# 厦門大學



## 信息学院软件工程系

《计算机网络》实验报告

题	目多	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_	<u>汪文青</u>	
学	号_	24320182203276	
实验	时间	2020年3月26日	

2020年4月7日

#### 1 实验目的

本实验是"用 PCAP 库侦听并解析 FTP 口令"实验的第二部分。

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

2015-03-14 13:05:16,60-36-DD-7D-D5-21,192.168.33.1,60-36-DD-7D-D5-72,192.168.33.2,student,software,SUCCEED

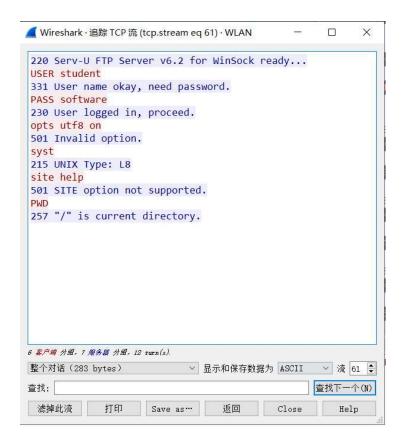
2015-03-14 13:05:16,60-36-DD-7D-D5-21,192.168.33.1,60-36-DD-7D-D5-72,192.168.33.2,student,software1,FAILED。

#### 2 实验环境

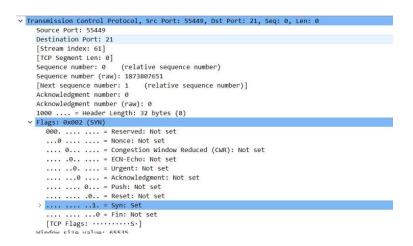
Windows 10, visual studio 2019, 编程语言 c, WinPCAP 工具包

### 3 实验结果

Tine 3 70.655935 1 70.713214 5 70.713229 5 70.778728 7 70.778784 9 70.843126 9 70.843730	Source Tp-LinkT_b1:0c:d0 192.168.0.105 192.168.0.105 121.192.180.66 192.168.0.105	Destination Broadcast 121.192.180.66 192.168.0.105	ARP TCP	Length Info   42 Who has 192.168.0.100? Tell 192.168.0.1
3 70.655935 1 70.713214 5 70.713229 5 70.778428 7 70.778784 3 70.778794 9 70.843126	Tp-LinkT_b1:0c:d0 192.168.0.105 192.168.0.105 121.192.180.66 192.168.0.105	Broadcast 121.192.180.66 121.192.180.66	ARP TCP	
3 70.655935 1 70.713214 5 70.713229 5 70.778428 7 70.778784 3 70.778794 9 70.843126	Tp-LinkT_b1:0c:d0 192.168.0.105 192.168.0.105 121.192.180.66 192.168.0.105	Broadcast 121.192.180.66 121.192.180.66	ARP TCP	
1 70.713214 5 70.713229 5 70.778428 7 70.778784 8 70.778794 9 70.843126	192.168.0.105 192.168.0.105 121.192.180.66 192.168.0.105	121.192.180.66 121.192.180.66	TCP	42 Who has 192.168.0.100? Tell 192.168.0.1
70.713229 70.778428 70.778784 870.778794 970.843126	192.168.0.105 121.192.180.66 192.168.0.105	121.192.180.66		
70.778428 70.778784 870.778794 970.843126	121.192.180.66 192.168.0.105		9.66	66 55449 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK PERM=1
7 70.778784 3 70.778794 9 70.843126	192.168.0.105	192,168,0,105	TCP	66 [TCP Out-Of-Order] 55449 → 21 [SYN] Seg=0 Win=65535 Len=0 MSS=1460 WS=
3 70.778794 9 70.843126			TCP	66 21 → 55449 [SYN, ACK] Seg=0 Ack=1 Win=8192 Len=0 MSS=1448 WS=256 SACK I
70.843126	OF SHARE SHEETING THE SHEET	121.192.180.66	TCP	54 55449 → 21 [ACK] Seg=1 Ack=1 Win=262144 Len=0
	192.168.0.105	121.192.180.66	TCP	54 [TCP Dup ACK 837#1] 55449 → 21 [ACK] Seg=1 Ack=1 Win=262144 Len=0
70.843730	121.192.180.66	192.168.0.105	FTP	103 Response: 220 Serv-U FTP Server v6.2 for WinSock ready
	192.168.0.105	121.192.180.66	TCP	54 55449 → 21 [ACK] Seq=1 Ack=50 Win=261888 Len=0
1 70.843747	192.168.0.105	121.192.180.66	TCP	54 [TCP Dup ACK 840#1] 55449 → 21 [ACK] Seg=1 Ack=50 Win=261888 Len=0
70.843921	192.168.0.105	121.192.180.66	FTP	68 Request: USER student
70.843929	192.168.0.105	121.192.180.66	TCP	68 [TCP Retransmission] 55449 → 21 [PSH, ACK] Seq=1 Ack=50 Win=261888 Len=
70.906263	121.192.180.66	192.168.0.105	FTP	90 Response: 331 User name okay, need password.
70.906817	192.168.0.105	121.192.180.66	TCP	54 55449 → 21   ACK   Seg=15 Ack=86 Win=261888 Len=0
70.906825	192.168.0.105	121.192.180.66	TCP	54 [TCP Dup <u>ACK 845#1] 55449</u> → 21 [ACK] Seq=15 Ack=86 Win=261888 Len=0
70.907145	192,168,0,105	121.192.180.66	FTP	69 Request: PASS software
3 70.907162	192.168.0.105	121,192,180,66	TCP	69 [TCP Retr <del>ansmission] 5544</del> 9 → 21 [PSH, ACK] Seg=15 Ack=86 Win=261888 Le
			TCP	54 21 → 55449 [ACK] Seg=86 Ack=30 Win=66560 Len=0
70.969502	121.192.180.66	192.168.0.105	FTP	84 Response: 230 User logged in, proceed.
70.969826	192,168,0,105	121,192,180,66	TCP	54 55449 → 21 ACK Seq=30 ACK=116 Win=261888 Len=0
70.969830	192.168.0.105	121,192,180,66	TCP	54 [TCP Dup ACK 851#1] 55449 → 21 [ACK] Seq=30 Ack=116 Win=261888 Len=0
	192.168.0.105		ETP	68 Request: opts utf8 on
70.970026	192.168.0.105	121,192,180,66	TCP	68 [TCP Retransmission] 55449 → 21 [PSH, ACK] Seg=30 Ack=116 Win=261888 Le
71.031844	121.192.180.66	192.168.0.105	FTP	75 Response: 501 Invalid option.
3.200427	192.168.0.105	121.192.180.66	TCP	54 [TCP Dup ACK 761#1] 55447 → 21 [ACK] Seg=1 Ack=1 Win=262144 Len=0
			FTP	103 Response: 220 Serv-U FTP Server v6.2 for WinSock ready
				54 55447 → 21 [ACK] Seg=1 Ack=50 Win=261888 Len=0
				54 <del>[TCP Dup ACK 764#1] 5544</del> 7 → 21 [ACK] Seq=1 Ack=50 Win=261888 Len=0
				68 Request: USER student
				68 TCP Retransmission 55447 → 21 [PSH, ACK] Seq=1 Ack=50 Win=261888 Le
				54 [TCP Retransmission] 55444 → 443 [FIN, ACK] Seq=1 Ack=1 Win=262144 Le
				54 [TCP Retransmission] 55444 → 443 [FIN. ACK] Seq=1 Ack=1 Win=262144 Le
				90 Response: 331 User name okay, need password.
				54 5544/ → 21   ACK   Seq=15 ACK=86 W1n=261888 Len=0
				54   TCP Dup ACK 771#1   55447 \rightarrow 21   ACK   Seq=15 ACK=86 Win=261888 Len=0
				64 Request: PASS str
				64 [TCP Retransmission] 55447 → 21 [PSH, ACK] Seq=15 Ack=86 Win=261888 L
				74 Response: 530 Not logged in. 54 55447 → 21 [ACK] Seq=25 Ack=106 Win=261888 Len=0
	70.843929 70.906263 70.906817 70.906817 70.907145 70.907162 70.968511 70.969502 70.969826 70.969830 70.970022	170.843920   192.168.0.105     170.966263   121.192.180.66     170.966263   192.168.0.105     192.168.0.105     170.96637   192.168.0.105     170.967145   192.168.0.105     170.967145   192.168.0.105     170.967145   192.168.0.105     170.968511   121.192.180.66     170.969826   121.192.180.66     170.969826   192.168.0.105     170.976927   192.168.0.105     170.97692	170.843929   192.168.0.105   121.192.180.66   170.966263   121.192.180.66   192.168.0.105   192.168.0.105   192.168.0.105   192.168.0.105   121.192.180.66   170.96627   192.168.0.105   121.192.180.66   170.96825   192.168.0.105   121.192.180.66   170.967145   192.168.0.105   121.192.180.66   170.968511   121.192.180.66   192.168.0.105   121.192.180.66   170.968511   121.192.180.66   192.168.0.105   121.192.180.66   170.968510   121.192.180.66   192.168.0.105   121.192.180.66   170.969826   192.168.0.105   121.192.180.66   170.969826   192.168.0.105   121.192.180.66   170.969826   192.168.0.105   121.192.180.66   170.970926   192.168.0.105   121.192.180.66   170.970926   192.168.0.105   121.192.180.66   170.970926   192.168.0.105   121.192.180.66   192.168.0.105   121.192.180.66   192.168.0.105   121.192.180.66   192.168.0.105   121.192.180.66   192.168.0.105   121.192.180.66   192.168.0.105   121.192.180.66   127.7754   192.168.0.105   121.192.180.66   127.77914   192.168.0.105   121.192.180.66   127.7991   192.168.0.105   121.192.180.66   127.7991   192.168.0.105   121.192.180.66   127.99090   192.168.0.105   121.192.180.66   123.343674   192.168.0.105   121.192.180.66   123.343674   192.168.0.105   121.192.180.66   123.343674   192.168.0.105   121.192.180.66   123.343674   192.168.0.105   121.192.180.66   123.343674   192.168.0.105   121.192.180.66   123.343674   192.168.0.105   121.192.180.66   123.343674   192.168.0.105   121.192.180.66   123.343674   192.168.0.105   121.192.180.66   123.343674   192.168.0.105   121.192.180.66   123.343674   192.168.0.105   121.192.180.66   123.343674   192.168.0.105   121.192.180.66   123.343674   192.168.0.105   121.192.180.66   123.343674   192.168.0.105   121.192.180.66   123.343674   192.168.0.105   121.192.180.66   122.192.180.66   123.343674   123.180.66   123.180.66   123.180.66   123.343674   123.180.66   123.180.66   123.180.66   123.180.66   123.343674   123.180.66   123.180.66   123.180.66   123.343674   123.180.66   123.180.66   123.180.66   123.180.66   123.	170.843929   192.168.0.105   121.192.180.66   TCP   170.966263   121.192.180.66   192.168.0.105   FTP   170.966263   192.168.0.105   FTP   192.168.0.105   121.192.180.66   TCP   170.966325   192.168.0.105   121.192.180.66   TCP   170.967162   192.168.0.105   121.192.180.66   TCP   170.967162   192.168.0.105   121.192.180.66   TCP   170.967811   121.192.180.66   192.168.0.105   TCP   170.968511   121.192.180.66   192.168.0.105   TCP   170.969826   192.168.0.105   121.192.180.66   TCP   170.969826   192.168.0.105   121.192.180.66   TCP   170.969826   192.168.0.105   121.192.180.66   TCP   170.976922   192.168.0.105   121.192.180.66   TCP   170.976925   192.168.0.105   121.192.180.66   TCP   170.976925   192.168.0.105   121.192.180.66   TCP   170.976925   192.168.0.105   121.192.180.66   TCP   170.976926   192.168.0.105   121.192.180.66   TCP   170.976926   192.168.0.105   121.192.180.66   TCP   170.976926   192.168.0.105   121.192.180.66   TCP   170.976926   192.168.0.105   121.192.180.66   TCP   170.976929   170.976



1. 观察第一个 TCP 报文段:客户端想服务器发送的请求连接包。 重要的数据,SYN=1, seq=0 (sequence number),表示连接请求。



2. 第二个 TCP 报文段:服务器向客户端发送的确认报文段。

重要数据,SYN=1,seq=0,ACK=1(并不 ACK number,值为 1 时,表示确认字段 有效),ACK number=1(这个才是确认号,表示期望收到对方下一段报文段的

第一个数据字节的序号 sequence number,也就是说希望下一段的 seq=1,这个也表示 1 之前的数据包已经接受了)

```
Transmission Control Protocol, Src Port: 21, Dst Port: 55449, Seq: 0, Ack: 1, Len: 0
    Source Port: 21
    Destination Port: 55449
                                 源端口
                                                           序列号 ACK 长度
                                            目的端口
    [Stream index: 61]
    [TCP Segment Len: 0]
    Sequence number: 0
                        (relative sequence number)
    Sequence number (raw): 2908842428
    [Next sequence number: 1
                              (relative sequence number)]
                               (relative ack number)
    Acknowledgment number: 1
    Acknowledgment number (raw) . 1973907652
```

3.第三个 TCP 报文段:客户端向服务器发送的确认报文段

重要数据,ACK=1, seq=1, ACK number=1

```
> Frame 837: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{C37D1402-020B-48AA-837D-029E
> Ethernet II, Src: IntelCor_21:04:c6 (3c:6a:a7:21:04:c6), Dst: Tp-LinkT_b1:0c:d0 (74:05:a5:b1:0c:d0)
> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 121.192.180.66
v Transmission Control Protocol, Src Port: 55449, Dst Port: 21, Seq: 1, Ack: 1, Len: 0
    Source Port: 55449
    Destination Port: 21
    [Stream index: 61]
    [TCP Segment Len: 0]
                         (relative sequence number)
    Sequence number: 1
    Sequence number (raw): 1873807652
    [Next sequence number: 1
                               (relative sequence number)]
    Acknowledgment number: 1
                                (relative ack number)
    Acknowledgment number (raw): 2908842429
    0101 .... = Header Length: 20 bytes (5)
```

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:

A	В	C	D	E	F	G	Н
2020/4/7 21:	14 3C-6A-A7-21-04-C6	192.168.0.105	D0-0C-B1-A5-05-74	121.192.180.66	anonymo	(IEUser@	FAILED
2020/4/7 21:	15 3C-6A-A7-21-04-C6	192.168.0.105	D0-0C-B1-A5-05-74	121.192.180.66	student	SSS	FAILED
2020/4/7 21:	15 3C-6A-A7-21-04-C6	192.168.0.105	D0-0C-B1-A5-05-74	121.192.180.66	student	123	FAILED
2020/4/7 21:	15 3C-6A-A7-21-04-C6	192.168.0.105	74-05-A5-B1-0C-D0	121.192.180.66	student	software	SUCCEED
2020/4/7 21:	15 3C-6A-A7-21-04-C6	192.168.0.105	D0-0C-B1-A5-05-74	121.192.180.66	student	software	SUCCEED
2020/4/7 21:	16 3C-6A-A7-21-04-C6	192.168.0.105	74-05-A5-B1-0C-D0	121.192.180.66	anonymo	(IEUser@	FAILED
2020/4/7 21:	16 3C-6A-A7-21-04-C6	192.168.0.105	74-05-A5-B1-0C-D0	121.192.180.66	student	wwq	FAILED
2020/4/7 21:	16 3C-6A-A7-21-04-C6	192.168.0.105	74-05-A5-B1-0C-D0	121.192.180.66	student	software	SUCCEED
2020/4/7 21:	16 3C-6A-A7-21-04-C6	192.168.0.105	D0-0C-B1-A5-05-74	121.192.180.66	student	software	SUCCEED
2020/4/7 21:	34 3C-6A-A7-21-04-C6	192.168.0.105	D0-0C-B1-A5-05-74	121.192.180.66	anonymo	(IEUser@	FAILED
2020/4/7 21:	34 3C-6A-A7-21-04-C6	192.168.0.105	74-05-A5-B1-0C-D0	121.192.180.66	student	wwq	FAILED
2020/4/7 21:	34 3C-6A-A7-21-04-C6	192.168.0.105	74-05-A5-B1-0C-D0	121.192.180.66	student	SSS	FAILED
2020/4/7 21:	34 3C-6A-A7-21-04-C6	192.168.0.105	74-05-A5-B1-0C-D0	121.192.180.66	student	str	FAILED
2020/4/7 21:	35 3C-6A-A7-21-04-C6	192.168.0.105	74-05-A5-B1-0C-D0	121.192.180.66	student	software	SUCCEED
2020/4/7 21:	35 3C-6A-A7-21-04-C6	192.168.0.105	74-05-A5-B1-0C-D0	121.192.180.66	student	software	SUCCEED

多次登陆学院 FTP 将监听到的上述信息以表格形式输出到硬盘中。程序输出格式实例如下:

121.192.180.66       anonymous       IEUser@       FAILED         121.192.180.66       student       sss       FAILED         121.192.180.66       student       123 FAILED         121.192.180.66       student       software       OK         121.192.180.66       student       software       OK         121.192.180.66       student       wwq       FAILED         121.192.180.66       student       software       OK         121.192.180.66       student       software       OK         121.192.180.66       anonymous       IEUser@       FAILED         121.192.180.66       student       wwq       FAILED         121.192.180.66       student       sss       FAILED         121.192.180.66       student       str       FAILED         121.192.180.66       student       str       FAILED         121.192.180.66       student       software       OK         121.192.180.66       student       software       OK	FTP	USER	PAS	STA
121.192.180.66     student     123 FAILED       121.192.180.66     student     software     OK       121.192.180.66     student     software     OK       121.192.180.66     anonymous     IEUser@ FAILED       121.192.180.66     student     wwq     FAILED       121.192.180.66     student     software     OK       121.192.180.66     student     software     OK       121.192.180.66     anonymous     IEUser@ FAILED       121.192.180.66     student     wwq     FAILED       121.192.180.66     student     sss     FAILED       121.192.180.66     student     str     FAILED	121.192.180.66	anonymous	IEUser@	FAILED
121.192.180.66       student       software       OK         121.192.180.66       student       software       OK         121.192.180.66       anonymous       IEUser@       FAILED         121.192.180.66       student       wwq       FAILED         121.192.180.66       student       software       OK         121.192.180.66       student       software       OK         121.192.180.66       anonymous       IEUser@       FAILED         121.192.180.66       student       wwq       FAILED         121.192.180.66       student       sss       FAILED         121.192.180.66       student       str       FAILED         121.192.180.66       student       str       FAILED         121.192.180.66       student       str       FAILED         121.192.180.66       student       str       FAILED         121.192.180.66       student       software       OK	121.192.180.66	student	SSS	FAILED
121.192.180.66       student       software       OK         121.192.180.66       anonymous       IEUser@       FAILED         121.192.180.66       student       wwq       FAILED         121.192.180.66       student       software       OK         121.192.180.66       student       software       OK         121.192.180.66       anonymous       IEUser@       FAILED         121.192.180.66       student       wwq       FAILED         121.192.180.66       student       sss       FAILED         121.192.180.66       student       str       FAILED         121.192.180.66       student       str       FAILED         121.192.180.66       student       str       FAILED         121.192.180.66       student       software       OK	121.192.180.66	student	123	FAILED
121.192.180.66     anonymous     IEUser@     FAILED       121.192.180.66     student     wwq     FAILED       121.192.180.66     student     software     OK       121.192.180.66     student     software     OK       121.192.180.66     anonymous     IEUser@     FAILED       121.192.180.66     student     wwq     FAILED       121.192.180.66     student     sss     FAILED       121.192.180.66     student     str     FAILED       121.192.180.66     student     str     FAILED       121.192.180.66     student     software     OK	121.192.180.66	student	software	OK
121.192.180.66     student     wwq     FAILED       121.192.180.66     student     software     OK       121.192.180.66     student     software     OK       121.192.180.66     anonymous     IEUser@     FAILED       121.192.180.66     student     wwq     FAILED       121.192.180.66     student     sss     FAILED       121.192.180.66     student     str     FAILED       121.192.180.66     student     str     FAILED       121.192.180.66     student     str     FAILED       121.192.180.66     student     software     OK	121.192.180.66	student	software	OK
121.192.180.66     student     software     OK       121.192.180.66     student     software     OK       121.192.180.66     anonymous     IEUser@     FAILED       121.192.180.66     student     wwq     FAILED       121.192.180.66     student     sss     FAILED       121.192.180.66     student     str     FAILED       121.192.180.66     student     str     FAILED       121.192.180.66     student     software     OK	121.192.180.66	anonymous	IEUser@	FAILED
121.192.180.66     student     software     OK       121.192.180.66     anonymous     IEUser@     FAILED       121.192.180.66     student     wwq     FAILED       121.192.180.66     student     sss     FAILED       121.192.180.66     student     str     FAILED       121.192.180.66     student     str     FAILED       121.192.180.66     student     software     OK	121.192.180.66	student	wwq	FAILED
121.192.180.66     anonymous     IEUser@     FAILED       121.192.180.66     student     wwq     FAILED       121.192.180.66     student     sss     FAILED       121.192.180.66     student     str     FAILED       121.192.180.66     student     str     FAILED       121.192.180.66     student     software     OK	121.192.180.66	student	software	OK
121.192.180.66     student     wwq     FAILED       121.192.180.66     student     sss     FAILED       121.192.180.66     student     str     FAILED       121.192.180.66     student     str     FAILED       121.192.180.66     student     software     OK	121.192.180.66	student	software	OK
121.192.180.66     student     sss     FAILED       121.192.180.66     student     str     FAILED       121.192.180.66     student     software     OK	121.192.180.66	anonymous	IEUser@	FAILED
121.192.180.66     student     str     FAILED       121.192.180.66     student     software     OK	121.192.180.66	student	wwq	FAILED
121.192.180.66 student software OK	121.192.180.66	student	SSS	FAILED
	121.192.180.66	student	str	FAILED
121.192.180.66 student software OK	121.192.180.66	student	software	OK
	121.192.180.66	student	software	OK

#### 4 实验总结

学习并分析了 TCP 数据包的结构、含义。分析了 TCP 连接的建立过程和数据 传输过程,观察了 TCP 握手和挥手的过程。在 wireshark 中要注意区分 ACK 和 ACK number。