

网络流量分析（高级）实验结果提交

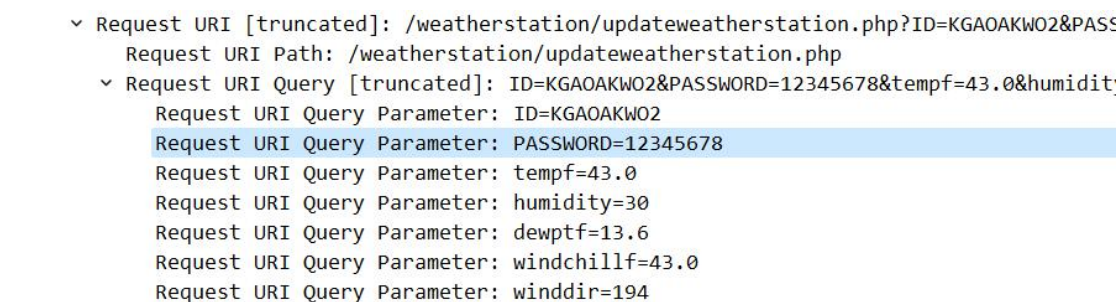
【验证实验 1】

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

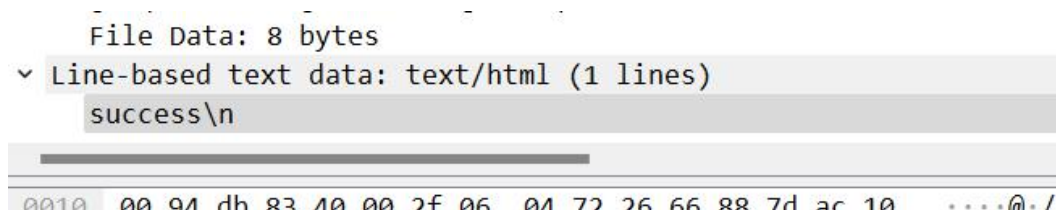


```

  ▾ Request URI [truncated]: /weatherstation/updateweatherstation.php?ID=KGAOAKWO2&PASS
    Request URI Path: /weatherstation/updateweatherstation.php
  ▾ Request URI Query [truncated]: ID=KGAOAKWO2&PASSWORD=12345678&tempf=43.0&humidit
    Request URI Query Parameter: ID=KGAOAKWO2
    Request URI Query Parameter: PASSWORD=12345678
    Request URI Query Parameter: tempf=43.0
    Request URI Query Parameter: humidity=30
    Request URI Query Parameter: dewptf=13.6
    Request URI Query Parameter: windchillf=43.0
    Request URI Query Parameter: winddir=194

```

图 1 - 1 用户 ID 和用户口令



```

  File Data: 8 bytes
  ▾ Line-based text data: text/html (1 lines)
    success\n

```

0010 00 01 dh 83 10 00 2f 06 01 72 26 66 88 7d ac 10 ...

图 1-2 服务器同意链接

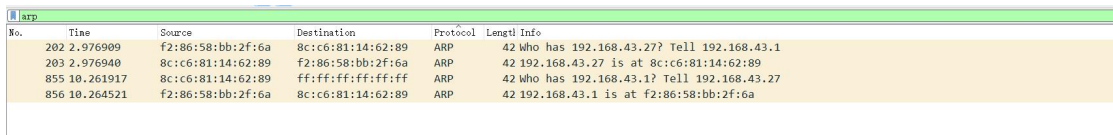
【验证实验-2】

启动 Wireshark 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。

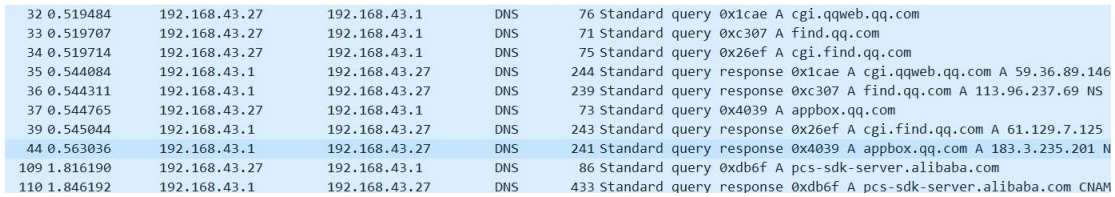
答: 1、计算机配置的默认网关为 192.168.43.1



No.	Time	Source	Destination	Protocol	Length	Info
202	2.976909	f2:86:58:bb:2f:6a	8c:c6:81:14:62:89	ARP	42	Who has 192.168.43.27? Tell 192.168.43.1
203	2.976940	8c:c6:81:14:62:89	f2:86:58:bb:2f:6a	ARP	42	192.168.43.27 is at 8c:c6:81:14:62:89
855	10.261917	8c:c6:81:14:62:89	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.43.1? Tell 192.168.43.27
856	10.264521	f2:86:58:bb:2f:6a	8c:c6:81:14:62:89	ARP	42	192.168.43.1 is at f2:86:58:bb:2f:6a

图 2-1 查询默认网关

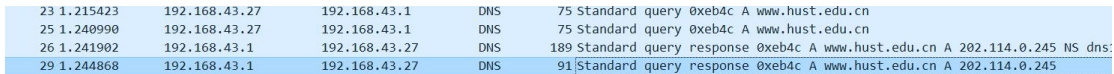
2、计算机配置的 DNS 服务器为 192.168.43.1



32	0.519484	192.168.43.27	192.168.43.1	DNS	76	Standard query 0x1cae A cgi.qqweb.qq.com
33	0.519707	192.168.43.27	192.168.43.1	DNS	71	Standard query 0xc307 A find.qq.com
34	0.519714	192.168.43.27	192.168.43.1	DNS	75	Standard query 0x26ef A cgi.find.qq.com
35	0.544084	192.168.43.1	192.168.43.27	DNS	244	Standard query response 0x1cae A cgi.qqweb.qq.com A 59.36.89.146
36	0.544311	192.168.43.1	192.168.43.27	DNS	239	Standard query response 0xc307 A find.qq.com A 113.96.237.69 NS
37	0.544765	192.168.43.27	192.168.43.1	DNS	73	Standard query 0x4039 A appbox.qq.com
39	0.545044	192.168.43.1	192.168.43.27	DNS	243	Standard query response 0x26ef A cgi.find.qq.com A 61.129.7.125
44	0.563036	192.168.43.1	192.168.43.27	DNS	241	Standard query response 0x4039 A appbox.qq.com A 183.3.235.201 N
109	1.816190	192.168.43.27	192.168.43.1	DNS	86	Standard query 0xdb6f A pcs-sdk-server.alibaba.com
110	1.846192	192.168.43.1	192.168.43.27	DNS	433	Standard query response 0xdb6f A pcs-sdk-server.alibaba.com CNAM

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



23	1.215423	192.168.43.27	192.168.43.1	DNS	75	Standard query 0xeb4c A www.hust.edu.cn
25	1.240990	192.168.43.27	192.168.43.1	DNS	75	Standard query 0xeb4c A www.hust.edu.cn
26	1.241902	192.168.43.1	192.168.43.27	DNS	189	Standard query response 0xeb4c A www.hust.edu.cn A 202.114.0.245 NS dns:
29	1.244868	192.168.43.1	192.168.43.27	DNS	91	Standard query response 0xeb4c A www.hust.edu.cn A 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、

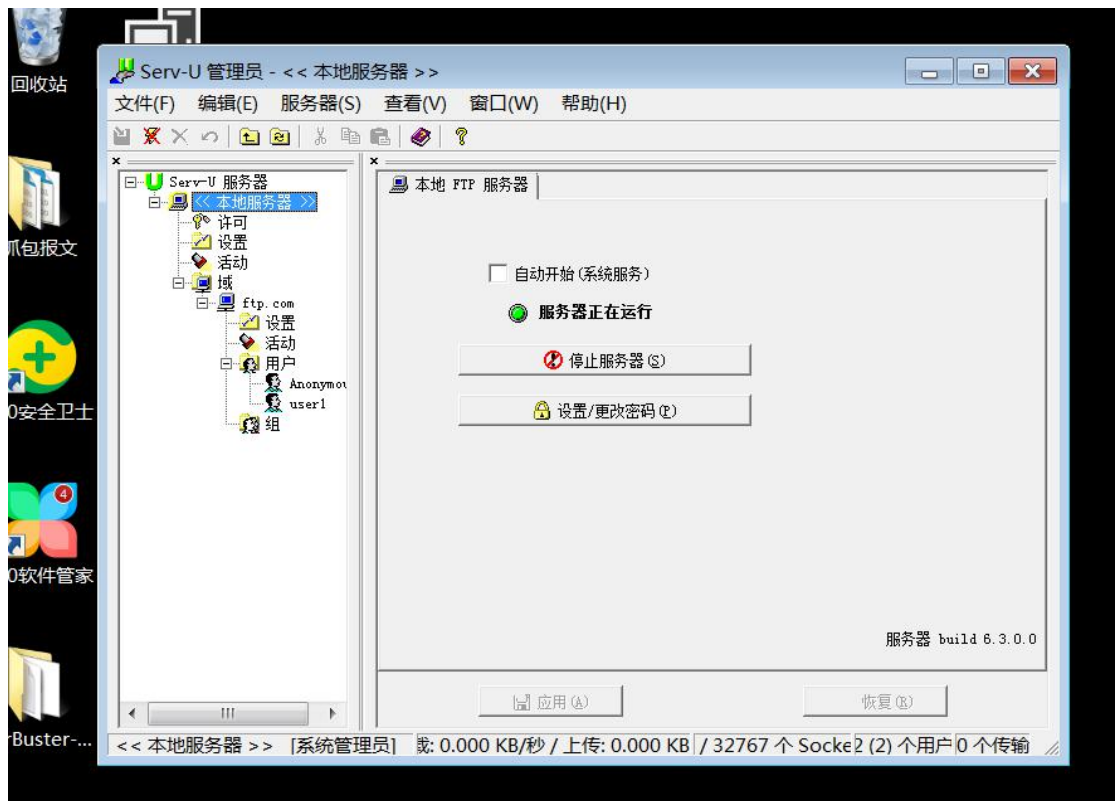


图 3-1 启动 FTP 服务器

2、

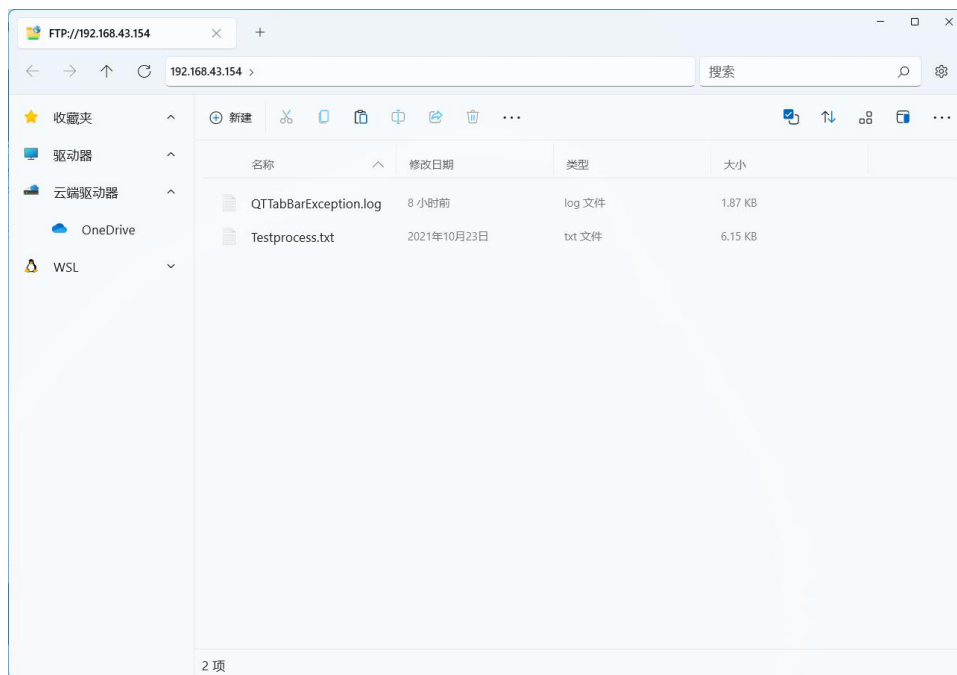


图 3-2 启动 FTP 客户端

No.	Time	Source	Destination	Protocol	Length	Info
154	3.784968	192.168.43.27	192.168.43.154	FTP	78	Request: STOR 1.txt

图 3-3 找到有 STOR 命令的 FTP 协议，发现其传输文件名为 txt

160	3.786752	192.168.43.27	192.168.43.154	FTP-DA...	76	FTP Data: 10 bytes (PASV) (STOR 1.txt)
161	3.786755	192.168.43.27	192.168.43.154	TCP	76	[TCP Retransmission] 5874 → 50143 [PSH, ACK] Seq=

图 3-4 找到用于传输数据的包

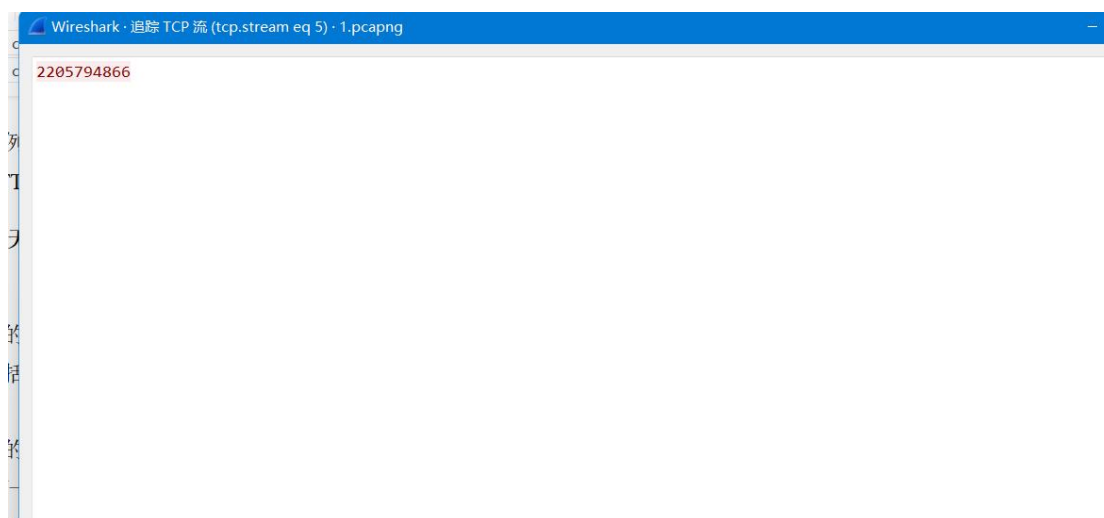


图 3-5 获取数据



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

```
d (480 bits) on interface unknown, id 0
, Dst: Dell_c0:56:f0 (00:21:70:c0:56:f0)
```

图 5-1 被攻击机的 MAC 地址

2、攻击发生在 4.64s 左右

54 4.646389	HewlettP_bf:91:ee	Dell_c0:56:f0	ARP	60 who has 172.16.0.107? Tell
55 4.646442	Dell_c0:56:f0	HewlettP_bf:91:ee	ARP	42 172.16.0.107 is at 00:21:70
56 4.646455	HewlettP_bf:91:ee	Dell_c0:56:f0	ARP	60 172.16.0.1 is at 00:25:b3:b

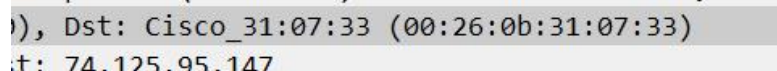
图 5-2 arp 欺骗过程

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、

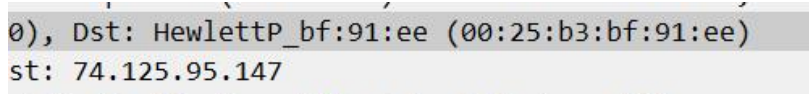


```
), Dst: Cisco_31:07:33 (00:26:0b:31:07:33)  
t: 74.125.95.147
```

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、



```
0), Dst: HewlettP_bf:91:ee (00:25:b3:bf:91:ee)  
st: 74.125.95.147
```

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。