

Hping3 version 1.4 Cheat Sheet

Mode (cont)

by ramkumaplays via cheatography.com/60600/cs/15755/

Ва	se 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

	packet rece	eivea
Mode		
default mode		TCP
-0	rawip	RAW IP mode
-1	icmp	ICMP mode
-2	udp	UDP mode
-8	scan	SCAN mode

		www.target.host
- 9	liste	en mode
IP		
-a	spoof	spoof source addess
	rand- dest	random destionation address mode
	rand- source	random source address mode
-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)
-f	frag	split packets in more frag
-X	 morefrag	set more fragments flag
-у	 dontfrag	set don't fragment flag
-g	fragoff	set the fragment offset
- m	mtu	set virtual mtu, impliesfrag if packet size > mtu
-0	tos	type of service (default 0x00), trytos help
- G	rroute	includes RECORD_ROUTE option and display the route buffer
	lsrr	loose source routing and record route
	ssrr	strict source routing and record route
- H	ipproto	set the IP protocol field, only in RAW IP mode

	Example: hpingscan 1-30,70-90 -S www.target.host		
liste	listen mode		
ooof	spoof source addess		
nd- t	random destionation address mode		
nd- rce	random source address mode		
	ttl (default 64)		
	id (default random)		
nid	use win* id byte ordering		
I	relativize id field (to estimate host traffic)		
ag	split packets in more frag		
refrag	set more fragments flag		
ıtfrag	set don't fragment flag		
agoff	set the fragment offset		
tu	set virtual mtu, impliesfrag if packet size > mtu		
S	type of service (default 0x00), trytos help		
oute	includes RECORD_ROUTE option and display the route buffer		
rr	loose source routing and record route		
srr	strict source routing and record route		
proto	set the IP protocol field, only in RAW IP mode		

ICMP		
- C	 icmptype	icmp type (default echo request)
- K	 icmpcode	icmp code (default 0)
	force-	send all icmp types (default send only supported types)
	icmp- gw	set gateway address for ICMP redirect (default 0.0.0.0)
	icmp-ts	Alias foricmpicmptype 13 (ICMP timestamp)
	icmp- addr	Alias foricmpicmptype 17 (ICMP address subnet mask)
	icmp- help	display help for others icmp options

UDP/TCP	
-S	base source port (default
baseport	random)

By ramkumaplays

cheatography.com/ramkumaplays/

Not published yet. Last updated 10th May, 2018. Page 1 of 1.

Sponsored by Readability-Score.com Measure your website readability! https://readability-score.com