

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 陈渝璇

学 号 24320182203181

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。

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。

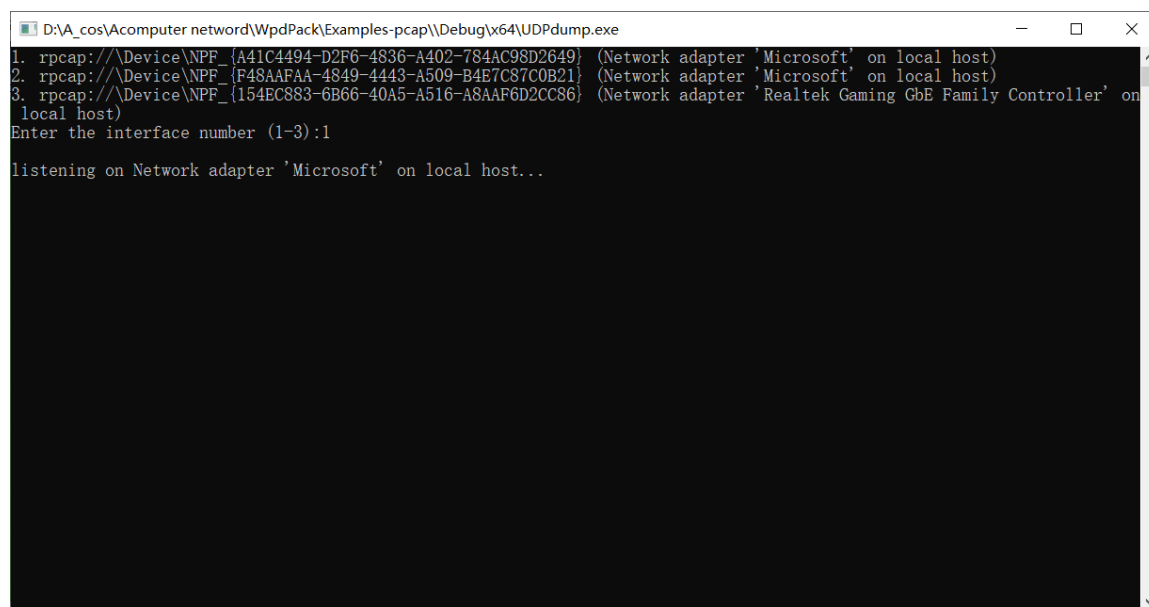
2 实验环境

操作系统：Window10

编程语言：c 语言

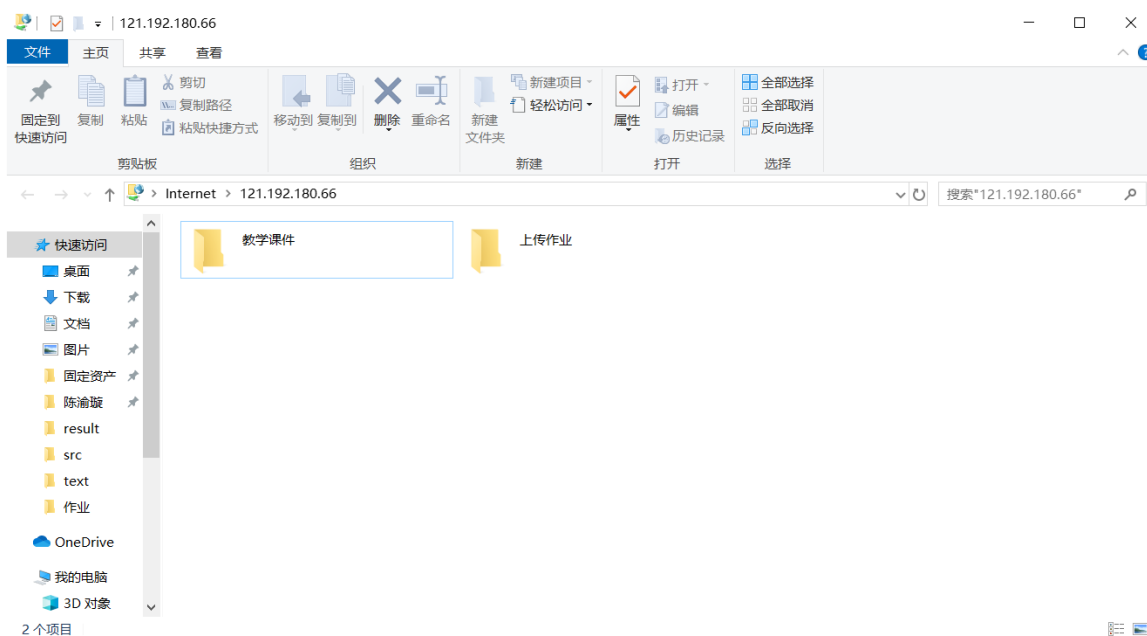
3 实验结果

运行程序



```
D:\A_cos\Acomputer network\WpdPack\Examples-pcap\Debug\x64\UDPdump.exe
1. rpcap://Device\NPF_{A41C4494-D2F6-4836-A402-784AC98D2649} (Network adapter 'Microsoft' on local host)
2. rpcap://Device\NPF_{F48AAFAA-4849-4443-A509-B4E7C87C0B21} (Network adapter 'Microsoft' on local host)
3. rpcap://Device\NPF_{154EC883-6B66-40A5-A516-A8AAF6D2CC86} (Network adapter 'Realtek Gaming GbE Family Controller' on local host)
Enter the interface number (1-3):1
listening on Network adapter 'Microsoft' on local host...
```

登录 ftp



失败与成功连接

```
D:\A_cos\Acomputer network\WpdPack\Examples-pcap\Debug\x64\UDPDump.exe
1. rpcap://Device\NPF_{A41C4494-D2F6-4836-A402-784AC98D2649} (Network adapter 'Microsoft' on local host)
2. rpcap://Device\NPF_{F48AAFAA-4849-4443-A509-B4E7C87C0B21} (Network adapter 'Microsoft' on local host)
3. rpcap://Device\NPF_{154EC883-6B66-40A5-A516-A8AAF6D2CC86} (Network adapter 'Realtek Gaming GbE Family Controller' on local host)
Enter the interface number (1-3):1

listening on Network adapter 'Microsoft' on local host...
2020-03-31 08:56:35, B4-69-21-6C-2A-B9, 192.168.1.109, 80-8F-1D-F8-75-7A, 121.192.180.66, anonymous, IEUser@, FAILED
2020-03-31 08:56:35, B4-69-21-6C-2A-B9, 192.168.1.109, 80-8F-1D-F8-75-7A, 121.192.180.66, student, software, SUCCEED
2020-03-31 08:56:36, B4-69-21-6C-2A-B9, 192.168.1.109, 80-8F-1D-F8-75-7A, 121.192.180.66, student, software, SUCCEED
2020-03-31 08:56:36, B4-69-21-6C-2A-B9, 192.168.1.109, 7A-75-F8-1D-8F-80, 121.192.180.66, student, software, SUCCEED
```

4 实验总结

结合上一次作业所学知识，这次增加了获取 ftp 的登录用户名与密码的操作。通过获取 user 与 pass 后面的字节至换行符为止，来获取用户名与密码，存储，然后输出。判断是否连接成功来输出成功与否标志。