命令行抓包工具tcpdump

tcpdump

tcpdump是一个用于截取网络分组，并输出分组内容的工具。tcpdump凭借强大的功能和灵活的截取策略，使其成为类UNIX系统下用于网络分析和问题排查的首选工具。 tcpdump提供了源代码，公开了接口，因此具备很强的可扩展性，对于网络维护和入侵者都是非常有用的工具。

YUM安装即可：yum install tcpdump -y

常用参数介绍：

-i 指定抓包网络接口

-c 在收到指定的数量的分组后，tcpdump就会停止

-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

-w 直接将分组写入文件中，而不是不分析并打印出来

-b 在数据-链路层上选择协议，包括ip、arp、rarp、ipx都是这一层的

-A，数据包的内容以 ASCII 显示，通常用来捉取 WWW 的网页数据包资料。

-X，可以列出十六进制 (hex) 以及 ASCII 的数据包内容，对于监听数据包内容很有用

-n 不把网络地址转换成名字

-nn 不进行端口名称的转换

-r 从指定的文件中读取包(这些包一般通过-w选项产生)

-S 将tcp的序列号以绝对值形式输出，而不是相对值

-t 不在每一行中输出时间戳

-tt 在每一行中输出非格式化的时间戳

-ttt 输出本行和前面一行之间的时间差

-tttt 在每一行中输出由date处理的默认格式的时间戳

tcpdump的表达式介绍

表达式是一个正则表达式，tcpdump利用它作为过滤报文的条件，如果一个报文满足表达式的条件，则这个报文将会被捕获。如果没有给出任何条件，则网络上所有的信息包将会被截获。

在表达式中一般如下几种类型的关键字：

第一种是关于类型的关键字，主要包括host，net，port，例如 host 210.27.48.2， 指明 210.27.48.2是一台主机，net 202.0.0.0/8指明202.0.0.0是一个网络地址，port 23 指明端口号是23。如果没有指定类型，缺省的类型是host。

第二种是确定传输方向的关键字，主要包括src，dst，dst or src，dst and src， 这些关键字指明了传输的方向。举例说明，src 210.27.48.2 ，指明ip包中源地址是 210.27.48.2

， dst net 202.0.0.0 指明目的网络地址是202.0.0.0。如果没有指明 方向关键字，则缺省是src or dst关键字。

第三种是协议的关键字，主要包括ether，fddi,tr，wlan，ip，ip6, arp, rarp, decnet, tcp and udp等类型。Fddi指明是在FDDI (分布式光纤数据接口网络)上的特定的网络协议，实际上它是”ether”的别名，fddi和ether 具有类似的源地址和目的地址，所以可以将fddi协议包当作ether的包进行处理和分析。 其他的几个关键字就是指明了监听的包的协议内容。如果没有指定任何协议，则tcpdump 将会监听所有协议的信息包。

除了这三种类型的关键字之外，其他重要的关键字如下：gateway， broadcast，less， greater， 还有三种逻辑运算，取非运算是 `!' or `not'， 与运算是`&&' or `and';或运算是`||' or `or' 。

举例说明：

想要截获所有210.27.48.1 的主机收到的和发出的所有的数据包：

#tcpdump host 210.27.48.1 -i ens32

想要截获主机210.27.48.1 和主机210.27.48.2 或210.27.48.3的通信，使用命令：（在命令行中使用括号时，一定要加斜杠）

#tcpdump host 210.27.48.1 and \(210.27.48.2 or 210.27.48.3 \)

如果想要获取主机210.27.48.1除了和主机210.27.48.2之外所有主机通信的ip包，使用命令：

#tcpdump ip host 210.27.48.1 and ! 210.27.48.2

如果想要获取主机210.27.48.1接收或发出的telnet包，使用如下命令：

#tcpdump tcp port 23 host 210.27.48.1

对本机的udp 123 端口进行监视 123 为ntp的服务端口

tcpdump udp port 123

系统将只对名为hostname的主机的通信数据包进行监视。主机名可以是本地主机，也可以是网络上的任何一台计算机。下面的命令可以读取主机hostname发送的所有数据：

#tcpdump -i eth0 src host hostname

下面的命令可以监视所有送到主机hostname的数据包：

#tcpdump -i eth0 dst host hostname

还可以监视通过指定网关的数据包：

#tcpdump -i eth0 gateway Gatewayname

如果想监视编址到指定端口的TCP或UDP数据包，那么执行以下命令：

#tcpdump -i eth0 host hostname and port 80

如果想要获取主机210.27.48.1除了和主机210.27.48.2之外所有主机通信的ip包,使用命令：

#tcpdump ip host 210.27.48.1 and ! 210.27.48.2

将结果保存为wireshark识别的文件

#tcpdump -i ens33 -nn port 22 and src host 192.168.5.189 -w test.pacpng

过滤源主机192.168.0.1和目的端口不是telnet的报头，并导入到tes.t.txt文件中：

#tcpdump src host 192.168.0.1 and dst port not telnet -l > test.txt

课后习题：

1、给自己的虚拟机安装tcpdump抓包工具

2、打开一个终端，ping www.baidu.com

3、打开另外一个终端，ping 8.8.8.8

4、通过ssh登录到自己的虚拟机

5、使用虚拟机的浏览器访问www.sina.com.cn网站

6、使用tcpdump 抓取和8.8.8.8通信的icmp报文，并保存到文件

7、使用tcpdump抓取网络中的SSH报文，并保存文件

8、使用tcpdump抓取网络中的访问www.sina.com.cn的http流量

9、使用tcmdump抓取网络中自己主机和www.baidu.com的ping包