

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 饶龙宇

学 号 24320182203256

实验时间 2020 年 3 月 25 日

2020 年 3 月 25 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

2 实验环境

编程环境：Windows10 Visual Studio 2019

编程语言：C++

3 实验结果

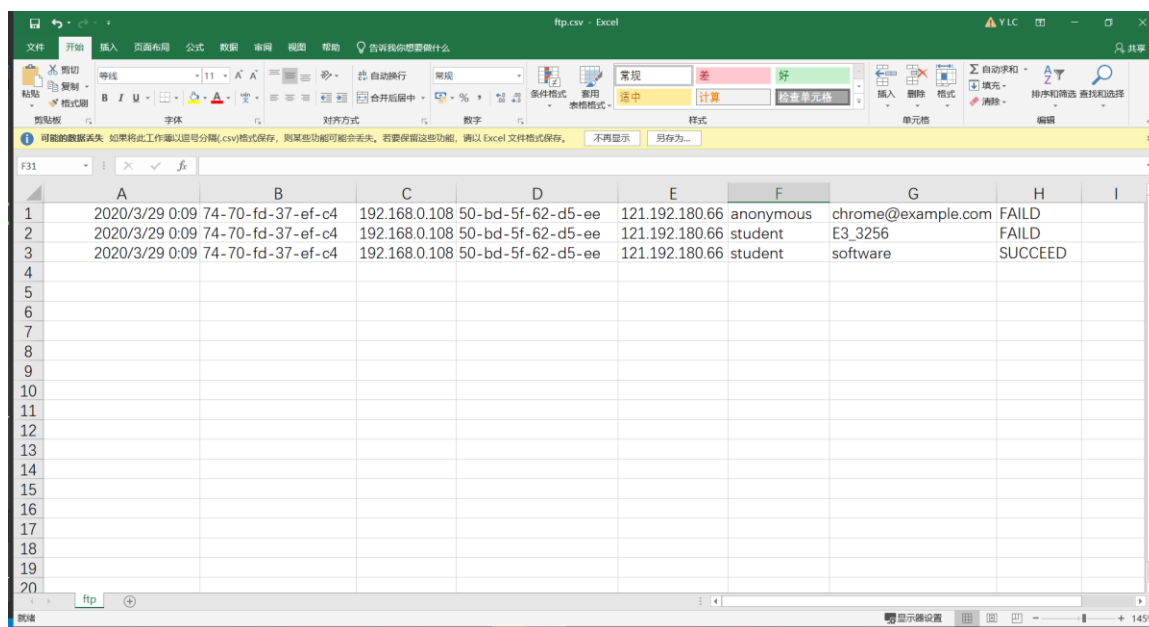
```

E:\Project\CNlab4\src\Debug\CNlab4.exe
1. rpcap://{4D45C982-404C-46C1-9C92-0161BF53A91C} (Network adapter 'Realtek PCIe GBE Family Controller' on local host)
2. rpcap://{11D61CF6-92DA-46D8-9415-1C6D1C3E4D5C} (Network adapter 'Oracle' on local host)
3. rpcap://{12C3FE26-6E7A-4EE5-9F3B-8D152F18D536} (Network adapter 'VMware Virtual Ethernet Adapter' on local host)
4. rpcap://{18D48D7D-F630-4E23-AF50-E01BD0D158F5} (Network adapter 'TAP-Windows Adapter V9' on local host)
5. rpcap://{A58A2AAF-78AB-4A79-8D5B-B341659D31B6} (Network adapter 'Microsoft' on local host)
6. rpcap://{C101CE9A-D941-4D32-8E53-6A352C463710} (Network adapter 'VMware Virtual Ethernet Adapter' on local host)
7. rpcap://{7544EA9C-A3E4-4D8D-BD5A-E26EE023EAEF} (Network adapter 'Microsoft' on local host)
8. rpcap://{9723E580-9B1A-4AE6-8364-836A8C41B86E} (Network adapter 'Microsoft' on local host)
Enter the interface number (1-8):8

listening on Network adapter 'Microsoft' on local host...
2020-3-29 00:09:12, 74-70-fd-37-ef-c4, 192.168.0.108, 50-bd-5f-62-d5-ee, 121.192.180.66, anonymous, chrome@example.com, FAILD
2020-3-29 00:09:21, 74-70-fd-37-ef-c4, 192.168.0.108, 50-bd-5f-62-d5-ee, 121.192.180.66, student, E3_3256, FAILD
2020-3-29 00:09:29, 74-70-fd-37-ef-c4, 192.168.0.108, 50-bd-5f-62-d5-ee, 121.192.180.66, student, software, SUCCEED

```

1.控制台输出



The screenshot shows an Excel spreadsheet with the following data:

	A	B	C	D	E	F	G	H	I
1	2020/3/29 0:09	74-70-fd-37-ef-c4	192.168.0.108	50-bd-5f-62-d5-ee	121.192.180.66	anonymous	chrome@example.com	FAILD	
2	2020/3/29 0:09	74-70-fd-37-ef-c4	192.168.0.108	50-bd-5f-62-d5-ee	121.192.180.66	student	E3_3256	FAILD	
3	2020/3/29 0:09	74-70-fd-37-ef-c4	192.168.0.108	50-bd-5f-62-d5-ee	121.192.180.66	student	software	SUCCEED	

2.监听网络上的 FTP 数据流，解析协议内容，并作记录与统计，形成 CSV 格式的日志。

4 实验总结

通过本次实验，我较实验三对 winPcap 库的使用有了更深的理解，但是遇到打开本地 FTP 服务器时无法监听到数据包的问题，只能借助于学院的 FTP 服务器，还未解决。