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 刘久一

学　　号 24320182203235

实验时间 2020 年 3 月 30 日

2020 年 3 月 30 日

1 实验目的

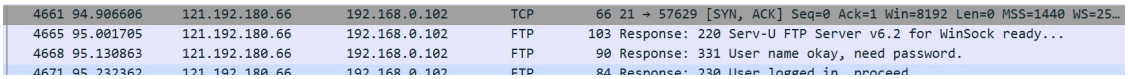
用 Wireshark 侦听并观察 TCP 数据段。观察其建立和撤除连接的过程，观察段 ID、 窗口机制和拥塞控制机制等。将该过程截图在报告中。 用 Wireshark 侦听并观察 FTP 数据，分析其用户名密码所在报文的上下文特征， 再总结出提取用户名密码的有效方法。基于 WinPCAP 工具包制作程序，实现监听网络上的 FTP 数据流，解析协议内容，并作记录与统计。对用户登录行为进行记录。 最终在文件上输出形如下列 CSV 格式的日志： 时间、源 MAC、源 IP、目标 MAC、目标 IP、登录名、口令、成功与否。

2 实验环境

Windows 10

Microsoft Virtual Studio 2019

3 实验结果



Wireshark · 追踪 TCP 流 (tcp.stream eq 93) · WLAN

```
220 Serv-U FTP Server v6.2 for WinSock ready...
USER student
331 User name okay, need password.
PASS software
230 User logged in, proceed.
opts utf8 on
501 Invalid option.
syst
215 UNIX Type: L8
site help
501 SITE option not supported.
PWD
257 "/" is current directory.
```

Wireshark · 追踪 TCP 流 (tcp.stream eq 11) · WLAN

```
220 Serv-U FTP Server v6.2 for WinSock ready..
USER student
331 User name okay, need password.
PASS software1
530 Not logged in.
```

首先打开 Wireshark 侦听数据流。发现欲跟踪的包中：头部为 331 的包代表确认用户名，头部为 530 的包代表密码是否正确；它们的 command 分别为"USER"和"PASS".

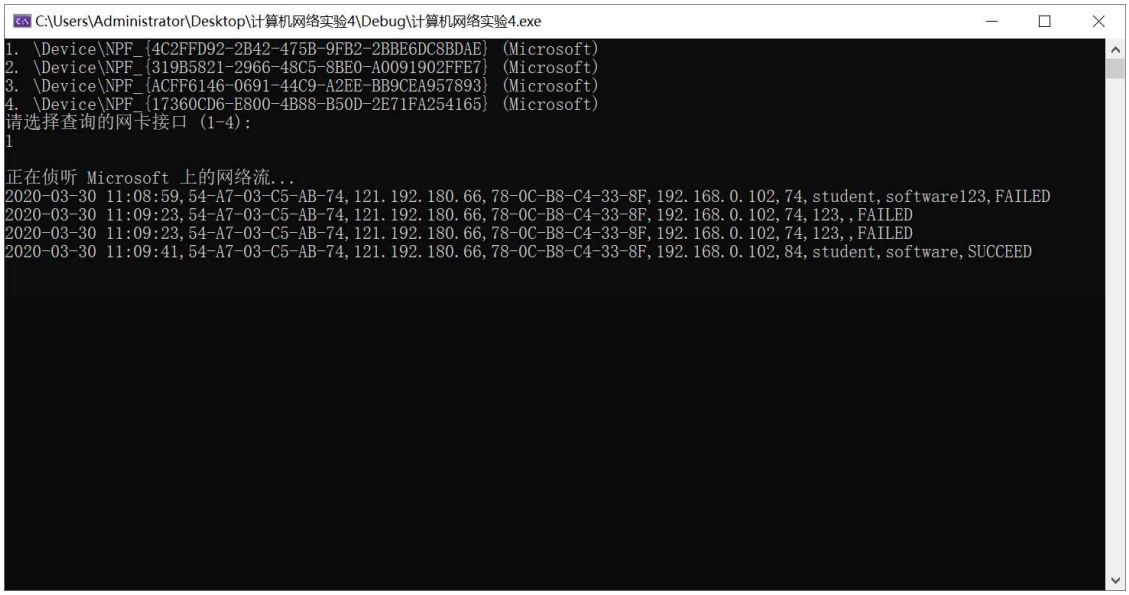
```
char packet_filter[] = "tcp";//只提取tcp
```

首先进行过滤设置。

```
if (command == "USER" || command == "PASS")
{
    std::string buf;//提取有效信息
    for (int i = ini + 5;; i++)
    {
        if (pkt_data[i] == 13)break;//休止符
        buf += (char)pkt_data[i];
    }
    if (command == "USER")m[srcipstr][0] = buf;//存取用户名
    else m[srcipstr][1] = buf;//存取密码
}
if (command == "230 " || command == "530 ")//登录成功/失败
{
    /*print*/
    printf("%04d-%02d-%02d %s,", 1900 + thistime->tm_year, 1 + thistime->tm_mon, thistime->tm_mday, timestr);
    mh.printsrcmac();
    printf(",%d.%d.%d.%d,",
        ih->saddr.byte1,
        ih->saddr.byte2,
        ih->saddr.byte3,
        ih->saddr.byte4);
    mh.printdstmac();
    printf(",%d.%d.%d.%d,",
        ih->daddr.byte1,
        ih->daddr.byte2,
        ih->daddr.byte3,
        ih->daddr.byte4);
    printf("%d,", header->len);
    std::cout << m[dstipstr][0] << "," << m[dstipstr][1]<< ",";
    if (command == "230 ")//登录成功
        std::cout << "SUCCEED" << std::endl;
```

在实验 3 的基础上，当口令为"USER","PASS"时，记录每个 ip 对应的用户名，密码；

当口令为"230 ","530 "时，一个完整的登陆操作完成，输出结果。



4 实验总结

通过这次实验我进一步加深理解了以太网的帧格式，同时锻炼了自己的编程能力。