厦門大學

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 **张晨远**

学　　号 **24320182203322**

实验时间 **2020 年 3 月 25 日**

2020 年 3 月 31 日

1 实验目的

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。将该过程截图在报告中。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。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

2 实验环境

操作系统：Windows 10　　编程语言：python

3 实验结果

TCP 三次握手建立连接的过程

Seq=0

Seq=0 Ack=1

Seq=1 Ack=1

```
TCP      66 52584 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 SACK_PERM=1
TCP      66 80 → 52584 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1440 SACK_PERM=1 WS=128
TCP      54 52584 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
```

TCP 四次挥手撤除连接

```
TCP      54 80 → 52584 [FIN, ACK] Seq=72502 Ack=616 Win=15872 Len=0
TCP      54 52584 → 80 [ACK] Seq=616 Ack=72503 Win=65536 Len=0
TCP      54 52584 → 80 [FIN, ACK] Seq=616 Ack=72503 Win=65536 Len=0
TCP      54 [TCP Retransmission] 52584 → 80 [FIN, ACK] Seq=616 Ack=72503 Win=65536 Len=0
TCP      54 [TCP Retransmission] 52584 → 80 [FIN, ACK] Seq=616 Ack=72503 Win=65536 Len=0
TCP      54 [TCP Retransmission] 52584 → 80 [FIN, ACK] Seq=616 Ack=72503 Win=65536 Len=0
TCP      54 [TCP Retransmission] 52584 → 80 [FIN, ACK] Seq=616 Ack=72503 Win=65536 Len=0
TCP      54 [TCP Retransmission] 52584 → 80 [FIN, ACK] Seq=616 Ack=72503 Win=65536 Len=0
TCP      54 52584 → 80 [RST, ACK] Seq=617 Ack=72503 Win=0 Len=0
```

Server 向 Client 发送 FIN 报文，进入 FIN_WAIT1

Client 向 Server 发送 ACK 报文，回应 FIN，Server 进入 CLOSE_WAIT,Server 收到 ACK 报文后进入 FIN_WAIT2

Client 向 Server 发送 FIN 报文，进入 LAST_ACK

经过多次重新传输后未收到回应，认为断开连接。

```
Sequence number: 57601    (relative sequence number)
Sequence number (raw): 2052601876
[Next sequence number: 59041    (relative sequence number)]
Acknowledgment number: 618    (relative ack number)
Acknowledgment number (raw): 2140672469
```

Sequence number 和 Ack number

```
Window size value: 124
[Calculated window size: 15872]
[Window size scaling factor: 128]
```

窗口大小和经过缩放因子计算后的实际可用窗口大小。

窗口起到一个缓冲的作用，指发送方在收到回复前最大可发送的数据量

拥塞窗口是发送方维护的一个虚拟窗口，发送方先设置一个最大报文长度的初始值，再通过慢启动，以指数增长的速率逼近临界窗口值。达到临界窗口值后，每经过一个往返时间 RTT 就把发送方的拥塞窗口 +1，即让拥塞窗口缓慢增大，按线性规律增长。

```
103 Response: 220 Serv-U FTP Server v6.2 for WinSock ready...
 68 Request: USER student
 90 Response: 331 User name okay, need password.
 69 Request: PASS software
 84 Response: 230 User logged in, proceed.
```

FTP 登录部分的报文

(1)Client 请求访问

(2)Server 回复 ready

(3)Client 发送 用户名

(4)Server 判断用户名并进行回复

(5)Client 发送 密码

(6)Server 判断密码回复结果，用户登陆成功。

2020-03-31 13:41:20.019583,94:b8:6d:9e:16:41,192.168.1.107,d4:83:04:66:08:e0,121.192.180.66,anonymous,IEUser@,Failed

2020-03-31 13:41:24.770407,94:b8:6d:9e:16:41,192.168.1.107,d4:83:04:66:08:e0,121.192.180.66,student,software,Succeed

编程实现对 FTP 口令的侦听

4 实验总结

了解 TCP 报文和 FTP 报文的内容，知晓了其中部分的应答机制