Ethical Hacking and Countermeasures
hping3 Cheat Sheet

hping3
Source: http://hping.org

hping is a command-line oriented TCP/IP packet assembler/analyzer for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols.

The following table lists the various Hping commands and their respective scanning methods.

Syntax

```
1.Scan Commands
2.IP Related Commands
3.TCP/UDP Related Commands
4.TCP Flags
5.ICMP Related Commands
6.Common hping Commands
7.Protocol Selection Commands
```

Scan Commands

hping Command	Description
`hping3 -q <Target> (or) hping3 --quiet <Target>`	Scans quietly
`hping3 -I<Target> (or) hping3 --interface <Target>`	Acts as an Interface
`hping3 -D <Target> (or) hping3 --debug <Target>`	Debugging info
`hping3 -c <Target> (or) hping3 --count <Target>`	Count response packets
`hping3 -V <Target> (or) hping3 --verbose <Target>`	Enable verbose output Example: hping3 -V -S <target ip>
`hping3 -i <Target> (or) hping3 --interval <Target>`	Wait (uX for X microseconds, for example -i u1000)
`hping3 -v <Target> (or) hping3 -- version <Target>`	Show version information and API used to access to data link layer, linux sock packet or libpcap
`hping3 -n <Target> (or) hping3 --numeric <Target>`	Numeric output
`hping3 -z <Target> (or) hping3 --bind <Target>`	Used to bind. Use ctrl+z to increment TTL
`hping3 -Z <Target> (or) hping3 --unbind <Target>`	Used to unbind
`hping3 --beep <Target>`	Beep for every matching packet received
`hping3 --flood <Target>`	Sent packets as fast as possible. Don't show replies
`hping3 --fast <Target>`	Sends 10 packets / sec
`hping3 --faster <Target>`	Sends 1 packet / µs

IP Related Commands

hping Command	Description
`hping3 -a <Target> (or) hping3 --spoof <Target>`	Spoof source address
`hping3 -A <Target> -p 80`	ACK scanning on port 80
`hping3 --rand-dest <Target>`	Random destination address mode Example: hping3 -1 10.0.1.x --rand-dest –I eth0
`hping3 --rand-source <Target>`	Random source address mode
`hping3 -t <Target> (or) hping3 --ttl <Target>`	Set TTL (time to live) value
`hping3 -N <Target> (or) hping3 --id <Target>`	id [default random]
`hping3 -H –ipproto <Target>`	Set the IP protocol field, only in RAW IP mode
`hping3 -W <Target> (or) hping3 --winid <Target>`	Use win* id byte ordering
`hping3 -r <Target> (or) hping3 --rel <Target>`	Relativize id field to estimate host traffic
`hping3 -f <Target> (or) hping3 --frag <Target>`	Split packets in more fragments
`hping3 -x <Target> (or) hping3 --morefrag <Target>`	Set more fragments flag
`hping3 -y <Target> (or) hping3 --dontfrag <Target>`	Set don't fragment flag
`hping3 -g <Target> (or) hping3 --fragoff <Target>`	Set fragment offset value
`hping3 -G <Target> (or) hping3 --rroute <Target>`	Includes RECORD_ROUTE option and display the route buffer
`hping3 -m <Target> (or) hping3 --mtu <Target>`	set virtual MTU, implies --frag if packet size >MTU
`hping3 -W <Target> (or) hping3 --winid <Target>`	Type of service (default 0x00)
`hping3 --lsrr <Target>`	Loose source routing and record route
`hping3 --ssrr <Target>`	Strict source routing and record route
`hping3 -x <Target> (or) hping3 --morefrag <Target>`	Set more fragments flag
`hping3 -y <Target> (or) hping3 --dontfrag <Target>`	Set don't fragment flag

TCP/UDP Related Commands

hping Command	Description
`hping3 -s <Target> (or) hping3 --baseport <Target>`	Base source port [random], +1 on received
`hping3 -p <Target> (or) hping3 --destport <Target>`	Destination port [0] if have, have: +port increased for each reply ++port increased for each sent
`hping3 -w <Target> (or) hping3 --win <Target>`	Set Win size [64]
`hping3 -O <Target> (or) hping3 --tcpoff <Target>`	Set fake TCP data offset
`hping3 --keep <Target>`	Still source port
`hping3 -b <Target> (or) hping3 --badcksum <Target>`	Send packets with a bad IP checksum
`hping3 -M <Target> (or) hping3 --setseq <Target>`	Set TCP sequence number
`hping3 -L <Target> (or) hping3 --setack <Target>`	Set TCP ack
`hping3 -Q <Target> (or) hping3 --seqnum <Target>`	Collects initial sequence number Example: hping3 <target ip> -Q -p 139 –s

TCP Flags

hping Command	Description
`hping3 -R <Target> (or) hping3 --rst <Target>`	Set Reset flag Example: hping3 –rst -S <target ip>
`hping3 -A <Target> (or) hping3 --ack <Target>`	Set ACK flag Example: hping3 –A <target ip> –p 80
`hping3 -F <Target> -p 80 (or) hping3 --fin <Target> -p 80`	Set FIN flag scan on port 80 Example: hping3 –F –P –U <target ip> –p 80
`hping3 -S <Target> (or) hping3 --syn <Target> -p 80`	Set SYN flag Example: hping3 -S 192.168.1.1 -a192.168.1.254 -p 22 --flood
`hping3 -U <Target> -p 80 (or) hping3 --urg <Target> -p 80`	Set URG flag scan on port 80 Example: hping3 –F –P –U <target ip> –p 80
`hping3 -X <Target> (or) hping3 --xmas <Target>`	Set X unused flag (0x40)
`hping3 -Y <Target> (or) hping3 --ymas <Target>`	Set Y unused flag (0x80)

Ethical Hacking and Countermeasures
hping3 Cheat Sheet

hping3
Source: http://hping.org

hping is a command-line oriented TCP/IP packet assembler/analyzer for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols.

The following table lists the various Hping commands and their respective scanning methods.

Syntax

```
1.Scan Commands
2.IP Related Commands
3.TCP/UDP Related Commands
4.TCP Flags
5.ICMP Related Commands
6.Common hping Commands
7.Protocol Selection Commands
```

ICMP Related Commands

hping Command	Description
`hping3 -C <Target> (or) hping3 --icmptype <Target>`	Set icmp type, default is ICMP echo request (implies --icmp).
`hping3 -K <Target> (or) hping3 --icmpcode <Target>`	Set icmp code, default is 0 (implies --icmp)
`hping3 --icmp-ipver <Target>`	Set IP version of IP header contained into ICMP data, default is 4
`hping3 --icmp-iphlen <Target>`	Set IP header length of IP header contained into ICMP data, default is 5 (5 words of 32 bits)
`hping3 --icmp-iplen ip <Target>`	Set IP packet length of IP header contained into ICMP data, default is the real length
`hping3 -i <Target> (or) hping3 --interval <Target>`	Set IP id of IP header contained into ICMP data, default is random
`hping3 --icmp-ipid <Target>`	Set IP protocol of IP header contained into ICMP data, default is TCP.
`hping3 --icmp-ipproto <Target>`	Set ICMP checksum, for default is the valid checksum.
`hping3 --icmp-cksum <Target>`	Alias for --icmp --icmptype 13 (ICMP timestamp)
`hping3 --icmp-ts <Target>`	Alias for --icmp --icmptype 17 (ICMP address subnet mask)
`hping3 --icmp-addr <Target>`	Set gateway address for ICMP redirect (default 0.0.0.0)
`hping3 --icmp-gw <Target>`	Sent packets as fast as possible. Don't show replies
`hping3 --icmp-help <Target>`	Display help for others ICMP options
`hping3 --force-icmp <Target>`	Send all ICMP types (default send only supported types)

Common hping Commands

hping Command	Description
`hping3 -E <Target> (or) hping3 --file <Target>`	File inserted into packet's data
`hping3 -e <Target> (or) hping3 --sign <Target>`	Add 'signature'
`hping3 -d <Target> (or) hping3 --data <Target>`	Data size of packet body size
`hping3 -j <Target> (or) hping3 --dump <Target>`	Dump received packets in hex
`hping3 -J <Target> (or) hping3 --print <Target>`	Print dump in printable character
`hping3 -B <Target> (or) hping3 --safe <Target>`	Safe lost packets will be resent
`hping3 -u <Target> (or) hping3 --end <Target>`	Tells when --file reached EOF and prevent rewind
`hping3 -T <Target> (or) hping3 --traceroute <Target>`	Traceroute mode
`hping3 --tr-keep-ttl <Target>`	Keeps TTL fixed
`hping3 --tr-stop <Target>`	Exit when receive the first not ICMP in traceroute mode
`hping3 --tr-no-rtt <Target>`	Don't show RTT
`hping3 --tcpexitcode <Target>`	Use last tcp->th_flags as exit code
`hping3 --tcp-mss <Target>`	Enable the TCP MSS option with the given value
`hping3 --tcp-timestamp <Target>`	Enable the TCP timestamp option to guess the HZ/uptime Example: hping3 -S <target ip> -p 80 --tcp-timestamp
`hping3 --apd-send <Target>`	Send the packet described with APD (see docs/APD.txt)

Protocol Selection Commands

hping Command	Description
`hping3 -0 <Target> (or) hping3 --rawip <Target>`	Raw IP mode
`hping3 -1 <Target> (or) hping3 --icmp <Target>`	ICMP mode Example: hping3 -1 <target ip>
`hping3 -2 <Target> (or) hping3 --udp <Target>`	UDP mode Example: hping3 -2 <target ip> –p 80
`hping3 -8 <Target> (or) hping3 --scan <Target>`	Scan mode Example: hping3 --scan 1-30,70-90 -S <target website> Example: hping3 -8 50-60 –S <target ip> -V
`hping3 -9 <Target> (or) hping3 --listen <Target>`	Listen mode Example: hping3 -9 HTTP –I eth0