# 网络流量分析（高级）实验结果提交

**【验证实验1】**

当Peter的气象数据接收器回复正常工作之后，我们又对气象数据接收器与服务器之间的通信进行了一次数据包捕获工作，捕获到的数据包保存在weather\_working.pcapng文件中，请分析该数据包，并将气象数据接收器与服务器通信时的用户ID和用户口令提取出来并截图证明之。

答：

ID=KGAOAKWO2

PASSWORD=12345678

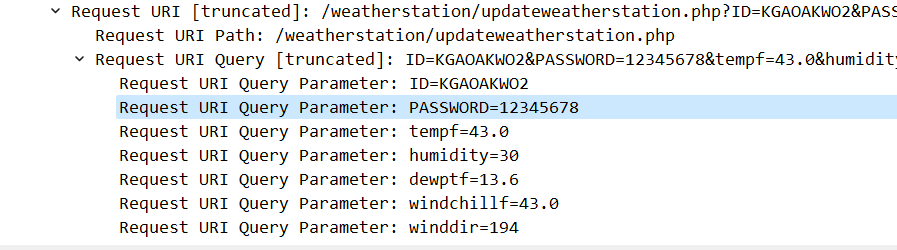


图1 - 1 用户ID和用户口令

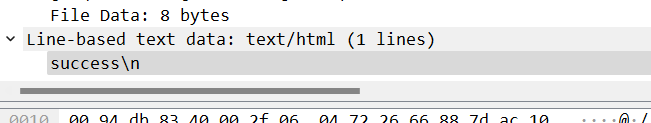


图1-2 服务器同意链接

**【验证实验-2】**

启动Wiresshark工具，对你访问某一个网站的数据交互进行捕获。对捕获的网络数据包进行分析，并回答下列问题：

1）你的计算机配置的默认网关是什么？请截图证明之；

2）你的计算机配置的DNS服务器是什么？请截图证明之；

3）你访问的网站的IP地址是什么？请截图证明之。

答：1、计算机配置的默认网关为192.168.43.1

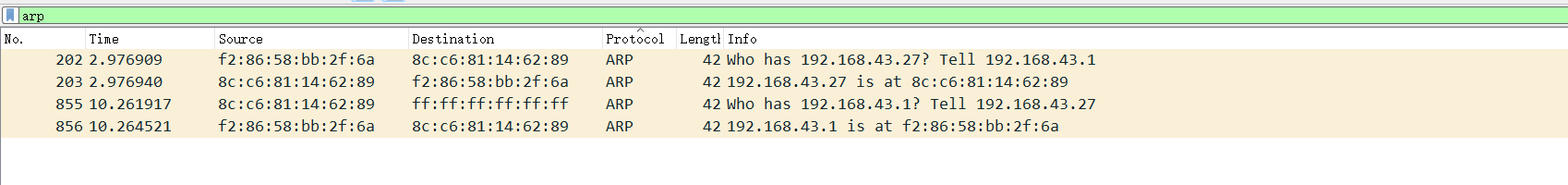


图2-1 查询默认网关

1. 计算机配置的DNS服务器为 192.168.43.1

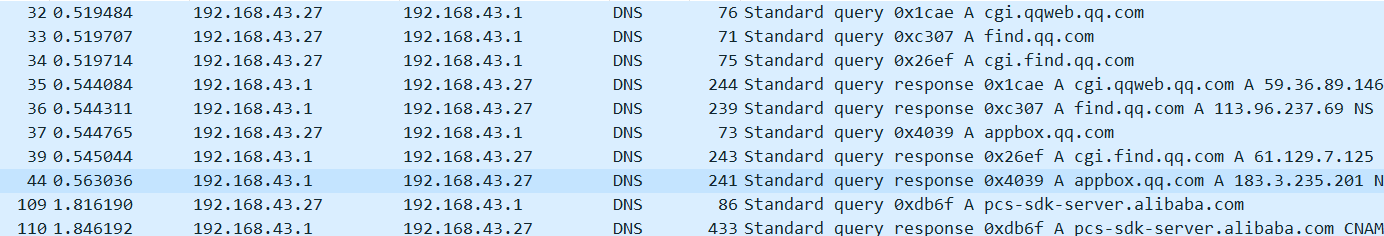


图2-2 查询默认DNS服务器

3、www.hust.edu.cn的ip地址是202.114.0.245

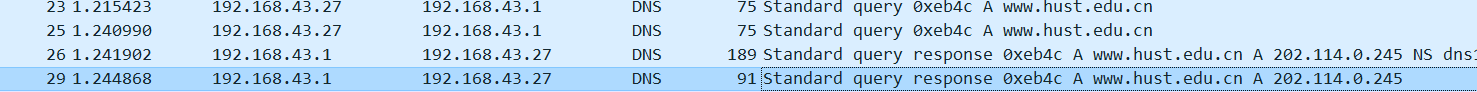


图2-3 查询访问网站的ip地址

**【验证实验-3】**

1. 安装Serv-U，这是一个FTP服务器软件。安装过程中注意配置相应的目录、用户名、口令等信息，其他参数可采用默认参数，不必修改，安装完成之后启动FTP服务器。
2. 两位同学为一组，A同学使用浏览器作为FTP客户端（地址栏中输入：ftp://B同学的地址）访问B同学的FTP服务器并上传一个文件。此时，B同学开启Wireshark捕获网络数据包，从数据包中提取A同学上传的文件，查看并显示该文件。截图说明从捕获数据包中提取图片文件的过程。A、B同学角色互换，重复上述操作。

答：1、



图3-1 启动FTP服务器

2、

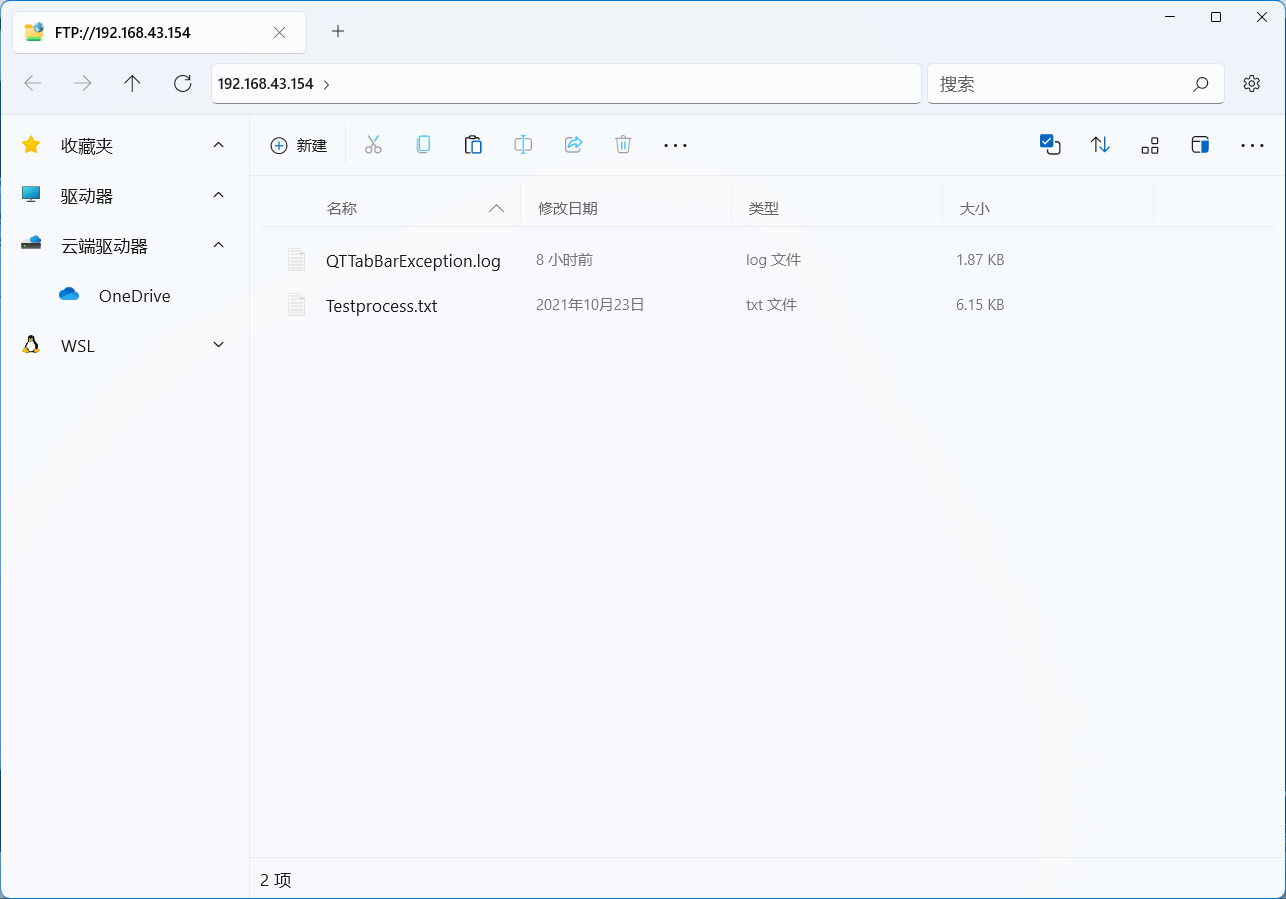


图3-2 启动FTP客户端

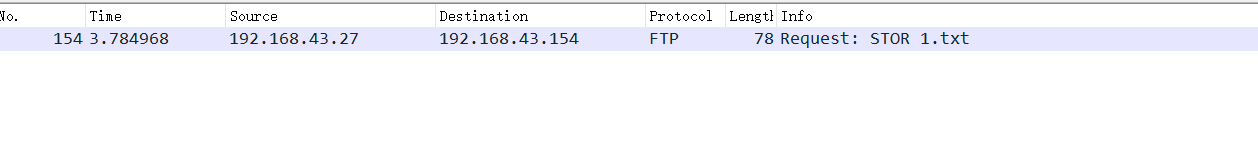


图3-3 找到有STOR命令的FTP协议，发现其传输文件名为txt



图3-4 找到用于传输数据的包

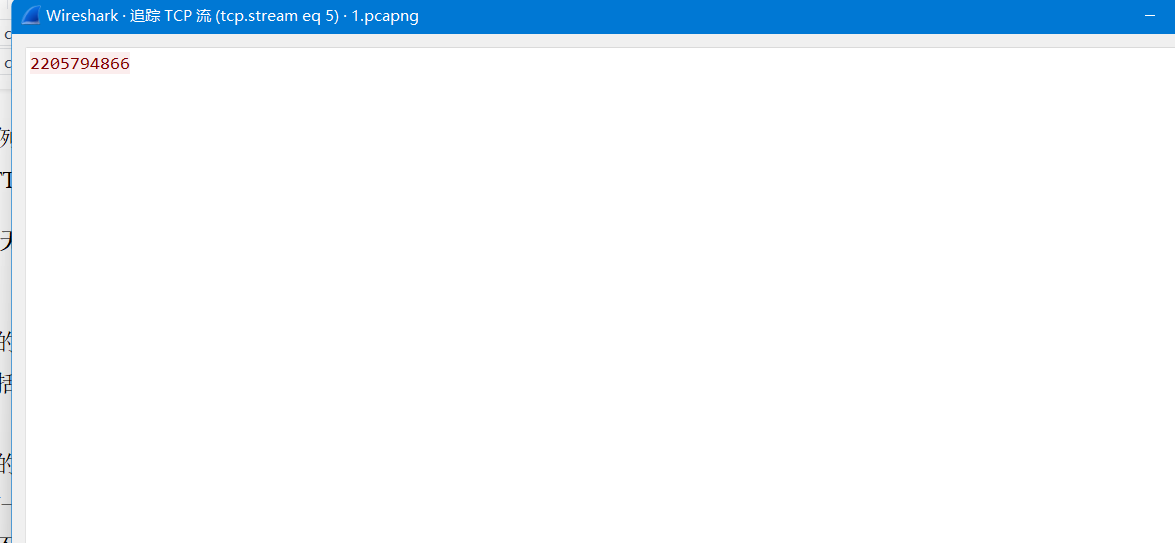


图3-5 获取数据

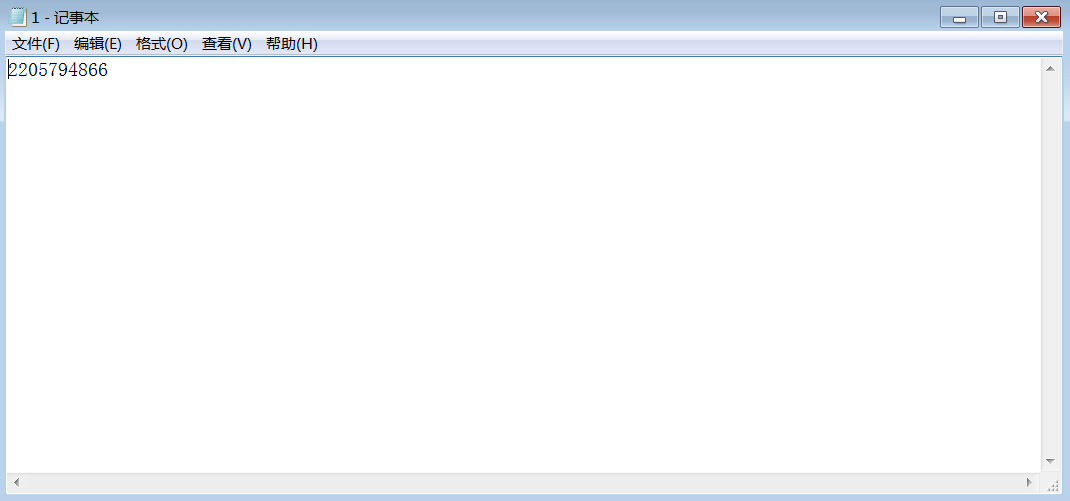


图3-6 实际传输文件

**【验证实验-4】**

使用Wireshark打开捕获文件***arppoison.pcap***，对数据包进行分析，回答下列问题：

1）从捕获的数据包分析，被攻击的主机MAC地址是什么？

2）攻击发生在什么时候呢？那几个数据包是攻击的关键数据包？请说明攻击关键数据包的序号。

3）正常情况下，被攻击主机的默认网关的MAC地址是什么？请截图证明之。

4）被攻击之后，被攻击主机认为它的默认网关的MAC地址是什么呢？请截图证明之。

5）这样的攻击，将导致什么样的后果？

答：

1. 被攻击机的MAC地址是00:21:70:c0:56:f0



图5-1 被攻击机的MAC地址

1. 攻击发生在4.64s左右

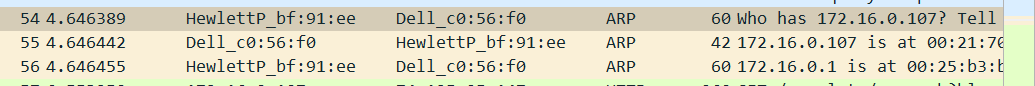


图5-2 arp欺骗过程

Arp包本应广播在局域网内，但Hewlettp\_bf:91:ee(00:25:b3:bf:91:ee)却将该包直接发现目标靶机，造成了该靶机的arp缓存中172.16.0.1网关的物理地址更换为攻击机的物理地址。

攻击关键数据包围54,56数据包。

在攻击前后过程中，网关的物理地址发生了改变，由此可确认发生了arp欺骗攻击。

3、



图5-3 正常情况下，默认网关MAC地址

由正常情况下的通信数据包可得知默认网关MAC地址为Cisco\_31:07:33(00:26:0b:31:07:33)。

4、



图5-4 被攻击后，默认网关地址

被攻击后的通信数据包，可知默认网关MAC地址被改为：Hewlettp\_bf:91:ee(00:25:b3:bf:91:ee)

5、该后果将导致被攻击机的上网流量经攻击机转发，造成通讯信息泄露。

**【本次实验的心得、体会、收获或者建议】**

通过本次本次实验，我学习到了许多关于网络通讯的知识，更加熟练地掌握了wireshark的使用。同时能够简单的对数据包进行分析，对于常见的报文进行解析，获取其中的数据信息，同时也学习到了不少关于通信协议的知识。通过最后一个实验，了解到了有关攻击的基本手段-arp攻击，明白了相应的操作原理。