**Telnet Project**

**Overview: This project highlights utilizing resources using a Telnet server on an Ubuntu VM machine.**

**Instructions:**

**Step 1: Add project for LabtainerVM from** [Ubuntu Lab Virtual Machine](https://ablative.gumroad.com/l/eplsqw)

**Step 2: Download LabtainerVM-VirtualBox.ova**

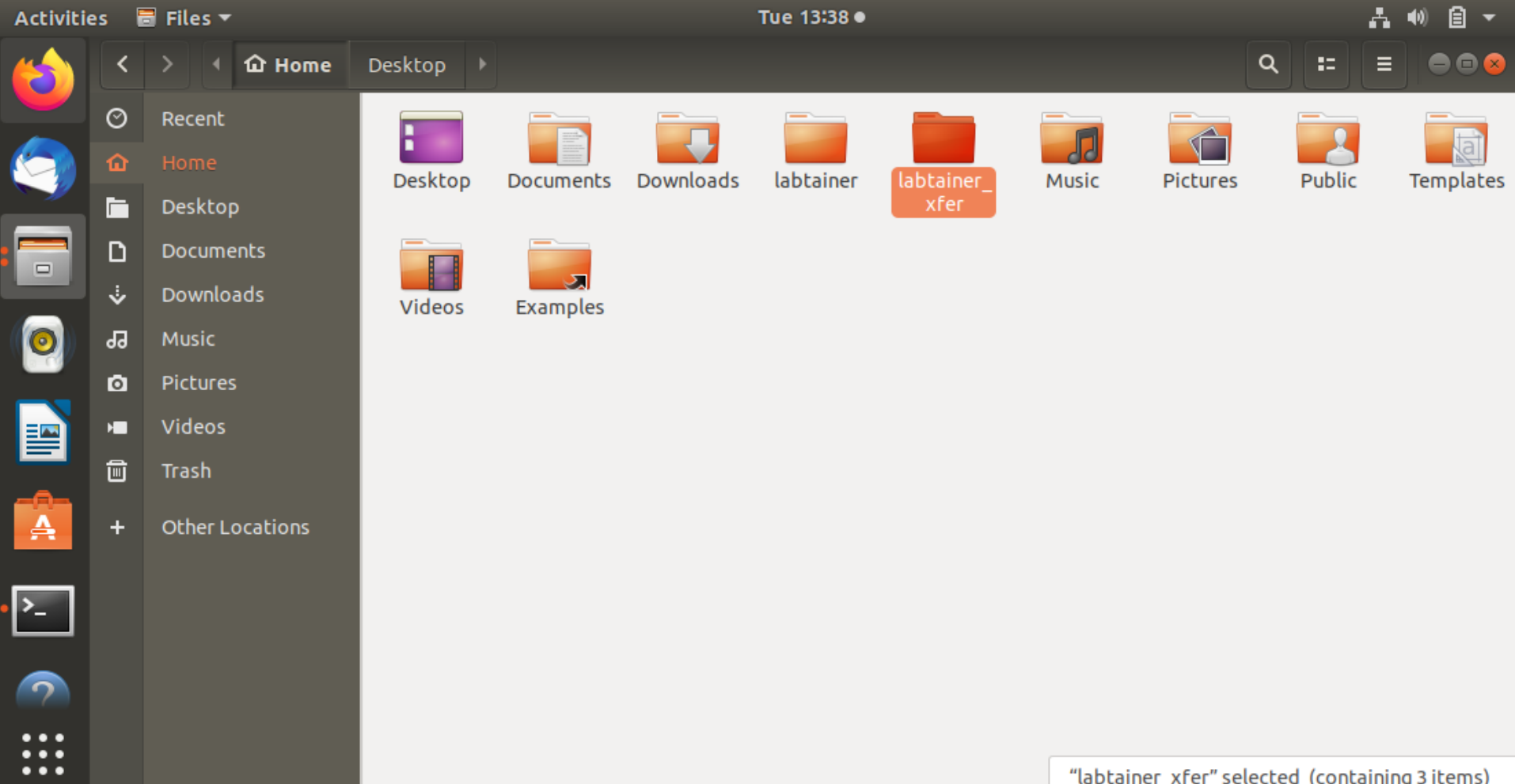
**Step 3: Open OVA file**

**Step 4: Launch LabtainerVM virtual machine**

**Getting Started**

**Once your VM has launched and the Ubuntu logo flashes you will be see a terminal on your screen. Select “Files” on the left of your screen and then select “Home”.**

**Click “labtainer\_xfer” file folder**

****

**Select “TelnetLab”**

**A screenshot of a computer

Description automatically generated**

**Select highlighted Zip file**

**A screenshot of a computer

Description automatically generated**

**Select Doc.zip**

**A screenshot of a computer

Description automatically generated**

**All the files listed for this lab will be here**

**A screenshot of a computer

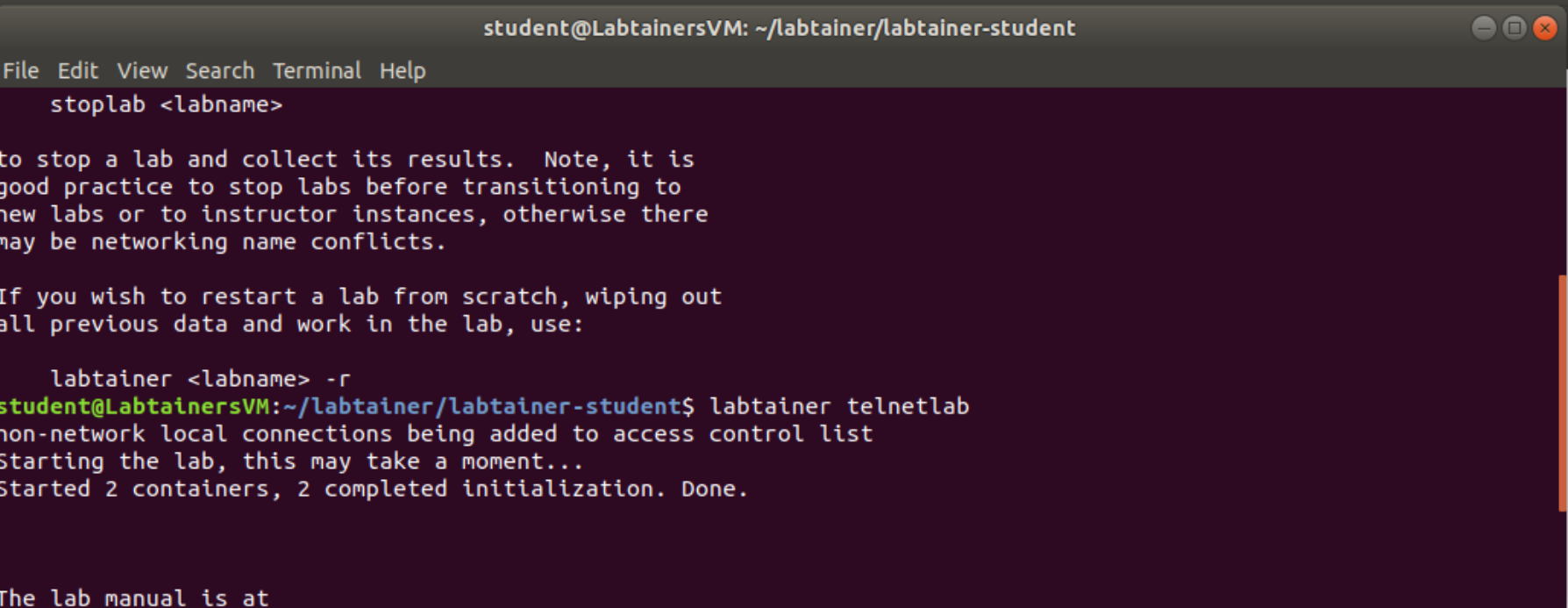
Description automatically generated**

**Performing the Lab:**

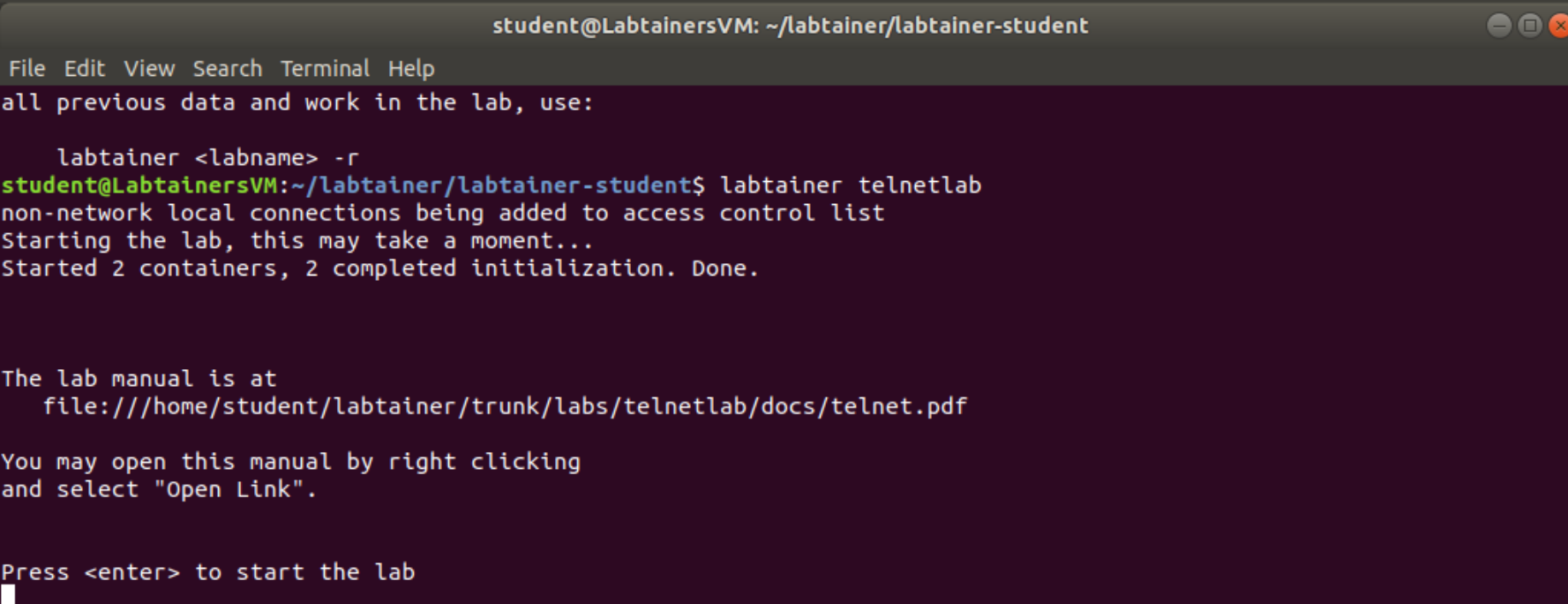
**Open “Telnet.pdf” file in doc.zip and follow the instructions.**

**Locate the terminal and enter the following command:**

labtainer telnetlab



Press “Enter” to start lab



**Notice two terminals will appear (Ubuntu Client and Ubuntu Server)**

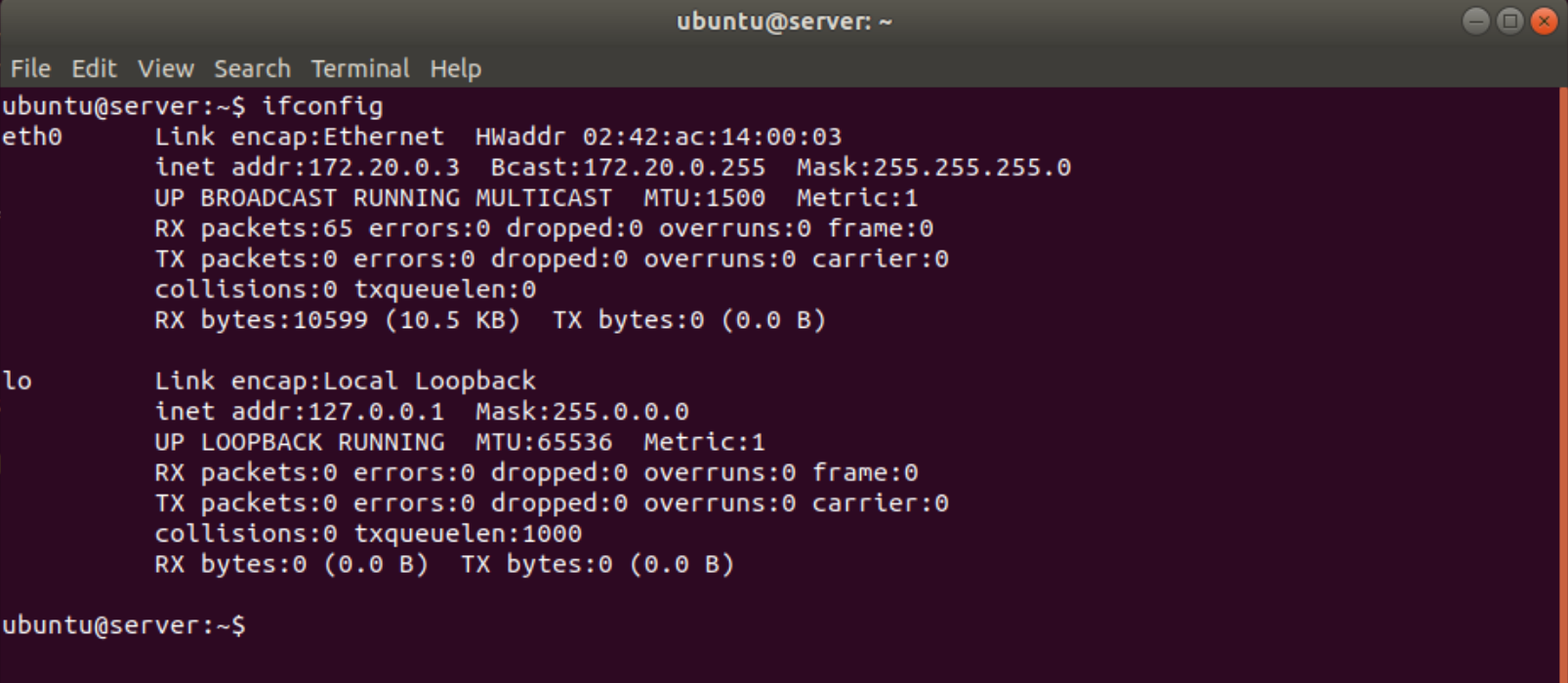
A screenshot of a computer

Description automatically generated

**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**



**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>**

A screenshot of a computer

Description automatically generated

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

**NOTE: While you type the password, no characters will display.**

Once you’ve logged in the Ubuntu client will turn into the Ubuntu Server

A screenshot of a computer

Description automatically generated

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

**View the file content by typing:**

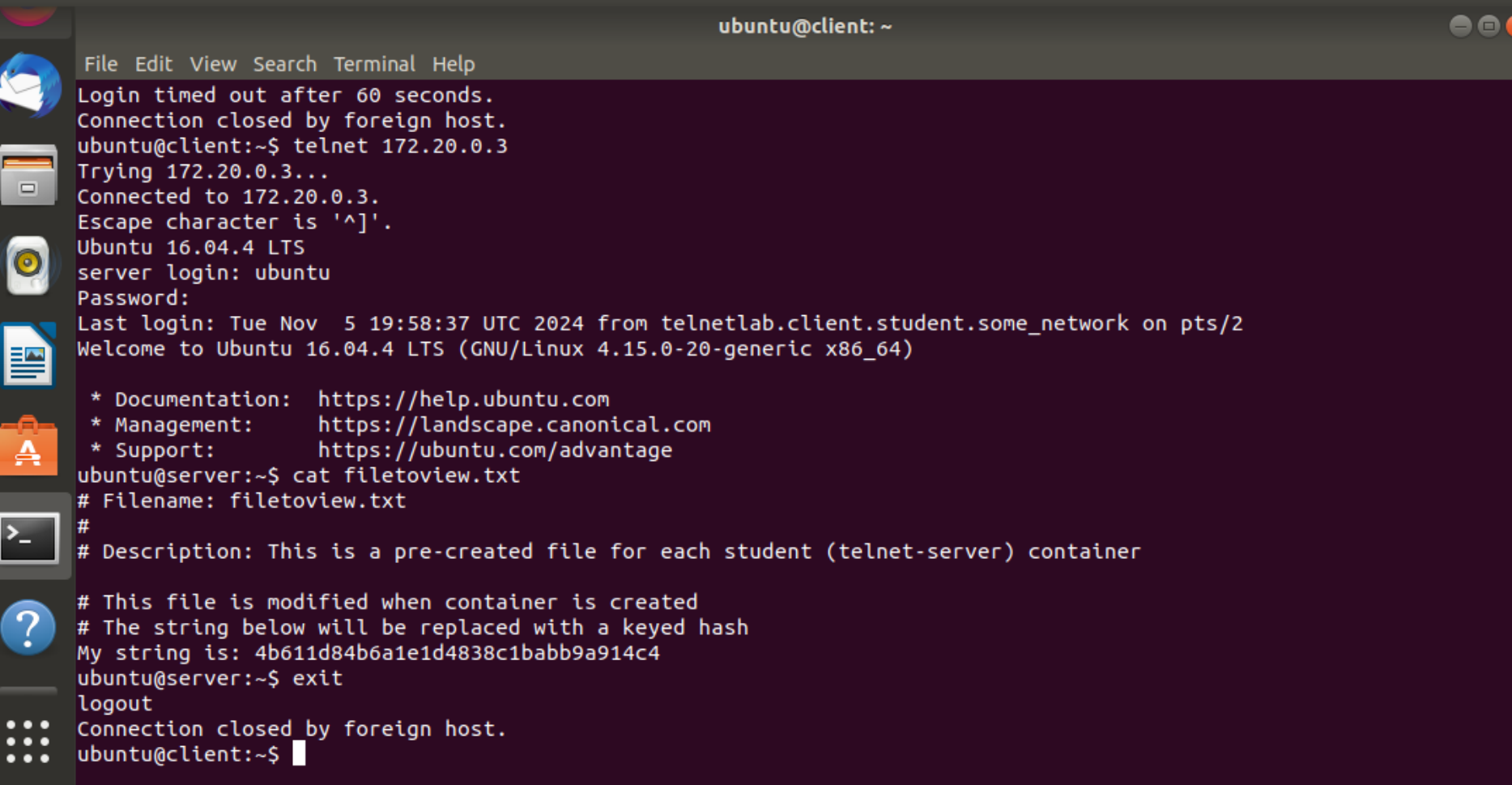
cat filetoview.txt (Cat will list out contents of .txt document)

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

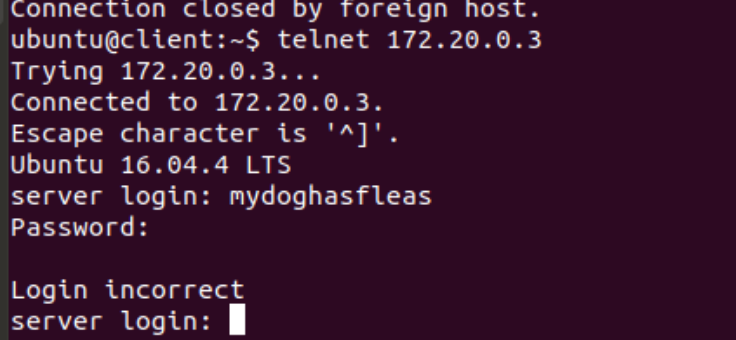
**3. View plaintext passwords.**

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

**sudo tcpdump -i eth0 -X tcpOn** the client start a telnet session, but when prompted for the password type “mydoghasfleas” (as you know this password is incorrect).

A screenshot of a computer

Description automatically generated



As you type each letter of the password, observe the tcpdump of the traffic. (Note: You will notice all of it when you attempt this lab)

A screenshot of a computer

Description automatically generated

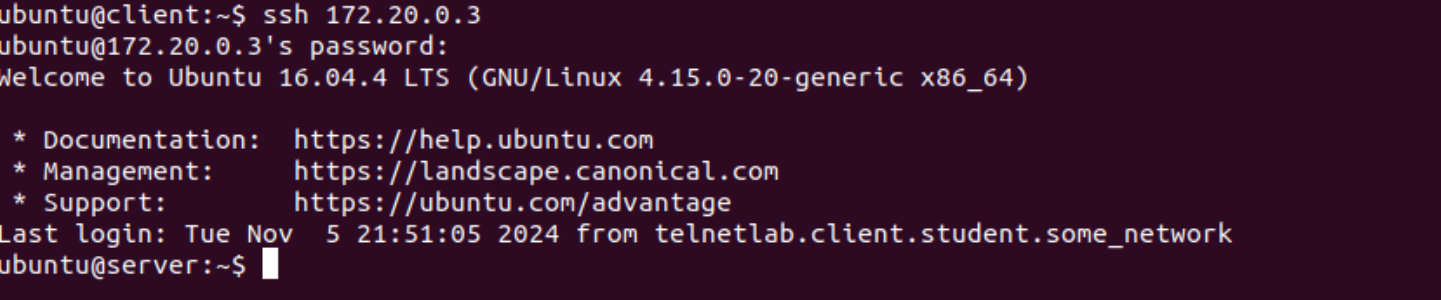
Keeping in mind that every other packet is an “ack”, do you see the password. What do you

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:**

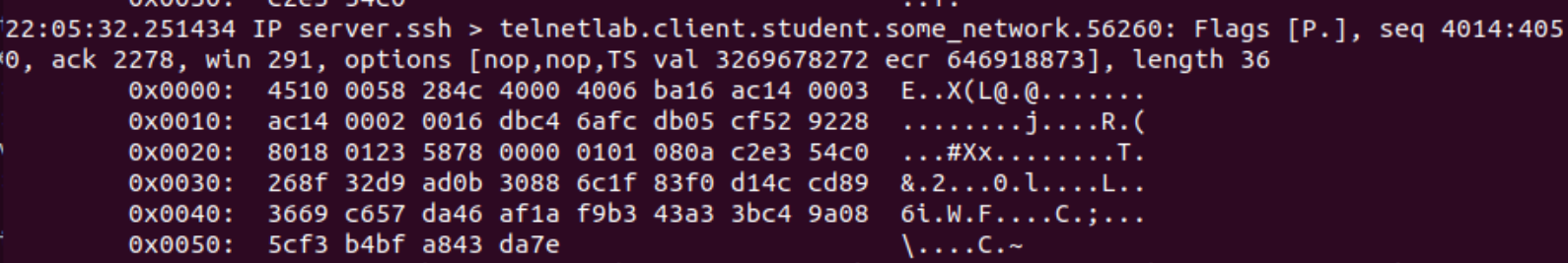
ssh <IP>



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.

**View the file content by typing:**

cat filetoview.txt **(Note: You will notice that the traffic with ssh looks different compared to Telnet. When Telnet was in use you could see the plaintext password and contents from the client. When SSH is deployed you see hashing instead)**



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

stoplab telnetlab