

Lab 1 Report: Basic Linux & Wireshark Tutorial

* Please **fill in the report** and submit the **pdf** to NYUClasses

Name: Shengwei Huang ID: Sh6203 Date: 9/30/2020

1 Objectives

- Get familiar with **Ubuntu** and **Linux commands**
- Learn the network measurement tool: **Wireshark**
 - Get fundamental understanding of cloud computing
 - Compare Dropbox and Google drive

2 Experiment Report

2.1 Get familiar with useful Linux commands

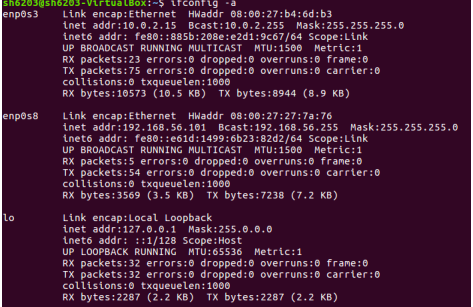
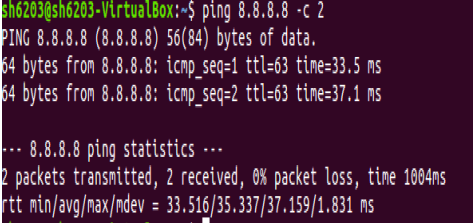
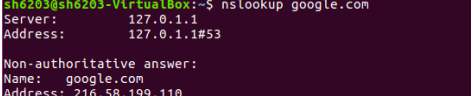
Please run these commands in Ubuntu and explain the commands yourself. (Score will be removed if the descriptions are directly copy-paste from websites. You can refer to <https://explainshell.com/#>)

Commands	Description
\$ sudo apt update	Check the packages can be upgraded and upgrade them
\$ sudo apt install net-tools	Check the version of net-tools and install it
\$ ls -a	List all files include hiding files
\$ mkdir new_folder	Create a new folder
\$ cd new_folder	Into new_folder
\$ cd ..	into the folder we want
\$ nano file.txt (add content and save)	create and edit a text file
\$ cat file.txt	Show the content of the file.txt
\$ cp file.txt new_folder	Copy the file.txt into new_folder
\$ mv new_folder/file.txt .	Move file.txt in new_folder to default directory
\$ rm -r new_folder	Remove folder new_folder
\$ ps	Show the current status of processes
\$ whereis tar	Search the tar file and show all path include tar
\$ whatis tar	Show the way to use tar command
\$ man tar	Show the mannual information of tar command
\$ history	Show what I had typed in the terminal
\$ git	Show the information of git, if it does not install git it will show no git installed
Ctrl-C	suspend

2.2 Get familiar with network debugging commands

Please run these commands in Ubuntu and explain the commands yourself. (You can refer to

<https://explainshell.com/#>)

Commands	Description	Screenshot
\$ ifconfig -a	Show the information of network devices	
\$ ping 8.8.8.8 -c 2	Send ICMP ECHO_REQUEST packets to network hosts, and it will stop after sending and receiving 2 ECHO_RESPONSE packet.	
\$ nslookup google.com	Query google.com servers interactively	

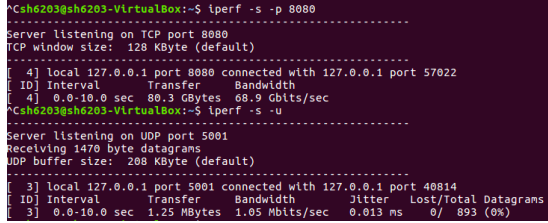
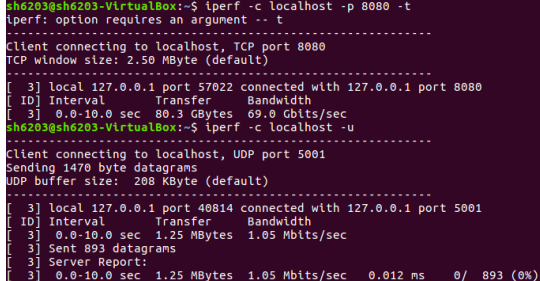
What is "localhost"?
Localhost is a hostname that refers to the current computer used to access it.
What is the ip of "localhost"?
127.0.0.1

1. hping3: TCP/IP packet assembler/analyzer

Assume you are a hacker and want to see which ports are open in one server, you can use: \$ sudo hping3 -c 40 -p ++3000 -i u50000 localhost Please explain the command and which TCP ports did you scan using this command.
Hping3 means send arbitrary TCP/IP packets to network hosts. Here the network hosts will be the localhost. And -c 40 means send packets will be stopped after sending 40 response packets. -p ++3000 means set the destination port will be 3000 and because there is ++ before 3000. So every time for sending packets the destination port 3000 will be increased by 1. -i u50000 means the interval. It will set wait to 50000 micro seconds between each packet.
In the packets you sent for scanning, are those TCP ports in source or destination field? (Hint: you can use "man hping3" for the manual or using Wireshark to capture the packets)
In destination field.

2. iperf: The ultimate speed test tool for TCP, UDP and SCTP (<https://iperf.fr/>)

iperf can be used for bandwidth measurement. Assume you are a curious engineer and try to measure the internal bandwidth between the two terminals. First, please open two terminals in Ubuntu. One of the terminal listens to the ports as a server, and the other one sends measurement packets as a client. On the two terminal, please modify these command and type in to the terminal:

	Server	Client
Commands	\$ iperf -s	\$ iperf -c localhost -p 8080 -t \$ iperf -c localhost -u
Description	To perform the throughput tests of network and run it in server mode. -p 8080 means set a server port as 8080 make client can be listened to. -u means use UDP port rather than TCP port.	lperf -c localhost -p 8080 -t: perform the ththroughput test of network and run it in the client mode. Also connect to the localhost. -p means to set the server port which will listen on. Here -p 8080 means connect to server port 8080. -t means the transmission time in seconds. The default time will be 10s. lperf -c localhost -u: perform the ththroughput test of network and run it in the client mode. Also connect to the localhost. -u means use UDP port rather than TCP port.
Screenshot		

3. ssh: Secure Shell (<https://www.ssh.com/ssh/>)

You can use ssh to login to Ubuntu remotely, using this command: \$ ssh <username>@<ip address>

Please set up the SSH key so that you can log into the Ubuntu without passwords, following step 1 to step 3 in <https://www.digitalocean.com/community/tutorials/how-to-set-up-ssh-keys-on-ubuntu-1604>

More details of how keys work in https://www.youtube.com/watch?v=Nb7cHMc4_og.

Now you want to test whether the keys work, and you use the command:

```
$ ssh localhost
```

Please attach a screenshot to prove that you can ssh to your own ubuntu without passwords.

```
[ShengweideMacBook-Pro:key shengwei Huang$ ssh sh6203@192.168.56.101
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-118-generic x86_64)
```

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

```
16 packages can be updated.
0 updates are security updates.
```

```
New release '18.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
```

```
Last login: Thu Sep 24 22:06:24 2020 from 192.168.56.1
sh6203@sh6203-VirtualBox:~$
```

Example: (SSH key success)

```
cia@hsn1c302:~$ ssh localhost
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-51-generic x86_64)
```

Example: (SSH key fails)

```
cia@hsn1c302:~$ ssh localhost
cia@localhost's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-51-generic x86_64)
```

2.3 Measure network traffic using Wireshark

- 1) Download Wireshark on your host OS. (<https://www.wireshark.org/download.html>)
- 2) Capture packets in your network environment **for ten minute**. (Wireless environment is preferred.)
- 3) Analyze each measurement result and provide the following statistics. Please explore the functions in Wireshark and use the functions to complete the lab.

The following functions may help you with the lab:

"Statistics" -> "Conversations"	Help you measure the data
"Analyze" -> "Expert Information"	find transmission errors
filter	You can use the filter to help you filter the broadcast packets. Ref. https://wiki.wireshark.org/DisplayFilters

Table 1 Network Traffic Measurement

	Results
Total number of packets captured	13828
Total number of bytes captured	8683800
Percentage of broadcast packets in packet numbers	0.101244%
Percentage of broadcast packets in bytes	0.011009%
Percentage of packets with transmission errors in packet numbers	0.08678%

Question 1: How do you set the filter to filter out broadcast packets and count their number?
What the filter did you set, what are their meaning and why?

Answer 1: eth.dst == ff:ff:ff:ff:ff:ff

This means Ethernet Broadcast only

Question 2: What kind of transmission errors did you observe in the Wireshark?
What makes Wireshark think there are transmission errors? (Hint: TCP, UDP connection protocol)
Please name **at least three**.

Answer 2: 1. Malformed Packet(Exception occurred) 2. New fragment overlaps old data(retransmission).

1. Malformed Packet
2. TCP Spurious Retransmission
3. TCP Out-Of-Order

2.4 Dropbox/Google drive traffic measurement

- 1) Create a Dropbox account, and install the client software (**not Dropbox on browser!**)
(<https://www.dropbox.com/install>)
- 2) Use Wireshark to capture the packets between the Dropbox client software and the cloud during the synchronization process (i.e., sync a file to dropbox).
- 3) Please find the domain name and IP of the server that help synchronizing the file.
 - a. Start packet capturing in WireShark
 - b. Put a 100MB file in the Dropbox folder
 - c. Find the connection that exchanges around 100MB of traffic (Functions in WireShark can help you with this.)

Table 2 Dropbox-Cloud Interactions

Server domain name	Server IP address	Amount of Traffic Exchanged
Dopbox-dns.com	162.125.82.12	112MB
Questions 1: What function did you use in WireShark to find the mapping of domain name and IP? What function did you use for getting the traffic amount?		
Answer 1:		
<ol style="list-style-type: none"> 1. Statistics -> Resolved Addresses 2. Statistics -> Conversation 		

- 4) Download Google drive client software (**not the one on browser!**)
(<https://www.google.com/drive/download/>)
- 5) Repeat the step 2) and step 3) with Google drive

Table 3 Google drive-Cloud Interactions

Server domain name	Server IP address	Amount of Traffic Exchanged
1e100.net	172.217.161.138	113M

2.5 Comparison between Dropbox and Google drive

- 1) Dropbox: In the folder that already have the 100MB file, now copy the file and **paste it in the same folder**. It will be uploaded to dropbox. Measure the number of bytes being uploaded.
- 2) Google drive: In the folder that already have the 100MB file, now copy the file and **paste it in the same folder**. It will be uploaded to cloud. Measure the number of bytes being uploaded.

Table 3 Comparison: Dropbox and GDrive

# of bytes uploaded to Dropbox	# of bytes uploaded to Google drive
93K	119M
Is there any difference in number of uploaded bytes between DropBox and GoogleDrive? Is so, why is there a difference between the above two numbers?	Answer: yes, there exists differences between them. In dropbox. When we copy the file, it only synchronize the changes compare to the original file which has been uploaded in the dopbox. So the byte will be smaller. In google drive, if we copy the file. It will reupload the whole file again. So the bytes in will be larger.

2.6 Wireshark capture files from each table

Please attach a google drive link of the Wireshark captured files (.pcaps).

<https://drive.google.com/drive/folders/15F297BGtNpBYcj7AalsPIM3Owd5uU3Kp?usp=sharing>

I can open it on my computer. Please check whether it can be open. If it has some problem. Please let me know.

3. File upload

- This report in pdf

We have zero tolerance to forged or fabricated data!! A single piece of forged/fabricated data would bring the total score down to zero.

Please read carefully through the instructions! ! ! ! ! ! ! !