Flinders UNIVERSITY
College of Science & Engineering

COMP2881 Operating Systems, DE
COMP9881 Operating Systems GE
Semester 1, 2020

CN Workshop05: Working with packets and network interfaces

Due: (check submission time on FLO)

Lab 5 is comprised of 5 tasks; Following completion of the checkpoints, a copy of the appropriate, makefile, source code and/or output for each task should be compiled into a single text file and uploaded to the relevant submission box on FLO for moderation. Speak to your demonstrator if you are unsure how to do this. While discussion of programming tasks with fellow students in labs is welcome and encouraged, please be mindful of the University's **Academic Integrity** policy and refrain from simply copying another student's code (even if they agree!). You will gain a much greater understanding of the material if you take the time to work through your own solutions, and you will be expected to be able to explain your code before being awarded checkpoints. Remember, the demonstrators are there to help if you get stuck.

Objectives

Upon completing this lab, you should be able to:

- Install tools from a software repository
- Create shell scripts for monitoring network activity
- Identify network interface metadata
- Use the command line tools to monitor packets/network traffic
- Use GUI tools to view packets/network traffic
- Using the tools; search, filter, inspect and identify different types of packets/protocols

Learning out comes;
- LO1: Understand computer network terminology and topologies, functions and architectures of computer networks
- LO2: Demonstrate the design and implementation of simple process and network level programs
- LO6: Appreciate the real-time nature of networked devices and communications and demonstrate an understanding of current and emerging methods for secure information transfer

Preparation

You may need to install tcpdump. It is recommended that you update the package repository before hand.

- Update the installer with the latest software repository, root user password is toor;

```
su -   # switch user to root
apt-get update  # update the package list from each repository
```

- Install networking tools from the software repository (wireshark may be installed on host OS instead);

```
apt-get install tcpdump
apt-get install wireshark
```

Task 1

Write a shell program that uses the following snippets to collect usage information on the ethernet interface, print out the results as per the example below. This small script is the basis for thinking about monitoring networks services on the network. Consider the material from the lecture about network monitoring about where this fits into managing your

Experiment with each of these on the command line to get an understanding how they work;

- Use the output of the ifconfig command to determine the network interfaces available;

```
$ /sbin/ifconfig -a
```

- Use the output of date in the time zone UTC

```
$ date  --utc
Sunday 21 October  23:32:28 UTC 2018
```

- Use the format specifier of date command to print year, month, day, hour, minute and seconds, eg;

```
$ date  +%D
10/22/18
```

- Use the output of the following command to collect bytes sent and received, select appropriate network interface;

```
$ cat /sys/class/net/eth1/statistics/tx_bytes
6537940985992
$ cat /sys/class/net/eth1/statistics/rx_bytes
297914460567432
```

- Use the return value from ping to determine if the default gateway is available;

```
$ ip route show # find IP address of default gateway
$ ping -c 1 192.168.1.1 # change to the default gateway on your system
$ echo $? # print out the return value

$ ping -c 1 192.168.1.1
$ if [ $? -ne 0 ] ; then echo "Gateway: Fail" ; else echo "Gateway: OK"  ; fi
```

- Use shell variables to store information to be printed, for example use this quote with back ticks “`” to run commands and copy their text output in to the string variable. No spaces around the assignment; “=“. Multiple variables can be printed out on the one line with echo.

```
$ export tbytes=`/sbin/ifconfig eth1 | grep "TX bytes" | sed -e "s/.*TX bytes://" | sed -e "s/(.*//"`
$ echo $tbytes
6537553143
```

- Use a while loop in your shell program, exit the program if the ping fails.

```
$ cat task.sh
#!/bin/sh
a=1
while [ $a -gt 0 ] # if a is greater than zero
do
 echo $a
 a=`expr $a + 1`
 sleep 10 # sleep for ten seconds
 ## BODY OF TEST GOES HERE
 ## if ping fails set loop counter to zero
done
```

Example output, printing out

```
$ task.sh
Time: 2018/10/12-16:40:02, Rx: 29999991 bytes, Tx: 6991 bytes, Gateway: OK.
Time: 2018/10/12-16:40:12, Rx: 29999992 bytes, Tx: 6992 bytes, Gateway: OK.
Time: 2018/10/12-16:40:22, Rx: 29999993 bytes, Tx: 6993 bytes, Gateway: OK.
Time: 2018/10/12-16:40:32, Rx: 29999994 bytes, Tx: 6994 bytes, Gateway: OK.
Time: 2018/10/12-16:40:42, Rx: 29999995 bytes, Tx: 6995 bytes, Gateway: OK.
Time: 2018/10/12-16:40:52, Rx: 29999996 bytes, Tx: 6996 bytes, Gateway: Failed!
Exiting.
```

See shell programming references;

```
man builtins
```

https://learncodethehardway.org/unix/bash_cheat_sheet.pdf

https://devhints.io/bash

Task 2

Use the `tcpdump` command in a terminal to *display* the *summary* of packets sent and received by applications running on your BYOD machine;

- Start `firefox`, similar web browser on the VM
- In a terminal, use `tcpdump` with the appropriate command line options to view all `http` traffic on the first network interface, for example as the `root` user;
  `tcpdump -i eth0 ...`

- In your web browser visit a web site;
  http://www.flinders.edu.au

- Use other tools like `ping`, to generate traffic on the interfaces
- Use `tcpdump` with the appropriate command line options to capture traffic from `eth0` or the first network interface and write to a file; `network-traffic.cap`
- We will use this file later with Wireshark to display the contents, so you can let this run for some time.

Demonstrate the following questions with the above activities;
Q) Can you capture packets with tcpdump and display in the terminal?
Q) Can you capture packets to a file with tcpdump?

See;
`man tcpdump`
https://danielmiessler.com/study/tcpdump/

Task 3

Use the `tcpdump` command in a terminal *inspect* the contents of packets sent and received by applications running on your BYOD machine;

- In a terminal, use `tcpdump` to inspect more about packets with these options

  `tcpdump -vvv -s 1500 ...`
- In your web browser visit a web site;

  http://www.flinders.edu.au
- Use `tcpdump` to capture traffic on specific ports

Demonstrate the following questions with the above activities;

Q) What does the `-vvv` and `-s 1500` flags do?

Q) Can you identify packets on `UDP` or `TCP` port 53, source and destination hosts when using the web browser?

Q) Can you identify packets with a protocols other than TCP/IP or UDP/IP ?

See;

man tcpdump

https://danielmiessler.com/study/tcpdump/

Task 4

Use the tcpdump command in a terminal to *capture* the packets sent and received by applications running on the VM. Take a screen shot of the window where you have run the following;

- Use wireshark to capture all traffic from `eth0` or the first network device to a file [FILE 1]
- Use wireshark to view only ICMP traffic

Q) Can you identify ICMP traffic on the network interface?
Or if running a VM, can you install and run wireshark on the host machine running the VM to capture the VMs traffic?

See;
man tcpdump
https://www.wireshark.org/docs/wsug_html_chunked/index.html
https://www.wireshark.org/docs/wsug_html_chunked/ChapterCapture.html
https://www.wireshark.org/docs/wsug_html_chunked/ChCapCaptureFilterSection.html

Task 5

Identify the latency of a host over the local network, it should typically be in milliseconds;

- Use the tools `tracepath`, `traceroute` and ping to determine the route trip times of packets to a host
- Install the above tools if not on your system already

Q) Can you run the following commands and compare the resulting times to the host www.flinders.edu.au;

$ tracepath www.flinders.edu.au

$ traceroute www.flinders.edu.au

$ ping -c 10 www.flinders.edu.au

Q) Identify which hosts/routers create the largest latency

Q) Do you see asymmetric routes, if so why might that be?

Q) Using `tcpdump` or `wireshark`, what type of traffic do these programs generate?

For more information on latency in the network;

https://www.techwalla.com/articles/network-latency-milliseconds-per-mile