[2012年1月MVP申请倒计时——13日截止](http://blog.csdn.net/blogdevteam/article/details/6799983)                            [“IT适合你吗？”智力挑战](http://www.cisco.com/web/CN/learnings/yc3/index.html?pnBAC=&POSITION=Homepage&COUNTRY_SITE=CN&CAMPAIGN=FY12Q1Youth+&CREATIVE=Banner2+FY12Q1Youth+&REFERRING_SITE=CSDN&SurveyCode=&KeyCode=500007_6%20)

[**tcpdump抓包分析TCP三次握手过程**](http://blog.csdn.net/renrenhappy/article/details/5929702)

分类： [TCP/IP与套接字编程](http://blog.csdn.net/renrenhappy/article/category/700059) 2010-10-09 15:11 566人阅读 [评论](http://blog.csdn.net/renrenhappy/article/details/5929702#comments)(0) [收藏](javascript:void(0);) [举报](http://blog.csdn.net/renrenhappy/article/details/5929702#report)

转：<http://hi.baidu.com/xxjjyy2008/blog/item/e6566bf837d91903d9f9fdd0.html>

一、 tcpdump使用

1、首先看下MAN手册

TCPDUMP(8)

NAME  
       tcpdump - dump traffic on a network

SYNOPSIS  
       tcpdump [ -AdDeflLnNOpqRStuUvxX ] [ -c count ]  
               [ -C file\_size ] [ -F file ]  
               [ -i interface ] [ -m module ] [ -M secret ]  
               [ -r file ] [ -s snaplen ] [ -T type ] [ -w file ]  
               [ -W filecount ]  
               [ -E [spi@ipaddr](mailto:spi@ipaddr) algo:secret,... ]  
               [ -y datalinktype ] [ -Z user ]  
               [ expression ]

选项：

-A        以ASCII码显示消息包

-c         指定包个数

-C        配合-w，当写入文件时，先检查文件大小是否已经超过1M，若超过，生成新文件，文件名为指定文件名加后缀1。

-d        将匹配信息包的代码以人们能够理解的汇编格式给出

-dd      将匹配信息包的代码以c语言程序段的格式给出

-ddd    将匹配信息包的代码以十进制的形式给出。

-D        列出可以抓包的所有网络接口

-e        显示链路层内容

-f         外部的IP以数字方式显示

-i         指定网络接口

-l         使标准输出变为缓冲行形式

-n        IP，端口用数字方式显示

-t 　　 在输出的每一行不打印时间戳；  
-v 　 　输出一个稍微详细的信息，例如在ip包中可以包括ttl和服务类型的信息；  
-vv 　 输出详细的报文信息；  
-c 　　 在收到指定的包的数目后，tcpdump就会停止；  
-F 　　 从指定的文件中读取表达式,忽略其它的表达式；  
-i 　　 指定监听的网络接口；  
-r 　　 从指定的文件中读取包(这些包一般通过-w选项产生)；  
-w 　　直接将包写入文件中，并不分析和打印出来；  
-T 　　 将监听到的包直接解释为指定的类型的报文，常见的类型有rpc （远程过程调用）和snmp（简单网络管理协议；）

-x        让十六进制显示包内容

2、过滤

（1）指定接口(-i)

如：tcpdump -i eth0

（2）指定IP地址(host)，可以辅加and , or ，!等逻辑符，以及src，dest等表示方向。

如：tcpdump host 192.168.1.23 捕获192.168.1.23发出或者收到的包

tcpdump -A host 192.168.1.90 and /( 192.168.1.104 or 192.168.1.105 /) 捕获192.168.1.23与192.168.1.104或者192.168.1.105之间往来的包

tcpdump host ! 192.168.1.23 捕获除192.168.1.23以外所有主机的包

tcpdump -A src 192.168.1.90 and dst 192.168.1.104 指定从90发往104的包

（3）指定端口(port)

如：tcpdump port 80 指定捕获80端口的包

（4）指定协议( 协议包括：ether, fddi, tr, wlan, ip, ip6, arp, rarp, decnet, tcp and udp)

如：tcpdump tcp 指定捕获TCP包

（5）其它(gateway, broadcast, less, greater)

如：tcpdump broadcast 所有广播包

二、三次握手过程分析

用netstat -an | grep LISTEN看一下，当前主机正在监听的端口，使用另一台机telnet过来，不输入任何内容，进行抓包。

我们这里以6000为例

tcpdump port 6000 -c 3 -n

内容如下：

21:07:17.790296 IP 192.168.1.104.2511 > 192.168.1.90.6000: S 3359422806:3359422806(0) win 64240 <mss1460,nop,nop,sackOK>  
21:07:17.790317 IP 192.168.1.90.6000 > 192.168.1.104.2511: S 3675079922:3675079922(0) ack 3359422807 win5840 <mss 1460,nop,nop,sackOK>  
21:07:17.790675 IP 192.168.1.104.2511 > 192.168.1.90.6000: . ack 1 win 64240

我们来对第一个包进行分析：

21:07:17（时间）.

790296（ID号）

IP (协议)

192.168.1.104.2511 > 192.168.1.90.6000: （源IP，端口，目的IP，端口）中间>表示方向

S (表示为SYN包，即发起连接包

    紧急指针— URG  
    确认序号有效—ACK  
    接收方应该尽快将这个报文段交给应用层—PSH  
    重建连接—RST  
    同步序号用来发起一个连接—SYN  
    发端完成发送任务—IN  
)

3359422806:3359422806(0) （IP包序号，相对序号为0）

win 64240 （数据窗口大小，告诉对方本机接收窗口大小，windows下默认为64240，可通过setsockopt动态修改，同样可以通过修改注册表项（HKEY\_LOCAL\_MACHINE/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters的TCPWindowSize)来更改默认值）

<mss1460,nop,nop,sackOK> 对应TCP包头中的选项字段

  MSS: Maxitum Segment Size 最大分段大小，MSS表示TCP传往另一端的最大块数据的长度。当一个连接建立时，连接的双方都要通告各自的MSS。如果一方不接收来自另一方的MSS值，则MSS就定为默认的536字节。

以上三个包正好是TCP连接的三次握手过程:

（1） A主机发送序号为3359422806的SYN包到B，同时带有自身的WIN和MSS大小。

（2） B主机收到后，发送SYN+ACK的返回包到A，也带自身的WIN和MSS大小，3675079922，同时为为上一个包的应答包3359422807。

（3） A主机返回ACK，包序号为1(相对序号，如果需要看绝对序号，可以在tcpdump命令中加-S)

http://hi.csdn.net/attachment/201010/9/0_12866089332Y90.gif

然后我们再来分析一下包的具体内容：

我们在tcpdump命令中加-x选项，后可得到如下内容：

22:07:13.436638 IP 192.168.1.104.2799 > 192.168.1.90.6000: S 3480877812:3480877812(0) win 64240 <mss 1460,nop,nop,sackOK>  
    0x0000: 4500 0030 b195 4000 8006 c51f c0a8 0168  
    0x0010: c0a8 015a 0aef 1770 cf79 faf4 0000 0000  
    0x0020: 7002 faf0 174e 0000 0204 05b4 0101 0402  
22:07:13.436675 IP 192.168.1.90.6000 > 192.168.1.104.2799: S 4226616929:4226616929(0) ack 3480877813 win 5840 <mss 1460,nop,nop,sackOK>  
    0x0000: 4500 0030 0000 4000 4006 b6b5 c0a8 015a  
    0x0010: c0a8 0168 1770 0aef fbed 0e61 cf79 faf5  
    0x0020: 7012 16d0 f10e 0000 0204 05b4 0101 0402  
22:07:13.437019 IP 192.168.1.104.2799 > 192.168.1.90.6000: . ack 1 win 64240  
    0x0000: 4500 0028 b196 4000 8006 c526 c0a8 0168  
    0x0010: c0a8 015a 0aef 1770 cf79 faf5 fbed 0e62  
    0x0020: 5010 faf0 39b2 0000

还是一样，我们对第一个包进行分析，第一个包为SYN包，应该为一个空包，即只包括IP头和TCP头。  
IP包头  
4 － IP版本号 IPV4  
5 － IP包头长度 5个32字节  
00 － TOS (000 0000 0)前三个BIT优先权，现已忽略；4 bit的TOS分别代表:最小时延、最大吞吐量、最高可靠性和最小费用， 均为0表示一般服务；最后1BIT未用。  
0030 －总长度，48个字节  
b195 －包唯一标识  
4000 －标志字段，和片偏移，用于分片  
80 － TTL(128)   
06 － 协议 TCP  
c51f － MAC  
c0a8 0168 － SRC IP，可以inet\_ntoa转换成点号分隔的IP。  
c0a8 015a － DST IP  
TCP包头  
0aef －源端口，十进制为2799  
1770 －目的端口，十进制为6000  
cf79 faf4 包序号，十进制为217554863  
0000 0000 确认序号，0，未设置ACK，确认序号无效  
7002 －TCP包头长度，标志位。（0111 000000 000010）前4bitTCP长度7个32BIT，中间6bit保留，后6bit为标志位（URG, ACK，PSH， RST， SYN， FIN），可以看出设置了倒数第二位，SYN位。  
faf0 － 窗口大小，十进制为64240  
174e － 校验和，覆盖了整个的 T C P报文段: T C P首部和T C P数据  
0000 － 紧急指针， 只有当URG标志置1时紧急指针才有效  
0204 05b4 0101 0402 － 选项字段，8个字节