

华东师范大学软件工程学院实验报告

实验课程：无线网络安全	姓名：	学号：
实验名称： Wireshark无线抓包实验	实验日期：2023.11.5	指导老师：张磊

实验目的

- 通过抓取Telnet连接中的明文用户名和口令，了解Telnet远程连接的工作过程，对网络攻击有一个初步的认识。

实验内容与实验步骤

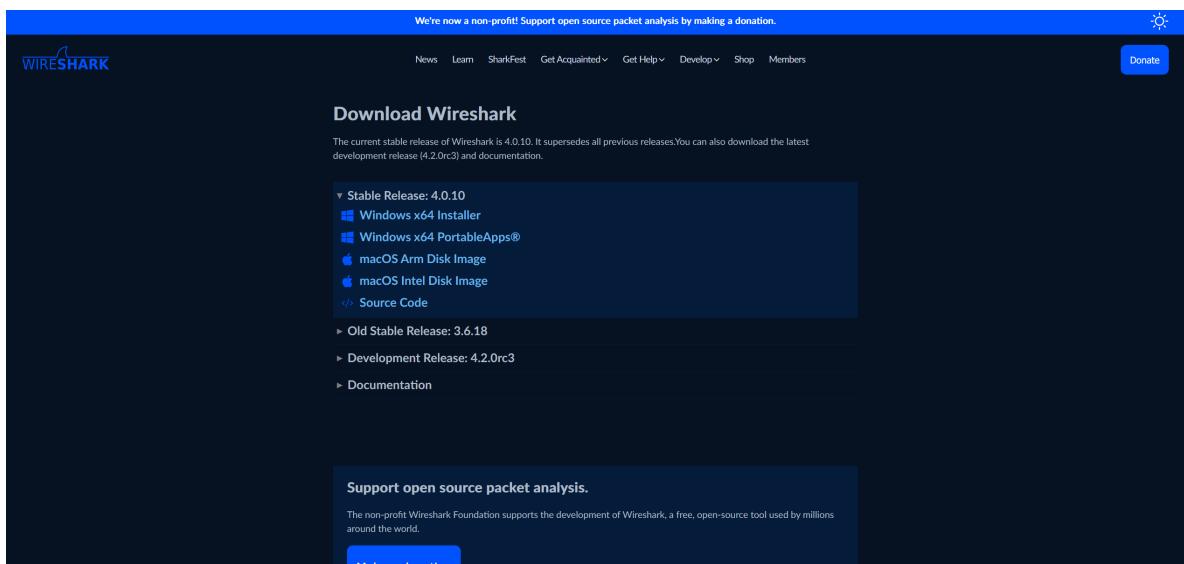
- 下载并安装Wireshark
- 要求搭建Telnet服务器
- 抓取明文用户名和口令

实验环境

- Wireshark
- VMware Workstation（用于运行Ubuntu系统）
- Telnet服务器

实验过程与分析

1. 实验准备：[Wireshark · Go Deep](#) 官网下载Wireshark，并按照程序指引安装Wireshark。



创建虚拟机，运行Ubuntu系统，并将虚拟机网络设置为“桥接模式”，保证虚拟机与主机之间处于同一网段。输入相关指令下载必要组件并实现搭建telnet服务器。

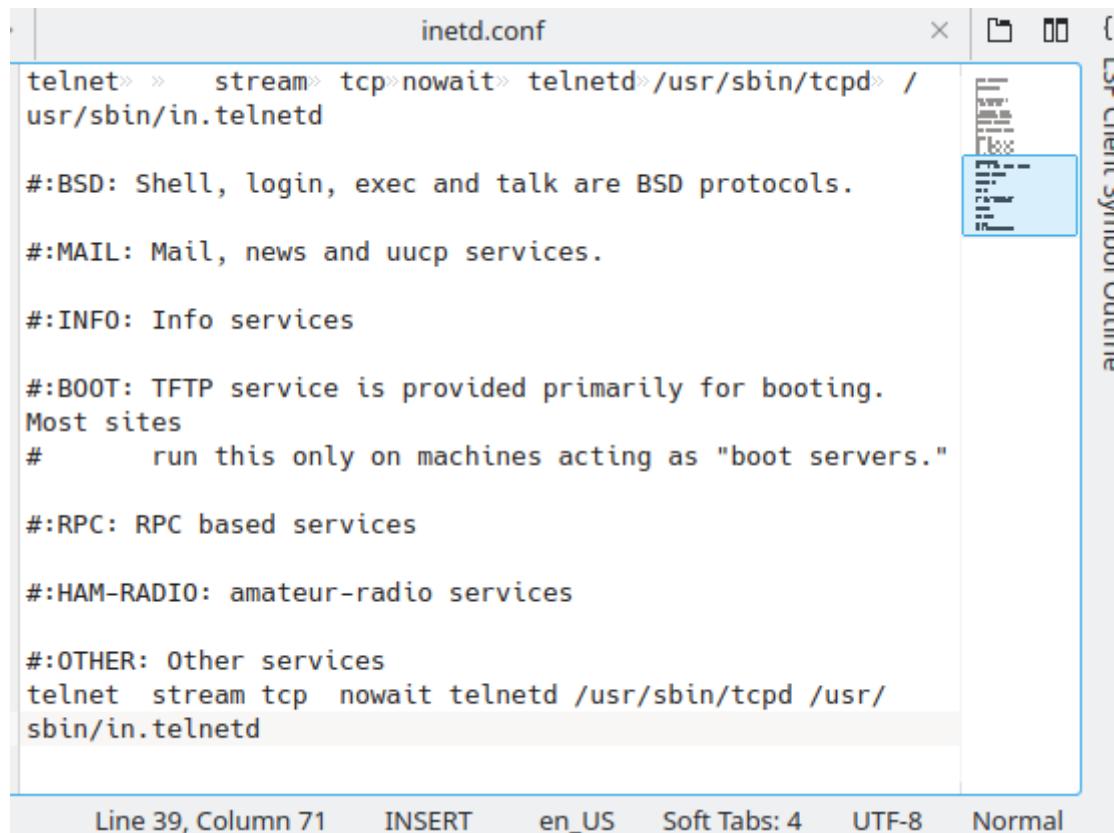
```
akari@akari-virtual-machine:~$ sudo apt-get install openbsd-inetd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  tcpd
The following NEW packages will be installed:
  openbsd-inetd tcpd
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 51.5 kB of archives.
After this operation, 206 kB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 https://mirror.sjtu.edu.cn/ubuntu jammy/universe amd64 tcpd amd64 7.6.q-31build2 [25.2 kB]
Get:2 https://mirror.sjtu.edu.cn/ubuntu jammy/universe amd64 openbsd-inetd amd64 0.20160825-5 [26.3 kB]
Fetched 51.5 kB in 0s (325 kB/s)
Selecting previously unselected package tcpd.
(Reading database ... 200972 files and directories currently installed.)
Preparing to unpack .../tcpd_7.6.q-31build2_amd64.deb ...
Unpacking tcpd (7.6.q-31build2) ...
Selecting previously unselected package openbsd-inetd.
Preparing to unpack .../openbsd-inetd_0.20160825-5_amd64.deb ...
Unpacking openbsd-inetd (0.20160825-5) ...
Setting up tcpd (7.6.q-31build2) ...
Setting up openbsd-inetd (0.20160825-5) ...
Created symlink /etc/systemd/system/multi-user.target.wants/inetd.service → /lib/systemd/system/inetd.service.
Processing triggers for man-db (2.10.2-1)
```

```
akari@akari-virtual-machine:~$ sudo apt-get install telnetd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  telnetd
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 40.7 kB of archives.
After this operation, 113 kB of additional disk space will be used.
Get:1 https://mirror.sjtu.edu.cn/ubuntu jammy/universe amd64 telnetd amd64 0.17-44build1 [40.7 kB]
Fetched 40.7 kB in 0s (299 kB/s)
Selecting previously unselected package telnetd.
(Reading database ... 200992 files and directories currently installed.)
Preparing to unpack .../telnetd_0.17-44build1_amd64.deb ...
Unpacking telnetd (0.17-44build1) ...
Setting up telnetd (0.17-44build1) ...
Adding user telnetd to group utmp
Processing triggers for man-db (2.10.2-1) ...
```

使用 ifconfig 指令获得搭建的telnet服务器的ip地址。如图，本次实验的ip地址为192.168.50.56。

```
akari@akari-virtual-machine:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.50.56  netmask 255.255.255.0  broadcast 192.168.50.255
      inet6 fe80::7264:8eb:b9d3:8c84  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:88:5f:f0  txqueuelen 1000  (Ethernet)
          RX packets 52552  bytes 74699319 (74.6 MB)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 7184  bytes 579927 (579.9 KB)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
      inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
          RX packets 274  bytes 24127 (24.1 KB)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 274  bytes 24127 (24.1 KB)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```



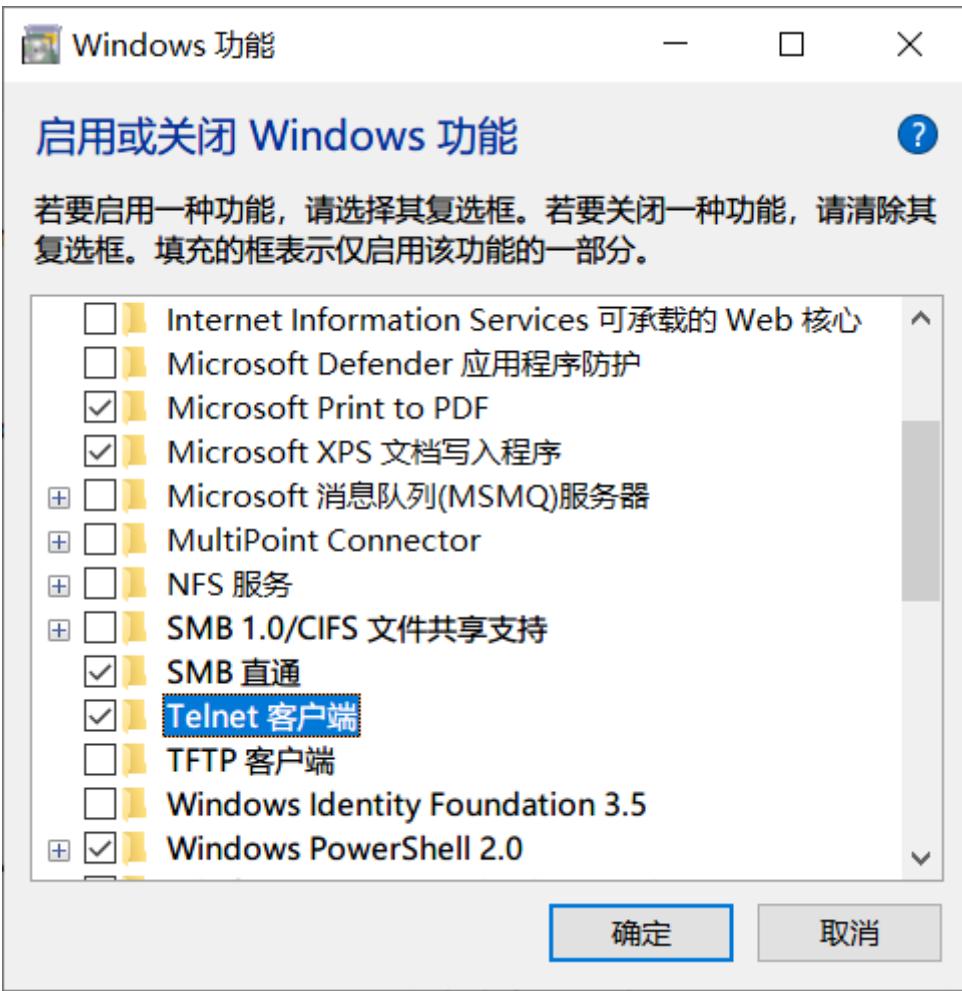
```
inetd.conf
telnet  stream  tcp nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.telnetd
#:BSD: Shell, login, exec and talk are BSD protocols.
#:MAIL: Mail, news and uucp services.
#:INFO: Info services
#:BOOT: TFTP service is provided primarily for booting.
Most sites
#       run this only on machines acting as "boot servers."
#:RPC: RPC based services
#:HAM-RADIO: amateur-radio services
#:OTHER: Other services
telnet  stream  tcp nowait  telnetd /usr/sbin/tcpd /usr/sbin/in.telnetd
```

Line 39, Column 71 INSERT en_US Soft Tabs: 4 UTF-8 Normal

确认telnet服务器已经成功连接本机

```
akari@akari-virtual-machine:~$ netstat -a |grep telnet
tcp        0      0 0.0.0.0:telnet          0.0.0.0:*                  LISTEN
```

除此之外，我们还需要在主机Windows上安装Telnet客户端，在控制面板-程序和功能-启用或关闭Windows功能里，勾选Telnet客户端即可。



至此，实验准备完成。

2. 实验过程：

完成准备后，打开电脑的cmd窗口，此时打开Wireshark，选择抓取与虚拟机桥接的网卡，设置Wireshark过滤器，以使得最终抓包结果为与telnet服务器相关的数据包。开启抓包功能。

然后在cmd窗口输入 telnet 192.168.50.56 并输入事先设置好的账户，登录到telnet服务器中。此次实验，输入的账户为akari，输入的密码为123456。

```
Windows PowerShell
版权所有 (C) Microsoft Corporation。保留所有权利。
尝试新的跨平台 PowerShell https://aka.ms/pscore6
PS C:\Users\Akai_Akari> telnet 192.168.50.56
```

可以看到弹出了远程主机的终端字符，说明已经通过Telnet与之建立连接。

```

Ubuntu 22.04.3 LTS
akari-virtual-machine login: akari
Password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-36-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

25 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Sun Nov 12 16:53:14 CST 2023 from DESKTOP-P1M22BS on pts/2
akari@akari-virtual-machine:~$ |

```

输入任意指令，本次实验为 ls

```

akari@akari-virtual-machine:~$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
akari@akari-virtual-machine:~$ |

```

输入指令 exit 退出telnet服务器。此时，关闭Wireshark的抓包功能。抓包过程结束。

3.实验结果分析：

在Wireshark上可以查看到此次实验的相关数据包。

下列是TCP连接时，“三次握手”的过程。

76 2.355204	192.168.50.18	192.168.50.56	TCP	66 62206 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
78 2.355422	192.168.50.56	192.168.50.18	TCP	66 23 → 62206 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
80 2.355505	192.168.50.18	192.168.50.56	TCP	54 62206 → 23 [ACK] Seq=1 Ack=1 Win=2102272 Len=0

下列是请求登录服务器时，telnet服务器返回的数据包，申请本机输入账号。

117 2.451192	192.168.50.18	192.168.50.56	TELNET	57 Telnet Data ...
119 2.451307	192.168.50.56	192.168.50.18	TELNET	103 Telnet Data ...
121 2.451336	192.168.50.18	192.168.50.56	TELNET	57 Telnet Data ...
172 4.811554	192.168.50.18	192.168.50.56	TELNET	55 Telnet Data ...
176 4.812130	192.168.50.56	192.168.50.18	TELNET	60 Telnet Data ...
186 6.163359	192.168.50.18	192.168.50.56	TELNET	55 Telnet Data ...
188 6.164094	192.168.50.56	192.168.50.18	TELNET	60 Telnet Data ...
195 7.211328	192.168.50.18	192.168.50.56	TELNET	55 Telnet Data ...
197 7.212002	192.168.50.56	192.168.50.18	TELNET	60 Telnet Data ...
206 7.891197	192.168.50.18	192.168.50.56	TELNET	55 Telnet Data ...
208 7.891602	192.168.50.56	192.168.50.18	TELNET	60 Telnet Data ...
215 8.211099	192.168.50.18	192.168.50.56	TELNET	55 Telnet Data ...
217 8.211637	192.168.50.56	192.168.50.18	TELNET	60 Telnet Data ...
244 13.147530	192.168.50.18	192.168.50.56	TELNET	56 Telnet Data ...
246 13.148135	192.168.50.56	192.168.50.18	TELNET	60 Telnet Data ...

下列是本机输入账号时发送的数据包。发现每当本机键盘输入账号时，发送一个数据包到 192.168.50.56。

172 4.811554	192.168.50.18	192.168.50.56	TELNET	55 Telnet Data ...
176 4.812130	192.168.50.56	192.168.50.18	TELNET	60 Telnet Data ...
186 6.163359	192.168.50.18	192.168.50.56	TELNET	55 Telnet Data ...
188 6.164094	192.168.50.56	192.168.50.18	TELNET	55 Telnet Data ...
195 7.211328	192.168.50.18	192.168.50.56	TELNET	55 Telnet Data ...
197 7.212002	192.168.50.56	192.168.50.18	TELNET	55 Telnet Data ...
206 7.891197	192.168.50.18	192.168.50.56	TELNET	55 Telnet Data ...
208 7.891602	192.168.50.56	192.168.50.18	TELNET	55 Telnet Data ...
215 8.211099	192.168.50.18	192.168.50.56	TELNET	55 Telnet Data ...
217 8.211637	192.168.50.56	192.168.50.18	TELNET	55 Telnet Data ...
244 13.147530	192.168.50.18	192.168.50.56	TELNET	56 Telnet Data ...
246 13.148135	192.168.50.56	192.168.50.18	TELNET	60 Telnet Data ...

服务器收到后，会返回收到的字符以表示成功接收。以下为了连贯，不再展示服务器发回的数据包。

176 4.812130	192.168.50.56	192.168.50.18	TELNET	60 Telnet Data ...
186 6.163359	192.168.50.18	192.168.50.56	TELNET	55 Telnet Data ...
188 6.164094	192.168.50.56	192.168.50.18	TELNET	60 Telnet Data ...
195 7.211328	192.168.50.18	192.168.50.56	TELNET	55 Telnet Data ...
197 7.212082	192.168.50.56	192.168.50.18	TELNET	60 Telnet Data ...
206 7.891197	192.168.50.18	192.168.50.56	TELNET	55 Telnet Data ...
208 7.891682	192.168.50.56	192.168.50.18	TELNET	60 Telnet Data ...
215 8.211999	192.168.50.18	192.168.50.56	TELNET	55 Telnet Data ...
217 8.211637	192.168.50.56	192.168.50.18	TELNET	60 Telnet Data ...
244 13.147530	192.168.50.18	192.168.50.56	TELNET	56 Telnet Data ...
244 13.148135	192.168.50.56	192.168.50.18	TELNET	60 Telnet Data ...

接下来我们便可以从主机向服务器发送的数据包中依次获得用户名的每一个字母。

> Frame 188: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{015A5815-9060-45AD-874D-D19424
> Ethernet II, Src: VMware_88:5f:f0 (00:0c:29:88:5f:f0), Dst: ASUSTekC_6c:4f:be (08:bf:b8:6c:4f:be)
> Internet Protocol Version 4, Src: 192.168.50.56, Dst: 192.168.50.18
> Transmission Control Protocol, Src Port: 23, Dst Port: 62206, Seq: 95, Ack: 60, Len: 1
Telnet
Data: k

> Frame 206: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{015A5815-9060-45AD-874D-D19424
> Ethernet II, Src: ASUSTekC_6c:4f:be (08:bf:b8:6c:4f:be), Dst: VMware_88:5f:f0 (00:0c:29:88:5f:f0)
> Internet Protocol Version 4, Src: 192.168.50.18, Dst: 192.168.50.56
> Transmission Control Protocol, Src Port: 62206, Dst Port: 23, Seq: 62, Ack: 98, Len: 1
Telnet
Data: r

> Frame 215: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{015A5815-9060-45AD-874D-D19424
> Ethernet II, Src: ASUSTekC_6c:4f:be (08:bf:b8:6c:4f:be), Dst: VMware_88:5f:f0 (00:0c:29:88:5f:f0)
> Internet Protocol Version 4, Src: 192.168.50.18, Dst: 192.168.50.56
> Transmission Control Protocol, Src Port: 62206, Dst Port: 23, Seq: 63, Ack: 99, Len: 1
Telnet
Data: i

> Frame 244: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_{015A5815-9060-45AD-874D-D19424
> Ethernet II, Src: ASUSTekC_6c:4f:be (08:bf:b8:6c:4f:be), Dst: VMware_88:5f:f0 (00:0c:29:88:5f:f0)
> Internet Protocol Version 4, Src: 192.168.50.18, Dst: 192.168.50.56
> Transmission Control Protocol, Src Port: 62206, Dst Port: 23, Seq: 64, Ack: 100, Len: 2
Telnet
Data: \r\n

下列是输入账号后，telnet服务器发送的请求本机输入密码的数据包。

> Frame 250: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF_{015A5815-9060-45AD-874D-D19424
> Ethernet II, Src: VMware_88:5f:f0 (00:0c:29:88:5f:f0), Dst: ASUSTekC_6c:4f:be (08:bf:b8:6c:4f:be)
> Internet Protocol Version 4, Src: 192.168.50.56, Dst: 192.168.50.18
> Transmission Control Protocol, Src Port: 23, Dst Port: 62206, Seq: 102, Ack: 66, Len: 10
Telnet
Data: Password:

下列是本机输入密码时发送的数据包。发现每当本机键盘输入相关字母密码时，发送一个数据包到192.168.50.56。此时服务器不会将密码再返回主机。

270 14.475493	192.168.50.18	192.168.50.56	TELNET	55 Telnet Data ...
274 14.659235	192.168.50.18	192.168.50.56	TELNET	55 Telnet Data ...
278 14.867610	192.168.50.18	192.168.50.56	TELNET	55 Telnet Data ...
282 15.083190	192.168.50.18	192.168.50.56	TELNET	55 Telnet Data ...
289 15.283190	192.168.50.18	192.168.50.56	TELNET	55 Telnet Data ...
305 15.484045	192.168.50.18	192.168.50.56	TELNET	55 Telnet Data ...
315 15.803406	192.168.50.18	192.168.50.56	TELNET	56 Telnet Data ...

> Frame 270: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{015A5815-9060-45AD-874D-D19424
> Ethernet II, Src: ASUSTekC_6c:4f:be (08:bf:b8:6c:4f:be), Dst: VMware_88:5f:f0 (00:0c:29:88:5f:f0)
> Internet Protocol Version 4, Src: 192.168.50.18, Dst: 192.168.50.56
> Transmission Control Protocol, Src Port: 62206, Dst Port: 23, Seq: 66, Ack: 112, Len: 1
Telnet
Data: 1

```

> Frame 274: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{015A5815-9060-45AD-874D-D19424
> Ethernet II, Src: ASUSTekC_6c:4f:be (08:bf:b8:6c:4f:be), Dst: VMware_88:5f:f0 (00:0c:29:88:5f:f0)
> Internet Protocol Version 4, Src: 192.168.50.18, Dst: 192.168.50.56
> Transmission Control Protocol, Src Port: 62206, Dst Port: 23, Seq: 67, Ack: 112, Len: 1
  ▼ Telnet
    Data: 2

> Frame 278: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{015A5815-9060-45AD-874D-D19424
> Ethernet II, Src: ASUSTekC_6c:4f:be (08:bf:b8:6c:4f:be), Dst: VMware_88:5f:f0 (00:0c:29:88:5f:f0)
> Internet Protocol Version 4, Src: 192.168.50.18, Dst: 192.168.50.56
> Transmission Control Protocol, Src Port: 62206, Dst Port: 23, Seq: 68, Ack: 112, Len: 1
  ▼ Telnet
    Data: 3

> Frame 282: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{015A5815-9060-45AD-874D-D19424
> Ethernet II, Src: ASUSTekC_6c:4f:be (08:bf:b8:6c:4f:be), Dst: VMware_88:5f:f0 (00:0c:29:88:5f:f0)
> Internet Protocol Version 4, Src: 192.168.50.18, Dst: 192.168.50.56
> Transmission Control Protocol, Src Port: 62206, Dst Port: 23, Seq: 69, Ack: 112, Len: 1
  ▼ Telnet
    Data: 4

> Frame 289: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{015A5815-9060-45AD-874D-D19424
> Ethernet II, Src: ASUSTekC_6c:4f:be (08:bf:b8:6c:4f:be), Dst: VMware_88:5f:f0 (00:0c:29:88:5f:f0)
> Internet Protocol Version 4, Src: 192.168.50.18, Dst: 192.168.50.56
> Transmission Control Protocol, Src Port: 62206, Dst Port: 23, Seq: 70, Ack: 112, Len: 1
  ▼ Telnet
    Data: 5

> Frame 305: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{015A5815-9060-45AD-874D-D19424
> Ethernet II, Src: ASUSTekC_6c:4f:be (08:bf:b8:6c:4f:be), Dst: VMware_88:5f:f0 (00:0c:29:88:5f:f0)
> Internet Protocol Version 4, Src: 192.168.50.18, Dst: 192.168.50.56
> Transmission Control Protocol, Src Port: 62206, Dst Port: 23, Seq: 71, Ack: 112, Len: 1
  ▼ Telnet
    Data: 6

```

下列是中断TCP连接时，“四次挥手”的过程。

1139 24.258998	192.168.50.18	192.168.50.56	TCP	54 55898 + 23 [ACK] Seq=84 Ack=935 Win=2181248 Len=0
1140 24.251818	192.168.50.18	192.168.50.56	TCP	54 [TCP Dup ACK 1139@1] 55898 + 23 [ACK] Seq=84 Ack=935 Win=2181248 Len=0
1141 24.251218	192.168.50.18	192.168.50.56	TCP	54 55898 + 23 [FIN, ACK] Seq=84 Ack=935 Win=2181248 Len=0
1143 24.251345	192.168.50.56	192.168.50.18	TCP	68 23 + 55898 [ACK] Seq=935 Ack=85 Win=64256 Len=0

可以看到，主机终端每输入一个字符，该字符便会以明文形式发送给主机，没有经过任何加密，因此，Telnet通信非常不安全。目前绝大多数服务器已经停用Telnet，改为更加安全的SSH协议。

至此，实验分析过程结束。

实验结果总结

- 通过此次实验，我们了解了如何安装Wireshark软件以及使用Wireshark软件进行数据包的抓取。我们同样学习了如何在Ubuntu系统上搭建telnet服务器并使该服务器与本机连接且获取服务器的相关信息。通过对数据包的分析，我们观察到了TCP连接的三次握手和四次挥手过程，了解了用户与telnet服务器交互时双方的数据包发送过程并且抓取到了用户的明文输入以及口令，对无线网抓包过程以及TCP连接过程有了进一步理解，获得了宝贵的知识。