**流量分析**

网络流量分析是指捕捉网络中流动的数据包，并通过查看包内部数据以及进行相关的协议、流量分析、统计等来发现网络运行过程中出现的问题。

**wireshark的基本使用方法**

**1. 数据包的统计**

1.1 协议分级统计：

1.2 端点的统计

1.3 ip的统计

1.4 http请求统计

**2. 数据包的过滤**

2.1 筛选协议

2.2 IP过滤

2.3 其他常见过滤

**3. 数据包的搜索**

**4. 数据包的还原**

**5. 数据的提取**

打开wireshark后，按ctrl+K，勾选需要抓包的网卡，点击Start开始抓包。

## **wireshark过滤器表达式**

### 协议过滤

TCP：只显示TCP协议的数据流

HTTP：只显示HTTP协议的数据流

ICMP：只显示ICMP协议的数据流

ARP：只显示ARP协议的数据流

DNS：显示DNS协议的数据流

### IP过滤

ip.addr = 192.168.116.138，只显示ip为192.168.116.138有关的数据流

ip.src = 192.168.116.138，只显示源IP地址为192.168.116.138的数据流

ip.dst = 192.168.116.138，只显示目标IP地址为192.168.116.138的数据流

### 端口过滤

tcp.port == 80，只显示80端口TCP数据流

udp.prot == 67，只显示67端口UDP数据流

tcp.srcport == 80, 只显示源地址的80端口数据流

tcp.dstport == 80，只显示目的地址80端口数据流

### 过滤HTTP协议

http.request.method=="GET" ，显示get请求

http.request.method=="POST" ，显示POST请求

http.request.url contains admin ，显示url中包含admin的 请求

http.request.code==404，显示状态码为404

### 连接符

and，or

如tcp.port == 80 and ip.addr = 192.168.116.138

## **wireshark着色规则**

Wireshark默认有一组着色规则，可以在Packet Details面板中展开包的帧部分，查看着色规则。

在View | Coloring Rules中，打开着色规则窗口，可以自己创建、删除、选中、去除。

## **数据流的追踪**

我们的一个完整的数据流一般都是由很多个包组成的，

所以当我们想查看某条数据包对于的数据流的话。可以选中数据，右键选择追踪流。

里面就会有**tcp流、udp流、ssl流、http流**。数据包属于哪种流就选择对应的流。

当我们选择了追踪流时，会弹出该流的完整的数据流还有这个数据流中包含的数据包，对话框下面可以选择数据流方向，顶部的过滤器就是该流的过滤规则。

## **数据包的统计分析**

### **协议分级统计**

协议分级统计功能可以查看所选包协议的分布情况，帮助识别可疑协议，和不正常的网络应用程序。

### **Endpoints**

在Endpoints窗口中，可以通过排序Bytes和Tx Bytes来判断占用带宽最大的主机

### **Conversations**

Conversions窗口可以看到两个主机之间发送/接收数据包的数量、字节大小以及数据的流向情况，也可以通过排序来判断占用最大带宽的主机

在Conversions窗口中只能看到会话的统计情况，无法看到包的具体内容。

这时可以使用快速过滤会话功能，过滤出想要查看的内容。

快速过滤会话的功能在Conversions窗口中进行操作，可以对选中的会话或者非选中的会话选择数据流向进行过滤。

## **数据包的大致结构**

第一行：数据包整体概述，

第二行：链路层详细信息，主要的是双方的mac地址

第三行：网络层详细信息，主要的是双方的IP地址

第四行：传输层的详细信息，主要的是双方的端口号。

第五行：TCP或UDP是传输的DATA，DNS这是域名的相关信息