Middle East Technical University

Department of Computer Engineering

CENG 435

Data Communications and Networking

Fall 2021–2022

THE - 1

Due date: 2021-11-30 23:59

1 Introduction

This assigment will cover application layer protocols and will serve as an introduction to Wireshark. In the first section, you will investigate the provided network capture to answer the questions. Then, you will capture some traffic yourself for the second section. You are asked to use your findings to prepare a report for the final submission. For each question, explain your answer using 2-5 sentences of your own words. Overall submission will include the `.pcap` file you have used to show your capture for part 2 as well as the `.pdf` report, see section 3 for details.

1.1 The Case of the Corporate File Server

To answer the questions in this section, you will need the `corporate.pcap` file available on ODTUClass. Open the file in `Wireshark` and inspect the traffic. Then, answer the following questions. For each question, do not forget to explain how you have reached the answer in detail. You can support your answers with screenshots. Citing outside sources are welcome and encouraged as well.

1.1.1 Questions

1. How many *legitimate* users does this system have? (that we know of)
2. What is the total number of successful logins to the system over the course of this capture?
3. What is the password of the user `bob`?
4. Has there been any *malicious* activity during this capture? If so, which IP address did it originate from?
5. Who downloaded the file "receipt.xlsx"?
6. Identify and explain the flaws of the system.

1.2 Capturing HTTP

In this section, you will generate your own network traffic and capture it. Do not forget to save your captures that you have used to answer this section in `.pcap` files for submission. For every question, support your answer using screenshots from the Wireshark window and, if necessary, the browser you have used.

1.2.1 Capture the Network Traffic

- Before starting the capture, open a browser tab, then go to `http://ceng.metu.edu.tr`, mind the *http*.
- For the next step, we will "hard reload" the page to disregard the cache of the browser, there are different ways to do this depending on your setup;
  - On Windows and Linux,
    - On "Mozilla Firefox": `Ctrl+Shift+R`
    - On "Google Chrome" and "Microsoft Edge": Right click the "refresh" button on the toolbar and select "Empty Cache and Hard Reload"
  - On macOS,
    - On "Mozilla Firefox", "Google Chrome" and "Safari": Hold the "Shift" key and click the "Reload" button on the navigation toolbar.
- In Wireshark, start the capture, switch to the browser and using the key combination for your operating system and browser, reload the page. The page will refresh.
- After the page has fully loaded, you can stop the capture.
- You might repeat this multiple times depending on the quality of your capture. Do not forget to save the version you used to answer the questions. The name of the `.pcap` file should be `e<your_student_id(7 digits)>.pcap`

1.2.2 Questions

1. How many queries were sent from your computer to the DNS server to get the `http://ceng.metu.edu.tr`'s address?
2. How many servers were queried for the DNS request?
3. What are the IP addresses of the queried DNS servers?
4. By looking at the destination address of the queried DNS servers (and their responses), can you tell whether the response was cached or not?
5. In which queries, were the first request sent to the `http://ceng.metu.edu.tr`'s server and the first response received from it?
   (a) What is the protocol of these requests?
   (b) Explain the reason why this protocol is used for the first request/response pair.
6. During the first HTTP request to `http://ceng.metu.edu.tr`'s server, was there any cookies sent with the request?
7. Using any of the HTTP requests to `http://ceng.metu.edu.tr`'s server;
   (a) What is the user-agent string of the request?
   (b) Does the user-agent string include the browser you are using? Are any other browsers mentioned? If so, why?

2 Other Specifications

- Feel free to ask questions through ODTUClass discussions or send me a mail on yigit@ceng.metu.edu.tr.
- See the course syllabus for the late submission policy.
- This is an individual assignment. Using any piece of code, discussion, explanation etc. that is not your own is strictly forbidden and constitutes as cheating. This includes friends, previous homeworks, or the Internet. The violators will be punished according to the department regulations.

3 Submission

- Upload your assigment report to the ODTUClass *Report Submission*.
- Submit your `.pcap` file through *Pcap Submission* on ODTUClass. The name of the `.pcap` file should be `e<your_student_id(7 digits)>.pcap`

3.1 Grading

- Please ensure that the screenshots you have included in your report are legible.
- Answers without explanations or screenshots to support them (e.g. answering just "5" to a "How many..." question) will get no grade.