用法: hping3 host [选项]

-h --help 显示帮助

-v --version 显示版本

-c --count 分组数

-i --interval 等待 (UX X微秒,例如 -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 [计]数字输出；

-q --quiet 安静的

-I --interface 接口名称(否则默认路由接口)

-V --verbose 详细模式

-D --debug debug命令的信息

-z --bind 绑定 ctrl+z to ttl (默认为DST端口)

-Z --unbind 把绑定打开 ctrl+z

--beep 每个匹配的数据都发生蜂鸣默认模式是TCP

-0 --rawip 原始IP模式

-1 --icmp ICMP模式

-2 --udp UDP模式

-8 --scan 扫描模式。

例如：hping扫描1-30,70-90的www.target.host

-9 --listen 监听模式

IP

-a --spoof 嗅探源地址

--rand-dest 随机目的地地址模式. see the man.

--rand-source 随机源地址模式. see the man.

-t --ttl ttl (默认 64)

-N --id id (默认 random)

-W --winid use win\* id byte排序

-r --rel 相对的ID字段 (估计主机流量)

-f --frag 更多的片段分包. (可以通过弱ACL)

-x --morefrag 设置更多碎片标志

-y --dontfrag 设置不碎片标志

-g --fragoff 设置片段偏移

-m --mtu 设置虚拟的MTU，意味着——片段如果包大小> MTU

-o --tos 服务类型（默认为0x00），尝试——TOS的帮助

-G --rroute 包括record\_route选项和显示路由缓存

--lsrr 松散源路由和Ecord路线

--ssrr 严格的源路由和记录路由

-H --ipproto 设置IP协议字段，只在原始IP模式下

ICMP

-C --icmptype ICMP类型（默认的回送请求）

-K --icmpcode ICMP编码（默认为0）

--force-icmp 发送ICMP类型（默认只发送支持的类型）

--icmp-gw 对于ICMP重定向设置网关地址（默认0.0.0.0）

--icmp-ts 别名：13（icmptype ICMP时间戳）

--icmp-addr 别名：icmptype ICMP 17（ICMP地址的子网掩码）

--icmp-help 其显示其他的ICMP的帮助UDP/TCP

-s --baseport 基源端口 （默认随机）

-p --destport [+][+]<端口> 目标端口（默认为0） ctrl+z inc/dec

-k --keep 保持源端口

-w --win winSize（默认为64）

-O --tcpoff 伪造的TCP数据集来替代真正的 数据集 (而不是tcphdrlen / 4)

-Q --seqnum 只显示TCP序列号

-b --badcksum (尝试) 发送换的 IP checksum

很多系统都会修复 IP checksum 所发送来的数据包

所以你会收到很多不好的UDP/TCP checksum来替代

-M --setseq 设置TCP序列号

-L --setack 设置TCP ACK

-F --fin 设置FIN标志

-S --syn 设置SYN标志

-R --rst RST标志设置

-P --push 设置PUSH标志

-A --ack 设置ACK标志

-U --urg 设置URG标志

-X --xmas 设置X unused 标志(0x40)

-Y --ymas 设置 Y unused标志(0x80)

--tcpexitcode 最后使用TCP -> th\_flags作为退出代码

--tcp-mss 使给定值TCP MSS选项

--tcp-timestamp 启用TCP时间戳选项猜测赫兹/运行时间

Common

-d --data 数据大小 (default is 0)

-E --file 文件中的数据

-e --sign 添加“签名”

-j --dump 在十六进制转储数据包

-J --print dump出可打印的特征

-B --safe 启用“安全”协议

-u --end 当file到达 EOF和prevent rewind时提示你

-T --Traceroute Traceroute模式 (意味着--绑定和TTL 1)

--tr-stop 退出时，traceroute模式接收第一不是ICMP

--tr-keep-ttl 保持固定源的TTL,有用的监视器只是 hop

--tr-no-rtt 在跟踪模式不计算RTT信息显示

ARS包描述（新的、不稳定的）

--apd-send 发送数据包描述的APD（见文档/ APD .txt）