

# 《计算机网络协议开发》实验报告

## 第 2 次实验： 逆向工程套接字编程实验

姓名： 元玉慧

学号： 101220151

10 级 计算机 系 4 班

邮箱： 15996250389@163.com

时间： 2013/03/22

实验补充材料：

实验中的设置为：host 114.212.191.33 and tcp 或者设置为 tcp.port == 5050

表示服务器的地址是：114.212.191.33，并且只处理 TCP 报文！

常用的过滤器：

源自某一 IP 地址（段） ip.src == value

IP 对匹配模式 源地址 <--> 目的地址

ip.src == value and ip.dst == value

ip.src == 10.180.22.205 and ip.dst == 10.180.22.209

匹配协议 ip tcp arp

匹配某一目的端口 TCP.dstport == value tcp.dstport == 23

## 一、实验目的

本次实验通过协议的逆向分析方法，掌握客户端套接字编程。

## 二、实验内容

1. 打开 wireshark，在 filter 中设置 ip.addr == 114.212.191.33；

【1】可以得到天气服务器的报文，可以看到抓取到了 3 次握手生成的数据包信息。

300 5.568890000	172.25.133.201	114.212.191.33	TCP	66 51558 > mmcc [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
301 5.570281000	114.212.191.33	172.25.133.201	TCP	66 mmcc > 51558 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=128
302 5.570402000	172.25.133.201	114.212.191.33	TCP	54 51558 > mmcc [ACK] Seq=1 Ack=1 Win=65700 Len=0

【2】输入 '#' 后，程序会退出，及通过 3 次握手正常退出。

300 5.568890000	172.25.133.201	114.212.191.33	TCP	66 51558 > mmcc [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
301 5.570281000	114.212.191.33	172.25.133.201	TCP	66 mmcc > 51558 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=128
302 5.570402000	172.25.133.201	114.212.191.33	TCP	54 51558 > mmcc [ACK] Seq=1 Ack=1 Win=65700 Len=0
10270 108.820496000	172.25.133.201	114.212.191.33	TCP	54 51558 > mmcc [FIN, ACK] Seq=1 Ack=1 Win=65700 Len=0
10271 108.822652000	114.212.191.33	172.25.133.201	TCP	56 mmcc > 51558 [FIN, ACK] Seq=1 Ack=2 Win=14720 Len=0
10272 108.822761000	172.25.133.201	114.212.191.33	TCP	54 51558 > mmcc [ACK] Seq=2 Ack=2 Win=65700 Len=0

【1】【2】中的 TCP 数据包都没有携带具体信息，所以 data 字段为空，没有 data 字段。

【3】输入南京，确认后，抓获 4 个报文：



123218	1530.908782000	172.25.133.201	114.212.191.33	TCP	87	51580 > mmcc [PSH, ACK] Seq=34 Ack=138 win=65700 Len=33
123219	1530.910145000	114.212.191.33	172.25.133.201	TCP	191	mmcc > 51580 [PSH, ACK] Seq=138 Ack=67 win=14720 Len=137
123222	1531.108595000	172.25.133.201	114.212.191.33	TCP	54	51580 > mmcc [ACK] Seq=67 Ack=275 win=65560 Len=0

0000	00 23 9c de d1 4a 00 26	c7 46 e0 8c 08 00 45 00	.#...J.& .F....E.
0010	00 49 6a 91 40 00 00 06	6c 45 ac 19 85 c9 72 d4	.!j.0.0. !e....r.
0020	bf 21 c9 7c 13 ba 85 92	52 69 68 37 75 17 50 18	! . .... Rih7u.P.
0030	40 29 c9 ac 00 00 01 41	6e 61 6e 6a 69 6e 67 00	@)....A nanjing.
0040	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
0050	00 00 00 00 00 00 01	00 00 00 00 00 00 00 00	.....

123218	1530.908782000	172.25.133.201	114.212.191.33	TCP	87	51580 > mmcc [PSH, ACK] Seq=34 Ack=138 win=65700 Len=33
123219	1530.910145000	114.212.191.33	172.25.133.201	TCP	191	mmcc > 51580 [PSH, ACK] Seq=138 Ack=67 win=14720 Len=137
123222	1531.108595000	172.25.133.201	114.212.191.33	TCP	54	51580 > mmcc [ACK] Seq=67 Ack=275 win=65560 Len=0

0000	00 23 9c de d1 4a 00 26	c7 46 e0 8c 08 00 45 00	.#...J.& .F....E.
0010	00 49 6a 91 40 00 00 06	6c 45 ac 19 85 c9 72 d4	.!j.0.0. !e....r.
0020	bf 21 c9 7c 13 ba 85 92	52 69 68 37 75 17 50 18	! . .... Rih7u.P.
0030	40 29 c9 ac 00 00 01 41	6e 61 6e 6a 69 6e 67 00	@)....A nanjing.
0040	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
0050	00 00 00 00 00 00 01	00 00 00 00 00 00 00 00	.....

[Calculated window size: 14720]			
[window size scaling factor: 128]			
[Checksum: 0xb0c2 [validation disabled]			
[Good checksum: False]			
[Bad checksum: False]			
[SEQ/ACK analysis]			
Data (137 bytes)			
Data: 43416e616e6a696e67000000000000000000000000000000...			
[Length: 137]			

000	00 26 c7 46 e0 8c 00 23	9c de d1 4a 08 00 45 00	.&.F...# ...J..E.
010	00 b1 8a 26 40 00 3f 06	4d 48 72 d4 bf 21 ac 19	...&@.?. Mhr...!
020	85 c9 13 ba c9 7c 68 37	75 17 85 92 52 8a 50 18	.... h7 u...R.P.
030	00 73 b0 c2 00 00 43 41	6e 61 6e 6a 69 6e 67 00	.S....CA nanjing.
040	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
050	00 00 00 00 00 00 07 dd	03 12 01 02 0b 26 00 00	.....
060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
070	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
080	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
090	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
0a0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
0b0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....

```

Please enter the given number to query
1.today
2.three days from today
3.custom day by yourself
(r>)back,(q>)cls,(#>)exit
=====
1
City: nanjing Today is: 2013/03/18 Weather information is as follows:
Today's Weather is: cloudy Wind-level: 11 Temp:38
2

```

【3.3】输入 2 后，确认，得到 3 个报文：

20678	81.905009000	114.212.191.33	172.25.132.42	TCP	191 [TCP Retransmission] mmcc > 56990 [PSH, ACK] Seq=1 Ack=34 W
20679	81.905065000	172.25.132.42	114.212.191.33	TCP	66 56990 > mmcc [ACK] Seq=34 Ack=138 Win=65560 Len=0 SLE=1 SRE
20871	83.773689000	172.25.132.42	114.212.191.33	TCP	87 56990 > mmcc [PSH, ACK] Seq=34 Ack=138 Win=65560 Len=33
20872	83.775472000	114.212.191.33	172.25.132.42	TCP	191 mmcc > 56990 [PSH, ACK] Seq=138 Ack=67 Win=14720 Len=137
20884	83.983795000	172.25.132.42	114.212.191.33	TCP	54 56990 > mmcc [ACK] Seq=67 Ack=275 Win=65424 Len=0

根据收到的报文确定需要填充的 sendline 信息，以及可以提取的 recvline 信息。

## 程序设计部分

weather/tcp.h

定义了要用的库文件以及端口号和城市的名字

```

1 #include<stdlib.h>
2 #include<stdio.h>
3 #include<sys/types.h>
4 #include<sys/socket.h>
5 #include<netinet/in.h>
6 #include<string.h>
7
8 #define MAXLINE 200
9 #define SERV_PORT 5050
10
11 char cname[35];
12

```

/weather/city.c

下面定义的发送数据域和接收数据域以及缓存信息的 buf 数组：

```

char sendline[MAXLINE], recvline[MAXLINE], buf[MAXLINE];
memset(sendline, 0, MAXLINE);
memset(recvline, 0, MAXLINE);
memset(buf, 0, MAXLINE);

```

根据接收到的报文的 data 域的字节判断输入的城市名字是否在服务器数据库中：

```

        if(recvline[0]=='B') {
            printf("sorry, Server does not have weather info for the input
city!\n");
            printf("Welcome to Wether Forecast Demo Program !\n");
            printf("Please input city name in chinese pinyin <e.g. nanjing
or beijing>\n");
            printf("<q> cls, <#> exit\n");
            continue;//City Wrong!
        }

        if(recvline[0]=='A') {
            system("clear");
            printf("Please enter the given number to query\n");
            printf("1. today\n");
            printf("2. three days from today\n");
            printf("3. custom day by your self\n");
            printf("<r> back, <q> cls, <#> exit\n");
            printf("=====\n");
            memset(cname, 0, 35);
            strcpy(cname,sendline+2);//store the cname
            break;    //City OK!
        }
    }
}

```

`\weather\query.c`

下面是在输入城市合法后查询 1,2,3 不同操作时对应的设置：

输入 1：

```

else if(strncmp(buf,"1",1)==0) {
    sendline[0]=1;
    sendline[1]='A';
    for(i=2; i<30; i++) sendline[i] = cname[i-2];
    send(sockfd, sendline, 33, 0);
    if(recv(sockfd, recvline, MAXLINE, 0) == 0){
        perror("The server terminated permaturely");
        exit(4);
    }
    year = ntohs(*( (short*)(recvline+32)));
    //printf("year  %02x\n",recvline[32]);
    printf("City: %s",cname);
    printf(" Today is: %d - %d - %d ", year, recvline[34], recvline[35]);
    printf(" Weather info is as follows:\n");
    printf("Today's weather is: ");
    switch(recvline[37]){
        case 0: printf(" shower "); break;
        case 1: printf(" clear "); break;
        case 2: printf(" cloudy "); break;
        case 3: printf(" rain "); break;
        case 4: printf(" fog "); break;
        default: printf("You are kidding! NO such weather! ");
    }
    break;
}

```

输入 2：

```

else if(strncmp(buf,"2",1)==0) {
    sendline[0]=1;
    sendline[1]='B';
    for(i=2; i<30; i++) sendline[i] = cname[i-2];

    send(sockfd, sendline, 33, 0);
    if(recv(sockfd, recvline, MAXLINE, 0) == 0){
        perror("The server terminated prematurely");
        exit(4);
    }

    printf("City: %s",cname);
    printf(" Today is: %d - %d - %d ", year, recvline[34], recvline[35]);
    printf(" Weather info is as follows:\n");

    printf("The 1th day's weather is: ");
    switch(recvline[37]){
        case 0: printf(" shower "); break;
        case 1: printf(" clear "); break;
        case 2: printf(" cloudy "); break;
        case 3: printf(" rain "); break;
        case 4: printf(" fog "); break;
        default: printf("You are kidding! NO such weather! ");
    }
break;

```

```

    printf("The 2th day's weather is: ");
    switch(recvline[40]){
        case 0: printf(" shower "); break;
        case 1: printf(" clear "); break;
        case 2: printf(" cloudy "); break;
        case 3: printf(" rain "); break;
        case 4: printf(" fog "); break;
        default: printf("You are kidding! NO such weather! ");
    }
break;
    }
    printf("Wind-level: %d Temp: %d \n",recvline[41], recvline[42]);

    printf("The 3rd day's weather is: ");
    switch(recvline[43]){
        case 0: printf(" shower "); break;
        case 1: printf(" clear "); break;
        case 2: printf(" cloudy "); break;
        case 3: printf(" rain "); break;
        case 4: printf(" fog "); break;
        default: printf("You are kidding! NO such weather! ");
    }
break;
    }
    printf("Wind-level: %d Temp: %d \n",recvline[44], recvline[45]);
} //case 2

```

输入 3 :

```

else if(strncmp(buf,"3",1)==0) {
    //
    memset(buf, 0, MAXLINE);
    if(fgets(buf, MAXLINE, stdin) != NULL){

        if(strncmp(buf,"q",1)==0) {
            system("clear");
            printf("Please enter the given number to query\n");
            printf("1. today\n");
            printf("2. three days from today\n");
            printf("3. custom day by your self\n");
            printf("<r> back, <q> cls, <#> exit\n");
            printf("=====\n");
            continue;
        }
        if(strncmp(buf,"#",1)==0) exit(0);
        if(strncmp(buf,"r",1)==0) {
            system("clear");
            printf("Welcome to Wether Forecast Demo Program !\n");
            printf("Please input city name in chinese pinyin <e.g. nanjing
or beijing>\n");
            printf("<q> cls, <#> exit\n");
            //
            city(sockfd);

```

```

        if(strncmp(buf,"9",1)>0){
            printf("Please enter the day number<below 10, e.g. 1 means
today>:\n");
            continue;
        }
        if(strncmp(buf,"6",1)>0){
            printf("Sorry, no given day's weather info for city %s !\n",
cname);
        }
        else if(strncmp(buf,"0",1)>0 && strncmp(buf,"6",1)<=0){
            sendline[0]=1;
            sendline[1]='A';
            for(i=2; i<30; i++) sendline[i] = cname[i-2];
            sendline[32]=buf[0];
            send(sockfd, sendline, 33, 0);
            if(recv(sockfd, recvline, MAXLINE, 0) == 0){
                perror("The server terminated permaturely");
                exit(4);
            }
            printf("City: %s",cname);
            printf(" Today is: %d - %d - %d ", year, recvline[34], recvline
[35]);

            printf(" Weather info is as follows:\n");
            printf("The %d day's weather is: ",sendline[32]-'0');

```

\weather\data\_cli.c

主要在 C.10 的基础上实现的。

添加修改如下：



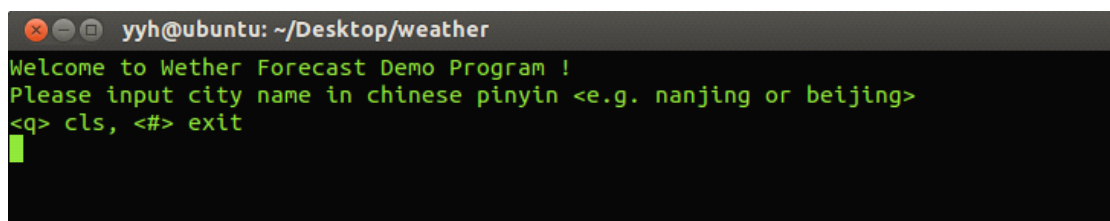
```
system("clear");
printf("Welcome to Wether Forecast Demo Program !\n");
printf("Please input city name in chinese pinyin <e.g. nanjing or beijing>\n");
printf("<q> cls, <#> exit\n");|

city(sockfd);
query(sockfd);
```

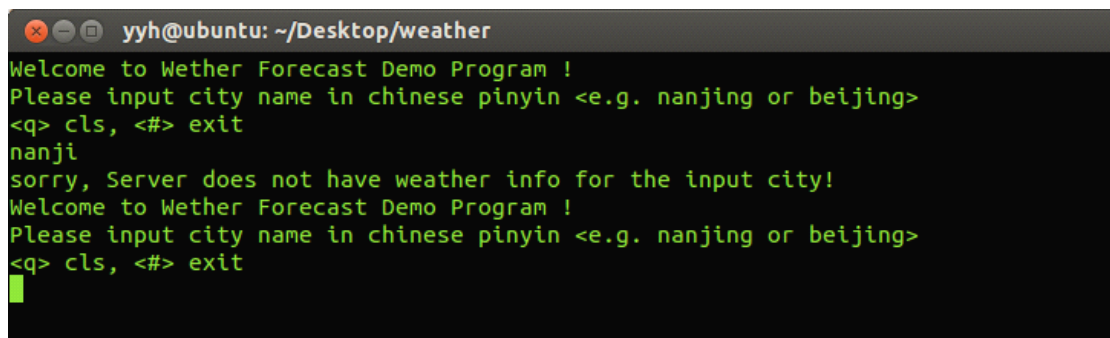
### 三、实验结果

对于 Linux 平台实验，请说明本次实验实现了哪些功能，并给出主要功能的实现截图。

通过编译执行 data\_cli.c 执行结果如下图：

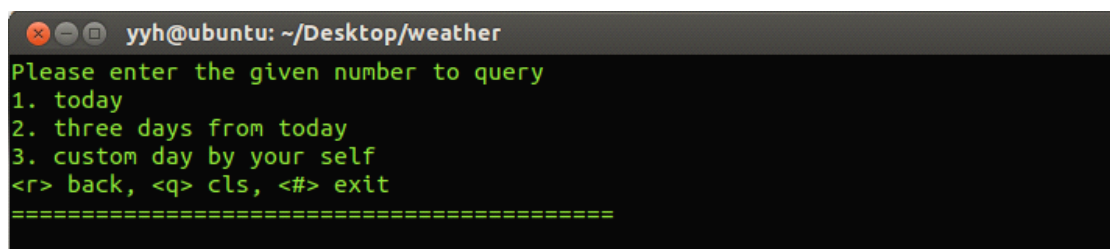


```
yyh@ubuntu: ~/Desktop/weather
Welcome to Wether Forecast Demo Program !
Please input city name in chinese pinyin <e.g. nanjing or beijing>
<q> cls, <#> exit
```



```
yyh@ubuntu: ~/Desktop/weather
Welcome to Wether Forecast Demo Program !
Please input city name in chinese pinyin <e.g. nanjing or beijing>
<q> cls, <#> exit
nanji
sorry, Server does not have weather info for the input city!
Welcome to Wether Forecast Demo Program !
Please input city name in chinese pinyin <e.g. nanjing or beijing>
<q> cls, <#> exit
```

输入南京后：



```
yyh@ubuntu: ~/Desktop/weather
Please enter the given number to query
1. today
2. three days from today
3. custom day by your self
<r> back, <q> cls, <#> exit
=====
```

一次查询不同类型模式：

- 1，显示当天的天气；
- 2，显示 3 天的天气；
- 3，可以输入要查询的天数，然后显示相应天数的天气；

```
yyh@ubuntu: ~/Desktop/weather
Please enter the given number to query
1. today
2. three days from today
3. custom day by your self
<r> back, <q> cls, <#> exit
=====
1
City: nanjing Today is: 2013 - 3 - 22 Weather info is as follows:
Today's weather is: shower Wind-level: 11 Temp: 20
2
City: nanjing Today is: 2013 - 3 - 22 Weather info is as follows:
The 1th day's weather is: shower Wind-level: 0 Temp: 0
The 2th day's weather is: shower Wind-level: 0 Temp: 0
The 3rd day's weather is: shower Wind-level: 0 Temp: 0
3
4
City: nanjing Today is: 2013 - 3 - 22 Weather info is as follows:
The 4 day's weather is: shower Wind-level: 0 Temp: 0
█
```

输入 r 可以返回到上一次操作界面；

输入 q 可以清屏操作；

输入 # 会直接退出程序：

```
yyh@ubuntu: ~/Desktop/weather
Please enter the given number to query
1. today
2. three days from today
3. custom day by your self
<r> back, <q> cls, <#> exit
=====
1
City: nanjing Today is: 2013 - 3 - 22 Weather info is as follows:
Today's weather is: rain Wind-level: 5 Temp: 32
#
yyh@ubuntu:~/Desktop/weather$ █
```

## 四、实验中遇到的问题及解决方案

没有解决的问题也可以写在这里。

错误反思：

【1】无法进入界面，输入后没有连接上服务器，是因为端口号没有修改，应该设置为 5050；

【2】city.c 的问题：

输入城市的名字，反映都是 B，就是说城市名不在数据库中，后来发现主要原因都是发送的数据包填充不正确，要参看做部分的 char 字段的内容，然后修改后，还有发送函数

Send(socketfd, sendline, strlen ( sendline ), 0)

中字段 str(sendline) 设置为固定值----33，然后发送报文 OK!

【3】query.c 的问题：

输入 1、2、3 选项可以按照不同的要求查询天气，但是输入 1 后，会报 segment fault，Core dumped，后来发现是

```
year = ntohs(*( (short*)recvline+32));
```

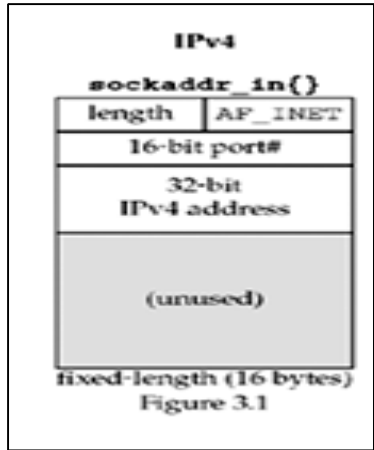
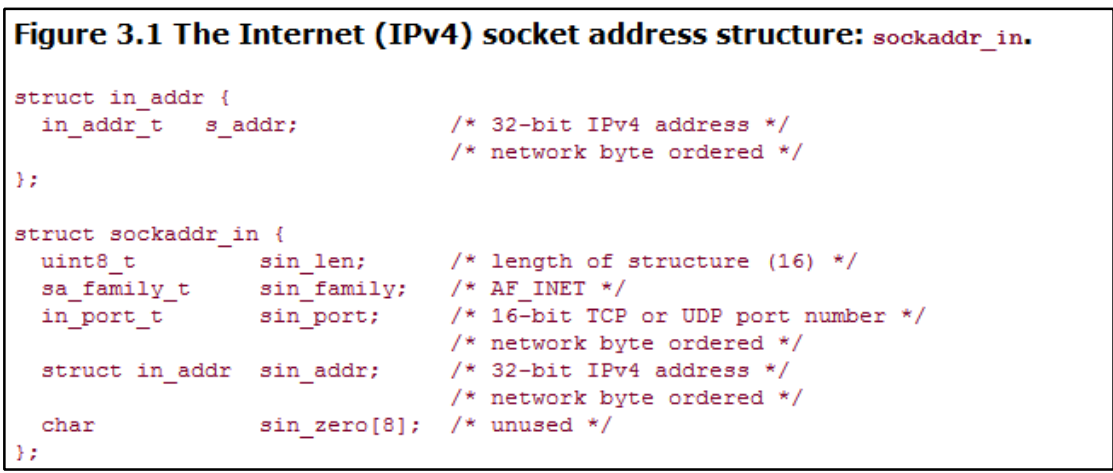
原来写成了 recvline[32]，区别字符串数组的[]操作时取单个字符，而+32 是去取偏移 32 处的地址。

【4】还有就是在读取报文的时候，wireshark 中报文的 data 段以左侧的 16 进制表示的字符为准，修改了很多 '0' 变成了 0；主要是在调用函数 strcmp() 时！

【5】测试 OK!

## 五、实验的启示/意见和建议

此次试验只是实现了客户端要求的基本功能，并没有涉及发送和接收的 TCP 数据结构：



可以设置 sin\_len 字段为想发送的报文和要接收的报文的长度，并把报文填充到 unused 字段中。

同时在设计向服务器发送请求报文和服务器向客户端发送报文时都是只发送了一次报文，在

局域网中可能不存在问题,但是此设计在万维网中是存在致命缺陷的( TCP 报文重发机制!)

**附：**本次实验你总共用了多长时间？包括学习时间、编写代码时间和测试时间。( 仅做统计用，时间长短不影响本次实验的成绩。)

实现客户端的基本功能大概用时为 18 小时吧，包括从开始到看懂报文，解析报文，实现代码，修改代码。

**实验心得：**这次实验的 90%都是自己独立完成的，在实现的过程中有和同学讨论过一些问题的处理方法和得到了同学的一些指点，发现某些同学去网上搜集整理学习信息的能力目前暂时高于我啊，我要继续努力，每天进步一点点，相信自己会有一天会成为自己想成为的“他”!! 加入谷歌，成为世界上最优秀的 IT 精英！

还有这学期要好好的看一下那本套接字编程的大块头，学习一下鸟哥的书，感觉这学期会很累很累很充实很充实，还要安排足够的时间准备托福，永远不放弃，这才是自己！