

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 3 用 PCAP 库监听并分析网络流量

班 级 软件工程 2018 级 1 班

姓 名 王奕飞

学 号 24320182203286

实验时间 2020 年 3 月 25 日

2020 年 3 月 25 日

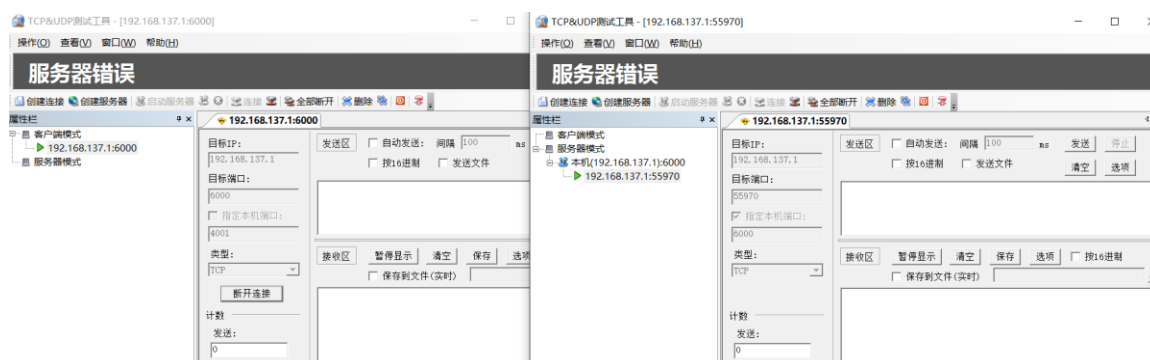
1 实验目的

2 实验环境

Visual studio 2017

3 实验结果

- (1) 观察 TCP 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
- 通过 TCP&UDP 测试工具 在本机上分别建立服务器和客户端，并进行连接



三次握手连接：

5	1.454058	192.168.137.1	192.168.137.1	TCP	56 55970 → 6000 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
6	1.454092	192.168.137.1	192.168.137.1	TCP	56 6000 → 55970 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
7	1.454123	192.168.137.1	192.168.137.1	TCP	44 55970 → 6000 [ACK] Seq=1 Ack=1 Win=2619648 Len=0

第一次握手，客户端发送一个 TCP，标志位为 SYN=1

第二次握手，服务器向客户端返回一个数据包，SYN=1，ACK=1

第三次握手，客户端收到服务器发来的包后检查确认序号。若正确，客户端会再向服务器端发送一个数据包，SYN=0，ACK=1

发送 24320182203286

捕获到这一帧

```

Sequence number: 1 (relative sequence number)
Sequence number (raw): 3552639125
[Next sequence number: 15 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 1509352869
0101 .... = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
Window size value: 10233
[Calculated window size: 2619648]
[Window size scaling factor: 256]
Checksum: 0x8b09 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
> [SEQ/ACK analysis]
> [Timestamps]
TCP payload (14 bytes)
TCP segment data (14 bytes)

```

000	02 00 00 00 45 00 00 36 e1 6c 40 00 80 06 00 00E..6 .l@.....
010	c0 a8 89 01 c0 a8 89 01 17 70 da a2 d3 c0 f8 95p.....
020	59 f6 e5 a5 50 18 27 f9 8b 09 00 00 32 34 33 32	Y...P..'.2432
030	30 31 38 32 32 30 33 32 38 36	01822032 86

捕获到内容，红框内分别为窗口的大小和发送的内容

断开连接

340	559.415811	192.168.137.1	192.168.137.1	TCP	44 55970 → 6000 [FIN, ACK] Seq=1 Ack=15 Win=2619648 Len=0
341	559.415844	192.168.137.1	192.168.137.1	TCP	44 6000 → 55970 [ACK] Seq=15 Ack=2 Win=2619648 Len=0
342	559.416079	192.168.137.1	192.168.137.1	TCP	44 6000 → 55970 [FIN, ACK] Seq=15 Ack=2 Win=2619648 Len=0
343	559.416103	192.168.137.1	192.168.137.1	TCP	44 55970 → 6000 [ACK] Seq=2 Ack=16 Win=2619648 Len=0

四次挥手断开连接

第一次挥手：客户端给服务器发送 TCP 包，用来关闭客户端到服务器的数据传送。将标志位 FIN 和 ACK 置为 1

第二次挥手：服务器收到这个 FIN，发回一个 ACK，seq=收到的 ACK+1，ACK=收到的 FIN

第三次挥手：服务器关闭与客户端的连接，发送一个 FIN 给客户端

第四次挥手：客户端发回 ACK 报文确认。

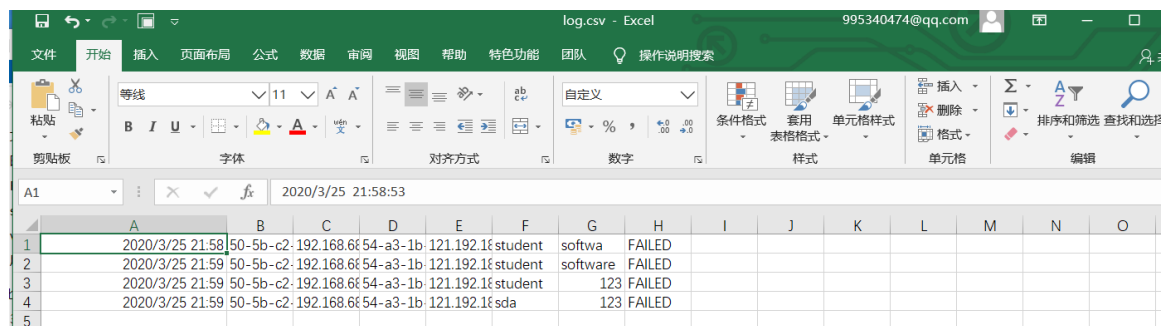
(2)。基于 WinPCAP 工具包制作程序，实现监听网络上的 FTP 数据流，解析协议内容，并作记录与统计。对用户登录行为进行记录。

选择端口并且对 ftp 进行解析

```
E:\计算机网络\lab4\Project2\x64\Debug\Project2.exe
1. \Device\NPF_{6FF1E734-015B-4F7F-8386-910AF69CE74B} (Microsoft)
2. \Device\NPF_{8CA33F2A-8F1D-41DA-9BFC-B7D73BD27493} (Microsoft)
3. \Device\NPF_{4853CCEC-FC97-4E6B-BF9F-2DFEB4FAD1C3} (Microsoft)
4. \Device\NPF_{C83149AE-5369-4702-81AF-3BD659B2909C} (Realtek PCIe GbE Family Controller)
Enter the interface number (1-4) 3
2020-3-25 21:58:53, 50-5b-c2-cd-3d-0d, 192.168.68.165, 54-a3-1b-31-00-e4, 121.192.180.66, student, softwa, FAILED
2020-3-25 21:59:2, 50-5b-c2-cd-3d-0d, 192.168.68.165, 54-a3-1b-31-00-e4, 121.192.180.66, student, software, FAILED
2020-3-25 21:59:9, 50-5b-c2-cd-3d-0d, 192.168.68.165, 54-a3-1b-31-00-e4, 121.192.180.66, student, 123, FAILED
2020-3-25 21:59:12, 50-5b-c2-cd-3d-0d, 192.168.68.165, 54-a3-1b-31-00-e4, 121.192.180.66, sda, 123, FAILED
```

主要方法就是暴力搜索 对每一个 ftp 的数据包，搜索是否有 USER 或者 PASS 这几个字母，匹配到，则后面就是对应的用户名和密码

输出到 csv 文件



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	2020/3/25 21:58	50-5b-c2-cd-3d-0d	192.168.68.165	54-a3-1b-31-00-e4	121.192.180.66	student	softwa	FAILED							
2	2020/3/25 21:59	50-5b-c2-cd-3d-0d	192.168.68.165	54-a3-1b-31-00-e4	121.192.180.66	student	software	FAILED							
3	2020/3/25 21:59	50-5b-c2-cd-3d-0d	192.168.68.165	54-a3-1b-31-00-e4	121.192.180.66	student	123	FAILED							
4	2020/3/25 21:59	50-5b-c2-cd-3d-0d	192.168.68.165	54-a3-1b-31-00-e4	121.192.180.66	sda	123	FAILED							

4 实验总结

对 tcp 的头部有了一个更清晰的了解，以及对于 tcp/ip 协议的三次握手，四次挥手的过程认识更加清晰。FTP 的报文头，以及各个格式理解更加深刻