

# 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  解析TCP段和FTP数据报

班    级            软件工程2018级1班

姓    名            方浩南

学    号            24320182203188

实验时间            2020年3月25日

2020 年 3 月 31 日

## 1 实验目的

观察 TCP 报文段并监听分析 FTP 协议

## 2 实验环境

Ubuntu 18.04, C语言, libpcap

## 3 实验结果

在实验三的基础上，针对这次要求设置pcap过滤器，只处理端口号为21的TCP数据包：

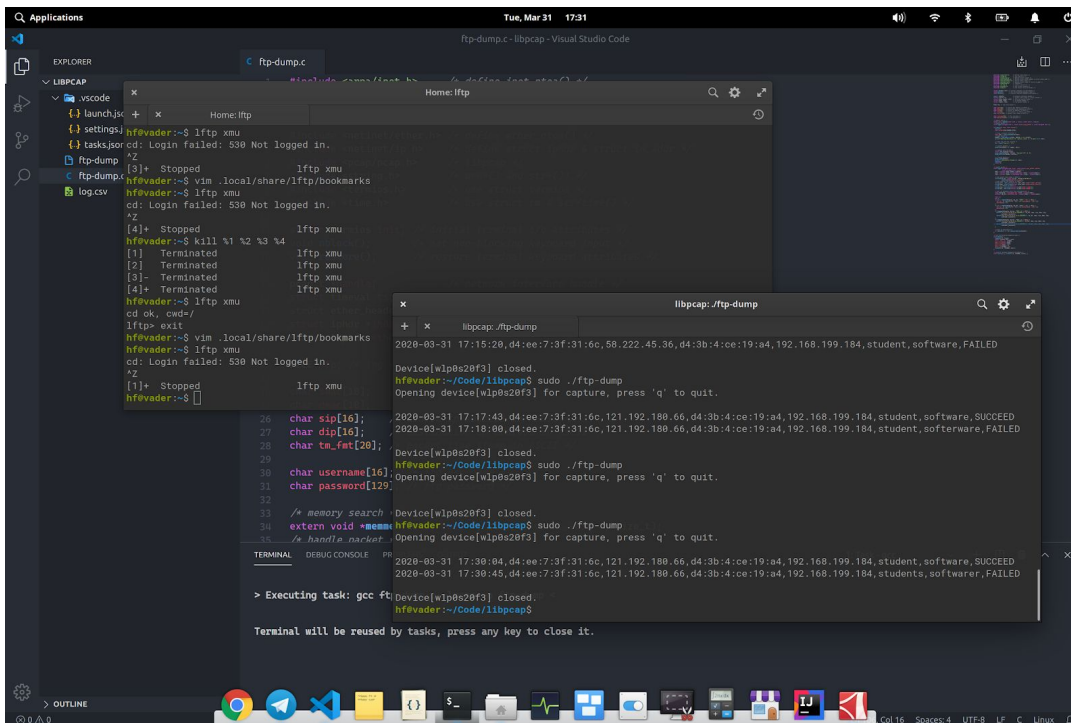
```
/* capture only tcp 53 */
struct bpf_program filter;
pcap_compile(handle, &filter, "tcp port 21", 0, 0);
pcap_setfilter(handle, &filter);
```

在数据报中搜索字符串USER、PASS、230和530并将相应的可见字符提取出来并记录：

```
/* get tcp datagram start and size(imprecise) */
void *datagram = (unsigned char *)thdr + sizeof(*thdr);
uint16_t dg_len = ihdr->tot_len - sizeof(*ihdr) - sizeof(*ehdr);

char *r;
int i;
if ((r = memmem(datagram, dg_len, "USER ", 5)) != NULL) {
    for (i = 0; isprint(r[5 + i]); ++i) username[i] = r[5 + i];
    username[i] = 0;
}
if ((r = memmem(datagram, dg_len, "PASS ", 5)) != NULL) {
    for (i = 0; isprint(r[5 + i]); ++i) password[i] = r[5 + i];
    password[i] = 0;
}
if (memmem(datagram, dg_len, "230", 3) != NULL) {
    printf("%s,%s,%s,%s,%s,%s,%s,SUCCEED\n", tm_fmt, smac, sip, dmac, dip,
        username, password);
    fprintf(fp, "%s,%s,%s,%s,%s,%s,%s,SUCCEED\n", tm_fmt, smac, sip, dmac, dip,
        username, password);
}
if (memmem(datagram, dg_len, "530", 3) != NULL) {
    printf("%s,%s,%s,%s,%s,%s,%s,FAILED\n", tm_fmt, smac, sip, dmac, dip,
        username, password);
    fprintf(fp, "%s,%s,%s,%s,%s,%s,%s,SUCCEED\n", tm_fmt, smac, sip, dmac, dip,
        username, password);
}
```

在收到服务器返回的代码后记录这次的用户名、密码和结果：



The screenshot shows a Linux desktop with a terminal window and a packet capture window. The terminal window displays the execution of a script named `ftp-dump.c`. The script uses `lftp` to attempt a login, and the output shows several failed login attempts. The packet capture window, titled `libpcap: /ftp-dump`, shows the capture of network traffic. It displays the IP addresses of the client and server, the port numbers, and the results of the login attempts. The output shows that the login attempts were successful, with the username `student` and password `software` being captured.

```
26 char sip[16];
27 char dip[16];
28 char tm_fmt[20];
29 char username[16];
30 char password[128];
31
32
33 /* memory search
34 extern void *memset;
35 /* handle packet:
36
37 2028-03-31 17:15:20, d4:ee:7:3f:31:6c, 56, 222.45.36, d4:3b:4:ce:19:a4, 192.168.199.184, student, software, FAILED
38 Device[wlp0s20f3] closed.
39 hfevader:~/Code/libpcap$ sudo ./ftp-dump
40 Opening device[wlp0s20f3] for capture, press 'q' to quit.
41 2028-03-31 17:17:43, d4:ee:7:3f:31:6c, 121, 192.180.66, d4:3b:4:ce:19:a4, 192.168.199.184, student, software, SUCCEEDED
42 2028-03-31 17:18:00, d4:ee:7:3f:31:6c, 121, 192.180.66, d4:3b:4:ce:19:a4, 192.168.199.184, student, software, FAILED
43 Device[wlp0s20f3] closed.
44 hfevader:~/Code/libpcap$ sudo ./ftp-dump
45 Opening device[wlp0s20f3] for capture, press 'q' to quit.
46 2028-03-31 17:30:04, d4:ee:7:3f:31:6c, 121, 192.180.66, d4:3b:4:ce:19:a4, 192.168.199.184, student, software, SUCCEEDED
47 2028-03-31 17:30:45, d4:ee:7:3f:31:6c, 121, 192.180.66, d4:3b:4:ce:19:a4, 192.168.199.184, students, software, FAILED
48 Device[wlp0s20f3] closed.
49 hfevader:~/Code/libpcap$
```

## 4 实验总结

通过这次实验对IP和TCP数据报有了具体的了解，对不同层级协议的前后关系有所体会，并且认识到FTP无报头、明文传输的特点。