

VPN Lab (Task 1 and 2)

Task 1: VM Setup

VM Settings:

Host U (NAT Network):

NAT Network IP address: 10.0.2.5

Host V (Internal Network):

Internal Network IP address: 192.168.60.101

VPN Server (NAT Network + Internal Network):

NAT Network IP address: 10.0.2.15

Internal Network IP address: 192.168.60.1

Task 2: Creating a VPN Tunnel using TUN/TAP

Test the VPN Tunnel:

Ping test on Host U:

```
Terminal File Edit View Search Terminal Help
[03/25/20]seed@VM:~/Lab8$ ifconfig -a
enp0s3
Link encap:Ethernet HWaddr 08:00:27:d2:78:ac
inet addr:10.0.2.5 Bcast:10.0.2.255 Mask:255.255.255.0
inet6 addr: fe80::905e:819f:d374:998a/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:6565 errors:0 dropped:0 overruns:0 frame:0
TX packets:4120 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:6201998 (6.2 MB) TX bytes:403445 (403.4 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:1362 errors:0 dropped:0 overruns:0 frame:0
TX packets:1362 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:107440 (107.4 KB) TX bytes:107440 (107.4 KB)

tun0
Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet addr:192.168.53.5 P-t-P:192.168.53.5 Mask:255.255.255.0
inet6 addr: fe80::91f2:ed19:d212:a4e3/64 Scope:Link
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
RX packets:212 errors:0 dropped:0 overruns:0 frame:0
TX packets:226 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:500
RX bytes:17808 (17.8 KB) TX bytes:18876 (18.8 KB)

[03/25/20]seed@VM:~/Lab8$ ping 192.168.60.101
PING 192.168.60.101 (192.168.60.101) 56(84) bytes of data.
64 bytes from 192.168.60.101: icmp_seq=1 ttl=63 time=0.732 ms
64 bytes from 192.168.60.101: icmp_seq=2 ttl=63 time=0.698 ms
64 bytes from 192.168.60.101: icmp_seq=3 ttl=63 time=0.804 ms
64 bytes from 192.168.60.101: icmp_seq=4 ttl=63 time=0.684 ms
64 bytes from 192.168.60.101: icmp_seq=5 ttl=63 time=0.692 ms
^C
--- 192.168.60.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4077ms
rtt min/avg/max/mdev = 0.684/0.722/0.804/0.044 ms
[03/25/20]seed@VM:~/Lab8$
```

Wireshark:

```
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/> Expression... +

No. Time Source Destination Protocol Length Info
2 2020-03-25 03:23:35.4659359... 192.168.53.5 192.168.60.101 ICMP 100 Echo (ping) request id=0x1689, seq=1/256, ttl=64 (rep...
3 2020-03-25 03:23:35.4659560... 10.0.2.5 10.0.2.15 UDP 128 36281 -> 55555 Len=84
4 2020-03-25 03:23:35.4666289... 10.0.2.15 10.0.2.5 UDP 128 55555 -> 36281 Len=84
5 2020-03-25 03:23:35.4666618... 192.168.60.101 192.168.53.5 ICMP 100 Echo (ping) reply id=0x1689, seq=1/256, ttl=63 (requ...
6 2020-03-25 03:23:36.4715837... 192.168.53.5 192.168.60.101 ICMP 100 Echo (ping) request id=0x1689, seq=2/512, ttl=64 (repl...
7 2020-03-25 03:23:36.4716127... 10.0.2.5 10.0.2.15 UDP 128 36281 -> 55555 Len=84
8 2020-03-25 03:23:36.4722300... 10.0.2.15 10.0.2.5 UDP 128 55555 -> 36281 Len=84
9 2020-03-25 03:23:36.4722681... 192.168.60.101 192.168.53.5 ICMP 100 Echo (ping) reply id=0x1689, seq=2/512, ttl=63 (requ...
10 2020-03-25 03:23:37.4952974... 192.168.53.5 192.168.60.101 ICMP 100 Echo (ping) request id=0x1689, seq=3/768, ttl=64 (repl...
11 2020-03-25 03:23:37.4953276... 10.0.2.5 10.0.2.15 UDP 128 36281 -> 55555 Len=84
12 2020-03-25 03:23:37.4960369... 10.0.2.15 10.0.2.5 UDP 128 55555 -> 36281 Len=84
13 2020-03-25 03:23:37.4960872... 192.168.60.101 192.168.53.5 ICMP 100 Echo (ping) reply id=0x1689, seq=3/768, ttl=63 (requ...
14 2020-03-25 03:23:38.5194304... 192.168.53.5 192.168.60.101 ICMP 100 Echo (ping) request id=0x1689, seq=4/1024, ttl=64 (rep...
15 2020-03-25 03:23:38.5194578... 10.0.2.5 10.0.2.15 UDP 128 36281 -> 55555 Len=84
16 2020-03-25 03:23:38.5200700... 10.0.2.15 10.0.2.5 UDP 128 55555 -> 36281 Len=84
17 2020-03-25 03:23:38.5201028... 192.168.60.101 192.168.53.5 ICMP 100 Echo (ping) reply id=0x1689, seq=4/1024, ttl=63 (req...
18 2020-03-25 03:23:39.5438489... 192.168.53.5 192.168.60.101 ICMP 100 Echo (ping) request id=0x1689, seq=5/1280, ttl=64 (rep...

Frame 6: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.53.5, Dst: 192.168.60.101
Internet Control Message Protocol

0000 00 04 ff fe 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010 45 00 00 54 3f 74 40 00 40 01 08 7a c0 a8 35 05 E..T7t0. @..z..5.
0020 c0 a8 3c 05 00 00 69 da 16 09 00 02 f8 06 7b 5e ..<e..i. ....{^
0030 12 32 07 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 .2.....
0040 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 .....!#"
0050 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 $%&'()*+ ,-./0123
0060 34 35 36 37 4567
```

Packet No.2: ICMP request packet from Host U(192.168.53.5 ip address in the tunnel) to Host V(192.168.60.101 ip address in the internal network of Host V and VPN server)

Packet No.3: UDP packet send by vpnclient program on Host U, contains the ICMP request body in packet No.1 and transferred on our VPN tunnel.

Packet No.4: UDP packet send by vpnsrvr program on our VPN server, contains the ICMP reply body from Host V and transferred on our VPN tunnel.

Packet No.5: ICMP reply packet from Host V to Host U, this packet is from the body of the UDP packet No.4.

Wireshark packet capture showing packet 3, a UDP packet from 10.0.2.5 to 10.0.2.15. The packet data is highlighted in red and labeled "UDP data". The packet details pane shows the following information:

- Frame 3: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface 0
- Linux cooked capture
- Internet Protocol Version 4, Src: 10.0.2.5, Dst: 10.0.2.15
- User Datagram Protocol, Src Port: 36281, Dst Port: 55555
- Data (84 bytes)
- Data: 450000543f184000400108d6c0a83505c0a83c65080073f1... [Length: 84]

The packet data is shown in hexadecimal and ASCII format. The ASCII format shows the text "E..T7.0. @.....5..<e..s.{^".

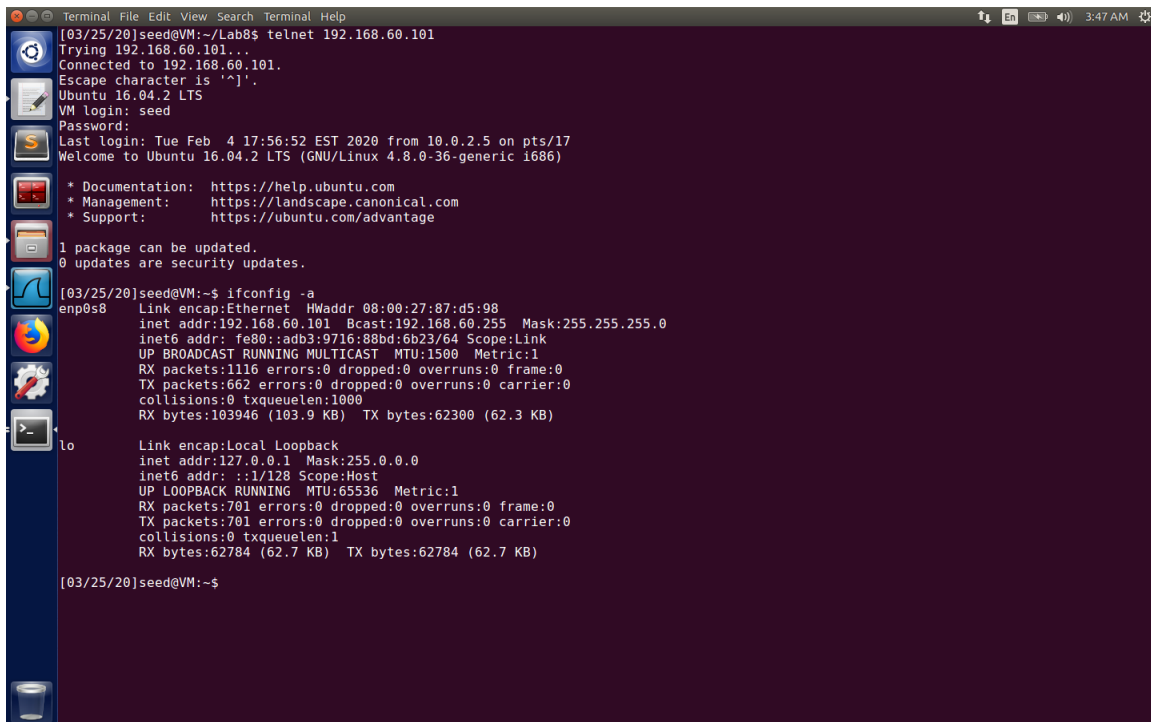
Wireshark packet capture showing packet 2, an ICMP Echo (ping) request from 192.168.53.5 to 192.168.60.101. The packet data is highlighted in red and labeled "ICMP packet without ethernet header (the first line)". The packet details pane shows the following information:

- Frame 2: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0
- Linux cooked capture
- Internet Protocol Version 4, Src: 192.168.53.5, Dst: 192.168.60.101
- Internet Control Message Protocol

The packet data is shown in hexadecimal and ASCII format. The ASCII format shows the text "E..T7.0. @.....5..<e..s.{^".

The data part of the UDP packet is actually the same as the whole ICMP request/reply except ethernet header (IP packet).

Telnet test on Host U:



A terminal window showing the execution of a telnet command from Host V to Host U (192.168.60.101). The connection is successful, and the user is prompted for a password. The terminal also shows the output of the 'ifconfig' command for the 'enp0s8' interface, displaying network configuration details such as IP address, netmask, and MTU.

```
[03/25/20]seed@VM:~/Lab8$ telnet 192.168.60.101
Trying 192.168.60.101...
Connected to 192.168.60.101.
Escape character is '^['.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Tue Feb  4 17:56:52 EST 2020 from 10.0.2.5 on pts/17
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.

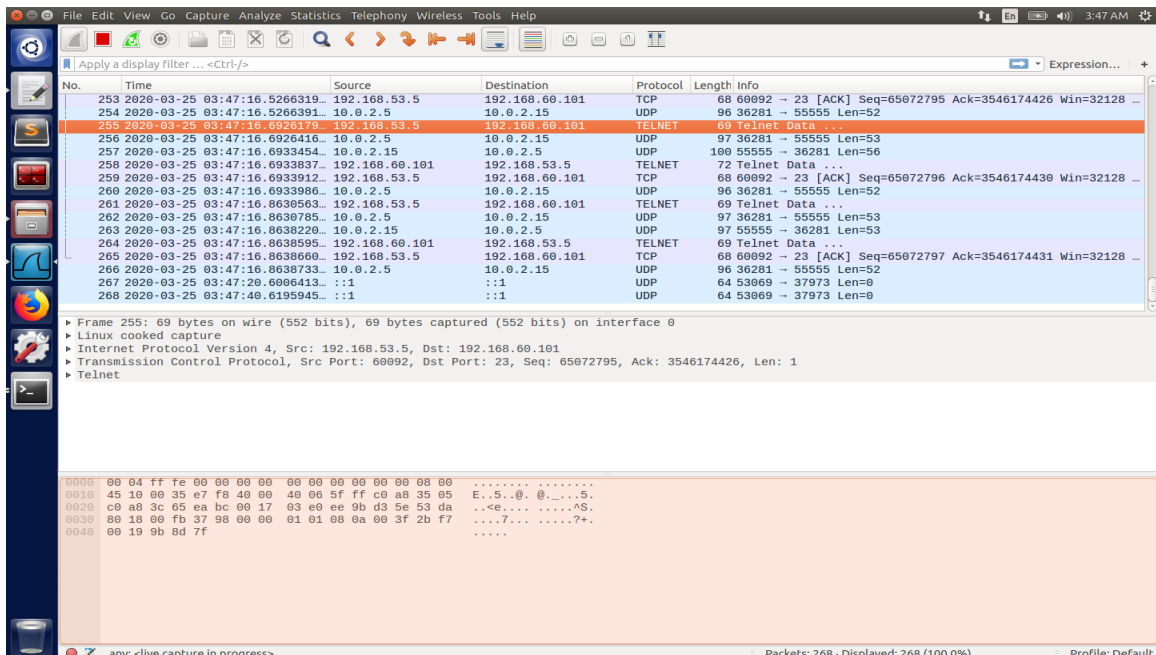
[03/25/20]seed@VM:~$ ifconfig -a
enp0s8    Link encap:Ethernet  HWaddr 08:00:27:87:d5:98
          inet addr:192.168.60.101  Bcast:192.168.60.255  Mask:255.255.255.0
          inet6 addr: fe80::adb3:9716:88bd:6b23/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1116 errors:0 dropped:0 overruns:0 frame:0
          TX packets:662 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:103946 (103.9 KB)  TX bytes:62300 (62.3 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:701 errors:0 dropped:0 overruns:0 frame:0
          TX packets:701 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:62784 (62.7 KB)  TX bytes:62784 (62.7 KB)

[03/25/20]seed@VM:~$
```

Host U connected with Host V using telnet.

Wireshark:



A screenshot of the Wireshark network protocol analyzer. The main pane displays a list of captured packets, with packet 255 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Telnet. The packet bytes pane shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates that 268 packets were captured and displayed.

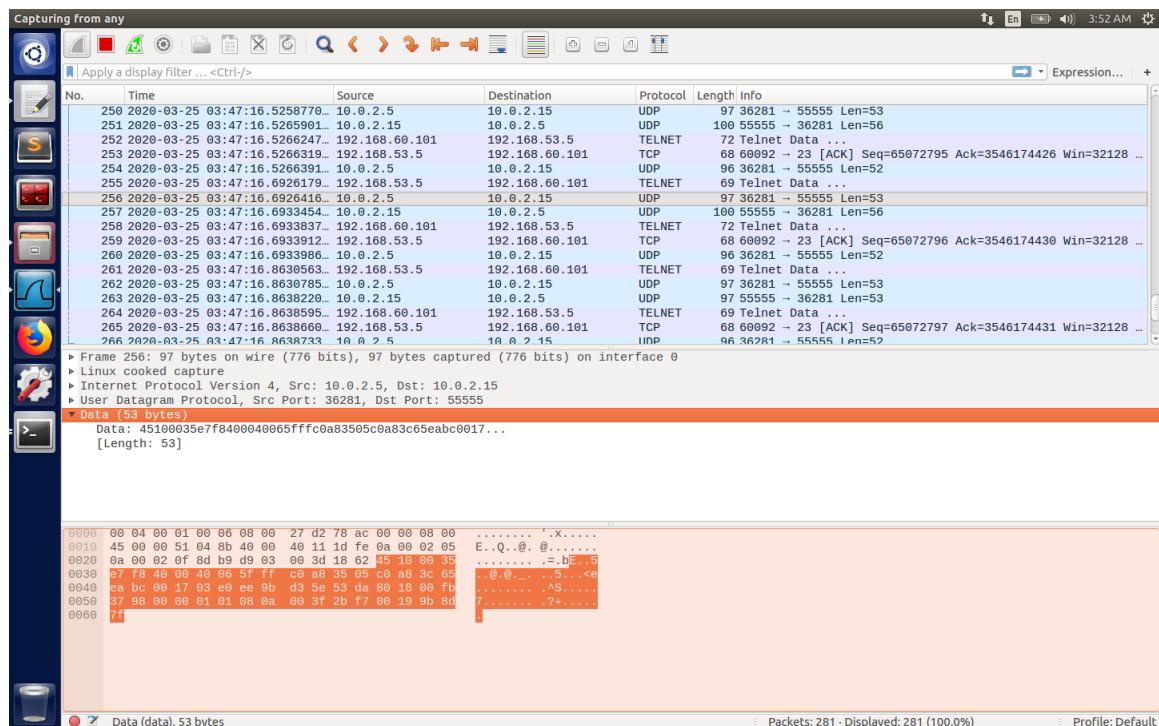
No.	Time	Source	Destination	Protocol	Length	Info
253	2020-03-25 03:47:16.5266319	192.168.53.5	192.168.60.101	TCP	68	60092 → 23 [ACK] Seq=65072795 Ack=3546174426 Win=32128 ...
254	2020-03-25 03:47:16.5266391	10.0.2.5	10.0.2.15	UDP	96	36281 → 55555 Len=52
255	2020-03-25 03:47:16.6926179	192.168.53.5	192.168.60.101	TELNET	60	Telnet Data ...
256	2020-03-25 03:47:16.6926416	10.0.2.5	10.0.2.15	UDP	97	36281 → 55555 Len=53
257	2020-03-25 03:47:16.6933454	10.0.2.15	10.0.2.5	UDP	100	55555 → 36281 Len=56
258	2020-03-25 03:47:16.6933837	192.168.60.101	192.168.53.5	TELNET	72	Telnet Data ...
259	2020-03-25 03:47:16.6933912	192.168.53.5	192.168.60.101	TCP	68	60092 → 23 [ACK] Seq=65072796 Ack=3546174430 Win=32128 ...
260	2020-03-25 03:47:16.6933986	10.0.2.5	10.0.2.15	UDP	96	36281 → 55555 Len=52
261	2020-03-25 03:47:16.8638563	192.168.53.5	192.168.60.101	TELNET	69	Telnet Data ...
262	2020-03-25 03:47:16.8638785	10.0.2.5	10.0.2.15	UDP	97	36281 → 55555 Len=53
263	2020-03-25 03:47:16.8638220	10.0.2.15	10.0.2.5	UDP	97	55555 → 36281 Len=53
264	2020-03-25 03:47:16.8638595	192.168.60.101	192.168.53.5	TELNET	69	Telnet Data ...
265	2020-03-25 03:47:16.8638660	192.168.53.5	192.168.60.101	TCP	68	60092 → 23 [ACK] Seq=65072797 Ack=3546174431 Win=32128 ...
266	2020-03-25 03:47:16.8638733	10.0.2.5	10.0.2.15	UDP	96	36281 → 55555 Len=52
267	2020-03-25 03:47:20.6006413	:::1	:::1	UDP	64	53069 → 37973 Len=0
268	2020-03-25 03:47:40.6195945	:::1	:::1	UDP	64	53069 → 37973 Len=0

Frame 255: 60 bytes on wire (552 bits), 60 bytes captured (552 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.53.5, Dst: 192.168.60.101
Transmission Control Protocol, Src Port: 60092, Dst Port: 23, Seq: 65072795, Ack: 3546174426, Len: 1
Telnet

0000 00 04 ff fe 00 00 00 00 00 00 00 00 00 00 00 00
0010 45 10 00 35 e7 f8 40 00 40 06 5f ff c0 a8 35 05 E..S..@.....
0020 c0 a8 3c 65 ea bc 00 17 03 e0 ee 9b d3 5e 53 da ..<e.....S..
0030 80 18 00 fb 37 98 00 00 01 01 08 0a 00 3f 2b f7?+..
0040 00 19 9b 8d 7f

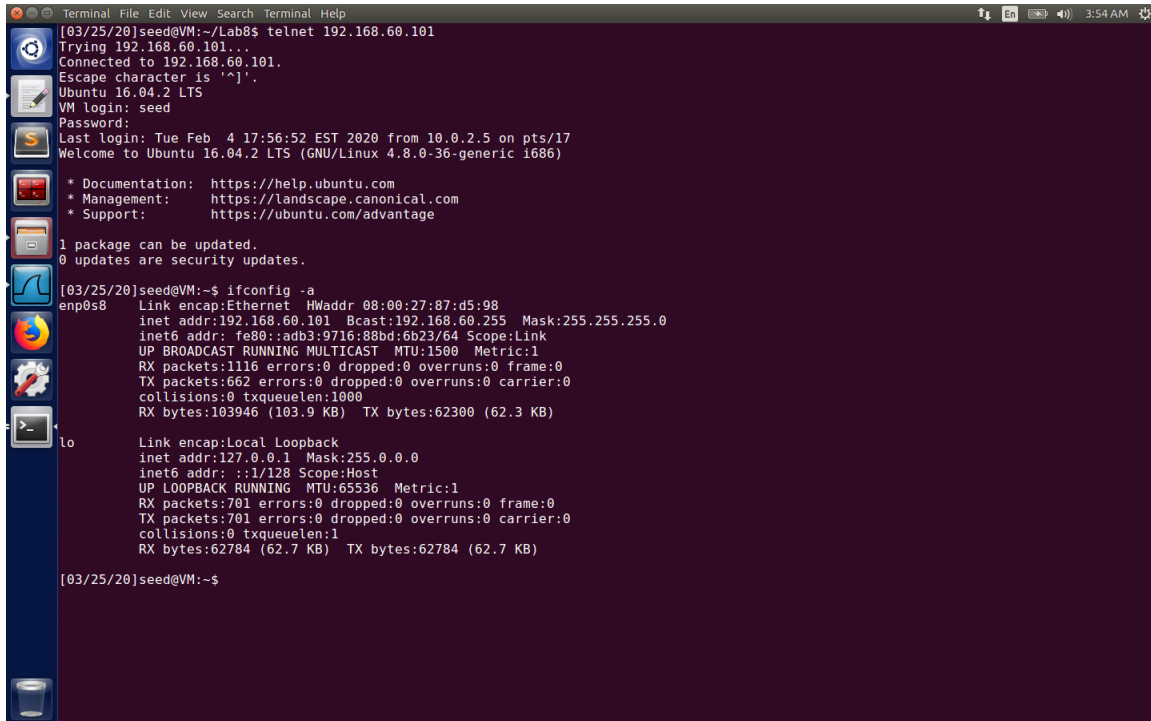
any: <live capture in progress> Packets: 268 - Displayed: 268 (100.0%) Profile: Default

For example, packet No.255, No.256, No.257 and No.258



Tunnel-Breaking Test:

After break the VPN tunnel, we cannot type in any single letter in the telnet window.

A terminal window with a dark purple background and a blue sidebar on the left containing icons for settings, a file manager, a terminal, and a power button. The terminal text shows a telnet connection to 192.168.60.101, a login prompt, and the execution of the ifconfig -a command. The output of ifconfig -a shows details for the enp0s8 interface (ethernet) and the lo interface (loopback).

```
[03/25/20]seed@VM:~/Lab8$ telnet 192.168.60.101
Trying 192.168.60.101...
Connected to 192.168.60.101.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Tue Feb  4 17:56:52 EST 2020 from 10.0.2.5 on pts/17
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.

[03/25/20]seed@VM:~$ ifconfig -a
enp0s8:
Link encap:Ethernet  HWaddr 08:00:27:87:d5:98
inet addr:192.168.60.101 Bcast:192.168.60.255 Mask:255.255.255.0
inet6 addr: fe80::adb3:9716:88bd:6b23/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:1116 errors:0 dropped:0 overruns:0 frame:0
TX packets:662 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:103946 (103.9 KB)  TX bytes:62300 (62.3 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:701 errors:0 dropped:0 overruns:0 frame:0
TX packets:701 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:62784 (62.7 KB)  TX bytes:62784 (62.7 KB)

[03/25/20]seed@VM:~$
```

After we reconnect the VPN tunnel, the telnet connection will be resumed. This is because after we broke the VPN tunnel, we cannot send packets on VPN tunnel, so the Host V will not receive any message (commands) from Host U. However, we did not make any operation to terminate the TELNET connection. For Host V, it's just like Host U does not type anything.