

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 赖彦丞

学 号 24320182203216

实验时间 2020 年 4 月 6 日

2020 年 4 月 6 日

1 实验目的

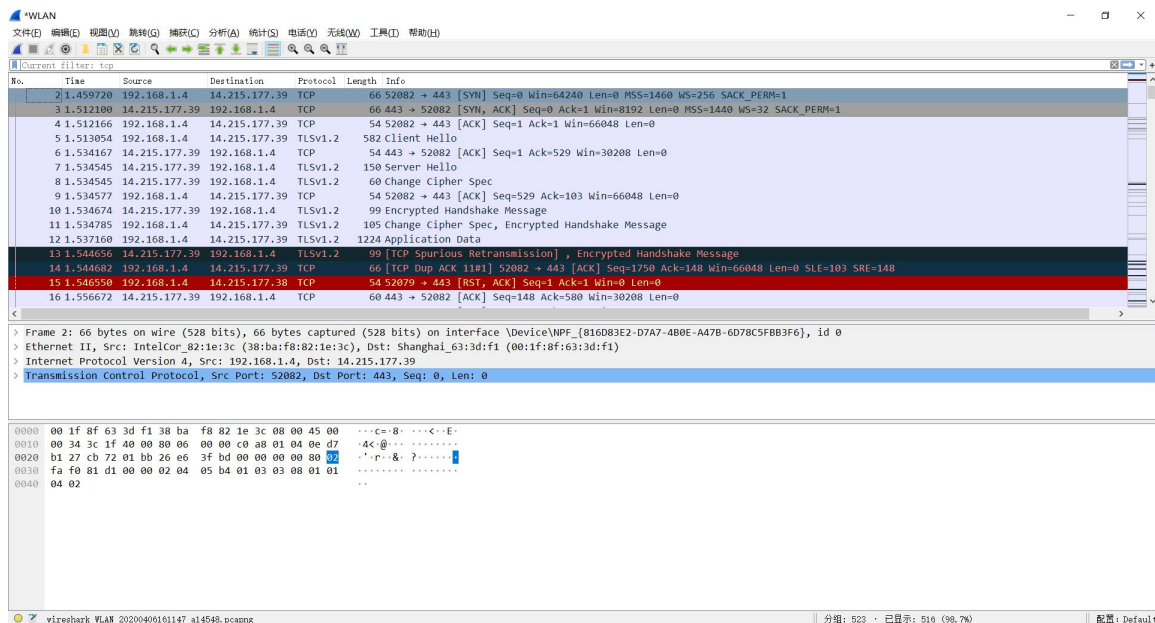
一, Wireshark 侦听并观察 TCP 数据段。观察其建立和撤除连接的过程, 观察段 ID、窗口机制和拥塞控制机制等。

二, 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

本实验在 Windows10 系统下完成, 编程语言是 C++, 用到的第三方库是 Pcap。

3 实验结果



访问了域名 www.baidu.com 进行 TCP 的分析,

客户端发送 TCP, 请求建立连接。服务器发了一个确认包。客户端再次发送确认包。在经过三次握手后建立连接。然后第四次挥手之后断开连接。

No.	Time	Source	Destination	Protocol	Length	Info
97	16.120129	121.192.180.66	192.168.1.4	TCP	66	21 → 51686 [SVN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
98	16.120217	192.168.1.4	121.192.180.66	TCP	54	51686 → 21 [ACK] Seq=1 Ack=1 Win=66048 Len=0
99	16.164926	121.192.180.66	192.168.1.4	FTP	103	Response: 220 Serv-U FTP Server v6.2 for WinSock ready...
100	16.165357	192.168.1.4	121.192.180.66	FTP	68	Request: USER student
101	16.210664	121.192.180.66	192.168.1.4	FTP	90	Response: 331 User name okay, need password.
102	16.211097	192.168.1.4	121.192.180.66	FTP	69	Request: PASS software
103	16.268114	121.192.180.66	192.168.1.4	FTP	84	Response: 230 User logged in, proceed.
104	16.302559	192.168.1.4	121.192.180.66	FTP	69	Request: OPTS UTF8 OFF
105	16.349547	121.192.180.66	192.168.1.4	FTP	75	Response: 501 Invalid option.
106	16.351912	192.168.1.4	121.192.180.66	FTP	59	Request: PWD
107	16.395696	121.192.180.66	192.168.1.4	FTP	85	Response: 257 "/" is current directory.
108	16.396237	192.168.1.4	121.192.180.66	FTP	60	Request: PASV
109	16.449429	121.192.180.66	192.168.1.4	FTP	105	Response: 227 Entering Passive Mode (121,192,180,66,230,33)
110	16.449715	192.168.1.4	121.192.180.66	FTP	62	Request: TYPE A
111	16.494894	121.192.180.66	192.168.1.4	FTP	74	Response: 200 Type set to A.
112	16.494998	192.168.1.4	121.192.180.66	FTP	60	Request: LIST

> Frame 112: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{816D83E2-D7A7-4B0E-A47B-6D78C5FBB3F6}, id 0
 > Ethernet II, Src: IntelCor_82:1e:3c (38:ba:f8:82:1e:3c), Dst: Shanghai_63:3d:f1 (00:1f:8f:63:3d:f1)
 > Internet Protocol Version 4, Src: 192.168.1.4, Dst: 121.192.180.66
 > Transmission Control Protocol, Src Port: 51686, Dst Port: 21, Seq: 64, Ack: 239, Len: 6
 > File Transfer Protocol (FTP)
 [Current working directory: /]

```

0000  00 1f 8f 63 3d f1 38 ba f8 82 1e 3c 08 00 45 00  ...C=8...<...E
0010  00 2e 1c b3 40 00 80 06 00 00 c0 a8 01 04 79 c0  .6...@... ..y
0020  b4 42 c9 e6 00 15 fe 37 21 c1 fb dc 6a cf 50 18  .B...7!...j.F
0030  01 02 ef d7 00 00 55 53 45 52 20 73 74 75 64 65  .....US ER stud
0040  6e 74 0d 0a                                     nt..

```

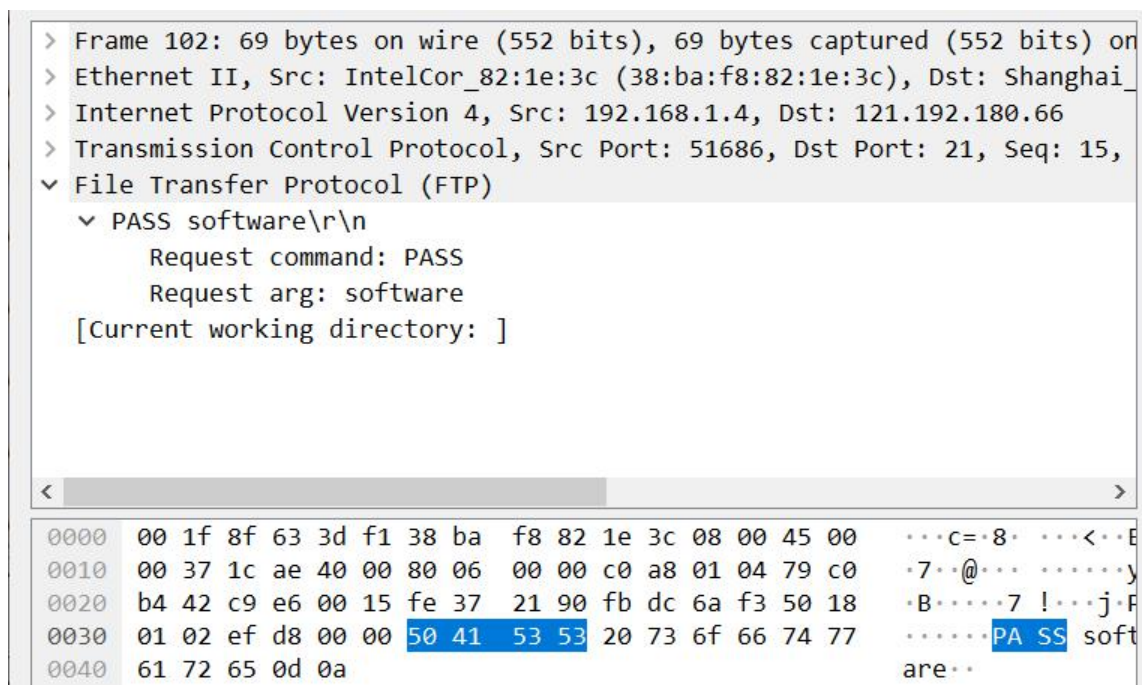
访问学院 FTP,分析 FTP 的内容.220 代表 FTP 被访问。331 表示需要密码，230 表示登陆成功。

>	Frame 100: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on
>	Ethernet II, Src: IntelCor_82:1e:3c (38:ba:f8:82:1e:3c), Dst: Shanghai_
>	Internet Protocol Version 4, Src: 192.168.1.4, Dst: 121.192.180.66
>	Transmission Control Protocol, Src Port: 51686, Dst Port: 21, Seq: 1, A
▼	File Transfer Protocol (FTP)
▼	USER student\r\n
	Request command: USER
	Request arg: student
	[Current working directory:]

```

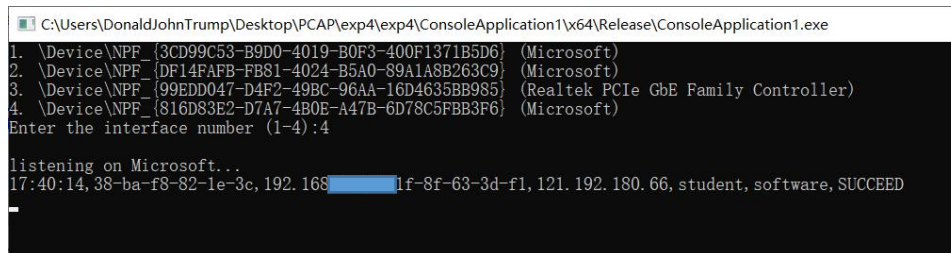
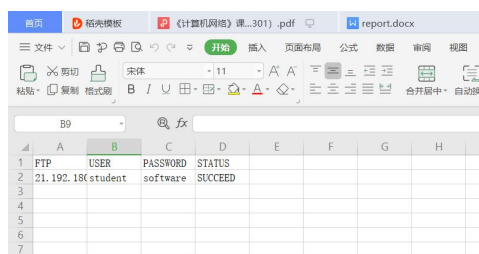
0000  00 1f 8f 63 3d f1 38 ba f8 82 1e 3c 08 00 45 00  ...C=8...<...E
0010  00 2e 1c b3 40 00 80 06 00 00 c0 a8 01 04 79 c0  .6...@... ..y
0020  b4 42 c9 e6 00 15 fe 37 21 82 fb dc 6a cf 50 18  .B...7!...j.F
0030  01 02 ef d7 00 00 55 53 45 52 20 73 74 75 64 65  .....US ER stud
0040  6e 74 0d 0a                                     nt..

```



可以看到,在 Request arg 其中的内容分别表示输入的用户名和密码。

在 Winpcap 编程过程中,可以通过修改 packet_handler 函数的功能实现对 TCP 包的解析和输出。



4 实验总结

学习到了 TCP 和 FTP 报文头的一些相关知识。

