

## ***Lab: MiniSniff***

### **Part I: Understanding minisniff:**

Study the source code of a raw packet sniffer called minisniff, which is available at <http://isis.poly.edu/kulesh/stuff/src/minisniff.tar.gz>. The source code is well documented and has enough explanation to walk you through each step of the sniffing process. Your task for this part is to understand minisniff completely and answer the following questions:

- 1) What library does minisniff use to capture packets? Where in the web can you find more information about this library?
- 2) Do some research and describe the advantages/disadvantage of using this library? Do not blindly copy and paste material from the web. Try to understand the material you find and write what you understood.
- 3) Are there any alternative libraries available to capture packets? (Open source only)
- 4) Explain the purpose of the following functions:
  - a. *pcap\_lookupdev*
  - b. *pcap\_open\_live*
  - c. *pcap\_lookupnet*
  - d. *pcap\_compile*
  - e. *pcap\_setfilter*
  - f. *pcap\_next*
  - g. *pcap\_loop*
  - h. *pcap\_dispatch*
- 5) There are five layers in the TCP/IP stack (application, transport, network, link, and physical). Up to what layer can minisniff decode data from the captured packets? Justify your answer using the code.

### **Part II: Extending minisniff**

- 1) Modify minisniff to capture, decode and display the password from a telnet session.
  - 2) Provide new code and screenshots.
- 
- 

### **Lab Instructions:**

You may need software like VMware or VirtualBox to set up a virtual machine to complete the lab.

Platform: Ubuntu (or other Unix-like operating systems)

1. set up a Linux machine. <http://blog.csdn.net/u013142781/article/details/50529030>
2. download minisniff from <http://isis.poly.edu/kulesh/stuff/src/minisniff.tar.gz>

3. download [libpcap-1.8.1.tar.gz](http://www.tcpdump.org/libpcap-1.8.1.tar.gz) from <http://www.tcpdump.org/>.
4. install libpcap
  - (1) you need to install all other required packages.

```
sudo apt-get install flex bison
```
  - (2) unzip archive file of libpcap, and cd the directory of libpcap

```
tar -zxvf libpcap-1.8.1.tar.gz
cd libpcap-1.8.1
```
  - (3) install libpcap

```
./configure
make
sudo make install
```
5. compile minisniff
  - (1) unzip minisniff.tar.gz and cd the directory of minisniff..

```
tar -zxvf minisniff.tar.gz
cd minisniff
```
  - (2) compile minisniff (see the instructions in README file of minisniff).

```
./make
```
6. run minisniff to capture 20 packets. (A small number will be better)

```
sudo ./minisniff 20
```
7. The program will be blocked due to its waiting for packages from network. The easiest way to make it work is opening a web browser or running “wget www.baidu.com” in another shell. If you have no internet, you can establish a telnet connection to this machine, which will be discussed below.

### **Possible Errors:**

#### **Error #1: "libpcap.so.1: cannot open shared object file"**

```
$ sudo ./minisniff 20
./minisniff: error while loading shared libraries: libpcap.so.1:
cannot open shared object file: No such file or directory
```

```
$ locate libpcap.so
/usr/lib/libpcap.so.0.8
/usr/lib/libpcap.so.1.0.0
```

**Case 1:** “libpcap.so.1” does not exist.

**Solution:** change the link of libpcap.so.

```
$ sudo ln -s /usr/lib/libpcap.so.1.0.0 /usr/lib/libpcap.so.1
```

**Case 2:** “/usr/lib/libpcap.so.1” already exists.

**Solution:** Update the cache of linker.

```
$ sudo ldconfig
```

Error #2: "pcap\_lookupdev: no suitable device found" or  
"./minisniff: pcap\_open\_live: ens33: You don't have permission to capture on that device (socket: Operation not permitted) "

```
$ ./minisniff 50
./minisniff: pcap_lookupdev: no suitable device found

$ ./minisniff 50
$ ./minisniff: pcap_open_live: ens33: You don't have permission to
capture on that device (socket: Operation not permitted)
```

Solution: you should use "sudo ./minisniff 50" or under "root" account.

### How to Enable Telnet service?

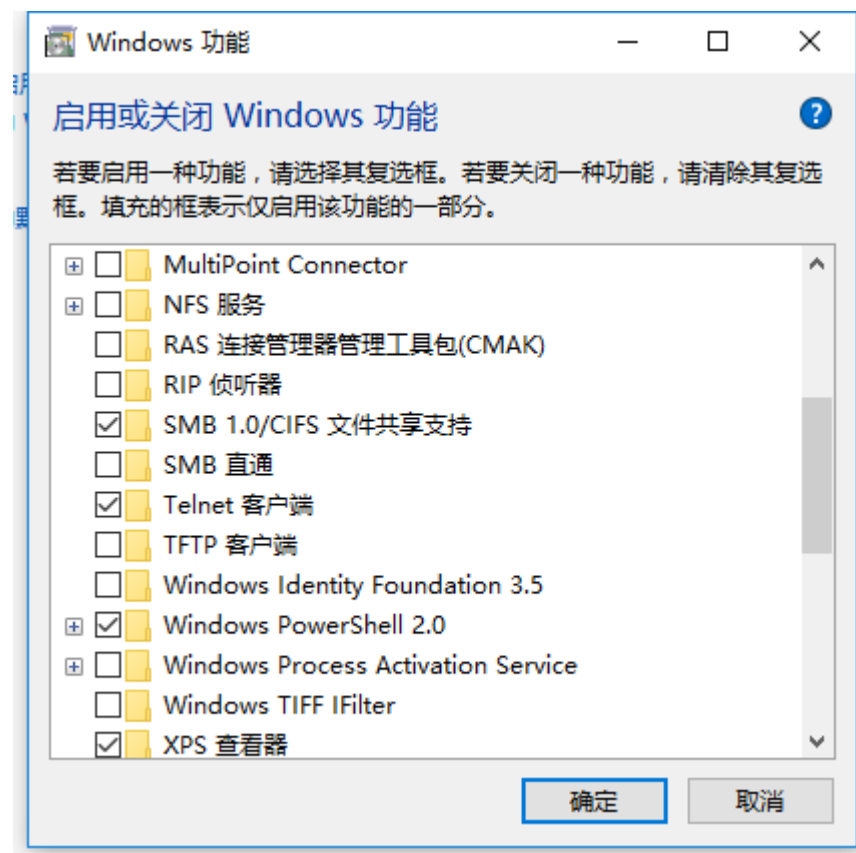
See <http://www.cyberciti.biz/faq/ubuntu-linux-enable-telnet-service/>

```
$ sudo apt-get install telnetd
$ sudo /etc/init.d/openbsd-inetd restart
```

### How to connect to a Telnet server?

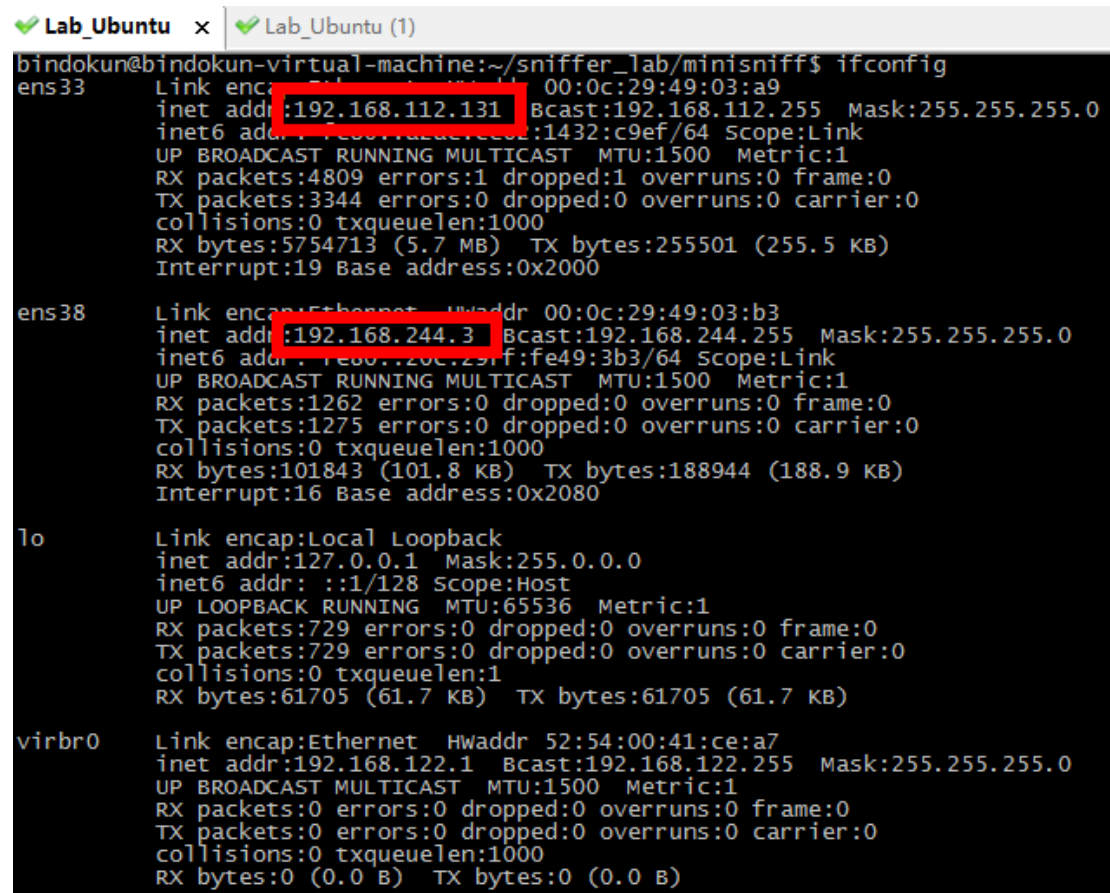
#### Windows:

1. “控制面板” -> “程序” -> “启用或关闭 Windows 功能”.



Enable “Telnet 客户端” and click “确定”. It may need reboot.

2. Open command line of windows and type “telnet ip\_addr”. ip\_addr is the ip of machine which runs Telnet service (Tip: running “ifconfig” on target machine to get ip address). For example:



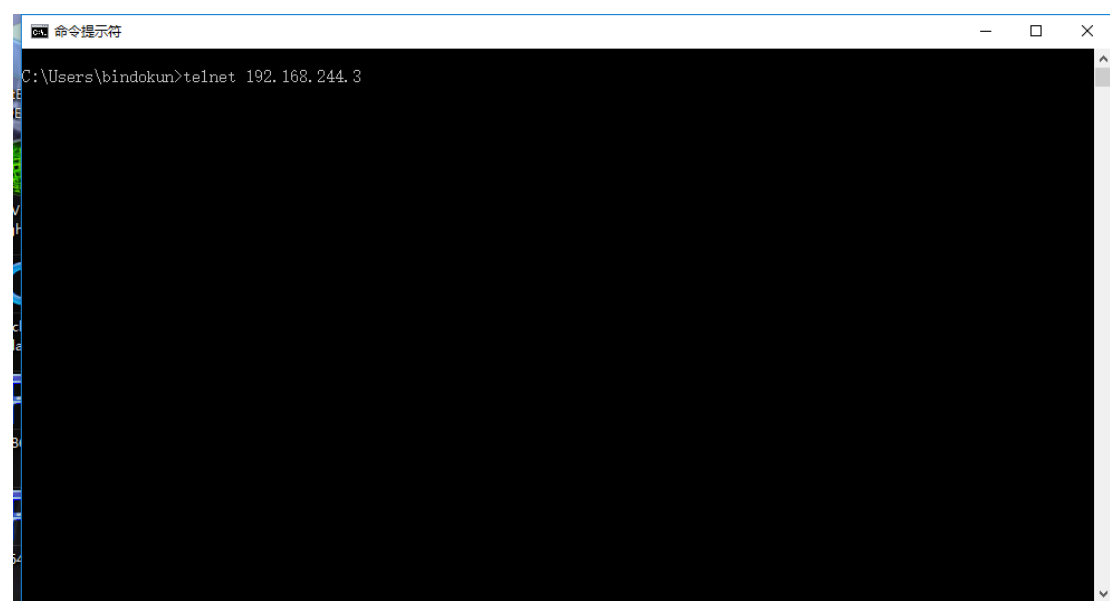
```
bindokun@bindokun-virtual-machine:~/sniffer_lab/minisniff$ ifconfig
ens33:  Link encap:Ethernet HWaddr 00:0c:29:49:03:a9
        inet addr:192.168.112.131 Bcast:192.168.112.255 Mask:255.255.255.0
        inet6 addr: fe80::20c:29ff:fe00:1432:c9ef/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:4809 errors:1 dropped:1 overruns:0 frame:0
        TX packets:3344 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:5754713 (5.7 MB) TX bytes:255501 (255.5 KB)
        Interrupt:19 Base address:0x2000

ens38:  Link encap:Ethernet HWaddr 00:0c:29:49:03:b3
        inet addr:192.168.244.3 Bcast:192.168.244.255 Mask:255.255.255.0
        inet6 addr: fe80::20c:29ff:fe49:3b3/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:1262 errors:0 dropped:0 overruns:0 frame:0
        TX packets:1275 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:101843 (101.8 KB) TX bytes:188944 (188.9 KB)
        Interrupt:16 Base address:0x2080

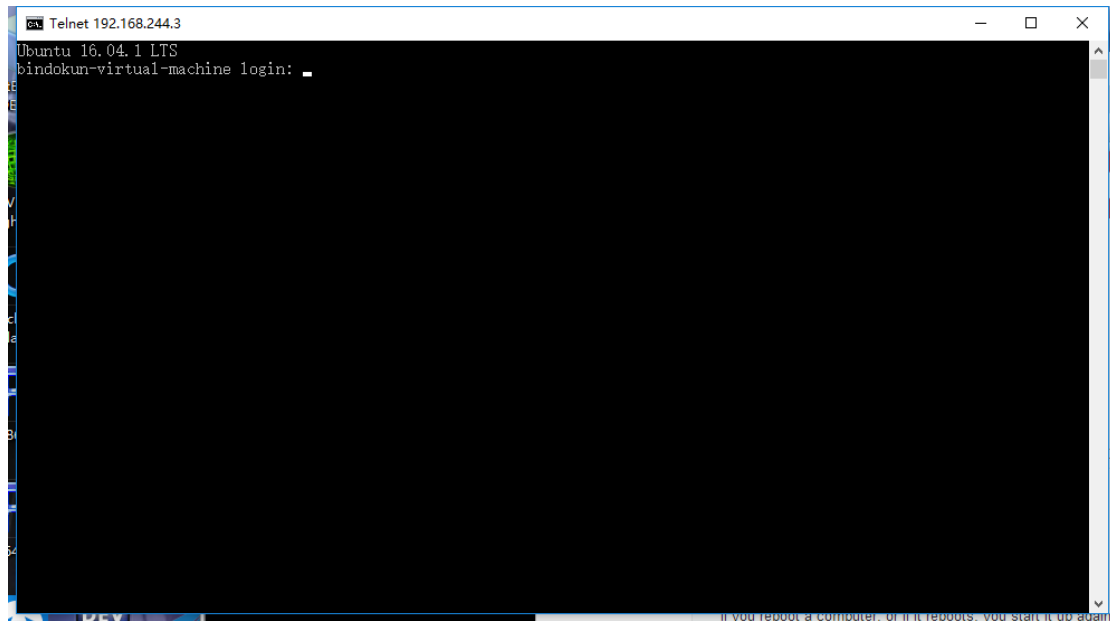
lo:     Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING MTU:65536 Metric:1
        RX packets:729 errors:0 dropped:0 overruns:0 frame:0
        TX packets:729 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:61705 (61.7 KB) TX bytes:61705 (61.7 KB)

virbr0: Link encap:Ethernet HWaddr 52:54:00:41:ce:a7
        inet addr:192.168.122.1 Bcast:192.168.122.255 Mask:255.255.255.0
        UP BROADCAST MULTICAST MTU:1500 Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
```

Both of them can be used. But you may have only one.



```
C:\Users\bindokun>telnet 192.168.244.3
```

**Linux:**

1. Set up another machine running Ubuntu which is in the same local area network with the target machine (you want to connect to).
2. Install telnet (May be not necessary)  
\$ sudo apt-get install telnetd
3. Type “telnet ip\_addr” in command line. ip\_addr is the ip of the machine you want to telnet to.