CS536 Lab3: A Synthesis Example via Wireshark

Due: April 14, 2023
Total points: 50 points

1 Goal

In this lab, you are going to use `Wireshark` to capture data packets while you use WiFi to do a synthesis example illustrated in the lecture slide and write some codes to analyze the packets captured by you. You can use C or Python to write the codes to offline analyze packets captured by `Wireshark`.

2 Instructions

1. Please read Chapter 6.7.
2. Part A (10 points): Use Wireshark to capture packets over WiFi.
   - First of all, please make sure that you use **PAL3.0** (Our campus wireless network), not Ethernet, different from chapter 6.7. Please close all the browsers and apps that use the Internet as much as you can. It is not really required but helpful to reduce packets captured by wireshark.
   - Please start packet capturing via Wireshark and then turn off WiFi. You then turn on WiFi, and then open a web browser and go to google.com. Please search "movie today" and when the search results return, you can stop packet capturing.
   - Please save the captured pcap file as *lab3.pcap*.
3. Part B (25 points): Please use Wireshark to check the trace captured in Part A and then answer the following questions.

   (a) (5 points) In the trace captured by you, how did it obtain the IP and MAC address of a gateway router? Which address was obtained first? Please show the involved packets or screenshot of these involved packets.

   (b) (5 points) In the trace captured by you, what was the IP address used by google.com? How did you get it? Please show the involved packets or screenshot of these involved packets.

   (c) (5 points) In the trace captured by you, can you see any packets relevant to intra-AS or inter-AS routing? If yes, please show the involved packets or screenshot of these involved packets. If no, please explain why.

   (d) (5 points) In the trace captured by you, please find the packets for TCP three-way handshaking. Please screenshot of these involved packets.

   (e) (5 points) In the trace captured by you, can you see any packets for HTTP GET messages and HTTP response messages? If yes, please show the first HTTP GET message (to www.google.com) and its HTTP response message or screenshot of them. If no, please explain why.

4. Part C (15 points): Please write your own code to analyze the captured pcap file and extract the packets needed in Part B. Please feel free to use C or Python3. Please run packet analysis in the following cases:

   - CASE A: Extract the IP address and MAC address of a gateway router.
   - CASE B: Extract the IP address of the destination website (here, www.google.com).
   - CASE C: Extract the packets for TCP three-way handshaking for the TCP connection between your computer and the destination website (here, www.google.com).

   Note that if there are more than one packet, please get them IN ORDER.

   If you choose to write Python3, you are recommended to use only `scapy` library. However, if you need other libraries, please provide a script (`install.sh`) to install all needed python3 lib so that your python3 code can run.

   Your code should support every case (A, B, C) and another mode "ALL" which run all the cases. To run your code, please use the following command

   ```
   ./lab3 [CASE] [Input pcap file] [Destination website]
   ```

   or

   ```
   python lab3.py [CASE] [Input pcap file] [Destination website]
   ```

   `[CASE]` is optional. It is by default ALL and it also accepts A, B or C. [Input pcap file] is mandatory and it should be lab3.pcap in this lab. [Destination website] is mandatory and it should be www.google.com in this lab. Note that we will change the destination website and pcap file when we grade. Thus, the hard coding cannot work out.

   Your code should print out the results in the following format where the first line starts with CASE NO (say, CASE A, CASE B, CASE C), the following lines followed by the results. Each line is similar to the header used in HTTP get request, which starts with a header name, followed by ": ", and the header value. Note there is a space after ":".

   For example, when the mode is set to "ALL", the sample output is as below, please strictly follow the semantics of the output:

   ```
   CASE A:
   IPAddr:  128.10.19.120
   MACAddr:  00:00:0c:9f:f0:01
   CASE B:
   IPAddr-DEST: 142.250.190.132
   CASE C:
   IPAddr-SRC: 10.186.159.135
   IPAddr-DEST: 142.250.190.132
   Port-DEST: 443
   SYN: 1
   ACK: 0
   IPAddr-SRC: 142.250.190.132
   IPAddr-DEST: 10.186.159.135
   Port-SRC: 443
   SYN: 1
   ACK: 1
   IPAddr-SRC: 10.186.159.135
   IPAddr-DEST: 142.250.190.132
   Port-DEST: 443
   SYN: 0
   ACK: 1
   ```

   Note that the value here may be different from you. For example, Google has many web servers; the destination IP address for www.google.com can change depending on various factors such as network location, server load, and DNS caching.

3 Materials to turn in

Please submit your assignment on **Gradescope**. Your should submit a zip file named as “Lab3_UID*.zip” including

- lab3.pcap
- all the source files (lab3.c or lab3.py). Please include install.sh if applicable. Please include a readme on how to compile and run your source code (if not exactly the same as our lab convention where we run gcc lab3.c and run lab3 if C and python3 lab3.py if Python3). It is not recommended, but please include it if needed.
- lab3.pdf, a lab report that answers the questions listed in Part B. Please include your name and student ID at the top of the first page.

4 More tips and Support

1. If you cannot use PAL3.0, you can test with your own WiFi network. Please check whether IPV4 or IPV6 is used. We accept both, but please make a note at the start of your report if you do not use PAL3.0 and if this WiFi networks uses IPv4 or IPv6.
2. If you want to use any late day, please send an email to cs536-ta@cs.purdue.edu and tell us. Please do not forget that each student can only use up to 3 late days for all the assignments.
3. Questions about the assignment should be posted on Campuswire or asked during PSOs or office hours.