Hping3

The hping3 is a command-line utility for analyzing TCP/IP packets. The hping3 command can be used instead of the ping command. Not only can the hping3 transmit ICMP echo requests, but it can also send TCP, UDP, and raw IP packets. The traceroute capability is supported by the hping3.

Installation:

Step 1: Update the package list using following command

- sudo apt update

Step 2: After updating the package list, hping3 can be installed using following mentioned command. For this exercise this tool will be installed on Ubuntu 20.04 OS:

```
seed@VM: ~
seed@VM:~$ sudo apt install -y hping3
[sudo] password for seed:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  hping3
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 106 kB of archives.
After this operation, 263 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 hping3 amd64 3.a2
.ds2-10 [106 kB]
Fetched 106 kB in 1s (185 kB/s)
Selecting previously unselected package hping3.
(Reading database ... 223973 files and directories currently installed.)
Preparing to unpack .../hping3_3.a2.ds2-10_amd64.deb ...
Unpacking hping3 (3.a2.ds2-10) ...
Setting up hping3 (3.a2.ds2-10) ...
Processing triggers for man-db (2.10.2-1) ...
seed@VM:~$
```

Step 3: Next the successful installation of hping3 can be checked using following command:

- hping3 --version

```
seed@VM: ~
seed@VM:~$ hping3 --version
hping3 version 3.0.0-alpha-2 ($Id: release.h,v 1.4 2004/04/09 23:38:56 antirez Exp $
)
This binary is TCL scripting capable
seed@VM:~$
```

Execution:

After successful installation and verification of Hping3 tool various switches within it can be identified using following command:

- hping3 -h

```
seed@VM: ~
seed@VM:~$ hping3 -h
usage: hping3 host [options]
  -h  --help      show this help
  -v  --version   show version
  -c  --count     packet count
  -i  --interval  wait (uX for X microseconds, for example -i u1000)
      --fast      alias for -i u10000 (10 packets for second)
      --faster    alias for -i u1000 (100 packets for second)
      --flood      sent packets as fast as possible. Don't show replies.
  -n  --numeric   numeric output
  -q  --quiet     quiet
  -I  --interface interface name (otherwise default routing interface)
  -V  --verbose   verbose mode
  -D  --debug     debugging info
  -z  --bind      bind ctrl+z to ttl           (default to dst port)
  -Z  --unbind    unbind ctrl+z
      --beep      beep for every matching packet received
Mode
  default mode     TCP
  -0  --rawip      RAW IP mode
  -1  --icmp       ICMP mode
  -2  --udp        UDP mode
  -8  --scan       SCAN mode.
                   Example: hping --scan 1-30,70-90 -S www.target.host
  -9  --listen     listen mode
IP
  -a  --spoof      spoof source address
  --rand-dest      random destionation address mode. see the man.
  --rand-source    random source address mode. see the man.
  -t  --ttl        ttl (default 64)
  -N  --id         id (default random)
  -W  --winid      use win* id byte ordering
  -r  --rel        relativize id field          (to estimate host traffic)
```

As observed Hping3 contains different options, and it can be used to run variety of scans against the target environment according to the requirement. However, majorly this tool is used for identifying underlying firewall within target domain or environment by sending crafted packets in ethical penetration tests whereas usage of this tool on any organization or any proprietary application should be avoided as it is considered illegal to use this tool within appropriate permissions.

Due to this restriction, throughout this exercise the tool is used only to perform normal passive scans against demo vulnerable websites to identify open ports or openly available information.

This tool can be used to identify open port on target domain as well as round trip time (RTT) using following command:

- sudo hping3 -S -p 80 -c 3 php.testsparker.com

```
seed@VM: ~
seed@VM:~$ sudo hping3 -S -p 80 -c 3 php.testsparker.com
[sudo] password for seed:
HPING php.testsparker.com (ens33 107.20.213.223): S set, 40 headers + 0 data bytes
len=46 ip=107.20.213.223 ttl=128 id=32012 sport=80 flags=SA seq=0 win=64240 rtt=88.8 ms
len=46 ip=107.20.213.223 ttl=128 id=32013 sport=80 flags=SA seq=1 win=64240 rtt=100.0 ms
len=46 ip=107.20.213.223 ttl=128 id=32014 sport=80 flags=SA seq=2 win=64240 rtt=87.6 ms

--- php.testsparker.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 87.6/92.1/100.0 ms
seed@VM:~$
```

As observed, this tool can be used to find open ports or services on target domains and can be used as alternate solution to Nmap for scanning the environment.

In addition, this tool can used in more details to see which services are enabled on target domain using following ICMP echo test command:

- sudo hping3 -1 -c 1 demo.testfire.net

```
seed@VM: ~
seed@VM:~$ sudo hping3 -1 -c 1 demo.testfire.net
HPING demo.testfire.net (ens33 65.61.137.117): icmp mode set, 28 headers + 0 data bytes
len=46 ip=65.61.137.117 ttl=128 id=32044 icmp_seq=0 rtt=72.1 ms

--- demo.testfire.net hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 72.1/72.1/72.1 ms
seed@VM:~$
```

As observed from above screenshot, there is 0% packet loss observed on demo target domain which means that ICMP is enabled on target web server. ICMP is frequently enabled for discoverability and network diagnostic purposes, such as 'traceroute' or 'ping' (ICMP echo). Having ICMP enabled exposes a server to denial-of-service attacks, which can be mitigated using rate limitations. If the ICMP echo is refused or dropped without a response, it is safe to conclude that the port is being screened by a firewall.

Using such techniques on actual target environment, it is possible to run command as mentioned above to detect open ports as well as services on web server on ethical penetration tests and accordingly crafted packets can be sent for identifying defensive tools such as firewalls or IPS devices on it.