厦門大學

软 件 学 院

《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

姓　　名　蔡艺敏

学　　号　24320182203166

班　　级　软件工程 2018 级 1 班

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

```
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

Win10，VS2015，WinPCAP，科来数据包播放器

3 实验结果

打开 ftp://121.192.180.66/捕捉我们需要的包：

No.	Time	Source	Destination	Protocol	Length	Info
151	8.413312	121.192.180.66	192.168.1.199	FTP	103	Response: 220 Serv-U FTP Server v6.2 for WinSock ready...
154	8.413781	192.168.1.199	121.192.180.66	FTP	70	Request: USER anonymous
156	8.504209	121.192.180.66	192.168.1.199	FTP	124	Response: 331 User name okay, please send complete E-mail address as password.
159	8.504498	192.168.1.199	121.192.180.66	FTP	68	Request: PASS IEUser@
161	8.594284	121.192.180.66	192.168.1.199	FTP	95	Response: 530 Sorry, no ANONYMOUS access allowed.
175	8.781069	121.192.180.66	192.168.1.199	FTP	103	Response: 220 Serv-U FTP Server v6.2 for WinSock ready...
178	8.781604	192.168.1.199	121.192.180.66	FTP	68	Request: USER student
180	8.873309	121.192.180.66	192.168.1.199	FTP	90	Response: 331 User name okay, need password.
183	8.873766	192.168.1.199	121.192.180.66	FTP	69	Request: PASS software
185	8.963262	121.192.180.66	192.168.1.199	FTP	84	Response: 230 User logged in, proceed.
188	8.963799	192.168.1.199	121.192.180.66	FTP	68	Request: opts utf8 on
190	9.051165	121.192.180.66	192.168.1.199	FTP	75	Response: 501 Invalid option.
193	9.051459	192.168.1.199	121.192.180.66	FTP	59	Request: PWD
195	9.139164	121.192.180.66	192.168.1.199	FTP	85	Response: 257 "/" is current directory.
219	14.514851	192.168.1.199	121.192.180.66	FTP	60	Request: noop
221	14.608211	121.192.180.66	192.168.1.199	FTP	73	Response: 200 Command okay.
224	14.608769	192.168.1.199	121.192.180.66	FTP	70	Request: CWD /[redacted]/
226	14.701502	121.192.180.66	192.168.1.199	FTP	90	Response: 250 Directory changed to /[redacted]
229	14.707188	192.168.1.199	121.192.180.66	FTP	62	Request: TYPE A
231	14.801528	121.192.180.66	192.168.1.199	FTP	74	Response: 200 Type set to A.
234	14.802737	192.168.1.199	121.192.180.66	FTP	60	Request: PASV
236	14.902753	121.192.180.66	192.168.1.199	FTP	105	Response: 227 Entering Passive Mode (121,192,180,66,193,11)
249	15.087858	192.168.1.199	121.192.180.66	FTP	60	Request: LIST
251	15.196157	121.192.180.66	192.168.1.199	FTP	107	Response: 150 Opening ASCII mode data connection for /bin/ls.
260	15.288719	121.192.180.66	192.168.1.199	FTP	78	Response: 226 Transfer complete.

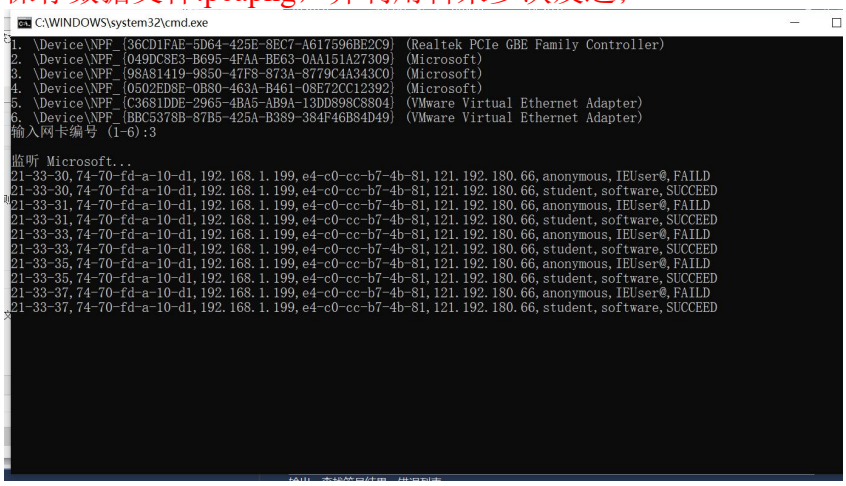
```
220 Serv-U FTP Server v6.2 for WinSock ready...
USER anonymous
331 User name okay, please send complete E-mail address as password.
PASS IEUser@
530 Sorry, no ANONYMOUS access allowed.
```

回调函数内登录名、口令和成功与否的判断：

```
if (com == "USER")
{
    string m_ip_message = get_request_m_ip_message(pkt_data);
    string user;
    ostringstream sout;
    for (int i = head + 5; pkt_data[i] != 13; i++)
    {
        sout << pkt_data[i];
    }

    user = sout.str();
    ftp[m_ip_message][0] = user;
}
if (com == "PASS")
{
    string m_ip_message = get_request_m_ip_message(pkt_data);
    string pass;
    ostringstream sout;
    for (int i = head + 5; pkt_data[i] != 13; i++)
    {
        sout << pkt_data[i];
    }
    pass = sout.str();
    ftp[m_ip_message][1] = pass;
}
if (com == "230 ")
{
    string m_ip_message = get_response_m_ip_message(pkt_data);
    ftp[m_ip_message][2] = "SUCCEED";
    print(header, m_ip_message);
}
if (com == "530 ")
{
    string m_ip_message = get_response_m_ip_message(pkt_data);
    ftp[m_ip_message][2] = "FAILD";
    print(header, m_ip_message);
}
```

保存数据文件.pcapng，并利用科来多次发送；



4 实验总结

对 TCP 的三次握手四次挥手有一定的理解，TCP 经过三次握手完成连接，经过四次挥手完成连接断开；FTP 是基于 TCP 的应用协议，支持 port 和 pasv 两种模式，实验了解了 FTP 通信协议过程，并对两个端口有一定理解。