**HPING 使用方法**

一、HPING和ping的区别：

典型ping程序使用的是ICMP回显请求来测试，而HPING可以使用任何IP报文，包括ICMP、TCP、UDP、RAWSOCKET。

二、下载：

HTTP：//WWW.HPING.ORG/

三、安装方法与普通软件同。

四、命令注释：

tsinghua@tsinghua-desktop:~$ hping2 --help

usage: hping host [options]

-h --help show this help ／／help

-v --version show version ／／版本

-c --count packet count ／／hping的包数量 和ping相同。

-i --interval wait (uX for X microseconds, for example -i u1000) ／／hping的间隔 u表示微妙，－－fast表示快速模式，一秒10个包。

--fast alias for -i u10000 (10 packets for second)

-n --numeric numeric output ／／表示不进行名称解析。

-q --quiet quiet ／／安静模式 只输出开始结束信息。

-I --interface interface name (otherwise default routing interface) ／／－使用网卡端口，缺省按路由表进行。

-V --verbose verbose mode ／／详细模式 一般显示很多包信息。

-D --debug debugging info ／／debug模式，定义hping2使用模式。

-z --bind bind ctrl+z to ttl (default to dst port)／／帮定快捷键

-Z --unbind unbind ctrl+z ／／撤销快捷键。

Mode ／／模式选择。

default mode TCP （缺省使用TCP进行PING处理）

-0 --rawip RAW IP mode ／／裸IP方式。使用RAWSOCKET方式。

-1 --icmp ICMP mode ／／ICMP模式。

-2 --udp UDP mode ／／UDP模式

-8 --scan SCAN mode. ／／扫描模式 指定扫描对应的端口。

Example: hping --scan 1-30,70-90 -S [http://www.target.host](http://www.target.host/)

-9 --listen listen mode ／／侦听模式，会接受指定的信息。侦听指定的信息内容。

IP ／／IP模式选择。

-a --spoof spoof source address ／／源地址欺骗。

--rand-dest random destionation address mode. see the man.随机目的地址模式。

--rand-source random source address mode. see the man. 随机源地址模式，具体信息看MAN。

-t --ttl ttl (default 64) ／／修改TTL值。

-N --id id (default random) －－hping中的ID值，缺省为随机值。

-W --winid use win\* id byte ordering 使用winid的模式，针对不同的操作系统。

-r --rel relativize id field (to estimate host traffic) ／／递减id区域模式。

-f --frag split packets in more frag. (may pass weak acl)／／分段，可以测试对方或者交换机碎片处理能力，缺省16字节。

-x --morefrag set more fragments flag ／／大量碎片，泪滴攻击。

-y --dontfrag set dont fragment flag ／／不可恢复的IP碎片。

-g --fragoff set the fragment offset ／／设置断偏移。

-m --mtu set virtual mtu, implies --frag if packet size > mtu ／／设置虚拟MTU值，当大于mtu的时候分段。

-o --tos type of service (default 0x00), try --tos help ／／tos字段，缺省0x00，尽力而为？

-G --rroute includes RECORD\_ROUTE option and display the route buffer ／／记录IP路由，并显示路由缓冲。

--lsrr loose source routing and record route ／／松散源路由

--ssrr strict source routing and record route ／／严格源路由。

-H --ipproto set the IP protocol field, only in RAW IP mode ／／设置ip协议域，仅在RAW ip模式使用。

ICMP ／／ICMP模式。

-C --icmptype icmp type (default echo request) ／／ICMP类型，缺省回显请求。

-K --icmpcode icmp code (default 0) ／／ICMP代码。

--force-icmp send all icmp types (default send only supported types) ／／强制ICMP类型。

--icmp-gw set gateway address for ICMP redirect (default 0.0.0.0) ／／ICMP重定向

--icmp-ts Alias for --icmp --icmptype 13 (ICMP timestamp) ／／icmp时间戳

--icmp-addr Alias for --icmp --icmptype 17 (ICMP address subnet mask) ／／icmp子网地址。

--icmp-help display help for others icmp options ／／ICMP帮助。

UDP/TCP ／／UDP／TCP模式。

-s --baseport base source port (default random) ／／缺省随机源端口

-p --destport [+][+]<port> destination port(default 0) ctrl+z inc/dec ／／缺省目的端口为0，连接后端口＋1。

-k --keep keep still source port ／／保持源端口

-w --win winsize (default 64) ／／win的滑动窗口。

-O --tcpoff set fake tcp data offset (instead of tcphdrlen / 4)／／设置伪造的数据偏移。

-Q --seqnum shows only tcp sequence number ／／tcp 连接序列号

-b --badcksum (try to) send packets with a bad IP checksum ／／IP包校验。

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 ／／设置TCP序列号

-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 ／／一大堆IP抱头的设置。

-X --xmas set X unused flag (0x40)

-Y --ymas set Y unused flag (0x80)

--tcpexitcode use last tcp->th\_flags as exit code

--tcp-timestamp enable the TCP timestamp option to guess the HZ/uptime ／／tcp的时间戳。

Common ／／通用设置

-d --data data size (default is 0) 发送数据包大小，缺省是0。

-E --file data from file ／／从文件中发送

-e --sign add 'signature' ／／标注签名

-j --dump dump packets in hex ／／以16进制显示包格式

-J --print dump printable characters ／／打印

-B --safe enable 'safe' protocol ／／开启安全模式，确保数据发送。

-u --end tell you when --file reached EOF and prevent rewind ／／到达报尾后提示。

-T --traceroute traceroute mode (implies --bind and --ttl 1)

--tr-stop Exit when receive the first not ICMP in traceroute mode

--tr-keep-ttl Keep the source TTL fixed, useful to monitor just one hop

--tr-no-rtt Don't calculate/show RTT information in traceroute mode

ARS packet description (new, unstable)

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

五、具体应用：

1、PING失效后的主机检测：

tsinghua@tsinghua-desktop:~$ ping 192.168.2.1

PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.

--- 192.168.2.1 ping statistics ---

19 packets transmitted, 0 received, 100% packet loss, time 18009ms

－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

tsinghua@tsinghua-desktop:~$ sudo hping2 -c 4 -n -i 2 192.168.2.1

HPING 192.168.2.1 (eth0 192.168.2.1): NO FLAGS are set, 40 headers + 0 data bytes

len=46 ip=192.168.2.1 ttl=64 id=43489 sport=0 flags=RA seq=0 win=0 rtt=1.0 ms

len=46 ip=192.168.2.1 ttl=64 id=43490 sport=0 flags=RA seq=1 win=0 rtt=0.6 ms

len=46 ip=192.168.2.1 ttl=64 id=43491 sport=0 flags=RA seq=2 win=0 rtt=0.7 ms

len=46 ip=192.168.2.1 ttl=64 id=43498 sport=0 flags=RA seq=3 win=0 rtt=0.6 ms

--- 192.168.2.1 hping statistic ---

4 packets transmitted, 4 packets received, 0% packet loss

round-trip min/avg/max = 0.6/0.8/1.0 ms

-c 发送4个报文 －n 不进行名称解析 －i 包发送时间间隔。

好处：即使主机阻塞了ICMP报文，也可以显示主机是否在运行的信息，在关掉ICMP的探测有效！

显示信息解释：len，返 回ip报文大小；ttl； id，IP的ID域；sport，源端口，flags，返回的IP报设置的TCP标志 （R：RESET，A：ACK；S：SYN；F：FIN；P：PUSH；U：URGENT）；seq：序列号；win：tcp窗口大小；rtt：往返 时，EIGRP似乎有这个设置。

2、防火墙规则测试：

hping有类似NMAP的方法来检测并收集关于潜在的防火墙的规则和能力的信息。

如果一个主机对ping没有任何相应，而对hping有响应，假定目标的主机为192.168.2.234.

一旦主机对hping作出了响应,那么下一步我们先用nmap先进行一个端口扫描,当然这个hping2也可以作.

tsinghua@tsinghua-desktop:~$ sudo nmap -sT -P0 -p 21-25 192.168.2.234

Starting Nmap 4.53 ( [http://insecure.org](http://insecure.org/) ) at 2008-08-14 15:56 CST

Interesting ports on 192.168.2.234:

PORT STATE SERVICE

21/tcp filtered ftp

22/tcp open ssh

23/tcp filtered telnet

24/tcp filtered priv-mail

25/tcp filtered smtp

Nmap done: 1 IP address (1 host up) scanned in 1.379 seconds

以上信息显示除了ssh端口外,其他端口被阻塞.然后可以试试用hping向各个被阻塞的端口发送空的报文.用-p的开关,可以对指定的目的端口进行hping.

tsinghua@tsinghua-desktop:~$ sudo hping2 -p 21 192.168.2.234

HPING 192.168.2.234 (eth0 192.168.2.234): NO FLAGS are set, 40 headers + 0 data bytes

24: len=46 ip=192.168.2.234 ttl=128 id=2461 sport=24 flags=RA seq=7 win=0 rtt=0.7 ms

len=46 ip=192.168.2.234 ttl=128 id=2462 sport=24 flags=RA seq=8 win=0 rtt=0.7 ms

25: len=46 ip=192.168.2.234 ttl=128 id=2463 sport=25 flags=RA seq=9 win=0 rtt=0.7 ms

len=46 ip=192.168.2.234 ttl=128 id=2464 sport=24 flags=RA seq=10 win=0 rtt=0.7 ms

前三个端口没有响应,端口 24 25 获得了RST/ACK响应.这说明,虽然这些端口被禁止PING,但没有工具在该端口上监听.然而为什么NMAP没有得到响应,因为NMAP虽然使用 TCP连接,但它在TCP报头中设置了TCP SYN标记位,而HPING 使用了空标记的报文,这就告诉我们说,在主机192.168.2.234上只阻塞进入的TCP连接.接下来使用hping创建一个SYN报文然后将其发送 到5个端口再测试.

tsinghua@tsinghua-desktop:~$ sudo hping2 -S -p 21 192.168.2.234

HPING 192.168.2.234 (eth0 192.168.2.234): S set, 40 headers + 0 data bytes

22: len=46 ip=192.168.2.234 ttl=128 id=10722 sport=22 flags=SA seq=1 win=0 rtt=1.2 ms

len=46 ip=192.168.2.234 ttl=128 id=10747 sport=22 flags=SA seq=2 win=0 rtt=0.7 ms

这次只有22端口响应,说明SSH端口是开放的,但有工具在上面监听,该端口没有进行过滤.

然后我们再创建一个ACK报文并发送:

tsinghua@tsinghua-desktop:~$ sudo hping2 -A -p 21 192.168.2.234

HPING 192.168.2.234 (eth0 192.168.2.234): A set, 40 headers + 0 data bytes

22: len=46 ip=192.168.2.234 ttl=128 id=12707 sport=22 flags=R seq=2 win=0 rtt=0.7 ms

len=46 ip=192.168.2.234 ttl=128 id=12708 sport=22 flags=R seq=3 win=0 rtt=0.7 ms

23: len=46 ip=192.168.2.234 ttl=128 id=12709 sport=23 flags=R seq=4 win=0 rtt=0.7 ms

len=46 ip=192.168.2.234 ttl=128 id=12710 sport=22 flags=R seq=5 win=0 rtt=0.7 ms

24: len=46 ip=192.168.2.234 ttl=128 id=12711 sport=24 flags=R seq=6 win=0 rtt=0.7 ms

len=46 ip=192.168.2.234 ttl=128 id=12712 sport=22 flags=R seq=7 win=0 rtt=0.7 ms

25: len=46 ip=192.168.2.234 ttl=128 id=12712 sport=25 flags=R seq=8 win=0 rtt=0.8 ms

len=46 ip=192.168.2.234 ttl=128 id=12713 sport=22 flags=R seq=9 win=0 rtt=0.7 ms

结果除了21端口外所有端口都响应了RST,说明了:

1.端口22是开放的,但有工具在上面监听.

2.24 25 上面没有工具监听,对NULL报文回显.

3.端口23针对ACK报文以RST进行了响应,但没有响应NULL报文.说明该端口被过滤,但是telnet服务运行在192.168.2.234上.

4.阻塞了进入的SYN报文但允许其他TCP报文通过,说明它采用的不是基于状态的报文防火墙.