print\_http\_info.c

用于输出监听到的tcp连接中的http相关信息

net2pcapfile.c

一个简易的抓包程序，将抓到的包存储为pcap格式的文件

pcap文件主要包括文件头和文件数据，文件数据为一个个数据包组成

数据包分为数据包头和数据

该程序中文件头部分写死，使用Writepcapheader()函数

文件数据从网卡获取，从nids\_last\_pcap\_header获取数据包头，nids\_last\_pcap\_data为数据包的数据

MAX设置缓存区大小，MAX\_TIME设置抓包个数(小于等于0时程序永久运行)

//fd为文件标识符

//filepath为写入数据的目标文件路径

//buf\_len为pcap数据缓存区的数据长度

//使用oragin标识存储pcap数据的缓存区的起点，buf为存储数据时的中间变量

liketcpdump.c

hexdump形式输出网卡经过的tcp/udp连接

nids\_params.device存储网卡名称

有两种运行方式

直接运行时，输出经过该网卡的tcp/udp连接的客户端与服务器端的ip和端口

带参数x时，输出经过该网卡的tcp/udp连接的客户端与服务器端的ip和端口，然后输出该链接中的数据(hexdump形式)