

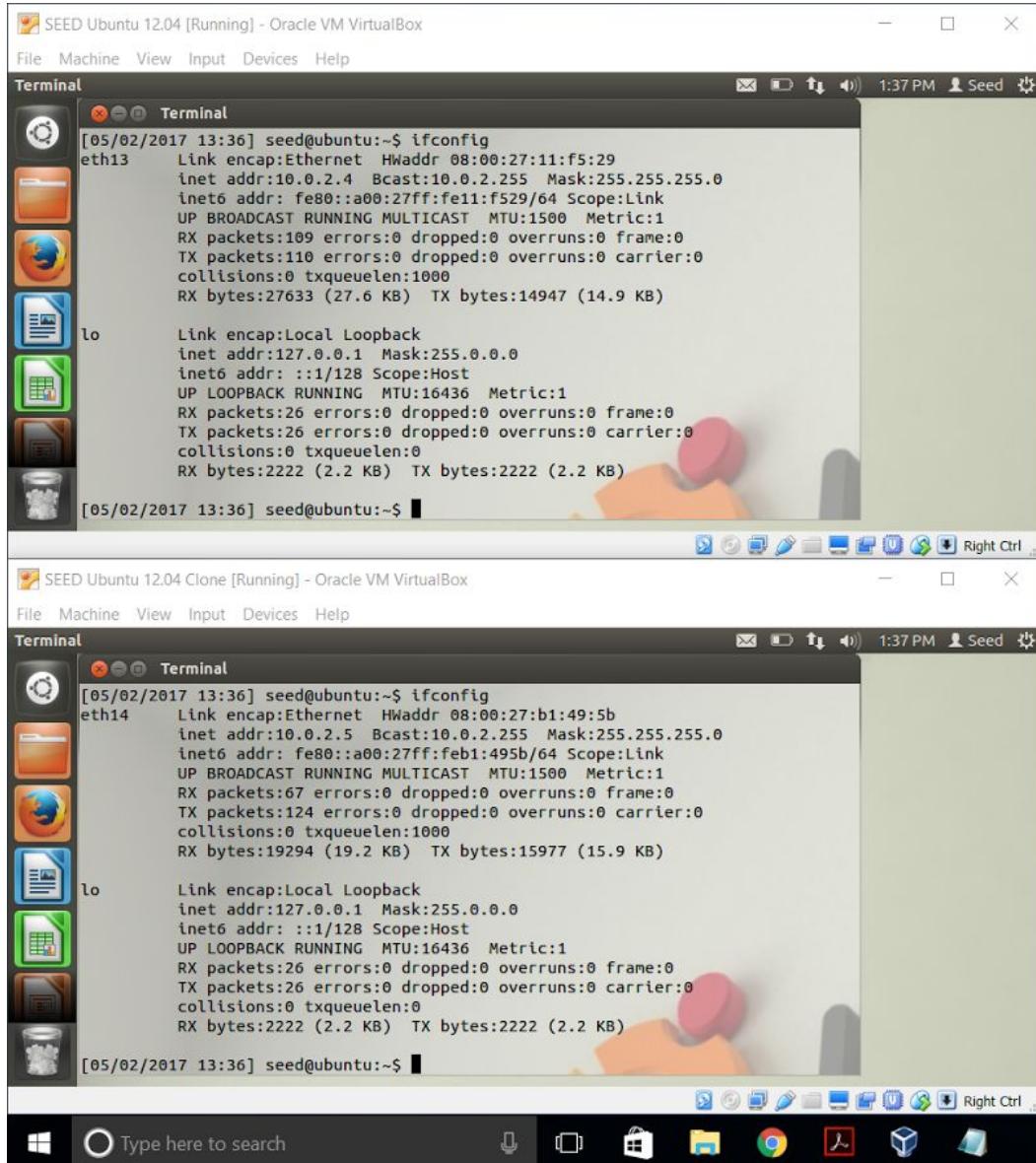
Pedro Ruelas

## Exercise 5

### 3.1 Problem 1: Verifying the Network

Output for terminal command:

```
$ ifconfig
```



The image shows two side-by-side screenshots of Oracle VM VirtualBox windows. Both windows display a terminal session running on an Ubuntu 12.04 host. The top window is titled "SEED Ubuntu 12.04 [Running] - Oracle VM VirtualBox" and the bottom window is titled "SEED Ubuntu 12.04 Clone [Running] - Oracle VM VirtualBox". Both terminals show the output of the "ifconfig" command.

```
[05/02/2017 13:36] seed@ubuntu:~$ ifconfig
eth13      Link encap:Ethernet HWaddr 08:00:27:11:f5:29
           inet addr:10.0.2.4 Bcast:10.0.2.255 Mask:255.255.255.0
           inet6 addr: fe80::a00:27ff:fe11:f529/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:109 errors:0 dropped:0 overruns:0 frame:0
             TX packets:110 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:27633 (27.6 KB) TX bytes:14947 (14.9 KB)

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:16436 Metric:1
             RX packets:26 errors:0 dropped:0 overruns:0 frame:0
             TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:2222 (2.2 KB) TX bytes:2222 (2.2 KB)

[05/02/2017 13:36] seed@ubuntu:~$ 

[05/02/2017 13:36] seed@ubuntu:~$ ifconfig
eth14      Link encap:Ethernet HWaddr 08:00:27:b1:49:5b
           inet addr:10.0.2.5 Bcast:10.0.2.255 Mask:255.255.255.0
           inet6 addr: fe80::a00:27ff:feb1:495b/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:67 errors:0 dropped:0 overruns:0 frame:0
             TX packets:124 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:19294 (19.2 KB) TX bytes:15977 (15.9 KB)

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:16436 Metric:1
             RX packets:26 errors:0 dropped:0 overruns:0 frame:0
             TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:2222 (2.2 KB) TX bytes:2222 (2.2 KB)

[05/02/2017 13:36] seed@ubuntu:~$ 
```

Output for terminal command:

```
$ ping -c 5 X.X.X.X
```

```

SEED Ubuntu 12.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:26 errors:0 dropped:0 overruns:0 frame:0
TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:2222 (2.2 KB) TX bytes:2222 (2.2 KB)

[05/02/2017 13:36] seed@ubuntu:~$ ping -c 5 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_req=1 ttl=64 time=0.612 ms
64 bytes from 10.0.2.5: icmp_req=2 ttl=64 time=0.293 ms
64 bytes from 10.0.2.5: icmp_req=3 ttl=64 time=0.288 ms
64 bytes from 10.0.2.5: icmp_req=4 ttl=64 time=0.372 ms
64 bytes from 10.0.2.5: icmp_req=5 ttl=64 time=0.405 ms

--- 10.0.2.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3997ms
rtt min/avg/max/mdev = 0.288/0.394/0.612/0.117 ms
[05/02/2017 13:39] seed@ubuntu:~$ 

SEED Ubuntu 12.04 Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:26 errors:0 dropped:0 overruns:0 frame:0
TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:2222 (2.2 KB) TX bytes:2222 (2.2 KB)

[05/02/2017 13:40] seed@ubuntu:~$ ping -c 5 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_req=1 ttl=64 time=0.210 ms
64 bytes from 10.0.2.4: icmp_req=2 ttl=64 time=0.327 ms
64 bytes from 10.0.2.4: icmp_req=3 ttl=64 time=0.236 ms
64 bytes from 10.0.2.4: icmp_req=4 ttl=64 time=0.326 ms
64 bytes from 10.0.2.4: icmp_req=5 ttl=64 time=0.335 ms

--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.210/0.286/0.335/0.057 ms
[05/02/2017 13:40] seed@ubuntu:~$ 

```

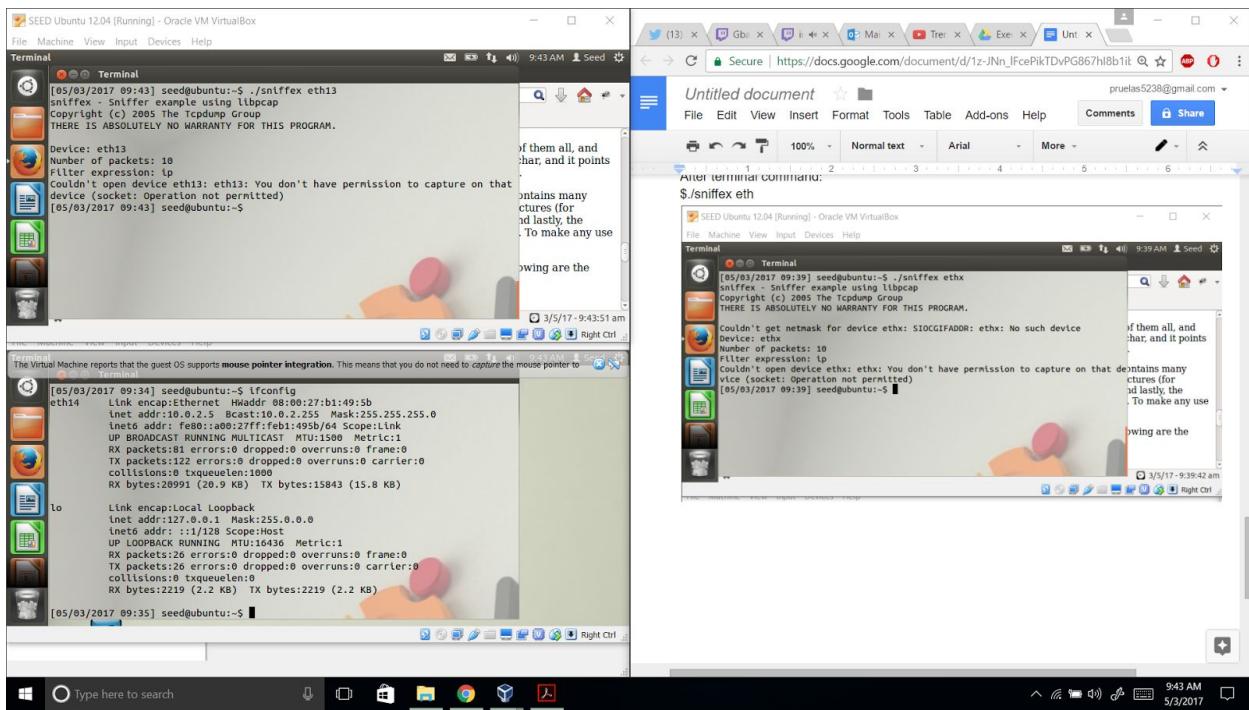
### 3.2 Problem 2: Writing a Packet Sniffer

#### Summary of the PCAP Library

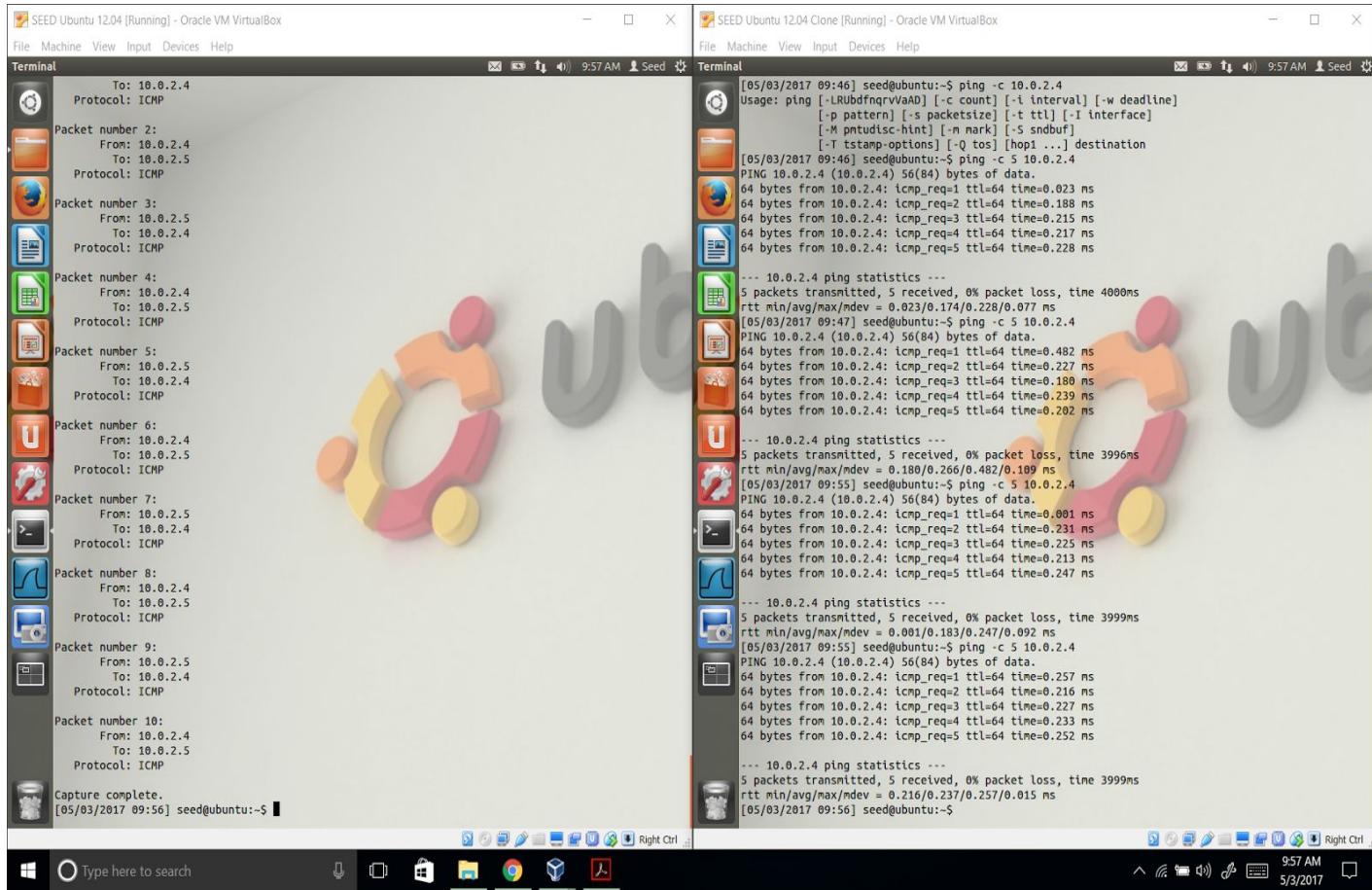
- The pcap library is used to view the traffic that is passing on an interface. One must inform the pcap on which device it will be viewing the traffic and inform what types of traffic it will be viewing. After running the pcap, it will view the traffic until it has received a set amount of packets specified by the user.

After terminal command:

\$./sniffex eth13



## Results for running the sniffer program in the first machine and pinging from the second.



After modifying the filter in the packet sniffer source code so that it captures TCP packets, the pings from the second machined are not being captured by the machine running the sniffer.

### 3.3 Problem 3: Password Sniffing

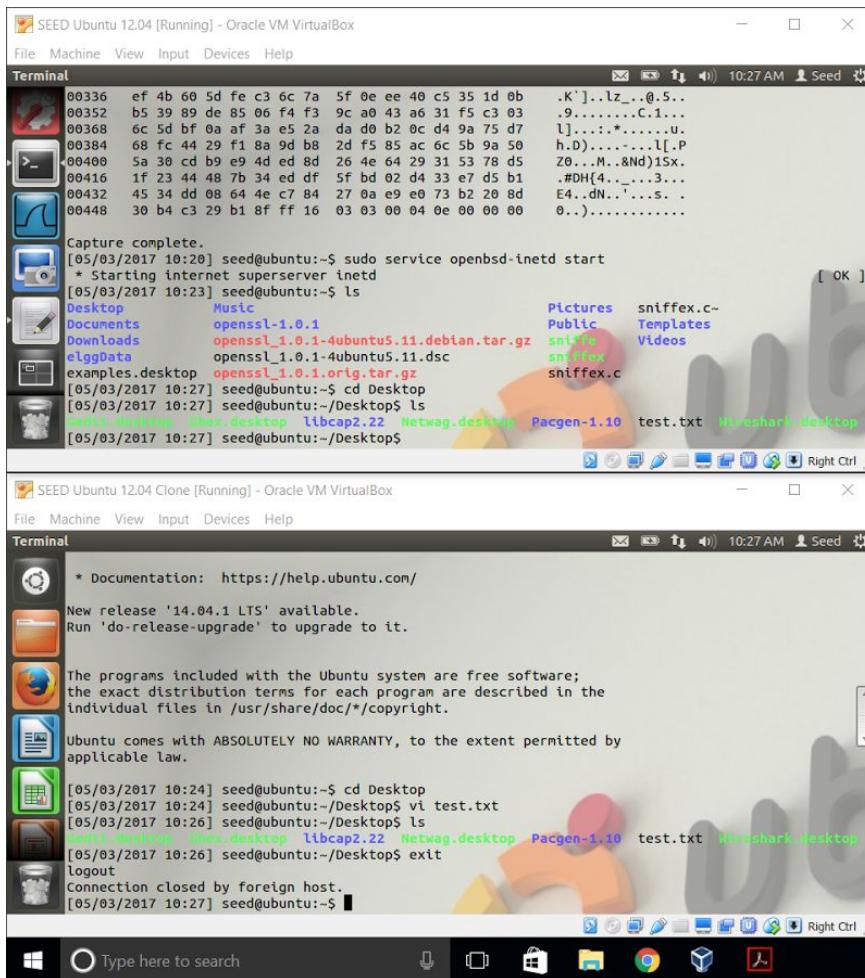
After running the terminal command below on the first machine

```
$ sudo service openbsd-inetd start
```

And using the terminal command below on the second machine

```
$ telnet 10.0.2.4
```

I logged from the second machine into the first and created a text file called "test.txt." After logging out, the text file was present on the first machine.



Trying to find the password of the user logging in.  
The password was visible.

```
SEED Ubuntu 12.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
Payload (12 bytes):
00000 0d 0a 50 61 73 73 77 6f 72 64 3a 20 ..Password:

Packet number 31:
From: 10.0.2.5
To: 10.0.2.4
Protocol: TCP
Src port: 58915
Dst port: 23

Packet number 32:
From: 10.0.2.5
To: 10.0.2.4
Protocol: TCP
Src port: 58915
Dst port: 23
Payload (1 bytes):
00000 64

Packet number 33:
From: 10.0.2.4
To: 10.0.2.5
Protocol: TCP
Src port: 23
Dst port: 58915

Packet number 34:
From: 10.0.2.5
To: 10.0.2.4
Protocol: TCP
Src port: 58915
Dst port: 23
Payload (1 bytes):
00000 65

Packet number 35:
From: 10.0.2.4
To: 10.0.2.5
Protocol: TCP
Src port: 23
Dst port: 58915

Packet number 36:
From: 10.0.2.5
To: 10.0.2.4
Protocol: TCP
Src port: 58915
Dst port: 23
Payload (1 bytes):
00000 65

Packet number 37:
From: 10.0.2.4
To: 10.0.2.5
Protocol: TCP
Src port: 23
Dst port: 58915

Packet number 38:
From: 10.0.2.5
To: 10.0.2.4
Protocol: TCP
Src port: 58915
Dst port: 23
Payload (1 bytes):
00000 73

Packet number 39:
From: 10.0.2.4
To: 10.0.2.5
Protocol: TCP
Src port: 23
Dst port: 58915

Packet number 40:
From: 10.0.2.5
To: 10.0.2.4
Protocol: TCP
Src port: 58915
Dst port: 23
Payload (2 bytes):
00000 0d 00 ..

Packet number 41:
From: 10.0.2.4
To: 10.0.2.5
Protocol: TCP
Src port: 23
Dst port: 58915

Packet number 42:
From: 10.0.2.4
To: 10.0.2.5
```

```
SEED Ubuntu 12.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
Packet number 36:
From: 10.0.2.5
To: 10.0.2.4
Protocol: TCP
Src port: 58915
Dst port: 23
Payload (1 bytes):
00000 65

Packet number 37:
From: 10.0.2.4
To: 10.0.2.5
Protocol: TCP
Src port: 23
Dst port: 58915

Packet number 38:
From: 10.0.2.5
To: 10.0.2.4
Protocol: TCP
Src port: 58915
Dst port: 23
Payload (1 bytes):
00000 73

Packet number 39:
From: 10.0.2.4
To: 10.0.2.5
Protocol: TCP
Src port: 23
Dst port: 58915

Packet number 40:
From: 10.0.2.5
To: 10.0.2.4
Protocol: TCP
Src port: 58915
Dst port: 23
Payload (2 bytes):
00000 0d 00 ..

Packet number 41:
From: 10.0.2.4
To: 10.0.2.5
Protocol: TCP
Src port: 23
Dst port: 58915

Packet number 42:
From: 10.0.2.4
To: 10.0.2.5
```

### Using Wireshark

- When using wireshark instead of my own packet sniffer, I am still able to locate the user's password by looking at the telnet data segments present in wireshark.

After these experiments it appears that using telnet as a method of remotely accessing a system is not secure and should be avoided since the password of a user can be retrieved without much difficulty.

### 3.4 Problem 4: SSH

When using SSH to login to the first virtual machine, I am unable to find the password entered at the second virtual machine through wireshark. When one looks through the packets, it appears impossible to determine the password.