Assignment 1

Due date: 13:00, October 2, 2024

Contact TAs: ntu.cnta@gmail.com

Instructions

- There are **TWO** parts in this assignment. In each part, there are several questions. Please read the description carefully and answer the questions in Chinese or English. **In each question, you need to describe how you find the answers.**
- Please use the designated tool to answer each question; otherwise, there will be some deductions.
- Please answer the problems sequentially, save them as a PDF file, and then upload them to Gradescope.
- Discussions are encouraged, and in your report, you need to cite the sources (either from textbooks, academic papers, website articles, or ChatGPT) and give credit to whom you discuss with.
- **Warning! DO NOT attack** the server we provided. Otherwise, you will get **F** in this course.

🦈 Playing with Sharks

In this part (**Problem 1–3**), you will be given `.pcapng` files that contain packets from a specific protocol. Answer the following questions by inspecting those files with Wireshark.

1 (20%) 👶 Baby shark

Sometimes, the network condition is poor in No Tear University, just like in the Third World. Recently, you were hired as a part-time network engineer to do some inspections. Today, your boss asks you to analyze a packet capture file `veryslow.pcapng` and answer the following questions. Make sure you can finish the tasks and make the descriptions clear. Otherwise, your boss will shout at you: "Even a baby can use Wireshark!"

1. (4%) Performance analysis is important in computer networks. Based on the measurements, we can determine a network's quality.
   (a) Data visualization is a good way to make your boss understand what happened. Please use Wireshark's built-in functions to show the throughput chart of this traffic. (Measure the number of bytes transmitted per second.)
   (b) According to your observation, what is the transmit rate limit (in Kbps) in this scenario?
2. (2%) Your boss is wondering what the user IP address is in the captured traffic. Explain your answer briefly. (The answer is definitely not `127.0.0.1` !)

3. (6%) It's said that there are some secrets in the following packets:

   (a) Packets originated from a "local" client connecting to a "remote" server via TCP port `1080`.

   (b) Packets originated from a "remote" client connecting to a "local" server via UDP port `2330`.

   Can you identify and display what the messages are, respectively? What's the main difference between TCP and UDP connections? Use the connections mentioned above as examples. (*Hint:* Look at the packet amount of them.)

4. (4%) In Wireshark, how can you distinguish between IPv4 and IPv6 packets by their headers? Please list two key fields to determine whether a packet uses IPv4 or IPv6. Take screenshots of the related fields in the frame and show them in your report.

5. (4%) Locate a DNS response packet that contains the IPv4 address of `zh.wikipedia.org`.

   (a) What types of resource records are present in the packet? Describe the differences between them.

   (b) What's the IP address of `zh.wikipedia.org`?

2 (20%) The course permission code

The new semester of No Tear University is coming. During the first week, students play wide games around the campus to get permission codes for their desired courses. Some outdoor courses are very popular, such as Introduction to Forest Biodiversity and Introduction to Field Geology, the so-called love bus. (Since students often fall in love and get together with their classmates in those courses.) Sometimes, students e-mail the course instructor in advance to get the course permission code. In some cases, instructors will preserve quotas for those who wrote an e-mail to them in advance. Here, we sniffed a stream `mail.pcapng`. It contains a stream that sends an e-mail. Please find out what protocol this stream uses and answer the following questions.

1. (4%) Which port is the server using in the stream in `mail.pcapng`? What is the application protocol of this stream and which port would the server typically use in this protocol?

2. (6%) What is the `sender`, `receiver`, and `subject` of this e-mail?

3. (4%) Did the student successfully get the course permission code? If yes, write down which course he wants to take, and what the permission code is. If not, write down why he can't get the permission code.

4. (6%) Most modern clients use Transport Layer Security (TLS) to send or receive e-mails. Is this client configured to use TLS? Are there disadvantages or problems without using TLS?

3 (20%) 📃 The problem sheet of midterm exam

At No Tear University, students aim to get perfect grades in their courses, aka A+ or GPA 4.3. Most students work diligently to achieve their goals, while only a few procrastinate until the midterm exams approach. Sometimes, past exam papers play an important role for students. Once students get the past exam papers, they can practice and may earn a higher grade. One day, a curious student sniffed a stream `ftp.pcapng`. This file seems to contain a stream that sends some files to TA's FTP server. Surprisingly, one of these files looks like the problem sheet of the midterm. Maybe the contents of that file are helpful for you guys to prepare for the midterm, and you might get a chance of earning a higher grade 💯 if you study them carefully. Please answer the following questions.

1. (4%) What is the `username` and `password` of TA's account?
2. (8%) Which port is the server listening to for FTP requests? What are the ports on the server we send the file contents with? (List all of them.)
3. (8%) Can you find the file of the midterm problem sheet on the server? Write down the (a) `filename` and (b) how many questions are there in the midterm sheet.

🔧 Getting Start with Useful Tools

We have taught you some basic usage of specific tools in class. In this part (**Problem 4–7**), you need to use those tools to answer the questions.

4 (10%) 👣 The path to the destination

Have you ever thought about how packets get from source to destination? `traceroute` is a tool to find the path from your local host to an IP. Please log in to CSIE workstation (e.g., ws1.csie.ntu.edu.tw) and do the following experiments.

1. (5%) Trace the route to `8.8.8.8`, and take a screenshot of the result. Explain how or what `traceroute` is utilized to find this path to `8.8.8.8`.
2. (5%) Trace the route to `198.51.100.23`, and take a screenshot of the result. You should see a very different outcome. What is the difference between this result and the last one? What could be the reasons that cause `traceroute` to behave like this?

5 (10%) ⛏ Dig out the domain information

Dig (Domain Information Groper) is a tool that can do domain name lookups. Please use `dig` to find out the answer to the following questions.

1. (4%) What is the IP of `csie.ntu.edu.tw`? Take a screenshot of the output of your command.
2. (6%) What is the IP of `amazon.com`? List at least two IPs and take a screenshot of the results. Briefly explain why someone would want to bind multiple addresses under a single domain.

6 (10%) Back to elementary school

Do you remember the excitement of surfing the Internet in your childhood? Most people use a browser the first time they access the Internet. Open a browser, type the name of your favorite sites on the search bar, and start playing games or watching videos. Obviously, browsers are one of the easiest and most prevalent ways to access the Internet. However, the devil is in the details. Let's make some observations according to the following questions.

1. (5%) Use your browser and go to `http://voip.csie.org:4090/`, type `username` (your student ID) and any `password` of your choice (don't actually type your password for other sites 😈) and press the send button. Using Wireshark, can you find the packet containing the password? Take a screenshot of the packet. (*Hint:* If you cannot access the webpage, try using Incognito Mode of your browsers.)
2. (5%) Now go to `https://voip.csie.org:4092` instead. Can you find the packet containing the password? If yes, take a screenshot; if not, what are the differences between this and the previous website that caused this?

7 (10%) Yet another curl?

You may have learned "curl" in Calculus during your freshman year. In vector calculus, the curl is a vector operator that describes the infinitesimal circulation of a vector field in three-dimensional Euclidean space, denoted by **curl F** or $\nabla \times \mathbf{F}$. This might sound like a nightmare for some of you, but don't be nervous! It won't bother you again in the Computer Networks course. 😇

Instead, you will learn another curl in the Computer Networks course. cURL is generally used to send requests/data to HTTP(S) servers. Nevertheless, it does much more than that!

1. (6%) When you press the send button to send the `username` and `password` to `http://voip.csie.org:4090`, you are actually sending a POST request. Try replicating your POST request in **Problem 6(1)** using cURL and write the command you used and a screenshot of the output in the report. (*Hint:* Perhaps you can use Wireshark to see how the webpage communicates with the server.)
2. (4%) In fact, your TA hid a secret argument on the website. Do the previous problem again, but add an additional POST argument `secret=CN` in your request. Write down the cURL command you use and what your TA wants to tell you in the response message.