

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 3 班

姓 名 宋润涵

学 号 24320182203266

实验时间 2020 年 3 月 25 日

2020 年 3 月 29 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。

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

Windows 10, Visual Studio 2019, WinPcap 4.1.2, C++

3 实验结果

建立 TCP 连接

66	3.707123	192.168.18.3	121.192.180.66	TCP	66	14103 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
68	3.802026	121.192.180.66	192.168.18.3	TCP	66	21 → 14103 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1452 WS=256 SACK_PERM=1
69	3.802086	192.168.18.3	121.192.180.66	TCP	54	14103 → 21 [ACK] Seq=1 Ack=1 Win=132096 Len=0
70	3.803755	203.119.247.189	192.168.18.3	TCP	66	[TCP Reset-Aliase ACK] 443 → 10715 [ACK] Seq=1 Ack=2 Win=65536 Len=0 SLEN=1 SRE=2

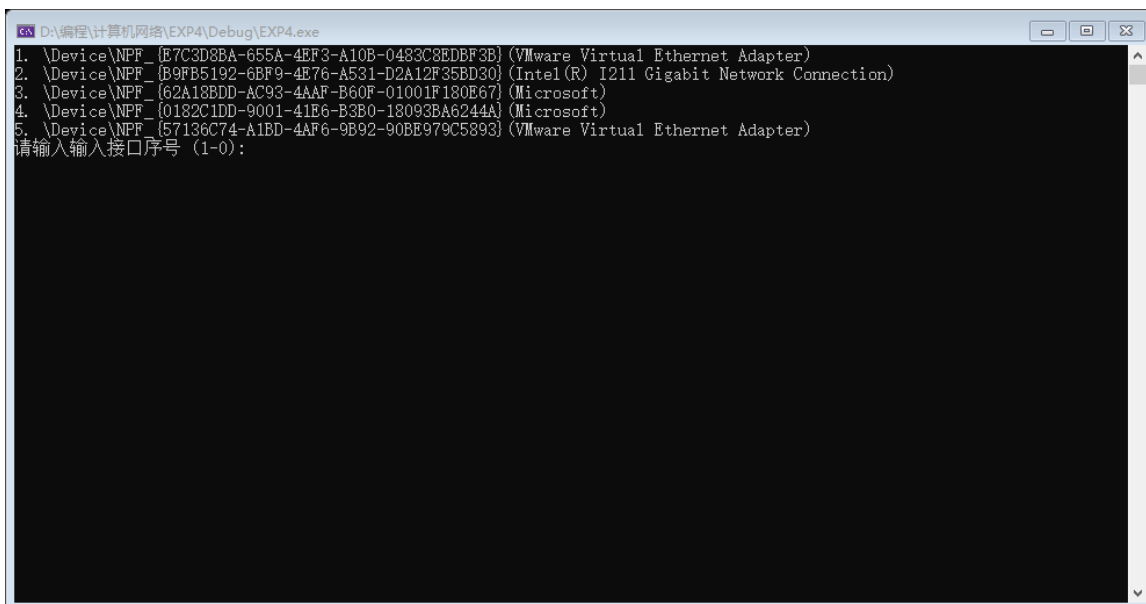
断开 TCP 连接

39	3.130191	192.168.18.3	121.192.180.66	TCP	54	14103 → 21 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
40	3.225940	121.192.180.66	192.168.18.3	TCP	60	21 → 14103 [ACK] Seq=1 Ack=2 Win=260 Len=0
41	3.227534	121.192.180.66	192.168.18.3	TCP	60	21 → 14103 [FIN, ACK] Seq=1 Ack=2 Win=260 Len=0
42	3.227567	192.168.18.3	121.192.180.66	TCP	54	14103 → 21 [ACK] Seq=2 Ack=2 Win=513 Len=0

段 ID 拥塞控制等等

```
Transmission Control Protocol, Src Port: 443, Dst Port: 10715, Seq: 1, Ack: 2, Len: 0
  Source Port: 443
  Destination Port: 10715
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 1 (relative sequence number)
  Sequence number (raw): 400303937
  [Next sequence number: 1 (relative sequence number)]
  Acknowledgment number: 2 (relative ack number)
  Acknowledgment number (raw): 1070252699
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x010 (ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    ....0... = Congestion Window Reduced (CWR): Not set
```

程序启动界面，输入需要监听的端口号后进入监听模式。



```
D:\编程\计算机网络\EXP4\Debug\EXP4.exe
1. \Device\NPF_{E7C3D8BA-655A-4EF3-A10B-0483C8EDBF3B} (VMware Virtual Ethernet Adapter)
2. \Device\NPF_{B9FB5192-6BF9-4E76-A531-D2A12F35BD30} (Intel(R) I211 Gigabit Network Connection)
3. \Device\NPF_{62A18BDD-AC93-4AAF-B60F-01001F180E67} (Microsoft)
4. \Device\NPF_{0182C1DD-9001-41E6-B3B0-18093BA6244A} (Microsoft)
5. \Device\NPF_{57136C74-A1BD-4AF6-9B92-90BE979C5893} (VMware Virtual Ethernet Adapter)
请输入输入接口序号 (1-0):
```

程序会监听 FTP 命令，并将命令显示出来，按 ESC 退出监听程序

```

D:\编程\计算机网络\EXP4\Debug\EXP4.exe
530 Not logged in.
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.
SYST
215 UNIX Type: L8
FEAT
211-Extension supported
CLNT
MDTM
MDTM YYYYMMDDHHMMSS[+-TZ],filename
SIZE
SITE PSWD;EXEC;SET;INDEX;ZONE;CHMOD;MSG
REST STREAM
XCRC filename,start,end
MODE Z
MLST Type*;Size*;Create;Modify*;Win32.ea*;
211 End
PWD
257 "/" is current directory.
TYPE I
200 Type set to I.
PASV
227 Entering Passive Mode (121,192,180,66,219,68)
MLSD
150 Opening BINARY mode data connection for MLSD.
226 Transfer complete.

```

程序会将登录信息保存在 CSV 文件中

	A	B	C	D	E	F	G	H	I
1	时间	源 MAC	源 IP	目标 MAC	目标 IP	登录名	口令	成功与否	
2	2020/3/29 15:27	B4-DE-DF-B7-46-FE	121.192.180.66.21	04-D4-C4-4F-39-BE	192.168.18.3.13974	student	softwar	FAILED	
3	2020/3/29 15:27	B4-DE-DF-B7-46-FE	121.192.180.66.21	04-D4-C4-4F-39-BE	192.168.18.3.13975	student	software	SUCCEED	
4									
5									
6									

4 实验总结

TCP 是一种较为可靠的传输协议，他是面向连接的。在此过程中他会进行三次握手（建立连接），四次挥手（撤除连接）。

本次实验使我对 WinPcap 的过滤系统有了进一步的了解，包括编译过滤器（compile）和设置过滤器（setFilter）

FTP 拥有主动模式和被动模式两种传输模式，其中 21 号端口是用来给服务端发送命令。在被动模式中服务器会给出一个端口用来传送数据。主动模式中，这个端口由客户端给出。