 ip=8.8.8.8 ttl=128 id=21710 icmp_seq=3 rtt=144.9 ms
len=46 ip=8.8.8.8 ttl=128 id=21711 icmp_seq=4 rtt=168.3 ms
len=46 ip=8.8.8.8 ttl=128 id=21712 icmp_seq=5 rtt=191.9 ms
len=46 ip=8.8.8.8 ttl=128 id=21713 icmp_seq=6 rtt=111.3 ms
len=46 ip=8.8.8.8 ttl=128 id=21714 icmp_seq=7 rtt=239.1 ms
len=46 ip=8.8.8.8 ttl=128 id=21715 icmp_seq=8 rtt=157.7 ms
1: len=46 ip=8.8.8.8 ttl=128 id=21716 icmp_seq=9 rtt=81.1 ms
len=46 ip=8.8.8.8 ttl=128 id=21717 icmp_seq=10 rtt=103.6 ms
xlen=46 ip=8.8.8.8 ttl=128 id=21718 icmp_seq=11 rtt=122.6 ms
zlen=46 ip=8.8.8.8 ttl=128 id=21719 icmp_seq=12 rtt=145.6 ms
len=46 ip=8.8.8.8 ttl=128 id=21720 icmp_seq=13 rtt=61.9 ms
clen=46 ip=8.8.8.8 ttl=128 id=21721 icmp_seq=14 rtt=84.4 ms
len=46 ip=8.8.8.8 ttl=128 id=21722 icmp_seq=15 rtt=107.7 ms
len=46 ip=8.8.8.8 ttl=128 id=21723 icmp_seq=16 rtt=125.8 ms
len=46 ip=8.8.8.8 ttl=128 id=21724 icmp_seq=17 rtt=151.8 ms
len=46 ip=8.8.8.8 ttl=128 id=21725 icmp_seq=18 rtt=271.0 ms
^C
--- 8.8.8.8 hping statistic ---
19 packets transmitted, 19 packets received, 0% packet loss
round-trip min/avg/max = 61.9/140.8/271.0 ms
```

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.

```
(root@kali)-[/home/kali]
# hping3 -A 8.8.8.8 -p 80
HPING 8.8.8.8 (eth0 8.8.8.8): A set, 40 headers + 0 data bytes
len=46 ip=8.8.8.8 ttl=128 id=21726 sport=80 flags=R seq=0 win=32767 rtt=3.8 ms
len=46 ip=8.8.8.8 ttl=128 id=21727 sport=80 flags=R seq=1 win=32767 rtt=6.9 ms
len=46 ip=8.8.8.8 ttl=128 id=21728 sport=80 flags=R seq=2 win=32767 rtt=6.5 ms
len=46 ip=8.8.8.8 ttl=128 id=21729 sport=80 flags=R seq=3 win=32767 rtt=6.0 ms
len=46 ip=8.8.8.8 ttl=128 id=21730 sport=80 flags=R seq=4 win=32767 rtt=5.3 ms
len=46 ip=8.8.8.8 ttl=128 id=21731 sport=80 flags=R seq=5 win=32767 rtt=4.3 ms
len=46 ip=8.8.8.8 ttl=128 id=21732 sport=80 flags=R seq=6 win=32767 rtt=3.8 ms
len=46 ip=8.8.8.8 ttl=128 id=21733 sport=80 flags=R seq=7 win=32767 rtt=7.4 ms
len=46 ip=8.8.8.8 ttl=128 id=21734 sport=80 flags=R seq=8 win=32767 rtt=1.6 ms
len=46 ip=8.8.8.8 ttl=128 id=21735 sport=80 flags=R seq=9 win=32767 rtt=9.3 ms
len=46 ip=8.8.8.8 ttl=128 id=21736 sport=80 flags=R seq=10 win=32767 rtt=7.4 ms
len=46 ip=8.8.8.8 ttl=128 id=21737 sport=80 flags=R seq=11 win=32767 rtt=7.0 ms
len=46 ip=8.8.8.8 ttl=128 id=21738 sport=80 flags=R seq=12 win=32767 rtt=6.5 ms
len=46 ip=8.8.8.8 ttl=128 id=21739 sport=80 flags=R seq=13 win=32767 rtt=1.0 ms
len=46 ip=8.8.8.8 ttl=128 id=21740 sport=80 flags=R seq=14 win=32767 rtt=10.6 ms
len=46 ip=8.8.8.8 ttl=128 id=21741 sport=80 flags=R seq=15 win=32767 rtt=4.9 ms
len=46 ip=8.8.8.8 ttl=128 id=21742 sport=80 flags=R seq=16 win=32767 rtt=7.5 ms
len=46 ip=8.8.8.8 ttl=128 id=21743 sport=80 flags=R seq=17 win=32767 rtt=6.5 ms
len=46 ip=8.8.8.8 ttl=128 id=21744 sport=80 flags=R seq=18 win=32767 rtt=4.4 ms
len=46 ip=8.8.8.8 ttl=128 id=21745 sport=80 flags=R seq=19 win=32767 rtt=8.7 ms
len=46 ip=8.8.8.8 ttl=128 id=21746 sport=80 flags=R seq=20 win=32767 rtt=6.6 ms
len=46 ip=8.8.8.8 ttl=128 id=21747 sport=80 flags=R seq=21 win=32767 rtt=5.7 ms
len=46 ip=8.8.8.8 ttl=128 id=21748 sport=80 flags=R seq=22 win=32767 rtt=9.3 ms
^C
--- 8.8.8.8 hping statistic ---
23 packets transmitted, 23 packets received, 0% packet loss
round-trip min/avg/max = 1.0/6.1/10.6 ms
```

3. Using the argument -2 in the command line specifies that Hping operates in UDP mode. We can use either --udp or -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.

```
(root@kali)-[/home/kali]
# hping3 -2 8.8.8.8 -p 80
HPING 8.8.8.8 (eth0 8.8.8.8): udp mode set, 28 headers + 0 data bytes
^C
--- 8.8.8.8 hping statistic ---
18 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```