Middle East Technical University

Department of Computer Engineering

CENG 435

Data Communications and Networking

Fall 2021–2022

THE - 4

Due date: 2022-01-21 23:59

1 Introduction

In this final Wireshark assignment, you will analyze ICMP (Internet Control Message Protocol) messages at the Network Layer. Complete the assignment on a Linux machine, listening on your main internet interface (wireless or ethernet). You can cite external sources (textbook, RFCs etc.).

2 ICMP Packet Analysis

2.1 Capture the Network Traffic

1. Start your capture with Wireshark on the interface you use to connect to the Internet
2. Get a terminal and run the `ping` command:

```
ping -c 7 8.8.8.8
```

   (You should not see a 100% packet loss at this step to continue with the assignment)

3. After the `ping` is finished, you can stop the capture and save the capture as `<name_surname>.pcap`
4. Make sure that you can see 7 `ICMP` requests and 7 `ICMP` responses in your capture
5. Take two screenshots that show the "Internet Control Message Protocol" details:
   - Wireshark "Packet Details" (by double clicking on the packet) window that shows an `ICMP` request
   - Packet details window of an `ICMP` response
6. Run the following command on a terminal to get your routing table information;

```
route -n
```

7. Include the screenshots of the `ICMP` request, response and the routing table in your report

3 Questions

1. What are the IP addresses of the source host and the destination host of the request and the reply packets?
2. Check the packet information of the request and the reply packets. Is there a port number information in those packets? Why/why not?
3. Regarding the "type" and "code" fields in the request and the reply packets:
   (a) What is the purpose of the "type" field?
   (b) What is the purpose of the "code" field?
   (c) Explain the values in the "type" and "code" fields.
4. By looking at the `ICMP` request packet information, find how many bytes are transferred in total. Then, explain where these bytes are used or what information they carry. Finally, sum them up and calculate the total transferred bytes (Ignore the headers before ICMP, you do not have to explain them in detail, writing how many bytes are used for these headers are enough. However, for the ICMP packet, explain these bytes field by field).
5. Considering your answer to the first question, take a look at the routing table you got above; explain in detail which rule should you remove so that the outgoing packets will be dropped and your machine cannot send any ping requests?

4 Submission

This is an individual assignment. Upload your report `<name_surname>.pdf` and your `<name_surname>.pcap` file to our ODTUClass page.

5 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.

5.1 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.