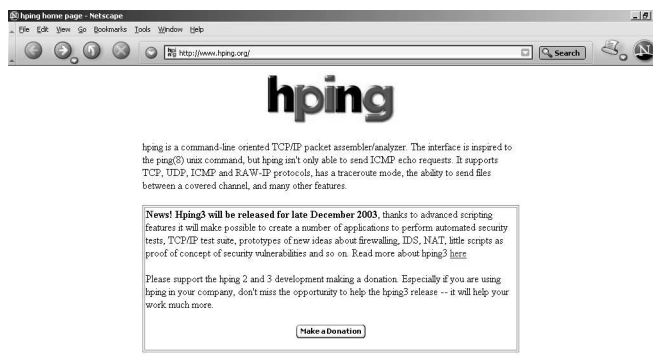


hping: a packet injection tool

David Morgan

© David Morgan 2003-2008

Installation



- download from the “hping 2.0.0 release candidate 3” link
- to get tarball `hping2.0.0-rc3.tar.gz`
- installation is smooth and uneventful
- call as “hping” or “hping2” but “man hping2” (*not* hping)

© David Morgan 2003-2008

hping -c 1 192.168.3.3

```
Tera Term - 192.168.3.4 VT
File Edit Setup Control Window Help
[root@EMACH1 root]# hping -c 1 192.168.3.3
HPING 192.168.3.3 (eth0 192.168.3.3): NO FLAGS are set, 40 headers + 0 data byte
s
len=46 ip=192.168.3.3 ttl=128 id=331 sport=0 flags=RA seq=0 win=0 rtt=0.6 ms
--- 192.168.3.3 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.6/0.6/0.6 ms
[root@EMACH1 root]#
```

Network capture analysis for the first hping command. The capture shows two packets:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.3.4	192.168.3.3	TCP	1810 > 0 [] Seq=1483365077 Ack=2087907366 Win=512 Len=0
2	0.000110	192.168.3.3	192.168.3.4	TCP	0 > 1810 [RST, ACK] Seq=0 Ack=1483365077 Win=0 Len=0

Annotations:

- talks to port 0 with no flags**: Points to the destination port 0 in the first packet.
- gets reset in response**: Points to the RST flag in the second packet.

Packet details for Frame 1 (60 on wire, 60 captured):

- Ethernet II
- Internet Protocol, Src Addr: 192.168.3.4 (192.168.3.4), Dst Addr: 192.168.3.3 (192.168.3.3)
- Transmission Control Protocol, Src Port: 1810 (1810), Dst Port: 0 (0), Seq: 1483365077, Len: 0
- source port: 1810 (1810)
- destination port: 0 (0)
- Sequence number: 1483365077
- Header length: 20 bytes
- Flags: 0x0000 ()
- window size: 512
- Checksum: 0xffff1 (correct)

© David Morgan 2003-2008

hping -a 100.1.1.1 192.168.3.3

```
Tera Term - 192.168.3.4 VT
File Edit Setup Control Window Help
[root@EMACH1 root]# hping -c 1 -a 100.1.1.1 192.168.3.3
HPING 192.168.3.3 (eth0 192.168.3.3): NO FLAGS are set, 40 headers + 0 data byte
s
--- 192.168.3.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@EMACH1 root]#
```

Network capture analysis for the second hping command. The capture shows three packets:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	100.1.1.1	192.168.3.3	TCP	1040 > 0 [] Seq=209214934 Ack=895038692 Win=512 Len=0
2	0.000104	100.1.1.1	100.1.1.1	TCP	0 > 1040 [RST, ACK] Seq=0 Ack=209214934 Win=0 Len=0
3	0.000116	192.168.3.2	192.168.3.3	TCP	Destination Unreachable

Annotations:

- gateway...**: Points to the source IP 192.168.3.2 in the third packet.
- ... says "can't"**: Points to the "Destination Unreachable" message in the third packet.
- "port closed" reply goes to spoofed address (of course!)**: Points to the destination IP 100.1.1.1 in the second packet.

Packet details for Frame 3 (82 on wire, 82 captured):

- Ethernet II
- Internet Protocol, Src Addr: 192.168.3.2 (192.168.3.2), Dst Addr: 192.168.3.3 (192.168.3.3)
- Internet Control Message Protocol
- Type: 3 (Destination unreachable)
- Code: 0 (Network unreachable)
- Checksum: 0x25c8 (correct)
- Internet Protocol, Src Addr: 192.168.3.3 (192.168.3.3), Dst Addr: 100.1.1.1 (100.1.1.1)
- Transmission Control Protocol, Src Port: 0 (0), Dst Port: 1040 (1040), Seq: 0, Ack: 209214934, Len: 0
- source port: 0 (0)
- destination port: 1040 (1040)
- Sequence number: 0
- Acknowledgement number: 209214934
- Header length: 20 bytes
- Flags: 0x0014 (RST, ACK)
- window size: 0
- Checksum: 0x18c5 (correct)

© David Morgan 2003-2008

Raw IP mode: hping -0

```

Tera Term - 192.168.3.4 VT
File Edit Setup Control Window Help
[root@EMACH1 root]# hping -c 1 -0 192.168.3.3
HPING 192.168.3.3 (eth0 192.168.3.3): raw IP mode set, 20 headers + 0 data bytes

--- 192.168.3.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@EMACH1 root]#
    
```

IP header followed by nothing

total IP len 20

Thinks sub-protocol is TCP

ethernet padding, doesn't count

© David Morgan 2003-2008

hping -0 -e signature

```

Tera Term - 192.168.3.4 VT
File Edit Setup Control Window Help
[root@EMACH1 root]# hping -c 1 -e "Greetings from Malpheus" -0 192.168.3.3
HPING 192.168.3.3 (eth0 192.168.3.3): raw IP mode set, 20 headers + 23 data bytes

--- 192.168.3.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@EMACH1 root]#
    
```

your arbitrary data

as IP's payload

malformed TCP??
...not TCP at all!

Greetings from Malpheus

© David Morgan 2003-2008

ICMP mode: hping -1

```
Tera Term - 192.168.3.4 VT
File Edit Setup Control Window Help
[root@EMACH1 root]# hping -c 1 -1 192.168.3.3
HPING 192.168.3.3 (eth0 192.168.3.3): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.3.3 ttl=128 id=2654 icmp_seq=0 rtt=0.6 ms

--- 192.168.3.3 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.6/0.6/0.6 ms
[root@EMACH1 root]#
```

issues ICMP-- echo request by default (so gets echo reply in return)

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.3.4	192.168.3.3	ICMP	Echo (ping) request
2	0.000097	192.168.3.3	192.168.3.4	ICMP	Echo (ping) reply

Frame 2 (42 on wire, 42 captured)
 Ethernet II
 Internet Protocol, Src Addr: 192.168.3.3 (192.168.3.3), Dst Addr: 192.168.3.4 (192.168.3.4)
 Internet Control Message Protocol
 Type: 0 (Echo (ping) reply)
 Code: 0
 Checksum: 0xe1f8 (correct)
 Identifier: 0x1e07
 Sequence number: 00:00

```
0000 00 40 05 a3 a8 bf 00 40 05 a3 42 26 08 00 45 00  .@....@..B&..E.
0010 00 1c 0a 5e 00 00 80 01 a9 2b c0 a8 03 03 c0 a8  ...d...@..E.....
0020 03 04 00 00 e1 f8 1e 07 00 00                ..... ..
```

3-2008

hping -1 -C icmp type

```
Tera Term - 192.168.3.4 VT
File Edit Setup Control Window Help
[root@EMACH1 root]# hping -c 1 -1 -C 11 192.168.3.3
HPING 192.168.3.3 (eth0 192.168.3.3): icmp mode set, 28 headers + 0 data bytes

--- 192.168.3.3 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@EMACH1 root]#
```

issue type 11 (ttl exceeded) instead of echo request

hping-1-C-Ethernet

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.3.4	192.168.3.3	ICMP	Time-to-live exceeded

Frame 1 (60 on wire, 60 captured)
 Ethernet II
 Internet Protocol, Src Addr: 192.168.3.4 (192.168.3.4), Dst Addr: 192.168.3.3 (192.168.3.3)
 Internet Control Message Protocol
 Type: 11 (Time-to-live exceeded)
 Code: 0 (TTL equals 0 during transit)
 Checksum: 0xf4ff (correct)

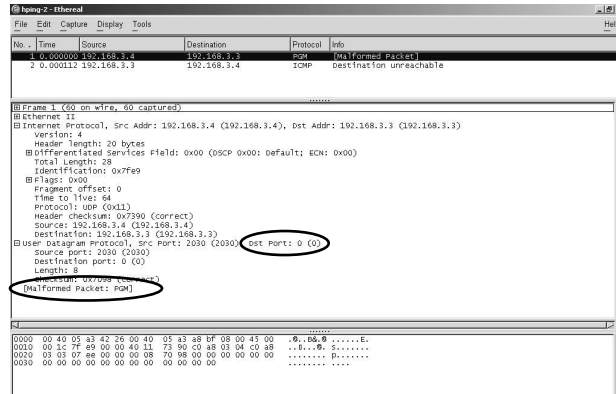
```
0000 00 40 05 a3 42 26 00 40 05 a3 a8 bf 08 00 45 00  .@....@..B&@.....E.
0010 00 1c 1c 44 00 00 40 01 d7 45 c0 a8 03 04 c0 a8  ...d...@..E.....
0020 03 03 00 00 f4 ff 00 00 00 00 00 00 00 00 00 00  ...D...@..E.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..@..... ..
```

jan 2003-2008

UDP mode: hping -2

```
Tera Term - 192.168.3.4 VT
File Edit Setup Control Window Help
[root@EMACH1 etc]# hping -c 1 -2 192.168.3.3
HPING 192.168.3.3 (eth0 192.168.3.3): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=192.168.3.3 name=UNKNOWN

--- 192.168.3.3 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@EMACH1 etc]#
```



© David Morgan 2003-2008

Want a packet that's not "malformed"? -- so form one

- must know the proper form (i.e., binary content) of the type of packet you want
- must compose it in a file
- hping -E will use your file content

© David Morgan 2003-2008

hping -2 -p 53

```
Tera Term - 192.168.3.4 VT
File Edit Setup Control Window Help
[root@EMACH1 utils]# hping -c 1 -2 -p 53 -d 31 -E file 206.13.29.12
HPING 206.13.29.12 (eth0 206.13.29.12): udp mode set, 26 headers, 31 data bytes
len=152 ip=206.13.29.12 ttl=247 id=10759 seq=0 rtt=2505.8 ms

--- 206.13.29.12 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 2505.8/2505.8/2505.8 ms
[root@EMACH1 utils]#
```

contains a preconstructed dns query in binary

a nameserver

```
capture-ethernet
File Edit Capture Display Tools Help
No. Time Source Destination Protocol Info
1 2.505000 192.168.3.4 206.13.29.12 DNS Standard query query www.cisco.com
2 2.505068 206.13.29.12 192.168.3.4 DNS Standard query response www.cisco.com
3 2.505068 192.168.3.4 206.13.29.12 ICMP Destination unreachable

Frame 1 (73 on wire, 73 captured)
Ethernet II
Internet Protocol, Src Addr: 192.168.3.4 (192.168.3.4), Dst Addr: 206.13.29.12 (206.13.29.12)
User Datagram Protocol, Src Port: 2434 (2434), Dst Port: 53 (53)
DNS Standard query (query)
Transaction ID: 0x0000
Flags: 0x0000 (Standard query)
0... = Response: Message is a query
..000 0... = Opcode: standard query (0)
....0... = Truncated: Message is not truncated
....1... = Recursion desired: Do query recursively
.....0... = Non-authenticated data ok: Non-authenticated data is unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.cisco.com: type A, class fnet

0000 00 a0 c9 1a a8 96 00 40 05 a3 a8 bf 08 00 45 00 .....@.....E
0010 00 3e db 02 00 00 40 11 f0 e9 c8 a8 03 04 ce 00 .....@.....
0020 10 00 00 85 00 33 00 77 81 1c 00 00 00 00 00 .....@.....
0030 00 00 00 00 00 00 77 77 77 05 63 69 73 63 6f .....WWW.CISCO
0040 00 69 6f 69 00 00 00 00 00 .....com.....
```

gets a real response

© David Morgan 2003-2008

Extending it

- not interactive – needs scripting

“Hping2 is the old version of the tool supporting the command line interface, while the new hping3 is the evolution that adds a Tcl scripting engine. ...If you plan to use hping in order to perform automated networks scans and security tests you can use hping3 scripts instead of hping2 + shell scripts, it is much more powerful!” - website

- scapy – another packet injection program
<http://www.secdev.org/projects/scapy/>

© David Morgan 2003-2008