Jarod Nakamoto

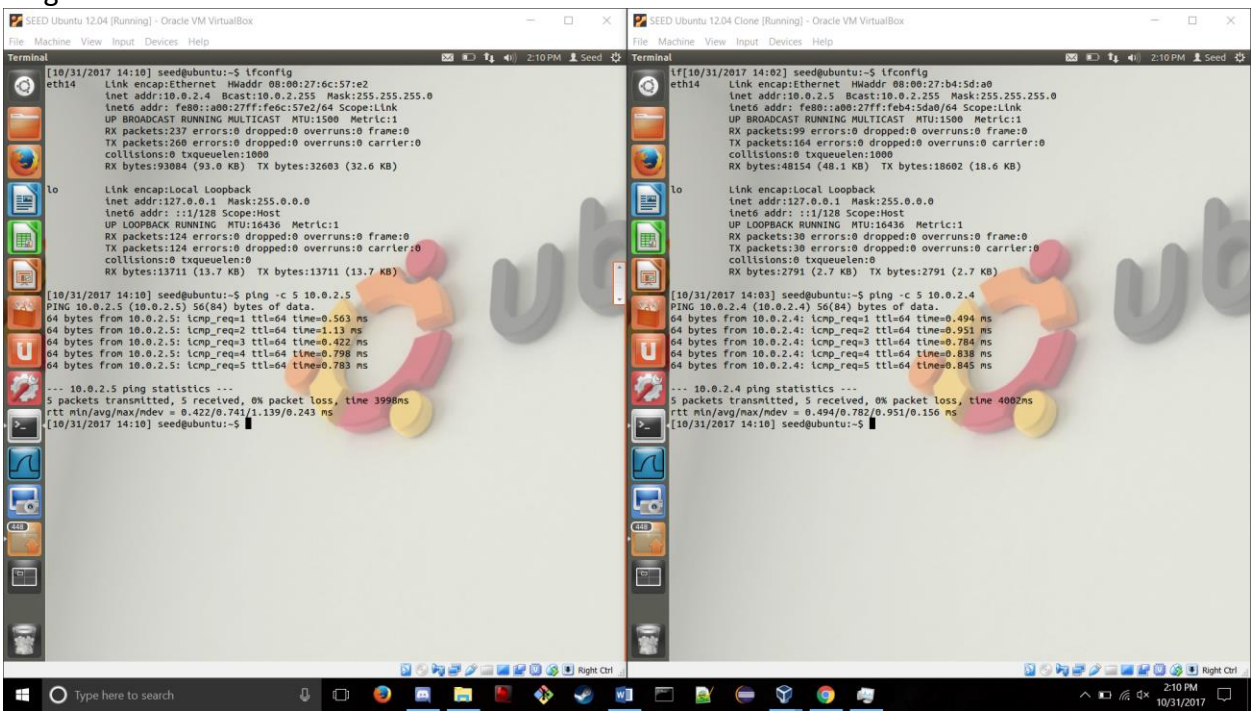
CS 380
Exercise 5

My repository for this class is under CS 380 – Computer Networks
https://github.com/jarodNakamoto/College-CS-Courses.git

3.1 Verifying the Network

IP config

Ping



3.2 Packet Sniffer

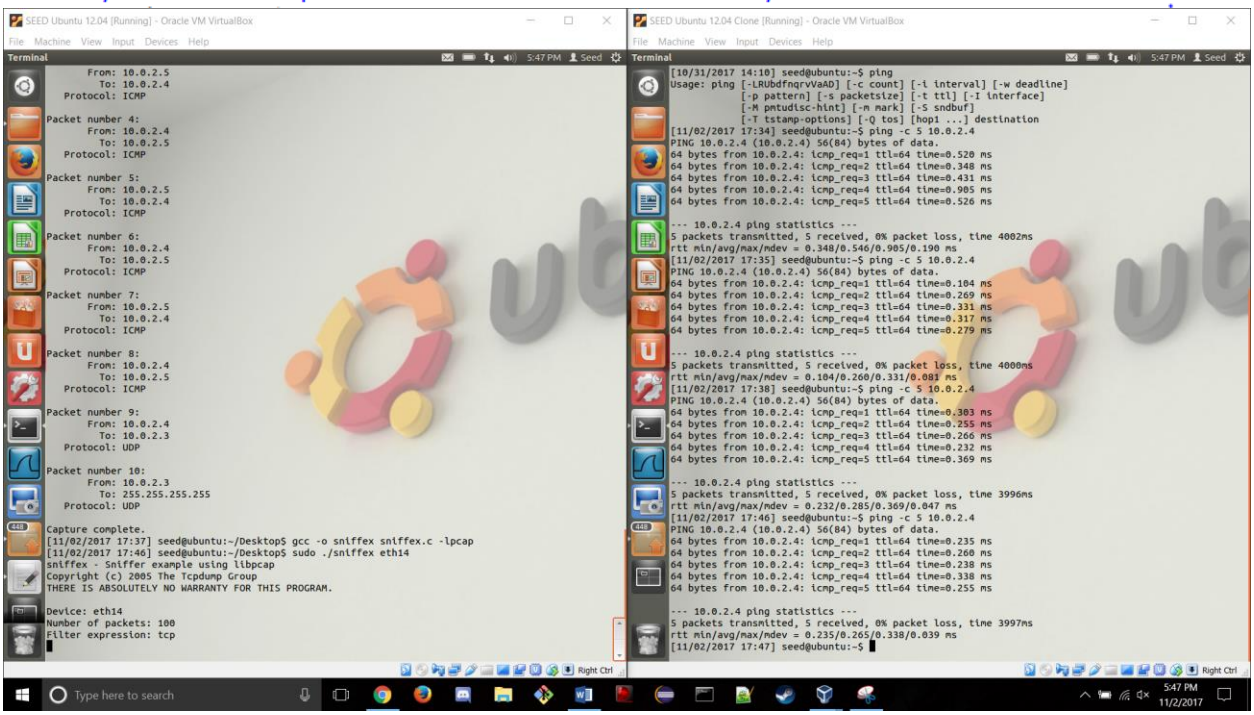
```
[11/02/2017 17:31] seed@ubuntu:~/Desktop$ gcc -o sniffex sniffex.c -lpcap
[11/02/2017 17:32] seed@ubuntu:~/Desktop$ ./sniffex NatNetwork
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.

Couldn't get netmask for device NatNetwork: SIOCGIFADDR: NatNetwork: No such device
Device: NatNetwork
Number of packets: 10
Filter expression: ip
Couldn't open device NatNetwork: NatNetwork: You don't have permission to capture on that device (s
ocket: Operation not permitted)
```

When pinging it with normal privileges, it says that we have insufficient privileges to run this program which means that the OS blocks it for security reasons.

```
[11/02/2017 17:35] seed@ubuntu:~/Desktop$ sudo ./sniffex eth14
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.

Device: eth14
Number of packets: 10
Filter expression: ip

Packet number 1:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: ICMP

Packet number 2:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: ICMP

Packet number 3:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: ICMP

Packet number 4:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: ICMP

Packet number 5:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: ICMP

Packet number 6:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: ICMP

Packet number 7:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: ICMP

Packet number 8:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: ICMP
```

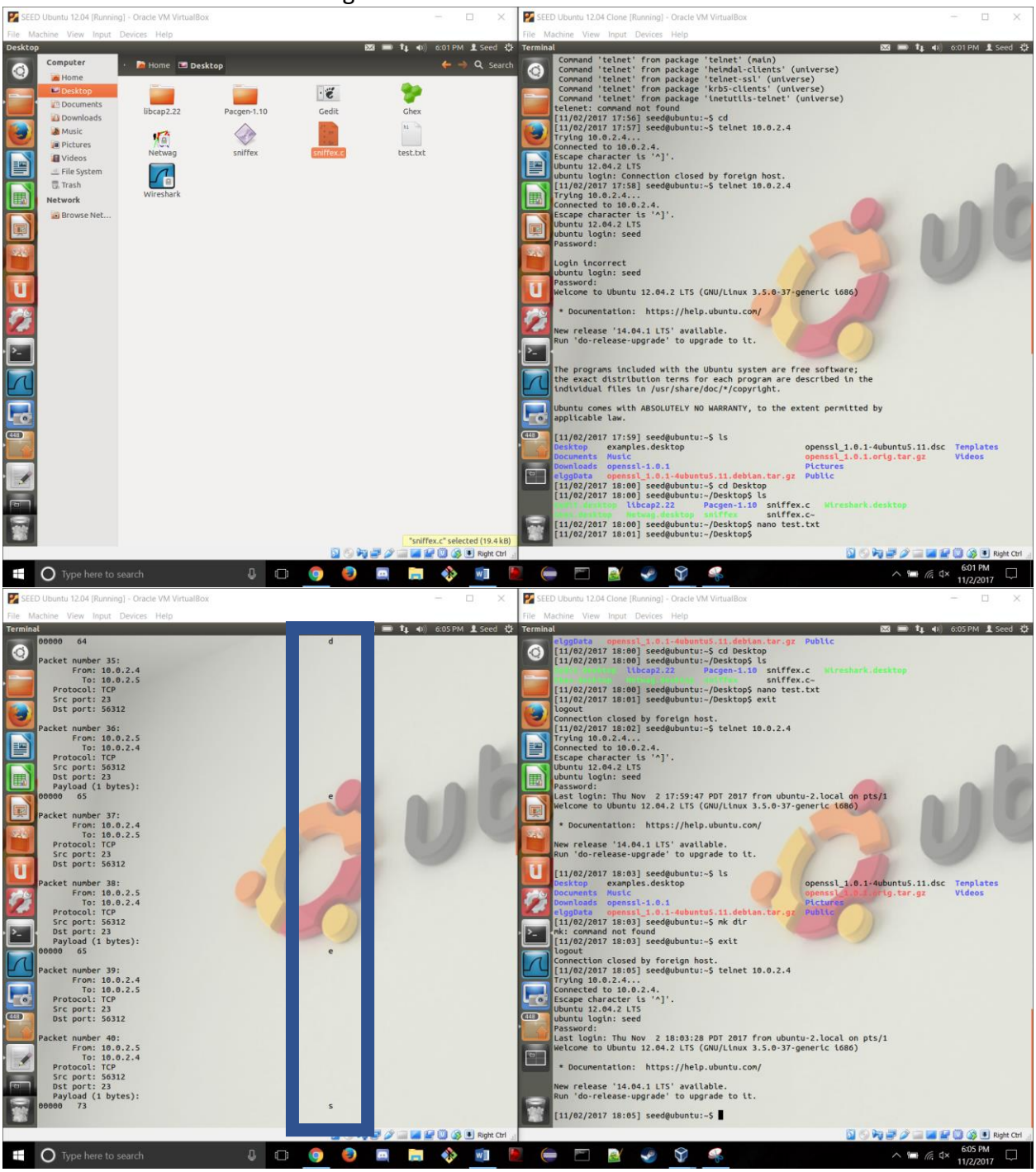
It works after running it in admin, so it was just a security block by the kernel.

```
int main(int argc, char **argv)
{

        char *dev = NULL;                       /* capture device name */
        char errbuf[PCAP_ERRBUF_SIZE];          /* error buffer */
        pcap_t *handle;                         /* packet capture handle */

        char filter_exp[] = "tcp";              /* filter expression [3] */
        struct bpf_program fp;                  /* compiled filter program (expression) */
        bpf_u_int32 mask;                       /* subnet mask */
        bpf_u_int32 net;                        /* ip */
        int num_packets = 10;                   /* number of packets to capture */

        print_app_banner();

        /* check for capture device name on command-line */
```

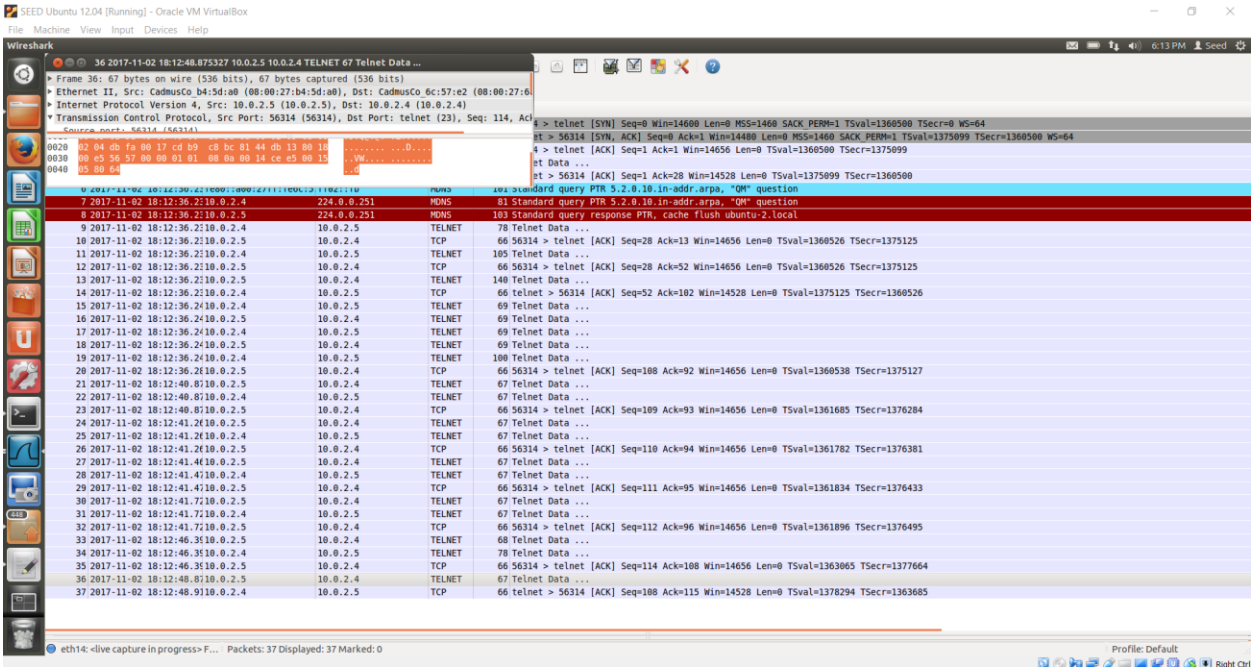


After pinging it twice, there was no change which means there are no tcp packets sent by ping.

3.3 Problem 3: Password Sniffing

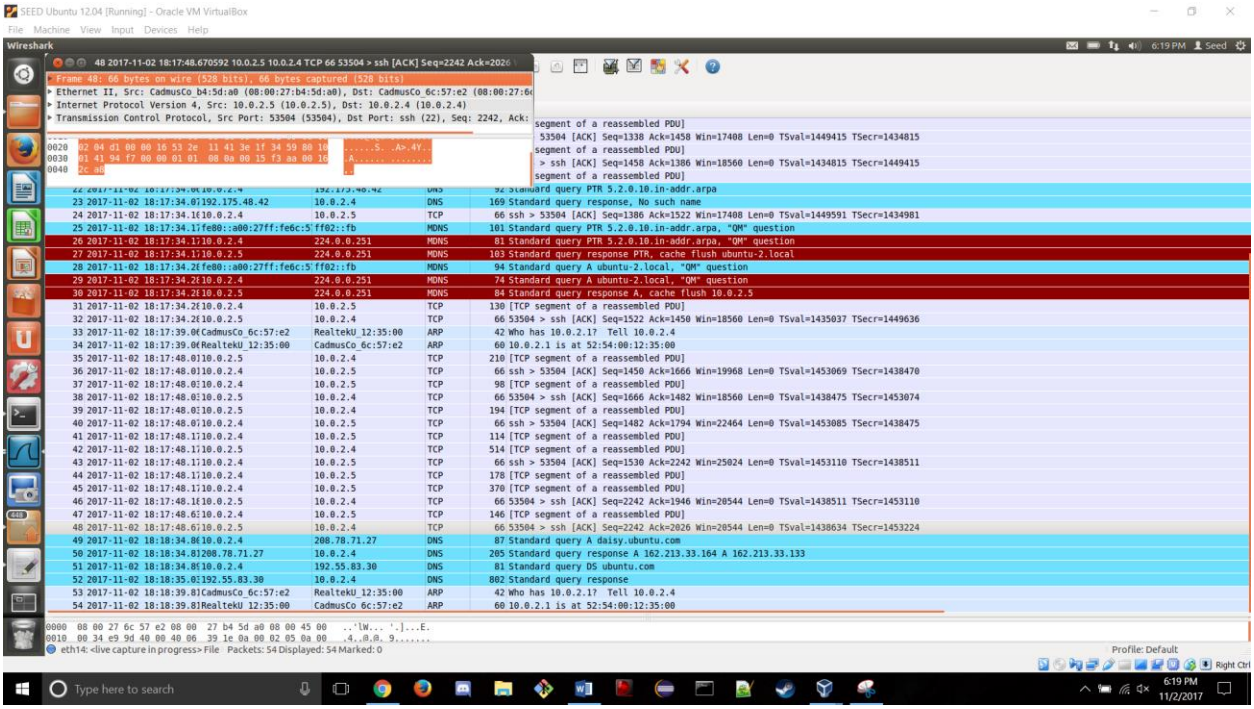


Using wireshark, it is still possible to find the users passwords at the bottom of the telenet packets.



Telenet's security is poor as anyone with enough knowledge and a sniffer can see the contents of the data.

3.4 Problem 4 SSH



Even where the password characters should be it is encrypted so the actual password is not found.