

Telnet Lab Exercise

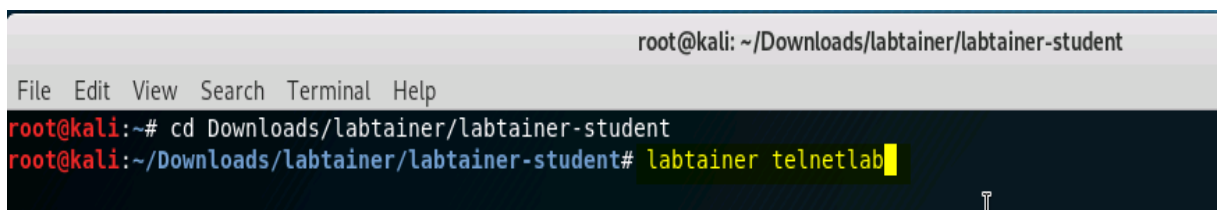
Overview

This labtainer exercise illustrates the use of a telnet client to access resources on a server. It is a simple lab intended to illustrate basic client server networking and the transmission of plaintext passwords over a network by telnet.

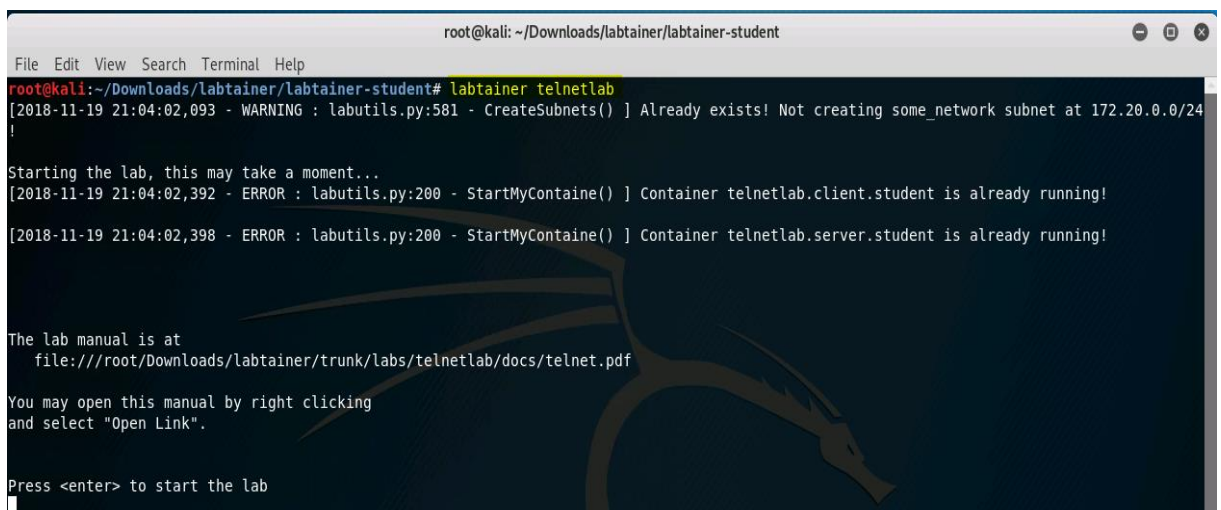
Performing the lab

The lab is started from the labtainer working directory on your Linux host, e.g., a Linux VM. From there, issue the command:

```
labtainer telnetlab
```



```
root@kali: ~/Downloads/labtainer/labtainer-student
File Edit View Search Terminal Help
root@kali:~# cd Downloads/labtainer/labtainer-student
root@kali:~/Downloads/labtainer/labtainer-student# labtainer telnetlab
```



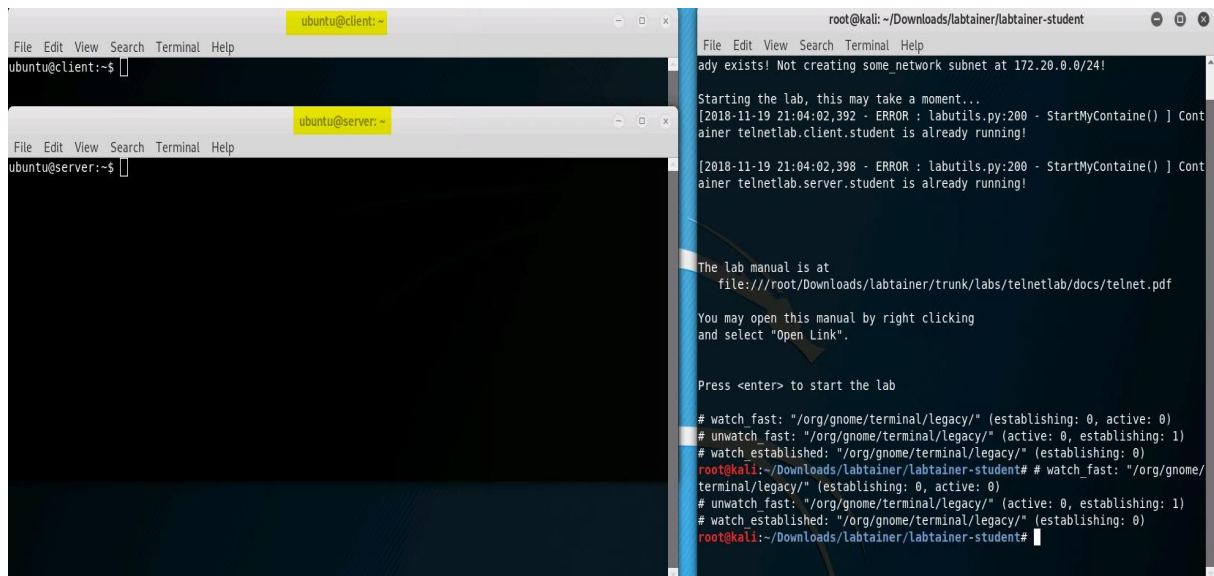
```
root@kali: ~/Downloads/labtainer/labtainer-student
File Edit View Search Terminal Help
root@kali:~/Downloads/labtainer/labtainer-student# labtainer telnetlab
[2018-11-19 21:04:02,093 - WARNING : labutils.py:581 - CreateSubnets() ] Already exists! Not creating some_network subnet at 172.20.0.0/24
!
Starting the lab, this may take a moment...
[2018-11-19 21:04:02,392 - ERROR : labutils.py:200 - StartMyContainee() ] Container telnetlab.client.student is already running!
[2018-11-19 21:04:02,398 - ERROR : labutils.py:200 - StartMyContainee() ] Container telnetlab.server.student is already running!

The lab manual is at
file:///root/Downloads/labtainer/trunk/labs/telnetlab/docs/telnet.pdf

You may open this manual by right clicking
and select "Open Link".

Press <enter> to start the lab
```

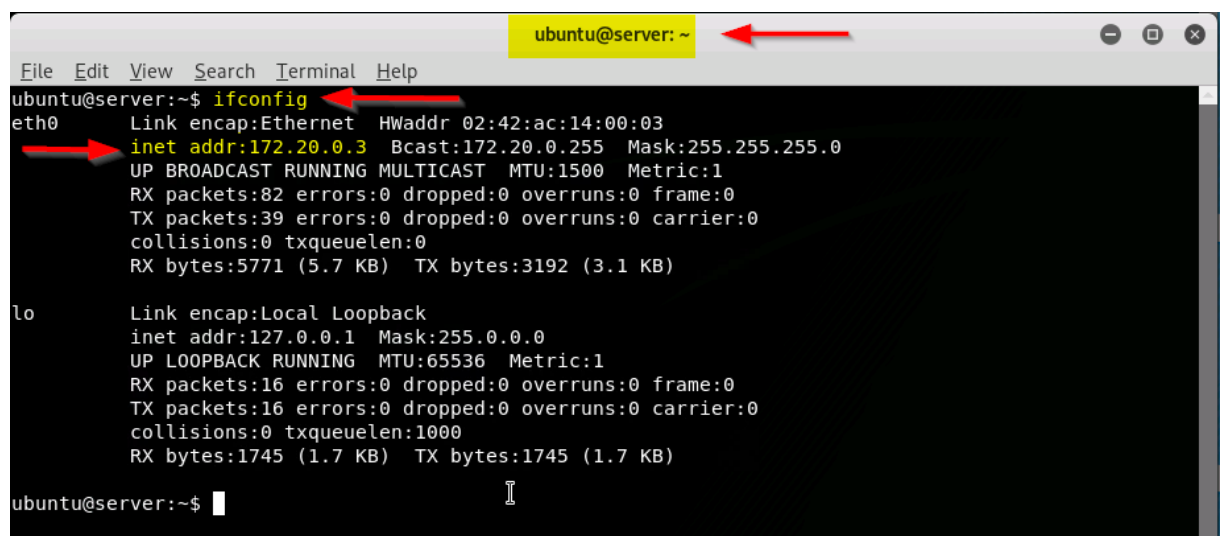
The resulting virtual terminals include one connected to a client computer, and a terminal connected to a server.



Tasks

1. Determine the server IP address

In the server window, type "ifconfig" to view the IP address of the server. The server IP address will follow the "inet addr:" label.



The image shows two terminal windows side-by-side. The top window is titled 'ubuntu@client: ~' and shows the output of the 'ifconfig' command. It displays details for the 'eth0' interface (IP: 172.20.0.2) and the 'lo' loopback interface (IP: 127.0.0.1). The bottom window is titled 'ubuntu@server: ~' and also shows the output of the 'ifconfig' command. It displays details for the 'eth0' interface (IP: 172.20.0.3) and the 'lo' loopback interface (IP: 127.0.0.1). Both windows show standard network statistics like RX/TX packets, errors, and bytes.

```
ubuntu@client: ~  
File Edit View Search Terminal Help  
ubuntu@client:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 02:42:ac:14:00:02  
          inet addr:172.20.0.2  Bcast:172.20.0.255  Mask:255.255.255.0  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:17 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:1382 (1.3 KB)  TX bytes:0 (0.0 B)  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          UP LOOPBACK RUNNING  MTU:65536  Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)  
  
ubuntu@server: ~  
File Edit View Search Terminal Help  
ubuntu@server:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 02:42:ac:14:00:03  
          inet addr:172.20.0.3  Bcast:172.20.0.255  Mask:255.255.255.0  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:1452 (1.4 KB)  TX bytes:0 (0.0 B)  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          UP LOOPBACK RUNNING  MTU:65536  Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)  
  
ubuntu@server:~$
```

2. Telnet to telnet server and display a file on the server

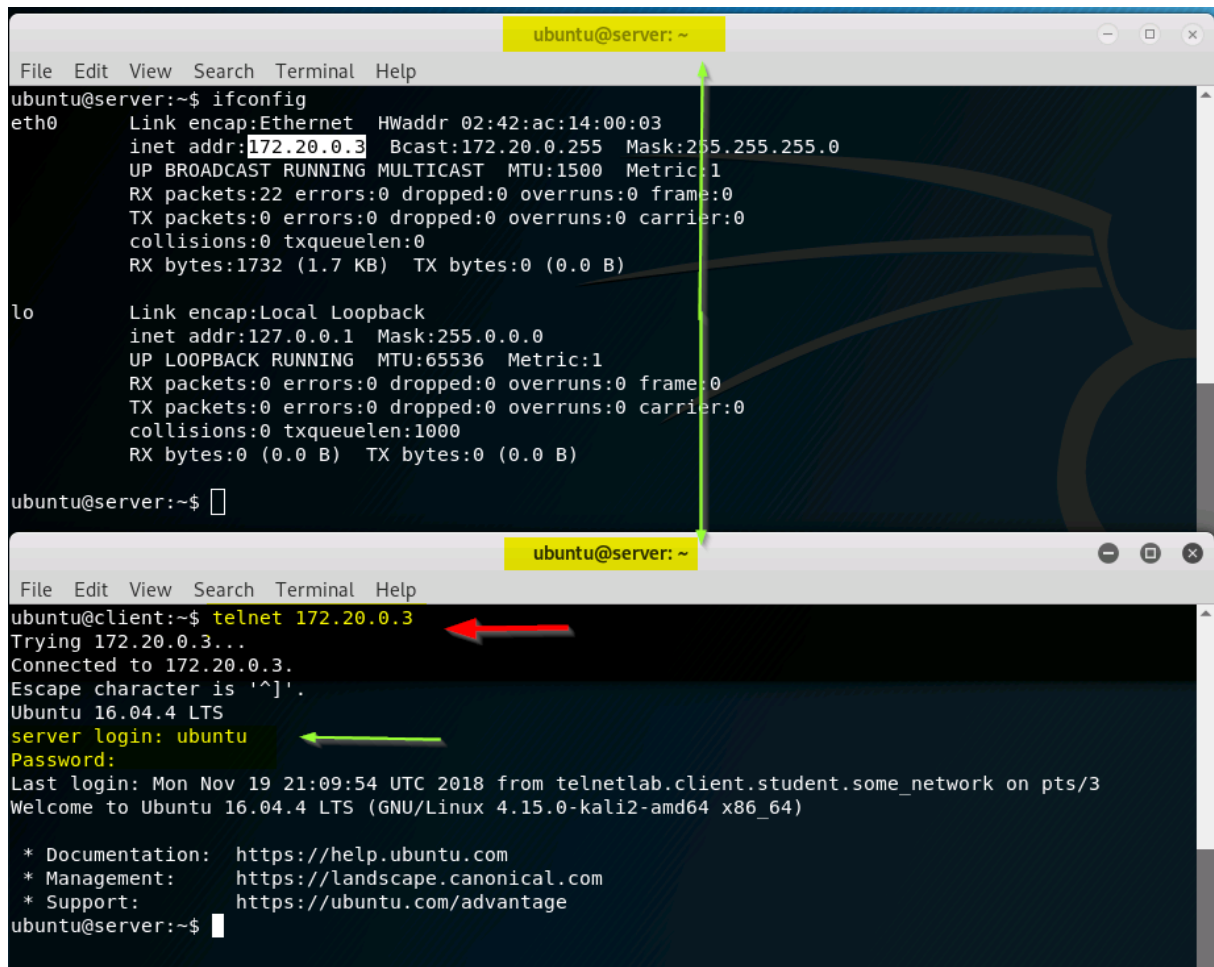
On the client computer, use the telnet command to access the server using its IP address:

telnet <IP>

The image shows two terminal windows. The top window is titled 'ubuntu@server: ~' and shows the output of the 'ifconfig' command. A red arrow points to the IP address '172.20.0.3' in the 'inet addr' line. The bottom window is titled 'ubuntu@client: ~' and shows the command 'telnet 172.20.0.3' being entered. A red arrow points to the IP address '172.20.0.3' in the command.

```
ubuntu@server: ~  
File Edit View Search Terminal Help  
ubuntu@server:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 02:42:ac:14:00:03  
          inet addr:172.20.0.3  Bcast:172.20.0.255  Mask:255.255.255.0  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:22 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:1732 (1.7 KB)  TX bytes:0 (0.0 B)  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          UP LOOPBACK RUNNING  MTU:65536  Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)  
  
ubuntu@server:~$  
  
ubuntu@client: ~  
File Edit View Search Terminal Help  
ubuntu@client:~$ telnet 172.20.0.3
```

You will be prompted for a user ID and then a password. Both of them are “ubuntu”



The image shows two terminal windows. The top window is titled 'ubuntu@server: ~' and displays the output of the 'ifconfig' command for 'eth0' and 'lo'. The 'eth0' interface has IP address 172.20.0.3. The bottom window is titled 'ubuntu@client: ~' and shows a 'telnet 172.20.0.3' command being executed. It shows a successful connection to 172.20.0.3, with the prompt 'server login: ubuntu' and 'Password:' followed by a login message and system information. A green arrow points from the IP address '172.20.0.3' in the top window to the 'telnet 172.20.0.3' command in the bottom window. A red arrow points from the 'server login: ubuntu' prompt to the 'Password:' prompt.

```
ubuntu@server:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 02:42:ac:14:00:03
          inet addr:172.20.0.3  Bcast:172.20.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:22 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1732 (1.7 KB)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

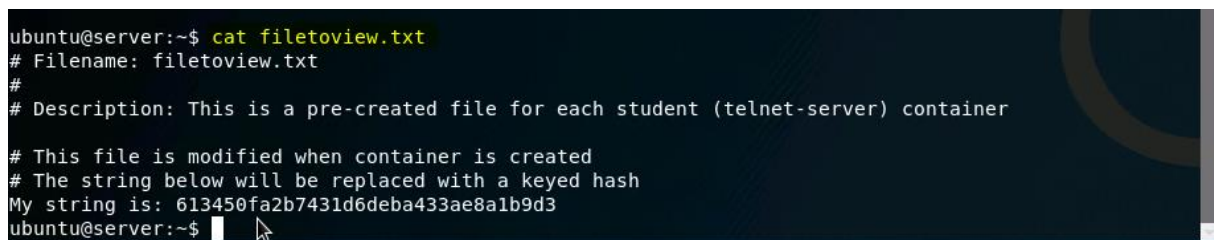
ubuntu@server:~$

ubuntu@client:~$ telnet 172.20.0.3
Trying 172.20.0.3...
Connected to 172.20.0.3.
Escape character is '^]'.
Ubuntu 16.04.4 LTS
server login: ubuntu
Password:
Last login: Mon Nov 19 21:09:54 UTC 2018 from telnetlab.client.student.some_network on pts/3
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.15.0-kali2-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
ubuntu@server:~$
```

There is a pre-created file on the server named “filetoview.txt” .

View the file content by typing: `cat filetoview.txt`



The image shows a terminal window titled 'ubuntu@server: ~' with the command 'cat filetoview.txt' executed. The output shows the content of the file, which includes a filename, a description, and a string to be replaced with a keyed hash.

```
ubuntu@server:~$ cat filetoview.txt
# Filename: filetoview.txt
#
# Description: This is a pre-created file for each student (telnet-server) container
#
# This file is modified when container is created
# The string below will be replaced with a keyed hash
My string is: 613450fa2b7431d6deba433ae8a1b9d3
ubuntu@server:~$
```

Exit the telnet session on the client via the “exit” command.



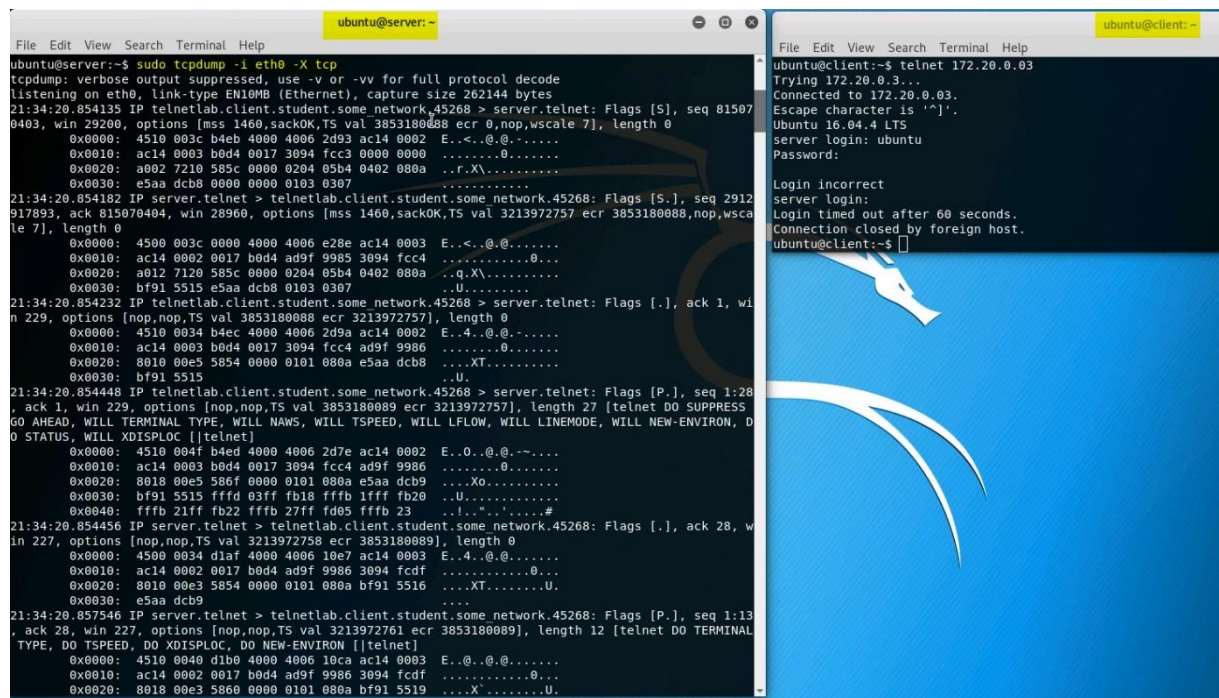
The image shows a terminal window titled 'ubuntu@server: ~' with the command 'exit' executed. The output shows 'logout' and 'Connection closed by foreign host.' followed by the prompt 'ubuntu@client:~\$'.

```
ubuntu@server:~$ exit
logout
Connection closed by foreign host.
ubuntu@client:~$
```

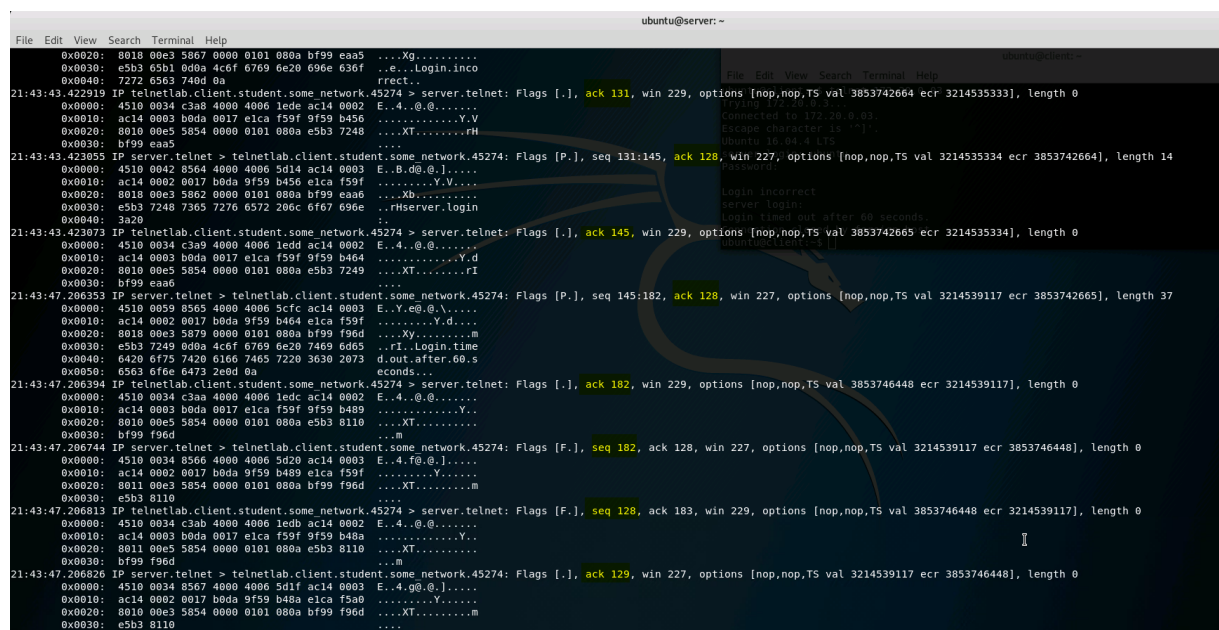

3. View plaintext passwords.

On the server, start tcpdump to display TCP network traffic with this command:

```
sudo tcpdump -i eth0 -X tcp
```



The image shows two terminal windows. The left window, titled 'ubuntu@server:~', displays the output of the command 'sudo tcpdump -i eth0 -X tcp'. It shows a series of network packets captured on the eth0 interface, including the telnet connection establishment and the login process. The right window, titled 'ubuntu@client:~', shows a telnet session initiated from the client to the server (172.20.0.3). The client prompts for a login and password, but the session ends with a 'Login incorrect' message and a 'Connection closed by foreign host.' notification.



The image shows a terminal window titled 'ubuntu@server:~' displaying the output of the command 'sudo tcpdump -i eth0 -X tcp'. It shows a series of network packets captured on the eth0 interface, including the telnet connection establishment and the login process. The right window, titled 'ubuntu@client:~', shows a telnet session initiated from the client to the server (172.20.0.3). The client prompts for a login and password, but the session ends with a 'Login incorrect' message and a 'Connection closed by foreign host.' notification.

On the client start a telnet session, but when prompted for the password type “mydoghasfleas” (as you know this password is incorrect). As you type each letter of the password, observe the tcpdump

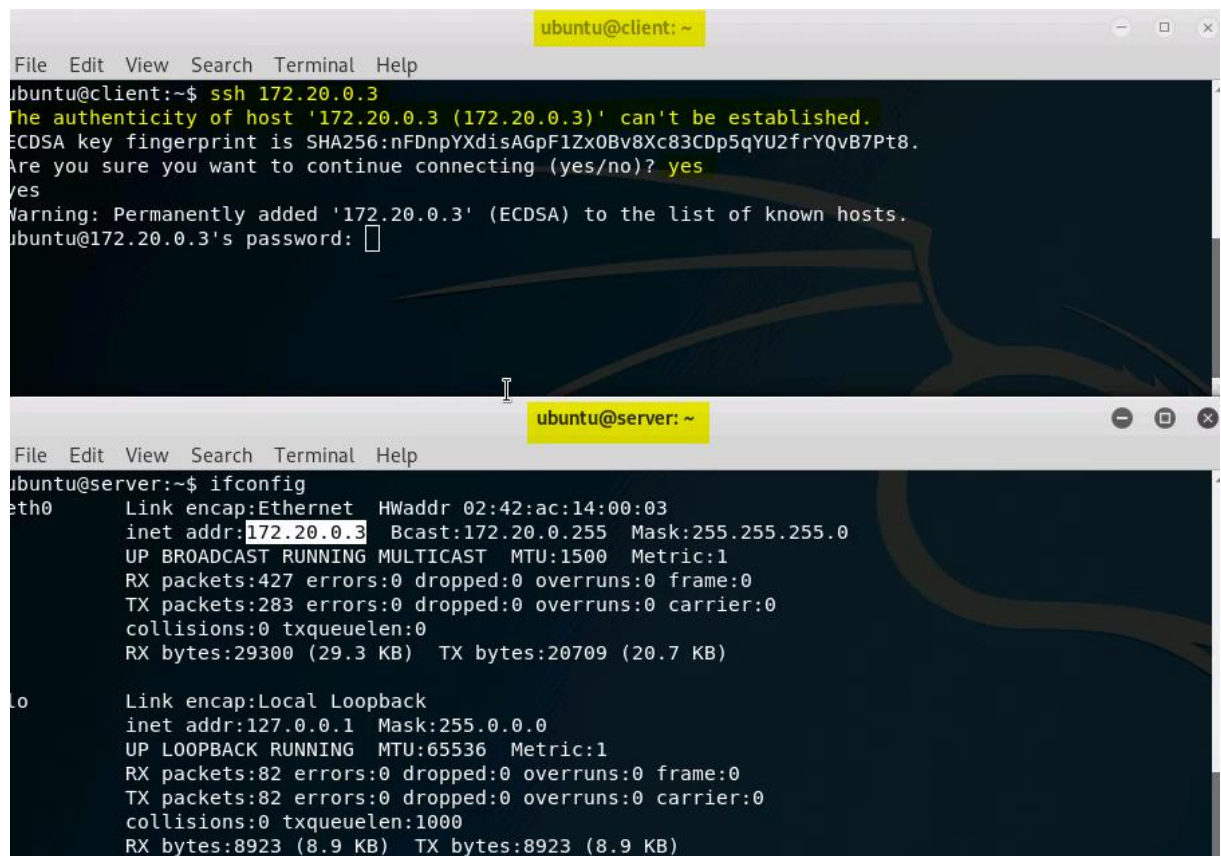
of the traffic. Keeping in mind that every other packet is an “ack” , do you see the password. What do you notice?

```
ubuntu@server: ~
File Edit View Search Terminal Help
21:49:37.572797 IP telnetlab.client.student.some.network.45276 > server.telnet: Flags [.], ack 112, win 229, options [nop,nop,TS val 3854096820 ecr 3214889489], length 0
0x0000: 4510 0034 4221 4000 4006 a065 ac14 0002 E..4B!@.e....
0x0010: ac14 0003 b0dc 0017 0e5c f7ca 8619 09bc .....\\.....
0x0020: 8010 00e5 5854 0000 0101 080a e5b8 d9b4 ...XT.....
0x0030: bf9f 5211 ..R.
21:49:37.583766 IP server.telnet > telnetlab.client.student.some.network.45276: Flags [P.], seq 112:206, ack 124, win 227, options [nop,nop,TS val 3214889500 ecr 3854096820], length 94
0x0000: 4510 0092 bc19 4000 4006 260f ac14 0003 E....@.0.&....
0x0010: ac14 0002 0017 b0dc 8619 09bc 0e5c f7ca .....\\.....
0x0020: 8018 00e3 58b2 0000 0101 080a bf9f 521c ....X.....R.
0x0030: e5b8 d9b4 4c61 7374 206c 6f67 696e 3a20 ...Last.login:.
0x0040: 4d6f 6e20 4e6f 7620 3139 2032 313a 3431 Mon.Nov.19.21:41
0x0050: 3a33 3920 5554 4320 3220 3138 2066 726f :39.UTC.2018,fro
0x0060: 6d20 7465 6c6e 6574 6c61 622e 636c 6965 m.telnetlab:clie
0x0070: 6e74 2e73 7475 6465 6e74 2e73 6f6d 655f nt.student.some
0x0080: 6e65 7477 6f72 6b20 6f6e 2070 7473 2f33 network.on.pts/3
0x0090: 0d0a ..
21:49:37.583804 IP telnetlab.client.student.some.network.45276 > server.telnet: Flags [.], ack 206, win 229, options [nop,nop,TS val 3854096831 ecr 3214889500], length 0
0x0000: 4510 0034 4222 4000 4006 a064 ac14 0002 E..4B"@.d....
0x0010: ac14 0003 b0dc 0017 0e5c f7ca 8619 0a1a .....\\.....
0x0020: 8010 00e5 5854 0000 0101 080a e5b8 d9bf ...XT.....
0x0030: bf9f 521c ..R.
21:49:37.596536 IP server.telnet > telnetlab.client.student.some.network.45276: Flags [P.], seq 206:422, ack 124, win 227, options [nop,nop,TS val 3214889512 ecr 3854096831], length 216
0x0000: 4510 010c bc1a 4000 4006 2594 ac14 0003 E....@.0.%....
0x0010: ac14 0002 0017 b0dc 8619 0a1a 0e5c f7ca .....\\.....
0x0020: 8018 00e3 592c 0000 0101 080a bf9f 5228 ....Y.....Rf
0x0030: e5b8 d9bf 5765 6c63 6f6d 6520 746f 2055 ...Welcome.to.U
0x0040: 6275 6e74 7520 3136 2e30 342e 3420 4c54 buntu.16.04.4.LT
0x0050: 5320 2847 4e55 2f4c 696e 7578 2034 2e31 S.(GNU/Linux.4.1
0x0060: 352e 302d 6b61 6c69 322d 616d 6436 3420 5.0-kali2-amd64.
0x0070: 7838 365f 3634 290d 0a0d 0a20 2a20 446f x86.64).....*.Do
0x0080: 6375 6d65 6e74 6174 696f 6e3a 2020 6874 cumentation:..ht
0x0090: 7470 733a 2f2f 6865 6c70 2e75 6275 6e74 tps://help.ubunt
0x00a0: 752e 636f 6d0d 0a20 2a20 4d61 6e61 6765 u.com...*.Manage
0x00b0: 6d65 6e74 3a20 2020 2020 6874 7470 733a ment:.....https:
0x00c0: 2f2f 6c61 6e64 7363 6170 652e 6361 6e6f //landscape.cano
0x00d0: 6e69 6361 6c2e 636f 6d0d 0a20 2a20 5375 nical.com...*.Su
0x00e0: 7070 6f72 743a 2020 2020 2020 2020 6874 pport:.....ht
0x00f0: 7470 733a 2f2f 7562 756e 7475 2e63 6f6d tps://ubuntu.co
0x0100: 2f61 6476 616e 7461 6765 0d0a /advantage..
21:49:37.596586 IP telnetlab.client.student.some.network.45276 > server.telnet: Flags [.], ack 422, win 237, options [nop,nop,TS val 3854096843 ecr 3214889512], length 0
0x0000: 4510 0034 4223 4000 4006 a063 ac14 0002 E..4B#@.c....
0x0010: ac14 0003 b0dc 0017 0e5c f7ca 8619 0af2 .....\\.....
0x0020: 8010 00ed 5854 0000 0101 080a e5b8 d9cb ...XT.....
0x0030: bf9f 5228 ..Rf
21:49:37.625185 IP server.telnet > telnetlab.client.student.some.network.45276: Flags [P.], seq 422:460, ack 124, win 227, options [nop,nop,TS val 3214889541 ecr 3854096843], length 38
0x0000: 4510 005a bc1b 4000 4006 2645 ac14 0003 E..Z..@.0.&....
0x0010: ac14 0002 0017 b0dc 8619 0af2 0e5c f7ca .....\\.....
0x0020: 8018 00e3 587a 0000 0101 080a bf9f 5245 ...XT.....
0x0030: bf9f 5245 ..Rf
```

4. Use SSH to protect communications with the server

From the client computer, use the SSH command to access the server using its IP address:

ssh <IP>



The image shows two terminal windows. The top window, titled 'ubuntu@client: ~', shows the execution of the 'ssh 172.20.0.3' command. It displays a warning about the host's authenticity, a SHA256 fingerprint, and a prompt to confirm the connection. The user responds with 'yes', and the terminal shows the user is now logged into the server as 'ubuntu@172.20.0.3's password:'. The bottom window, titled 'ubuntu@server: ~', shows the output of the 'ifconfig' command. It displays details for the 'eth0' interface (Ethernet) and the 'lo' interface (Local Loopback).

```
ubuntu@client: ~  
File Edit View Search Terminal Help  
ubuntu@client:~$ ssh 172.20.0.3  
The authenticity of host '172.20.0.3 (172.20.0.3)' can't be established.  
ECDSA key fingerprint is SHA256:nFDnpYXdisAGpF1Zx0Bv8Xc83CDp5qYU2frYQvB7Pt8.  
Are you sure you want to continue connecting (yes/no)? yes  
yes  
Warning: Permanently added '172.20.0.3' (ECDSA) to the list of known hosts.  
ubuntu@172.20.0.3's password:   
  
ubuntu@server: ~  
File Edit View Search Terminal Help  
ubuntu@server:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 02:42:ac:14:00:03  
          inet addr:172.20.0.3  Bcast:172.20.0.255  Mask:255.255.255.0  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:427 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:283 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:29300 (29.3 KB)  TX bytes:20709 (20.7 KB)  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          UP LOOPBACK RUNNING  MTU:65536  Metric:1  
          RX packets:82 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:82 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:8923 (8.9 KB)  TX bytes:8923 (8.9 KB)
```

The first time you SSH to a server, SSH will warn you that the “authenticity of the host… can’ t be established” . Type “yes” at the prompt.


```
ubuntu@server: ~  
File Edit View Search Terminal Help  
ubuntu@server:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 02:42:ac:14:00:03  
          inet addr:172.20.0.3  Bcast:172.20.0.255  Mask:255.255.255.0  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:62 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:30 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:6845 (6.8 KB)  TX bytes:5401 (5.4 KB)  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          UP LOOPBACK RUNNING  MTU:65536  Metric:1  
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:212 (212.0 B)  TX bytes:212 (212.0 B)  
  
ubuntu@server:~$ sudo tcpdump -i eth0 -X tcp
```

```
ubuntu@client: ~  
File Edit View Search Terminal Help  
ubuntu@client:~$ ssh 172.20.0.3
```

```
ubuntu@server:~$ cat filetoview.txt  
# Filename: filetoview.txt  
#  
# Description: This is a pre-created file for each student (telnet-server) container  
  
# This file is modified when container is created  
# The string below will be replaced with a keyed hash  
My string is: 613450fa2b7431d6deba433ae8a1b9d3  
ubuntu@server:~$
```


from the host labtainer working directory. You can always restart the labtainer and continue your work where you left off. When the Labtainer is stopped, a zip file is created and saved to a location displayed beneath the stoplab. When you are completely finished send that file to your instructor.

```
root@kali:~/Downloads/labtainer/labtainer-student# stoplab telnetlab
Results stored in directory: /root/labtainer_xfer/telnetlab
root@kali:~/Downloads/labtainer/labtainer-student#
```

```
root@kali:~/Downloads/labtainer/labtainer-student# checkwork telnetlab
telnetlab lab is not running, looking for previous results...
Labname

Student      |
=====
What is automatically assessed for this lab:
  failed_login: Failed login as expected.
  telnetview: viewed file from telnet
  sshview: viewed file from ssh
root@kali:~/Downloads/labtainer/labtainer-student#
```