

# 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。

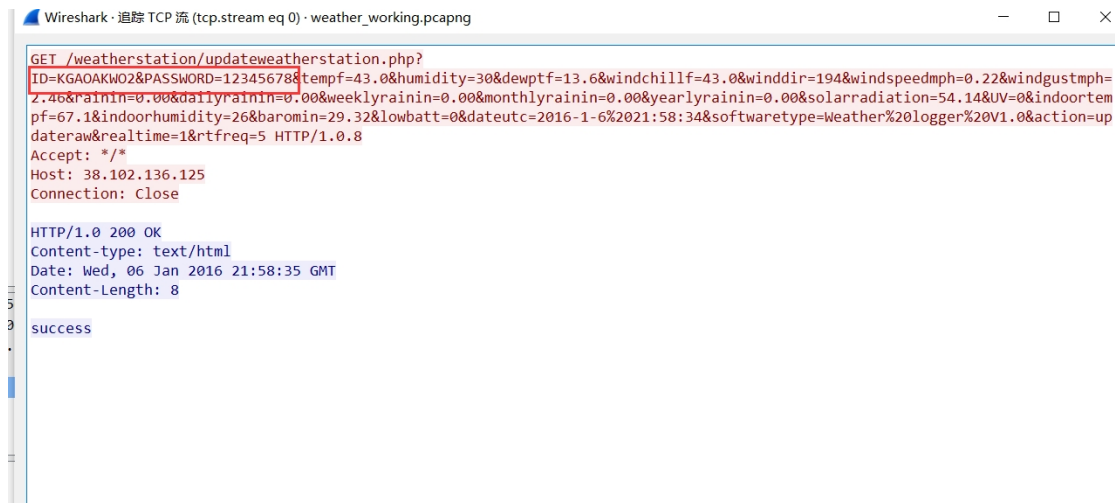


图 1-对 HTTP 进行追踪流

通过追踪流可以发现用户 ID 和密码为 **ID=KGAOAKWO2&PASSWORD=12345678**



图 2-返回登陆成功的消息

## 【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)

9 0.307000	LAPTOP-JED5PFSL.loc...	Broadcast	ARP	42 Who has 10.22.63.254? Tell 10.22.34.84
11 0.317621	RuijieNe_7d:4c:bd	LAPTOP-JED5PFSL.loc...	ARP	60 10.22.63.254 is at 14:14:4b:7d:4c:bd
12 0.364067	LAPTOP-JED5PFSL.loc...	Broadcast	ARP	42 Who has 10.22.63.254? Tell 10.22.34.84
13 0.375084	RuijieNe_7d:4c:bd	LAPTOP-JED5PFSL.loc...	ARP	60 10.22.63.254 is at 14:14:4b:7d:4c:bd

图 2-1 查询默认网关

默认网关为 10.22.63.254，证明如下：

1082 6.518653	LAPTOP-JED5PFSL.loc...	dns.hust.edu.cn	DNS	75 Standard query 0x15c7 A www.hust.edu.cn
---------------	------------------------	-----------------	-----	--

图 2-2 DNS 包

通过解析网络地址，发现此 dns 包是在向 dns 服务器查询 ip 地址，由于这个 dns 数据包会以默认网关的地址进行封装并发送到默认网关进行路由转发，故查看此 DNS 包的内容。

941 5.774390	dns.hust.edu.cn	LAPTOP-JED5PFSL.loc...	DNS	283 Standard query response 0x0000 A connectiv...
1082 6.518653	LAPTOP-JED5PFSL.loc...	dns.hust.edu.cn	DNS	75 Standard query 0x15c7 A www.hust.edu.cn
1084 6.518926	LAPTOP-JED5PFSL.loc...	dns.hust.edu.cn	DNS	75 Standard query 0x4292 AAAA www.hust.edu.cn
1085 6.519053	LAPTOP-JED5PFSL.loc...	dns.hust.edu.cn	DNS	76 Standard query 0xfc9f A news.hust.edu.cn

Wireshark - 分组 1082 - hust.edu.cn_final.pcapng	
>	Frame 1082: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{76CFCE10-9D1A-4013-9F...
>	Ethernet II, Src: LAPTOP-JED5PFSL.local (98:af:65:c9:4c:99), Dst: RuijieNe_7d:4c:bd (14:14:4b:7d:4c:bd)
>	Destination: RuijieNe_7d:4c:bd (14:14:4b:7d:4c:bd)
>	Source: LAPTOP-JED5PFSL.local (98:af:65:c9:4c:99)
>	Type: IPv4 (0x0800)
>	Internet Protocol Version 4, Src: LAPTOP-JED5PFSL.local (10.22.34.84), Dst: dns.hust.edu.cn (202.114.0.131)
>	0100 .... = Version: 4
>	.... 0101 = Header Length: 20 bytes (5)
>	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
>	Total length: 61

图 2-3 DNS 包中的目标 mac 地址

由红框可知，默认网关的 mac 地址为 (14:14:4b:7d:4c:bd)，与最初捕捉到的 arp 数据包 mac 地址相符，故默认网关为 10.22.63.154。

2)

553	LAPTOP-JED5PFSL.loc...	dns.hust.edu.cn	DNS
926	LAPTOP-JED5PFSL.loc...	dns.hust.edu.cn	DNS
953	LAPTOP-JED5PFSL.loc...	dns.hust.edu.cn	DNS
967	LAPTOP-JED5PFSL.loc...	dns.hust.edu.cn	DNS

图 2-4 DNS 服务器（解析地址版）

3653	10.22.34.84	202.114.0.131	DNS
3926	10.22.34.84	202.114.0.131	DNS
9053	10.22.34.84	202.114.0.131	DNS
9267	10.22.34.84	202.114.0.131	DNS
5838	202.114.0.131	10.22.34.84	DNS

图 2-5 DNS 服务器

DNS 服务器：202.114.0.131

3)

A news.hust.edu.cn CNAME zhanqun9.hust.edu.cn A 210.
AAAA www.hust.edu.cn AAAA 2001:250:4000:2000::245

图 2-6 DNS 服务器返回的 ip 地址

从 DNS 服务器中查询到 hust.edu.cn 的 ipv6 地址为 2001:250:4000:2000::245

### 【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：

80 3.267773	192.168.49.1	192.168.49.129	FTP	69 Request: STOR test.txt
82 3.269820	192.168.49.1	192.168.49.129	TCP	60 62783 → 21 [ACK] Seq=89 Ack=418 Win=1020 Len=0
83 3.270070	192.168.49.1	192.168.49.129	FTP-DA...	83 FTP Data: 29 bytes (PASV) (STOR test.txt)

图 3-1 找到有 STOR 命令的 FTP 协议，发现文件格式为 txt

83	3.270070	192.168.49.1	192.168.49.129	FTP-DA...	83 FTP Data: 29 bytes (PASV) (STOR test.txt)
----	----------	--------------	----------------	-----------	--

图 3-2 在第 83 个包中发现用于传输数据的数据包

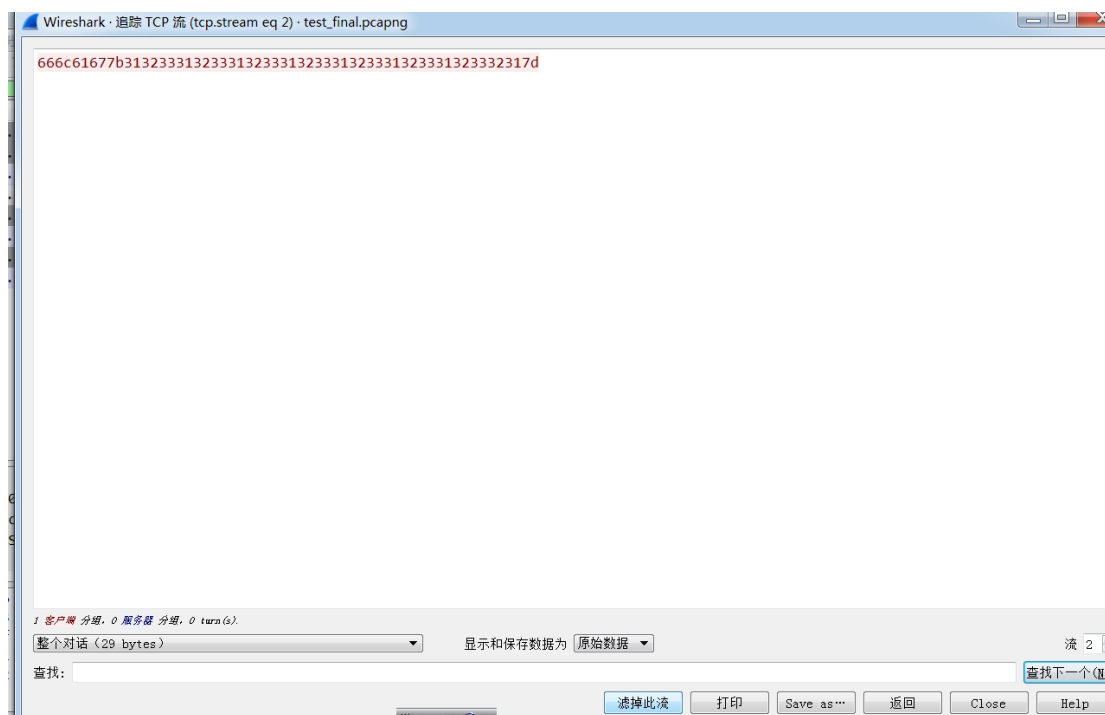


图 3-3 提取原始数据

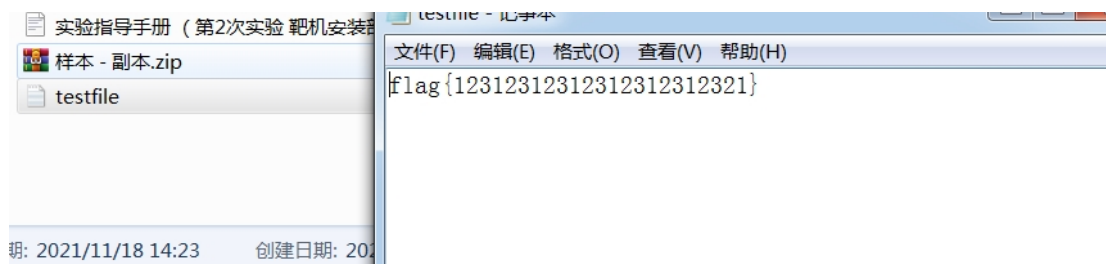


图 3-4 保存数据并将格式改为 txt 文件

### 【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)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.0.107	12.153.20.41	DNS	74	Standard query 0x18cd A www.google.com
2	0.001829	12.153.20.41	172.16.0.107	DNS	326	Standard query response 0x18cd A www.google.com CNAME www.l.google.com
3	0.010656	172.16.0.107	74.125.95.147	TCP	74	45691 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=0

> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface unknown, id 0

▼ Ethernet II, Src: Dell\_c0:56:f0 (00:21:70:c0:56:f0), Dst: Cisco\_31:07:33 (00:26:0b:31:07:33)

> Destination: Cisco\_31:07:33 (00:26:0b:31:07:33)

> Source: Dell\_c0:56:f0 (00:21:70:c0:56:f0)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 172.16.0.107, Dst: 12.153.20.41

> User Datagram Protocol, Src Port: 57692, Dst Port: 53

> Domain Name System (query)

图 4-1 被攻击主机的 mac 地址

通过查看包中数据可得知 mac 地址为 (00:21:70:c0:56:f0)

2)

54	4.646389	HewlettP_bf:91:ee	Dell_c0:56:f0	ARP	60	Who has 172.16.0.107? Tell 172.16.0.1
55	4.646442	Dell_c0:56:f0	HewlettP_bf:91:ee	ARP	42	172.16.0.107 is at 00:21:70:c0:56:f0
56	4.646455	HewlettP_bf:91:ee	Dell_c0:56:f0	ARP	60	172.16.0.1 is at 00:25:b3:bf:91:ee
57	6.553250	172.16.0.107	74.125.95.147	HTTP	960	GET /complete/search?hl=en&client=hn&xnTds=17259.18168.24483.25233

图 4-2 攻击的数据包

攻击的数据包为 54 和 56, 分析如下:

54	4.646389	HewlettP_bf:91:ee	Dell_c0:56:f0	ARP	60	Who has 172.16.0.107? Tell 172.16.0.1
55	4.646442	Dell_c0:56:f0	HewlettP_bf:91:ee	ARP	42	172.16.0.107 is at 00:21:70:c0:56:f0

Wireshark · 分组 54 · arppoison.pcapng

> Frame 54: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface unknown, id 0

▼ Ethernet II, Src: HewlettP\_bf:91:ee (00:25:b3:bf:91:ee), Dst: Dell\_c0:56:f0 (00:21:70:c0:56:f0)

> Destination: Dell\_c0:56:f0 (00:21:70:c0:56:f0)

> Source: HewlettP\_bf:91:ee (00:25:b3:bf:91:ee)

Type: ARP (0x0806)

图 4-3 异常的目标地址

数据包 54 由 HewlettP 发送的 ARP 请求, 本应该广播给内网中的所有主机, 但只是单独发给受害者。同时, 虽然 ARP 数据包中有攻击者的 MAC 地址, 但是其列出来的却是路由器的 IP 地址。故 HewlettP 为攻击者。

3)

正常情况下, 默认网关的 MAC 地址为 (00:26:0b:31:07:33), 因为该地址对应的硬件为 Cisco, 一般为路由器。

1 0.000000	172.16.0.107	12.153.20.41	DNS	74 Standard query 0x18cd A www.goo
2 0.001829	12.153.20.41	172.16.0.107	DNS	326 Standard query response 0x18cd
3 0.010656	172.16.0.107	74.125.95.147	TCP	74 45691 → 80 [SYN] Seq=0 Win=5840

Wireshark · 分组 1 · arppoison.pcapng

> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface unknown, id 0

> Ethernet II, Src: Dell\_c0:56:f0 (00:21:70:c0:56:f0), Dst: Cisco\_31:07:33 (00:26:0b:31:07:33)

> Internet Protocol Version 4, Src: 172.16.0.107, Dst: 12.153.20.41

> User Datagram Protocol, Src Port: 57692, Dst Port: 53

> Domain Name System (query)

Transaction ID: 0x18cd

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

图 4-4 默认网关的 MAC 地址

4)

观察被攻击后的数据包，主机认为其默认网关的地址为攻击者 HewlettP 的 MAC 地址

55 4.646442	Dell_c0:56:f0	HewlettP_bf:91:ee	ARP	42 172.16.0.107 is at 00:21:70:c0:56:f0
56 4.646455	HewlettP_bf:91:ee	Dell_c0:56:f0	ARP	60 172.16.0.1 is at 00:25:b3:bf:91:ee
57 6.553250	172.16.0.107	74.125.95.147	HTTP	960 GET /complete/gsearch?hl=en&client=hp&expIds=17259,18168,
58 6.593436	74.125.95.147	172.16.0.107	TCP	784 80 → 45691 [PSH, ACK] Seq=6471 Ack=2364 Win=10432 Len=718
59 6.593514	172.16.0.107	74.125.95.147	TCP	66 45691 → 80 [ACK] Seq=2364 Ack=7189 Win=25472 Len=0 TSval=

Wireshark · 分组 57 · arppoison.pcapng

> Frame 57: 960 bytes on wire (7680 bits), 960 bytes captured (7680 bits) on interface unknown, id 0

> Ethernet II, Src: Dell\_c0:56:f0 (00:21:70:c0:56:f0), Dst: HewlettP\_bf:91:ee (00:25:b3:bf:91:ee)

> Internet Protocol Version 4, Src: 172.16.0.107, Dst: 74.125.95.147

> Transmission Control Protocol, Src Port: 45691, Dst Port: 80, Seq: 1470, Ack: 6471, Len: 894

> Hypertext Transfer Protocol

图 4-5 默认网关地址被修改

5)

中间人攻击会导致用户和服务器的数据被窃听，导致数据的泄露。

#### 【本次实验的心得、体会、收获或者建议】

通过本次实验，学习到了更多网络通信的相关知识，更加熟练地掌握了 wireshark 的使用。同时简单地试着对数据包进行解析，不仅更加加深对不同数据包结构的理解，同时也了解到了不同协议的功能与运行过程。通过最后一个实验，粗略地了解到中间人攻击的手段，这也引起了我对网络安全的更大兴趣，希望今后更加努力学习。

建议：课前可提早发布预习内容以便同学们了解此次实验所需要接触的协议或网络通讯知识，方便同学们在课上实操时巩固知识点。