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 2 班

姓　　名 汪文青

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

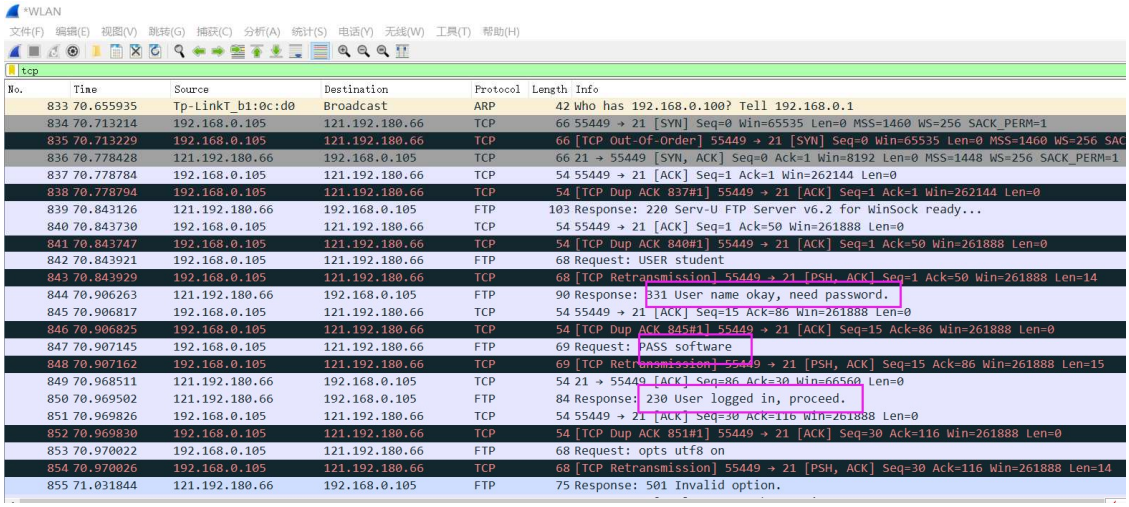
2015-03-14 13:05:16,60-36-DD-7D-D5-21,192.168.33.1,60-36-DD-7D-D5-72,192.168.33.2,student,software,SUCCEED

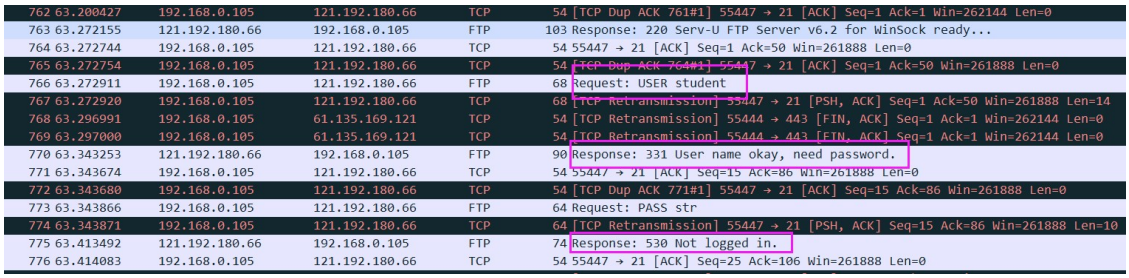
2015-03-14 13:05:16,60-36-DD-7D-D5-21,192.168.33.1,60-36-DD-7D-D5-72,192.168.33.2,student,software1,FAILED。

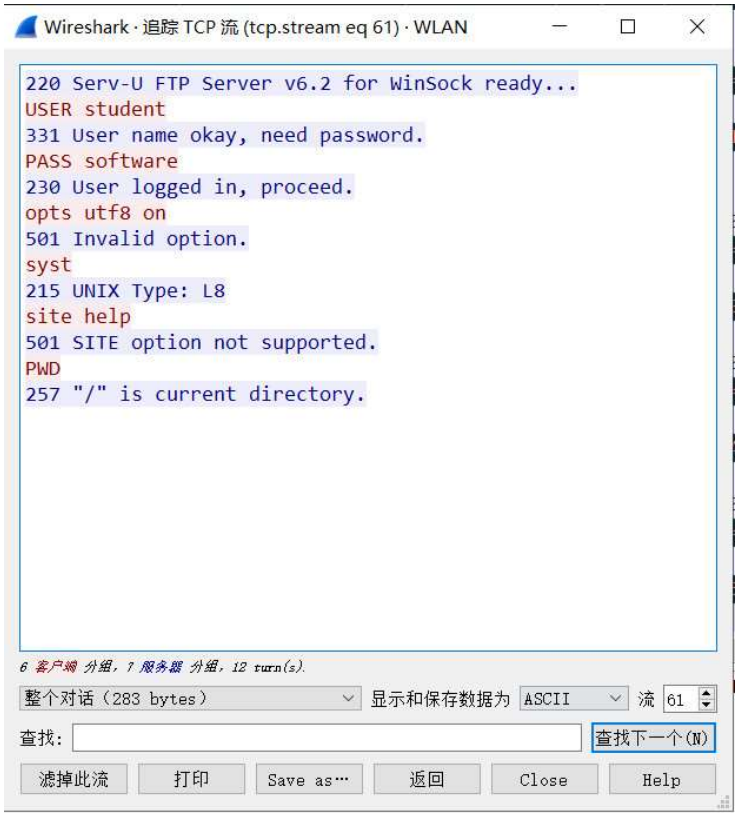
2 实验环境

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

3 实验结果

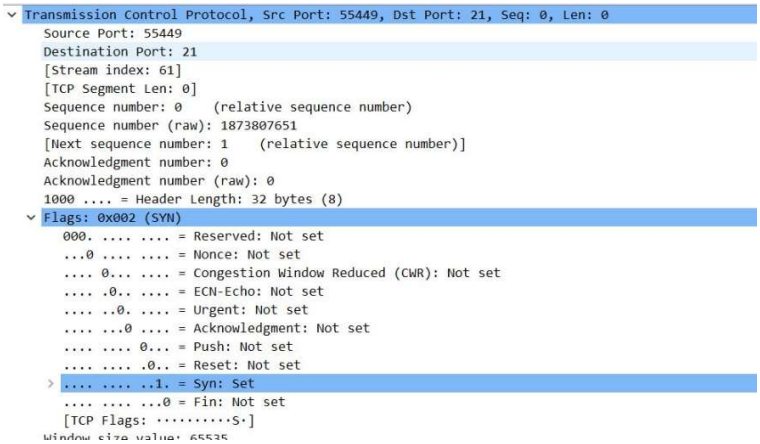

*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
tcp
No. Time Source Destination Protocol Length Info
833 70.655935 Tp-LinkT_b1:0c:d0 Broadcast ARP 42 Who has 192.168.0.100? Tell 192.168.0.1
834 70.713214 192.168.0.105 121.192.180.66 TCP 66 55449 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
835 70.713229 192.168.0.105 121.192.180.66 TCP 66 [TCP Out-Of-Order] 55449 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SAC
836 70.778428 121.192.180.66 192.168.0.105 TCP 66 21 → 55449 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1448 WS=256 SACK_PERM=1
837 70.778784 192.168.0.105 121.192.180.66 TCP 54 55449 → 21 [ACK] Seq=1 Ack=1 Win=262144 Len=0
838 70.778794 192.168.0.105 121.192.180.66 TCP 54 [TCP Dup ACK 837#1] 55449 → 21 [ACK] Seq=1 Ack=1 Win=262144 Len=0
839 70.843126 121.192.180.66 192.168.0.105 FTP 103 Response: 220 Serv-U FTP Server v6.2 for WinSock ready...
840 70.843730 192.168.0.105 121.192.180.66 TCP 54 55449 → 21 [ACK] Seq=1 Ack=50 Win=261888 Len=0
841 70.843747 192.168.0.105 121.192.180.66 TCP 54 [TCP Dup ACK 840#1] 55449 → 21 [ACK] Seq=1 Ack=50 Win=261888 Len=0
842 70.843921 192.168.0.105 121.192.180.66 FTP 68 Request: USER student
843 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=14
844 70.906263 121.192.180.66 192.168.0.105 FTP 90 Response: 331 User name okay, need password.
845 70.906817 192.168.0.105 121.192.180.66 TCP 54 55449 → 21 [ACK] Seq=15 Ack=86 Win=261888 Len=0
846 70.906825 192.168.0.105 121.192.180.66 TCP 54 [TCP Dup ACK 845#1] 55449 → 21 [ACK] Seq=15 Ack=86 Win=261888 Len=0
847 70.907145 192.168.0.105 121.192.180.66 FTP 69 Request: PASS software
848 70.907162 192.168.0.105 121.192.180.66 TCP 69 [TCP Retransmission] 55449 → 21 [PSH, ACK] Seq=15 Ack=86 Win=261888 Len=15
849 70.968511 121.192.180.66 192.168.0.105 TCP 54 21 → 55449 [ACK] Seq=86 Ack=30 Win=66560 Len=0
850 70.969502 121.192.180.66 192.168.0.105 FTP 84 Response: 230 User logged in, proceed.
851 70.969826 192.168.0.105 121.192.180.66 TCP 54 55449 → 21 [ACK] Seq=30 Ack=116 Win=261888 Len=0
852 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
853 70.970022 192.168.0.105 121.192.180.66 FTP 68 Request: opts utf8 on
854 70.970026 192.168.0.105 121.192.180.66 TCP 68 [TCP Retransmission] 55449 → 21 [PSH, ACK] Seq=30 Ack=116 Win=261888 Len=14
855 71.031844 121.192.180.66 192.168.0.105 FTP 75 Response: 501 Invalid option.


762 63.200427 192.168.0.105 121.192.180.66 TCP 54 [TCP Dup ACK 761#1] 55447 → 21 [ACK] Seq=1 Ack=1 Win=262144 Len=0
763 63.272155 121.192.180.66 192.168.0.105 FTP 103 Response: 220 Serv-U FTP Server v6.2 for WinSock ready...
764 63.272744 192.168.0.105 121.192.180.66 TCP 54 55447 → 21 [ACK] Seq=1 Ack=50 Win=261888 Len=0
765 63.272754 192.168.0.105 121.192.180.66 TCP 54 [TCP Dup ACK 764#1] 55447 → 21 [ACK] Seq=1 Ack=50 Win=261888 Len=0
766 63.272911 192.168.0.105 121.192.180.66 FTP 68 Request: USER student
767 63.272920 192.168.0.105 121.192.180.66 TCP 68 [TCP Retransmission] 55447 → 21 [PSH, ACK] Seq=1 Ack=50 Win=261888 Len=14
768 63.296991 192.168.0.105 61.135.169.121 TCP 54 [TCP Retransmission] 55444 → 443 [FIN, ACK] Seq=1 Ack=1 Win=262144 Len=0
769 63.297000 192.168.0.105 61.135.169.121 TCP 54 [TCP Retransmission] 55444 → 443 [FIN, ACK] Seq=1 Ack=1 Win=262144 Len=0
770 63.343253 121.192.180.66 192.168.0.105 FTP 90 Response: 331 User name okay, need password.
771 63.343674 192.168.0.105 121.192.180.66 TCP 54 55447 → 21 [ACK] Seq=15 Ack=86 Win=261888 Len=0
772 63.343680 192.168.0.105 121.192.180.66 TCP 54 [TCP Dup ACK 771#1] 55447 → 21 [ACK] Seq=15 Ack=86 Win=261888 Len=0
773 63.343866 192.168.0.105 121.192.180.66 FTP 64 Request: PASS str
774 63.343871 192.168.0.105 121.192.180.66 TCP 64 [TCP Retransmission] 55447 → 21 [PSH, ACK] Seq=15 Ack=86 Win=261888 Len=10
775 63.413492 121.192.180.66 192.168.0.105 FTP 74 Response: 530 Not logged in.
776 63.414083 192.168.0.105 121.192.180.66 TCP 54 55447 → 21 [ACK] Seq=25 Ack=106 Win=261888 Len=0



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。

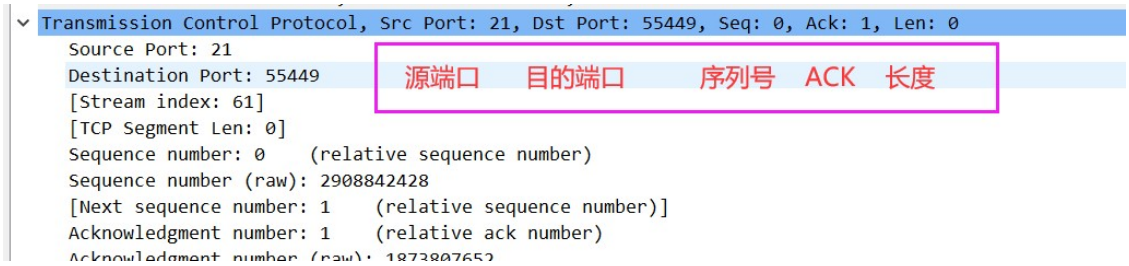
   重要的数据,SYN=1, seq=0 (sequence number),表示连接请求。



2. 第二个 TCP 报文段:服务器向客户端发送的确认报文段。

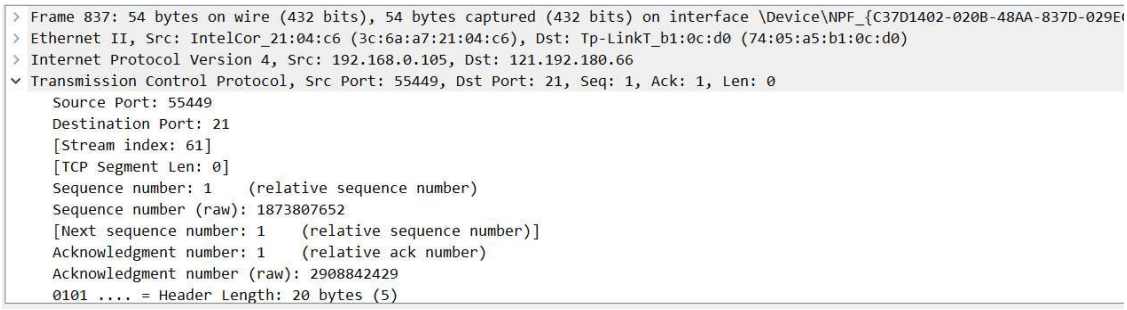
   重要数据,SYN=1,seq=0,ACK=1(并不 ACK number,值为 1 时,表示确认字段有效),ACK number=1(这个才是确认号,表示期望收到对方下一段报文段的

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)



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



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	B	C	D	E	F	G	H
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	anonymou	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	anonymou	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	anonymou	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：

FTP	USER	PAS	STA
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	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	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。