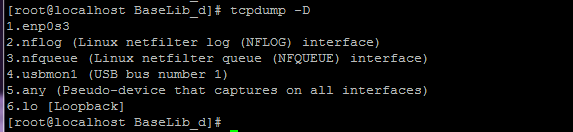
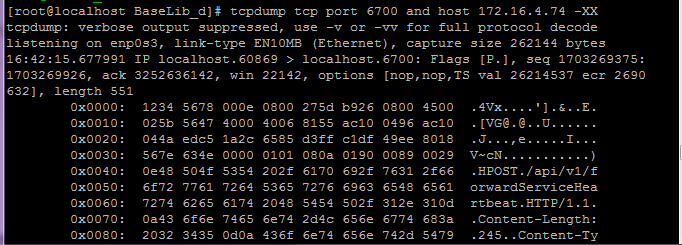
**TCPDUMP使用实例**

1. **以信鸽音频转码服务为例。**

1.1 Tcpdump -D 列出可用于抓包的接口。将会列出接口的数值编号和接口名，它们都可以用于"-i"后。



1.2 抓取指定ip的指定端口传输的包。 -XX (以16进制和ASCII两种方式同时输出。)

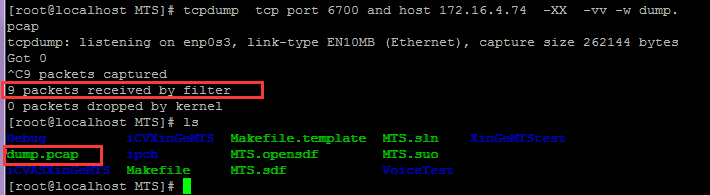


1.3 抓取指定条件包，并保存文件。使用wireshark查看。

-XX

-vv 显示详细信息。这里得到了“Got 0” 信息。显示抓到多少包。

-w 指定保存路径和文件名。由于我这里没写路径，就在当前路径下保存。



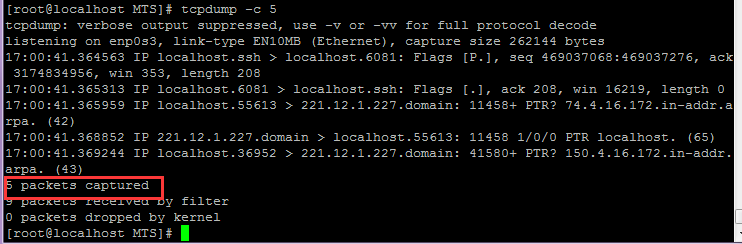
接下来。Dump.pcap文件即可以使用wireshark软件查看。

1. **Tcpdump 用法整理。（只整理常用参数）**

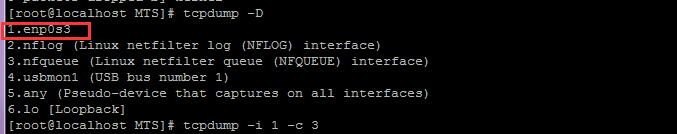
2.1 选项

2.1.1抓包选项

-c : 指定抓取包数量

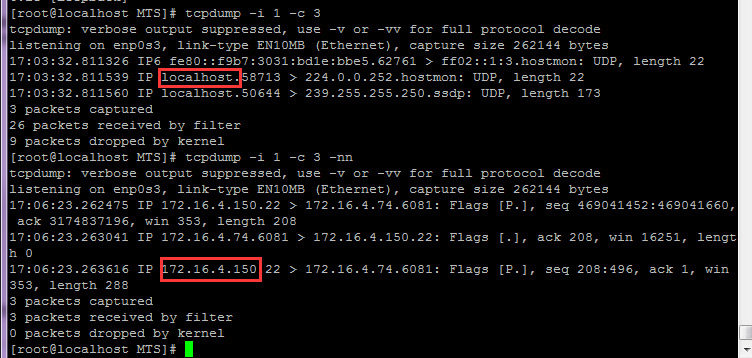


-i interface: 指定tcpdump需要监听的接口。（可以配合-D获取）。若未指定，系统默认搜寻编号最小的。



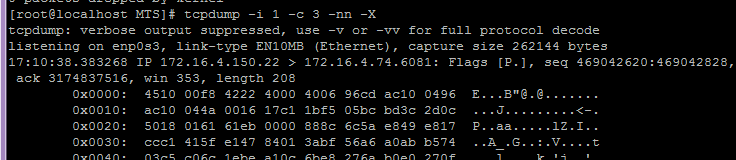
也即默认抓取enp0s3网卡的包。

-nn 对地址以数字方式显示，否则显示主机名。并把端口也显示为数字。



2.1.2 输出选项

-X 输出包的头部信息。(会以16进制和ASCII两种方式输出)



-XX 输出包的头部数据，比-X详细。

-v 当分析和打印的时候，产生详细输出。

-vv 比-v详细。

-vvv 比-vv详细。

2.1.3 其他功能性选项

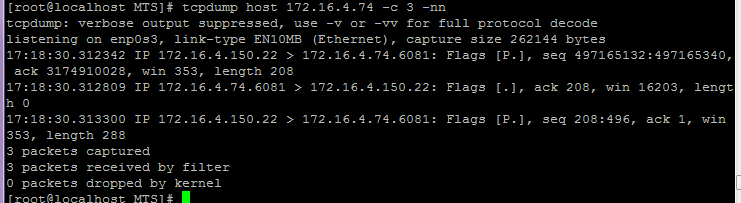
-D ： 列出可用于抓包的接口。 接口数字可用于 “-i”参数后。

-w : 将抓包数据输出到文件中，而不输出在标准输出里面。

2.2 常用过滤表达式示例

2.2.1 监视指定主机的数据包。

Tcpdump host 172.16.4.74



2.2.2 截获主机发出的所有数据。

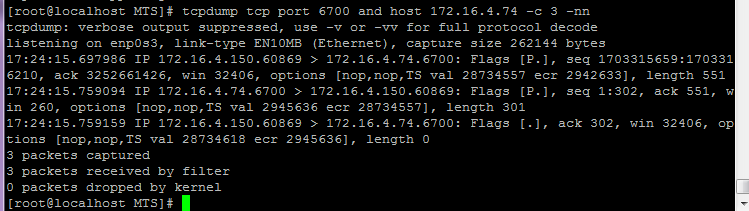
Tcpdump src host 172.16.4.74

2.2.3 截获所有发送到主机的数据包

Tcpdump dst host 172.16.4.150

2.2.4 监视指定主机和端口的数据包。

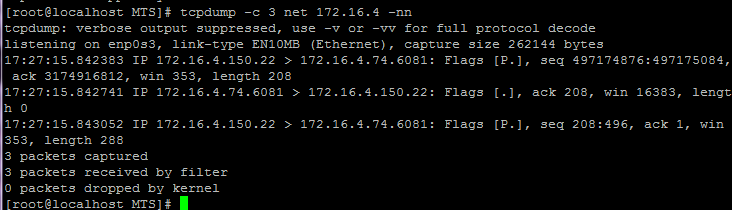
Tcpdump tcp port 6700 and host 172.16.4.74



2.2.5 将tcp改为udp。则开始抓udp包。

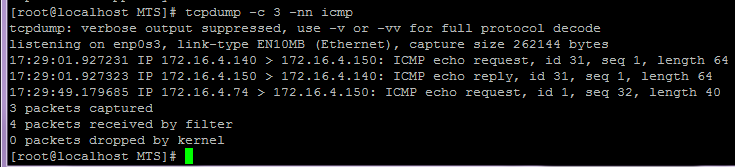
2.2.6 监视指定网络的数据包。(本网段是172.16.4)

Tcpdump -c3 net 172.16.4



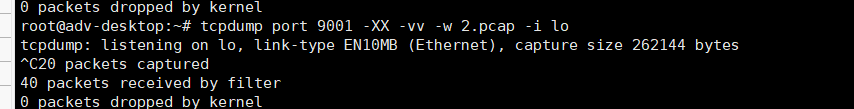
2.2.7 抓取ping包

Tcpdump -c 3 -nn icmp



2.2.8 抓取本机9001端口发往本机的包

-i lo



常用抓包参数

sudo tcpdump host 10.211.92.141 -XX -vv -w sccomm.pcap