

廈門大學



信息学院软件工程系

《计算机网络》实验报告

题 目 实验四 观察 TCP 报文段并侦听分析 FTP 协议

班 级 软件工程 2018 级 2 班

姓 名 林正男

学 号 20420172201787

实验时间 2020 年 3 月 25 日

2020 年 3 月 27 日

1 实验目的

1.用 Wireshark 侦听并观察 TCP 数据段。观察其建立和撤除连接的过程，观察段 ID、窗口机制和拥塞控制机制等。


2. 用 Wireshark 侦听并观察 FTP 数据，分析其用户名密码所在报文的上下文特征，再总结出提取用户名密码的有效方法。

2 实验环境

Windows10 c++ wireshark

3 实验结果

添加 FTP 站点 ? ×

 **站点信息**

FTP 站点名称(I):

内容目录
物理路径(H):

创建自己的 ftp



授权一个名 `user` 的用户，口令为 `123`

但因为都是一台计算机的地址，wireshark 或者编写的 winpcap 程序只能检测到经由网卡的数据传输，无法检测到 localhost 的数据传输。

```
C:\WINDOWS\system32>route add [REDACTED] mask 255.255.255.255 [REDACTED]
操作完成!

C:\WINDOWS\system32>
```

改变 IP 地址，使传输的数据经由网卡，但 ftp 也会因为其改变而无法打开，没用两台电脑，所以暂时使用学院 ftp 做测试，待开学后可用机房电脑测试。

50	3.242c36	121.168.1.4	121.192.180.66	TCP	66 7551 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
52	3.136177	121.192.180.66	121.168.1.4	TCP	66 21 → 7551 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
53	3.336314	121.168.1.4	121.192.180.66	TCP	54 7551 → 21 [ACK] Seq=1 Ack=1 Win=262144 Len=0
54	3.430991	121.192.180.66	121.168.1.4	FTP	103 Response: 220 Serv-U FTP Server v6.2 for WinSock ready...

图示即为与 ftp 建立连接的三次握手过程，第 4 条即为 ftp 消息已建立连接

91.4.578902	192.168.1.4	1.192.180.66	TCP	54.7552 + 21	[FIN, ACK] Seq=49 Ack=168 Win=261888 Len=0
92.4.669576	192.192.180.66	192.168.1.4	TCP	60.21 + 7552	[ACK] Seq=168 Ack=50 Win=66048 Len=0
93.4.670291	192.192.180.66	192.168.1.4	TCP	60.21 + 7552	[FIN, ACK] Seq=168 Ack=50 Win=66048 Len=0
94.4.670342	192.168.1.4	192.192.180.66	TCP	54.7552 + 21	[ACK] Seq=50 Ack=169 Win=261888 Len=0

图示即为四次挥手与 ftp 服务器断开连接

74	3.801602	192.168.1.4	121.192.180.66	TCP	54	7552 → 21 [ACK] Seq=1 Ack=50 Win=261888 Len=0
77	3.892650	192.168.1.4	121.192.180.66	TCP	54	7552 → 21 [ACK] Seq=15 Ack=86 Win=261888 Len=0
80	3.982513	192.168.1.4	121.192.180.66	TCP	54	7552 → 21 [ACK] Seq=30 Ack=116 Win=261888 Len=0
84	4.072568	192.168.1.4	121.192.180.66	TCP	54	7552 → 21 [ACK] Seq=44 Ack=137 Win=261888 Len=0

图示即为滑动窗口实现流量控制

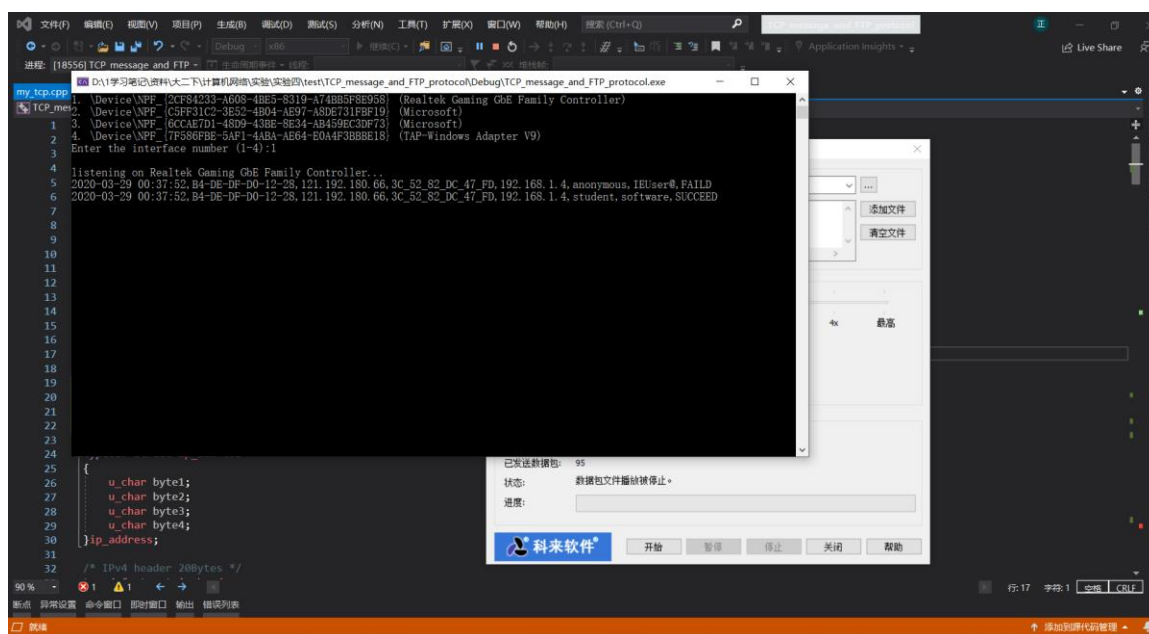
50	3.242636	192.168.1.4	121.192.180.66	TCP	66	7551 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
52	3.336177	121.192.180.66	192.168.1.4	TCP	66	21 → 7551 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1

慢开始与拥塞避免

0010	00 36 1e 90 40 00 06 2c 83 c0 a8 01 04 79 c0	6 y
0020	b4 42 1d 80 00 15 7f 14 59 62 8d ab 07 94 50 18	B Yb p
0030	03 ff 21 53 00 00 55 53 45 52 20 73 74 75 64 65	--IS--US ER Studen
0040	5e 74 0d 0a	nt
0010	00 37 1e 92 40 00 06 2c 80 c0 a8 01 04 79 c0	7 y
0020	b4 42 1d 80 00 15 7f 14 59 70 8d ab 07 b8 50 18	B Yp p
0030	03 ff b8 2c 00 00 50 41 53 53 20 73 6f 66 74 72	---PA SS softw
0040	61 72 65 0d 0a	are
0020	01 04 00 15 1d 80 8d ab 07 b8 7f 14 59 7f 50 18	-----Y P-
0030	01 02 6e dc 00 00 32 33 30 20 55 75 65 72 20 6f	--n--23 0 User: l
0040	8 65 62 65 64 20 69 6e 2c 20 70 72 6f 63 65 65	logged in , proceed
0050	54 2a 0d 0a	le

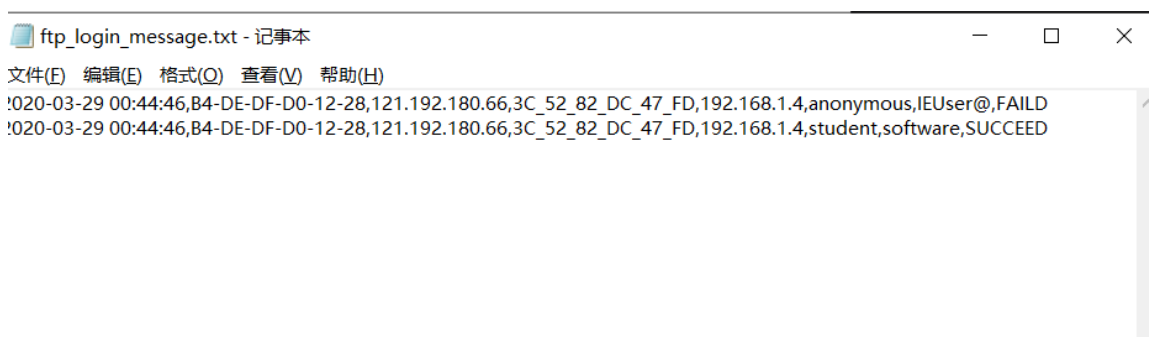
图示即为用户名，口令，即连接成功提示头部分别为 USER，PASS，230

连接失败头部为 530



在终端测试输出

第一次是匿名访问，由于学院 ftp 没有开启所以失败，第二次正确账户，口令成功连接



重定向将 CSV 格式日志输出到文件

4 实验总结

1. 学会了通过过滤器获得 TCP 信号的方法
2. 学习了 TCP 中的三次握手四次挥手的原理
3. 学习了 TCP 的窗口流量控制与拥塞控制方法

