# 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 1 班

姓　　名 詹世彬

学　　号 24320182203321

实验时间 2020 年 3 月 25 日

**2020 年 3 月 25 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

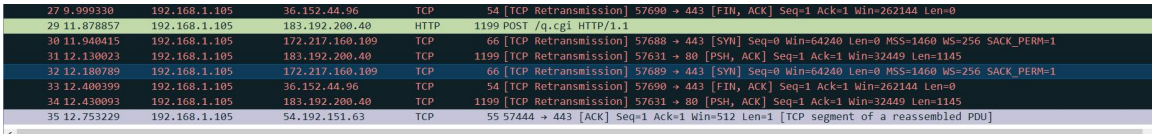
2 用 Wireshark 侦听并观察 FTP 数据，分析其用户名密码所在报文的上下文特征，在总结出提取用户名密码的有效办法。基于 Winpcap 工具包制作程序，实现监听网络上的 FTP 数据流，解析协议内容并记录与统计。

# 2 实验环境

Window 10 操作系统、Visual Studio2020、Winpcap

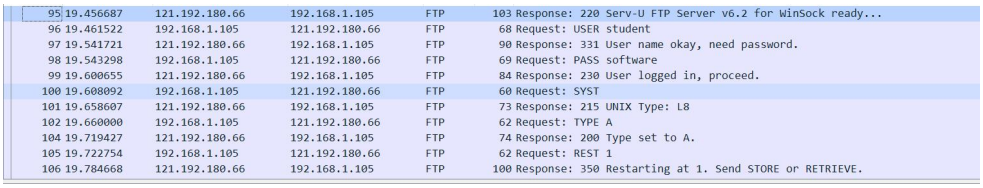
# 3 实验结果

1、侦听并观察 TCP 数据段



| | | | | | | |
|---|---|---|---|---|---|---|
| 27 | 9.999330 | 192.168.1.105 | 36.152.44.96 | TCP | 54 | [TCP Retransmission] 57690 → 443 [FIN, ACK] Seq=1 Ack=1 Win=262144 Len=0 |
| 29 | 11.878857 | 192.168.1.105 | 183.192.200.40 | HTTP | 1199 | POST /q.cgi HTTP/1.1 |
| 30 | 11.940415 | 192.168.1.105 | 172.217.160.109 | TCP | 66 | [TCP Retransmission] 57688 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 31 | 12.130023 | 192.168.1.105 | 183.192.200.40 | TCP | 1199 | [TCP Retransmission] 57631 → 80 [PSH, ACK] Seq=1 Ack=1 Win=32449 Len=1145 |
| 32 | 12.180789 | 192.168.1.105 | 172.217.160.109 | TCP | 66 | [TCP Retransmission] 57689 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 33 | 12.400399 | 192.168.1.105 | 36.152.44.96 | TCP | 54 | [TCP Retransmission] 57690 → 443 [FIN, ACK] Seq=1 Ack=1 Win=262144 Len=0 |
| 34 | 12.430093 | 192.168.1.105 | 183.192.200.40 | TCP | 1199 | [TCP Retransmission] 57631 → 80 [PSH, ACK] Seq=1 Ack=1 Win=32449 Len=1145 |
| 35 | 12.753229 | 192.168.1.105 | 54.192.151.63 | TCP | 55 | 57444 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment of a reassembled PDU] |

2、侦听并观察 FTP 数据

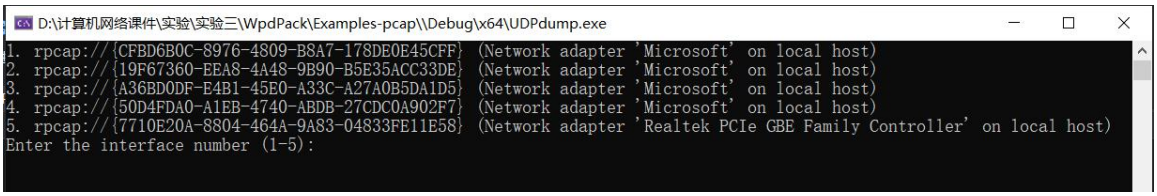


| | | | | | | |
|---|---|---|---|---|---|---|
| 95 | 19.456687 | 121.192.180.66 | 192.168.1.105 | FTP | 103 | Response: 220 Serv-U FTP Server v6.2 for WinSock ready... |
| 96 | 19.461522 | 192.168.1.105 | 121.192.180.66 | FTP | 68 | Request: USER student |
| 97 | 19.541721 | 121.192.180.66 | 192.168.1.105 | FTP | 90 | Response: 331 User name okay, need password. |
| 98 | 19.543298 | 192.168.1.105 | 121.192.180.66 | FTP | 69 | Request: PASS software |
| 99 | 19.600655 | 121.192.180.66 | 192.168.1.105 | FTP | 84 | Response: 230 User logged in, proceed. |
| 100 | 19.608092 | 192.168.1.105 | 121.192.180.66 | FTP | 60 | Request: SYST |
| 101 | 19.658607 | 121.192.180.66 | 192.168.1.105 | FTP | 73 | Response: 215 UNIX Type: L8 |
| 102 | 19.660000 | 192.168.1.105 | 121.192.180.66 | FTP | 62 | Request: TYPE A |
| 104 | 19.719427 | 121.192.180.66 | 192.168.1.105 | FTP | 74 | Response: 200 Type set to A. |
| 105 | 19.722754 | 192.168.1.105 | 121.192.180.66 | FTP | 62 | Request: REST 1 |
| 106 | 19.784668 | 121.192.180.66 | 192.168.1.105 | FTP | 100 | Response: 350 Restarting at 1. Send STORE or RETRIEVE. |

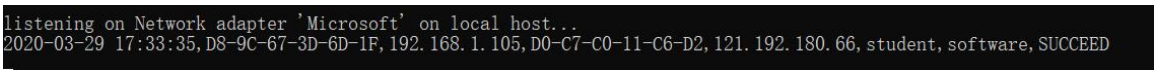
观察得出登录名以‘USER’开头，密码以‘PASS’开头，登录成功以‘230’开头，登录失败以‘530’开头，由此来进行下一步的编程。

3、基于 Winpcap 工具包制作程序，实现监听网络上的 FTP 数据流，解析协议内容并记录与统计，程序的运行结果如下：

（1）首先选择合适的网卡




（2）侦听结果如下：




格式：时间、源 MACA、源 IP、目标 MAC、目标 IP、登录名、口令、成功与否

（3）将结果记录和统计，输出到 record.csv 文件中


# 4 实验总结

通过这次实验，对 Winpcap 和 Wireshark 有了更深刻的了解，对 FTP 数据和 TCP 数据有了更深刻的认识，并且通过基于 Winpcap 工具包制作程序，对 Winpcap 工具包的使用更加熟悉，提高了自身的代码编辑能力和代码阅读能力。