CSci 4271W (011 and 012 sections) Lab Instructions

Lab 7 **March 17th, 2025**

Ground Rules. You may choose to complete this lab in a group of up to three students. Before you leave the lab, **make sure you have submitted to Gradescope, you included all group members on the submission, and the autograder found all required files!**

1 `wireshark`

In lecture 13, we saw that networking protocols are arranged in a "stack", with each level encapsulating data at the previous levels. In this lab, we'll see one of the most useful tools for inspecting network traffic and understanding what a network host is doing, wireshark.

Wireshark is a network capture and parsing tool, that can be used to capture network traffic and parse the contents into human-readable (sometimes) form. Wireshark knows about many application and transport protocols; here we'll just see what it can do for a small number of examples. You will probably find it useful to open the Wireshark user's guide and browse to Chapter 3 to help understand some of the instructions below. (And bookmark the user's guide for later use!)

2 Install Wireshark

Log in to your VM with X-forwarding enabled, i.e. in the CSELabs terminal run:

```
$ ssh -X student@csel-xsme-s25-csci4271-NNN
```

Once you've logged in, install wireshark in your VM by running the following command:

```
$ sudo apt-get install wireshark
```

This will download about 40MB of files and take a few minutes to finish. You may be prompted with an option to install Wireshark so it can be used by non-root users; we'll just use it as root in this lab (for convenience) so either option is fine.

3 Start Wireshark

Once wireshark is installed, you can start it by typing

```
$ sudo wireshark
```

In your VM terminal. This should open a new window with the wireshark GUI. You'll see a menubar, what looks like a location bar (with greyed text saying "Apply a display filter") and in the main window, another drop-down bar with a green "bookmark" icon and ghosted text "Enter a capture filter." Below this you'll see a list of network "interfaces" that can be sniffed. The top interface will start with `en` - this is the ethernet interface we'll usually be interested in. If you

just double click on this text, you'll start a "capture session" that captures all of the traffic to and from your VM. Wait a few seconds, then click the square red "stop capture" button in the toolbar directly beneath the menubar.

Now below the "Apply a display filter" bar, you'll see three panes. The top (packet list) pane is a list of all the packets captured - a lot of stuff is going on! Most of these are from the SSH session that is carrying the contents of the wireshark window back to your CSELabs machine and your mouse interactions to the VM. They're pretty useless to us, but you can see *some* of the nifty features of Wireshark already. Click on one of the rows in the packet list pane, and the middle pane will populate with the "packet details." Here you can expand information about each of the levels of encapsulation, e.g. the Ethernet Frame, the IP datagram, and the TCP header. The bottom pane is the "packet bytes frame" and as you click on the packet details, notice that the corresponding bytes are highlighted below.

OK, that captured a lot of data that we can't even really read. Let's capture a few interesting sessions. Start by "closing" the current capture with "File > Close" and select "Continue without Saving" when wireshark prompts you. You'll go back to the screen we saw at the beginning with the choice to enter a "capture filter."

3.1 Capture a DNS lookup

In your VM terminal window, type <`Ctrl-Z`> to pause the wireshark process, then at the shell prompt, put wireshark into the background with

```
$ bg
```

Switch back to the wireshark window and in the "Capture Filter" textbox, type "`port 53`". Double click on the top, `en..` interface. Then go back to your VM terminal and run

```
$ ping neverssl.com
```

Switch back to wireshark and hit the big red "stop capture" square button again. You should see at least two packets in the packet list pane. Double click on the second one to see the response packet in a separate window. Can you find what IP address `neverssl.com` resolves to? What about the "transaction ID" for your request?

Save the output of this capture by choosing "File > Save" and entering a filename, like "nssldns.pcapng". Then close the file so we can do another capture.

3.2 Capture a HTTP session

On a normal machine, we could capture an HTTP session with the filter "`tcp port http`". However, because our VMs are set up to use a proxy host (more about this on Thursday!) we will instead enter the capture filter "`tcp port 3128`" to capture the traffic sent to the OIT http proxy. Type this into the capture filter box, double click the `en..` interface, and then switch back to your VM terminal and run:

```
$ wget http://neverssl.com
```

After a few seconds, press the big red stop button again. Now we can see some interesting traffic in the packet list pane. For example, you should see a sequence of three TCP packets with descriptions starting `[SYN]`, `[SYN,ACK]`, and `[ACK]` – this is the well-known "3-part handshake" that starts every TCP session. You'll also see some differently highlighted packets that have `HTTP` in the Protocol column. If you click in the second of these, you can see what the proxy's response was to the request for `neverssl.com`. In the bottom, "packet bytes" pane, you should see a "Reassembled TCP" tab that will allow you to see the entire response. What was the response?

Next try clicking on the menu "Analyze > Follow > HTTP Stream". You should see the entire sequence of the download. What User-Agent string did Wget send with its request? What was the title of the downloaded page (look for the <`title`> tag in the blue response text)? Close the "follow HTTP stream" window, and save this capture session (using "File > Save") as "nsslhttp.pcapng".

3.3 Merging captures

Merging capture files can be useful if we want to combine multiple sessions. Let's merge the DNS and HTTP request files: Go to "File > Merge" and select "nssldns.pcapng" from the file dialog. Now your packet list pane should have both the DNS query and the HTTP session retrieving `neverssl.com`. Save this new capture in `/home/student/` as `nsslmerged.pcapng`. (Note: wireshark may attempt to save this in the `/tmp` directory, so make sure you select the `/home/student` folder in the "Save As" dialog.)

3.3.1 `chown`ing the pcap file

Because we ran wireshark as root (with `sudo`), the pcap file we created is owned by root. Since we need to access this file via `scp` to upload it for the lab assignment, we'll need to modify the file so it's owned by the `student` user on your VM. So in a VM terminal, we'll use the `chown` command to do that:

```
$ sudo chown student:student nsslmerged.pcapng
```

3.4 All done!

Once you've saved your merged capture files, you're done with Lab 7! Remember to quit wireshark using "File > Quit" so you can log out of your VM, then use `scp` to copy the `nsslmerged.pcapng` file off of your VM, so you can submit the file to the Lab 7 assignment on Gradescope. Make sure you include all of your group members in the submission!

Once you've submitted the file, the autograder will test to make sure the proper file was submitted, check that it includes the DNS lookup and HTTP session, and notify you if it's missing, within a few minutes.

Congratulations, you've finished Lab 7!