Telnet Lab Exercise

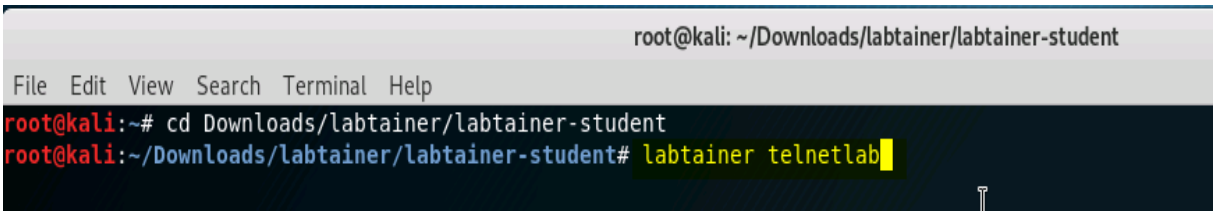
Overview

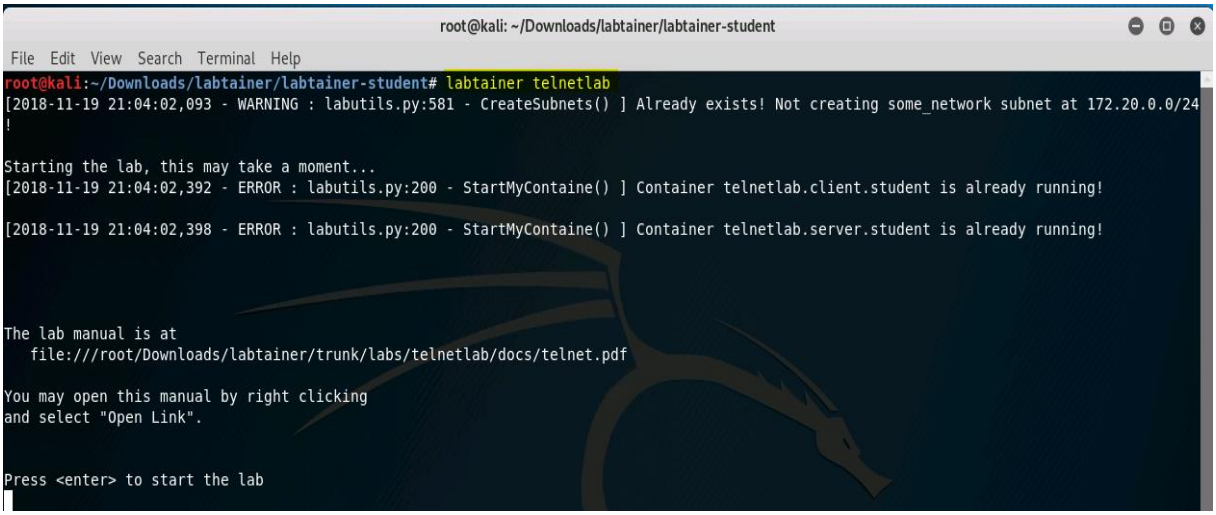
This labtainer exercise illustrates the use of a telnet client to access resources on a server. It is a simple lab intended to illustrate basic client server networking and the transmission of plaintext passwords over a network by telnet.

Performing the lab

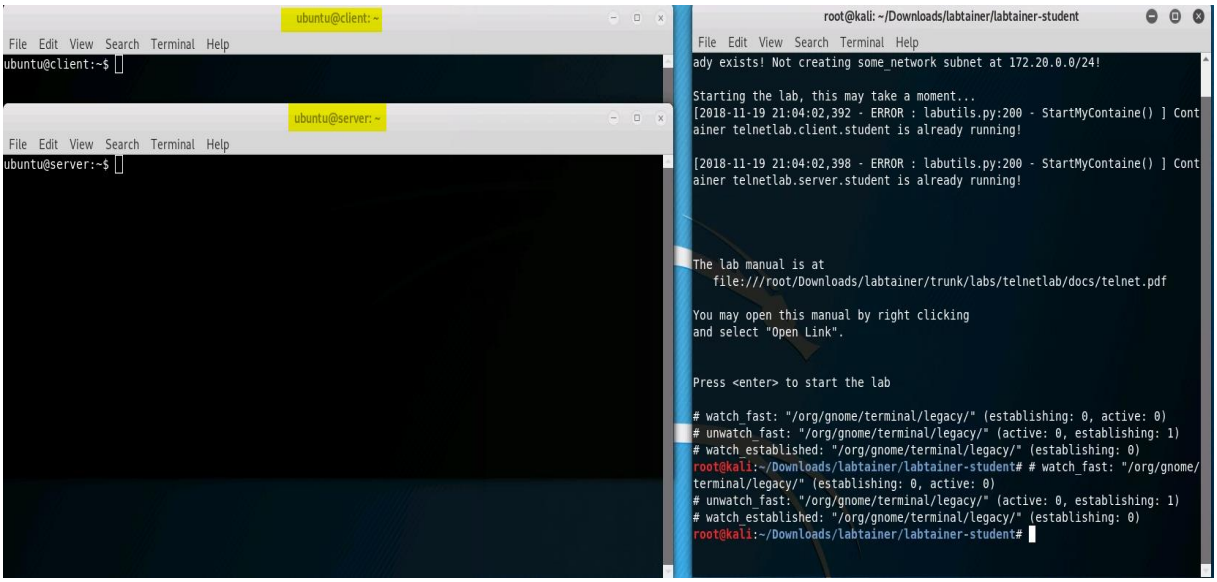
The lab is started from the labtainer working directory on your Linux host, e.g., a Linux VM. From there, issue the command:

labtainer telnetlab





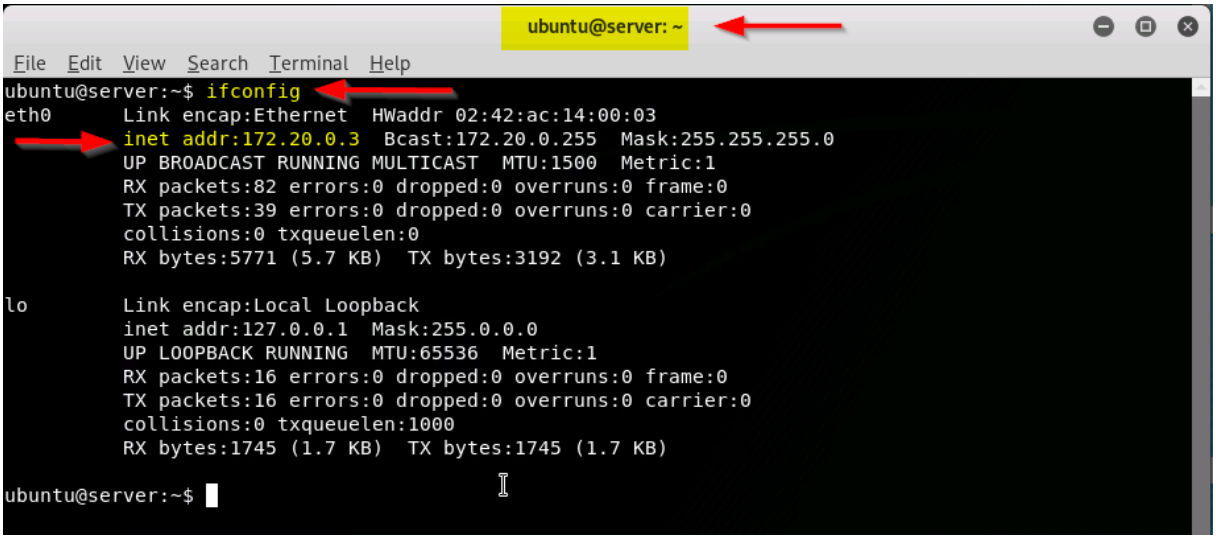
The resulting virtual terminals include one connected to a client comptuer, and a terminal connected to a server.



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.



```
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 comptuer, use the telnet command to access the server using its IP address:

telnet <IP>

```
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”

```
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@server: ~
File  Edit  View  Search  Terminal  Help
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

```
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:~$
```

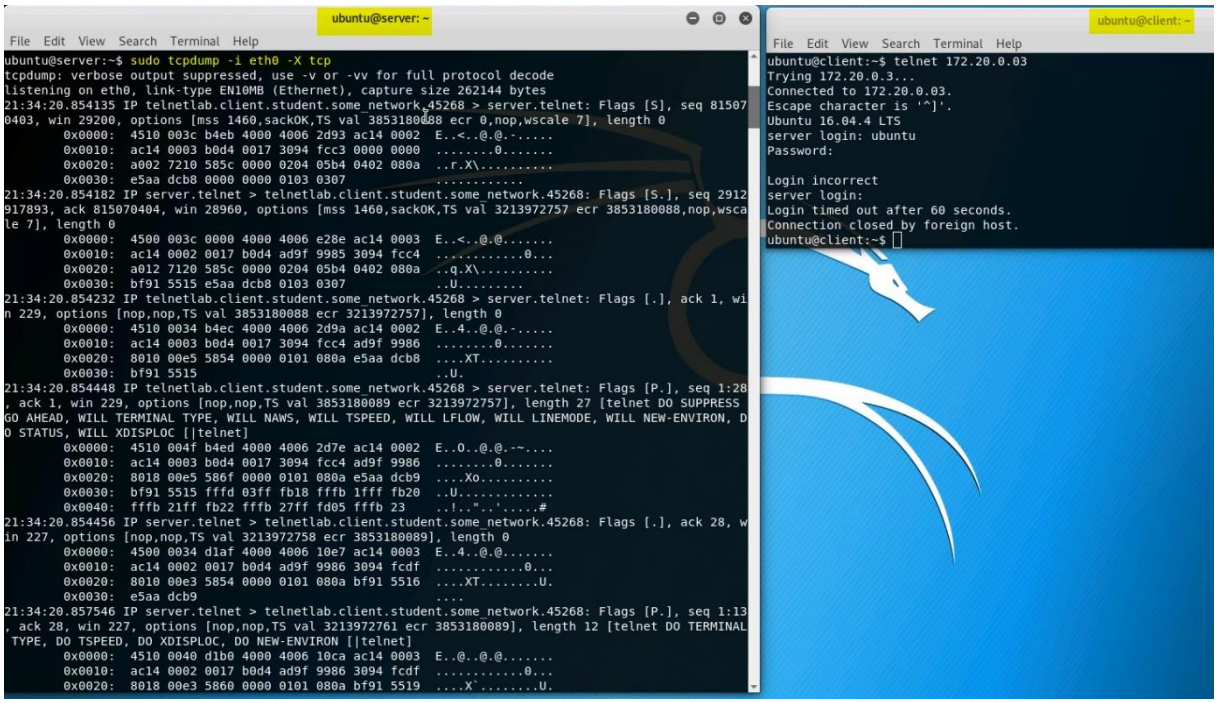
Exit the telnet session on the client via the “exit” command.

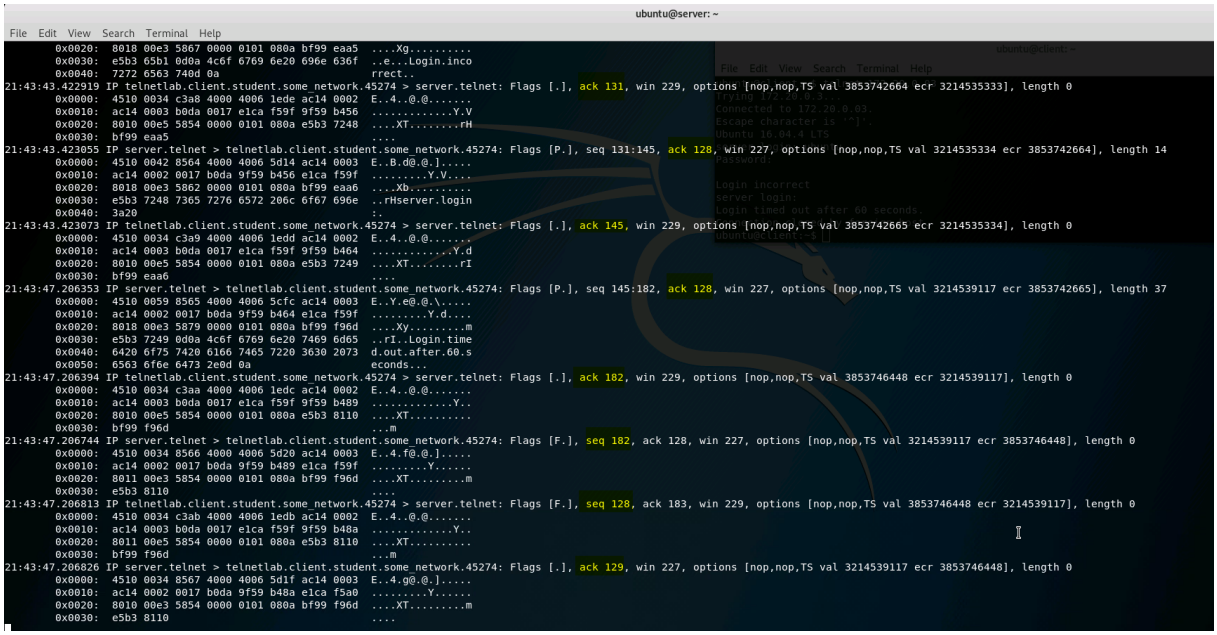
```
ubuntu@server:~$ exit
logout
Connection closed by foreign host.
ubuntu@client:~$
```

3. View plaintext passwords.

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

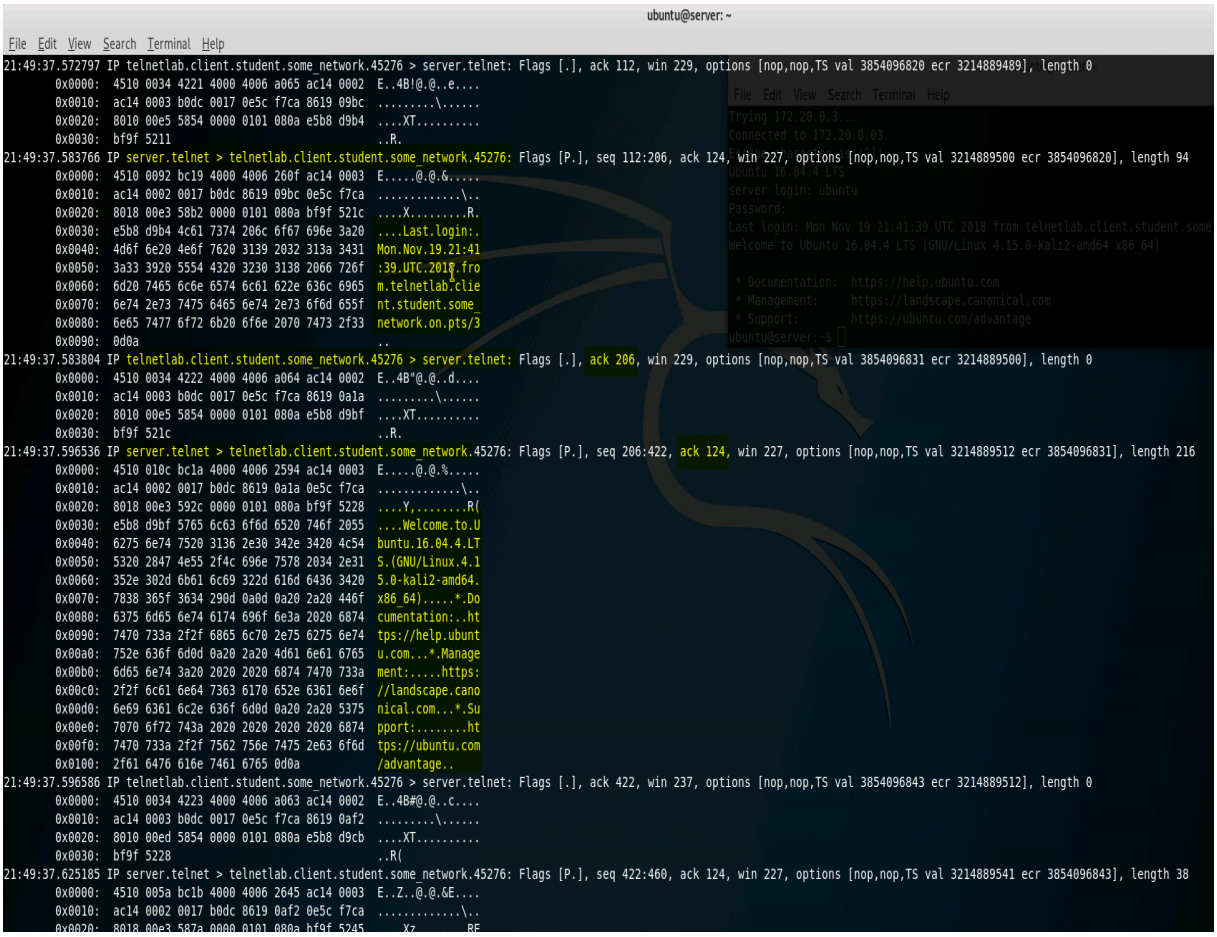
```
sudo tcpdump -i eth0 -X tcp
```





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

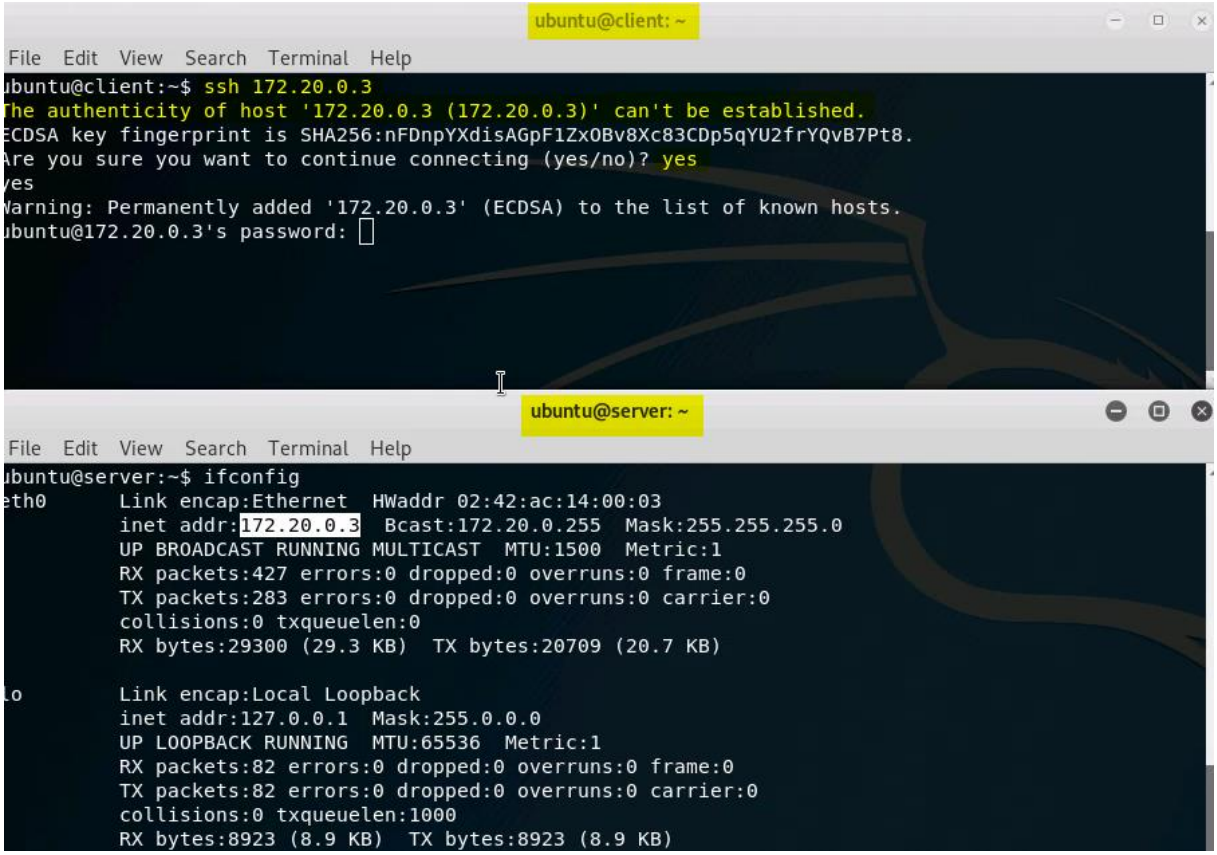
of the traffic. Keeping in mind that every other packet is an “ack”, do you see the password. What do you notice?



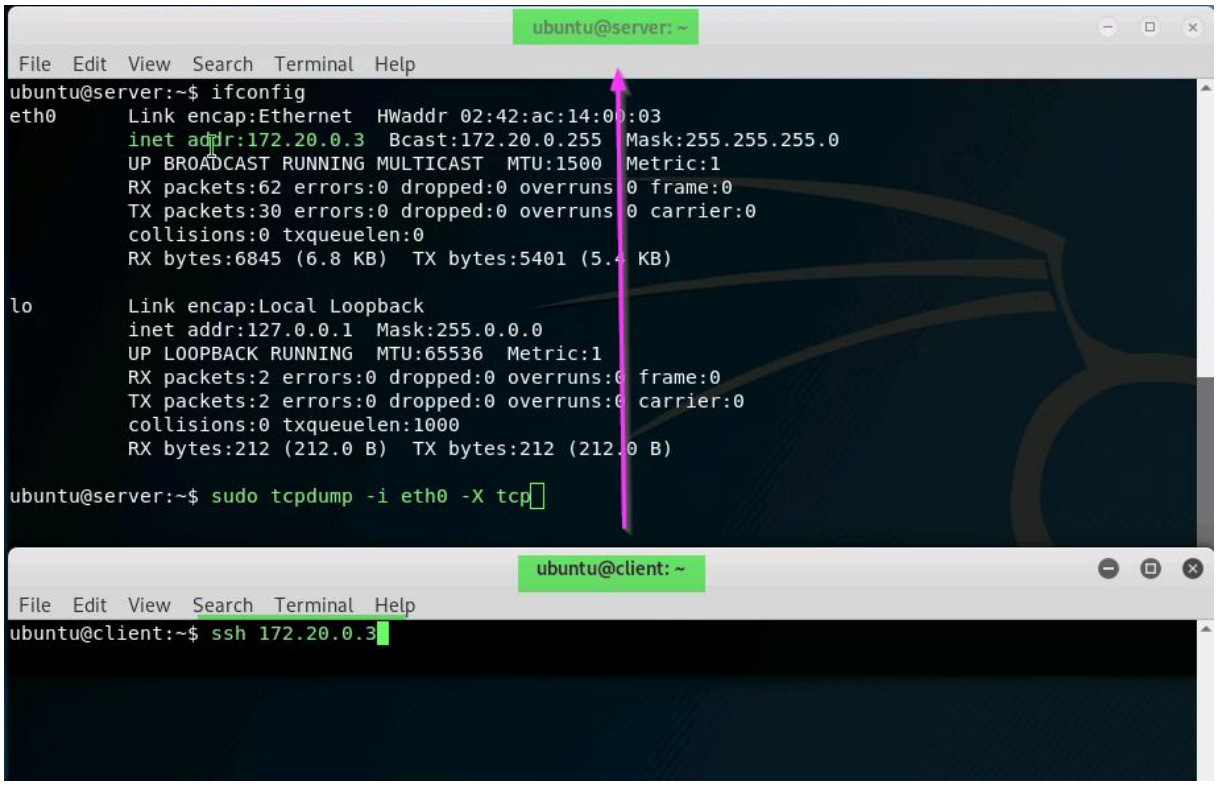
4. **Use SSH to protect communications with the server**

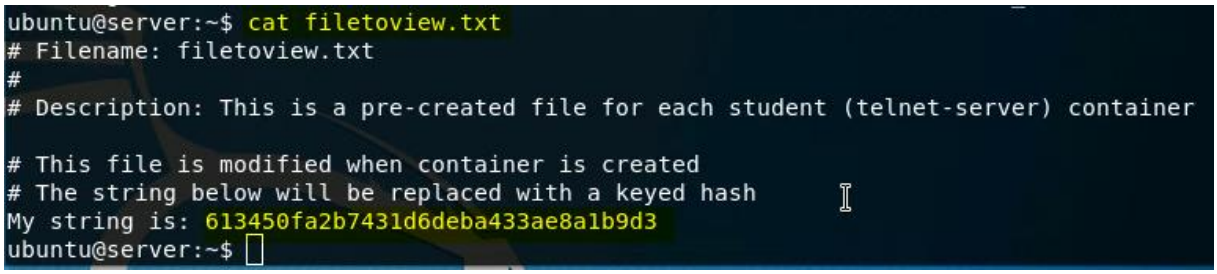
From the client computer, use the SSH command to access the server using its IP address:

ssh <IP>



The 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:~$

```
ubuntu@client:~$ ssh 172.20.0.3
ubuntu@172.20.0.3's password:
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
Last login: Sat Nov 24 14:25:20 2018 from 172.20.0.2
ubuntu@server:~$
```

ubuntu

```
ubuntu@server:~$ sudo tcpdump -i eth0 -X tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:25:39.195751 IP telnetlab.client.student.some_network.55974 > server.ssh: Flags [S], seq 20102898
55, win 29200, options [mss 1460,sackOK,TS val 3709951032 ecr 0,nop,wscale 7], length 0
        0x0000:  4500 003c bcf0 4000 4006 259e ac14 0002  E..<..@.@.%.....
        0x0010:  ac14 0003 daa6 0016 77d2 96bf 0000 0000  ........w.......
        0x0020:  a002 7210 585c 0000 0204 05b4 0402 080a  ..r.X\..........
        0x0030:  dd21 5c38 0000 0000 0103 0307            .!\8........
14:25:39.195793 IP server.ssh > telnetlab.client.student.some_network.55974: Flags [S.], seq 3817082
996, ack 2010289856, win 28960, options [mss 1460,sackOK,TS val 3912451050 ecr 3709951032,nop,wscale
 7], length 0
        0x0000:  4500 003c 0000 4000 4006 e28e ac14 0003  E..<..@.@.......
        0x0010:  ac14 0002 0016 daa6 e384 1074 77d2 96c0  ...........tw...
        0x0020:  a012 7120 585c 0000 0204 05b4 0402 080a  ..q.X\..........
        0x0030:  e933 43ea dd21 5c38 0103 0307            .3C..!\8....
14:25:39.195821 IP telnetlab.client.student.some_network.55974 > server.ssh: Flags [.], ack 1, win 2
29, options [nop,nop,TS val 3709951032 ecr 3912451050], length 0
        0x0000:  4500 0034 bcf1 4000 4006 25a5 ac14 0002  E..4..@.@.%.....
        0x0010:  ac14 0003 daa6 0016 77d2 96c0 e384 1075  ........w......u
        0x0020:  8010 00e5 5854 0000 0101 080a dd21 5c38  ....XT.......!\8
        0x0030:  e933 43ea                                .3C.
14:25:39.196187 IP telnetlab.client.student.some_network.55974 > server.ssh: Flags [P.], seq 1:42, a
ck 1, win 229, options [nop,nop,TS val 3709951032 ecr 3912451050], length 41
        0x0000:  4500 005d bcf2 4000 4006 257b ac14 0002  E..]..@.@.%{....
        0x0010:  ac14 0003 daa6 0016 77d2 96c0 e384 1075  ........w......u
        0x0020:  8018 00e5 587d 0000 0101 080a dd21 5c38  ....X}.......!\8
        0x0030:  e933 43ea 5353 482d 322e 302d 4f70 656e  .3C.SSH-2.0-Open
        0x0040:  5353 485f 372e 3270 3220 5562 756e 7475  SSH_7.2p2.Ubuntu
```

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

```
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:~$
```

Observe the tcpdump output, and note that there is no readable plain text.

Stop the Labtainer

When the lab is completed, or you'd like to stop working for a while, run:

```
stoplab telnetlab
```

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#
```