CS408 – Computer Networks – Spring 2022

Homework #2 (Related to Lab #2)

Deadline: 07.04.2023, Time: 23:55

Network Packet Capture & Analysis

Introduction

In this homework, you will use the Wireshark packet sniffer that we have seen in Lab 2. Wireshark allows us to display the contents of packets being sent/received from/by protocols at different levels of the TCP/IP protocol stack.

First, you have to apply the steps mentioned below. After that, answer the following questions. **Clearly indicate what your answer is and how you obtained the answer by referring to the *pcap* file (you may use pcap screenshots).** We also ask you to save the captured network traffic into a *pcap* file. In addition, you are **required** to submit a *pcap* file together with the document that you list your answers! Submission policy is described at the end of this document.

Steps (Do these before answering the questions!)

1. Start the Wireshark tool, choose the right network interface, and start the sniffing process.
2. Clear the ARP cache (using arp -d * command in cmd.exe window).
3. Clear the DNS cache (using ipconfig /flushdns command in cmd.exe window)
4. Browse http://www.columbia.edu/cu/computinghistory/ using your web browser (please use *http* not https).
5. Browse http://www.columbia.edu/history/ using your web browser (please use *http* not https).
6. Send ICMP Echo packet to tudelft.nl domain using *ping* tool. If you receive more than 4 reply lines, you can break with control-c key from the keyboard (for Mac users).
7. Stop sniffing and save packets into a *pcap* file.

Questions (to be answered via pcap analysis)

1. What is the IP address of http://www.columbia.edu/cu/computinghistory/ website?
2. What are the source port and destination port of the HTTP request used to get http://www.columbia.edu/cu/computinghistory/ ?
3. What is the IP address of tudelft.nl domain?
4. What are the *type numbers* of the ICMP Echo request and ICMP Echo reply (used for ping)?
5. What is the *length of the Data* field of ICMP Echo reply packet from tudelft.nl?

6. Write a *Wireshark filter* for showing packets with source IP address 192.105.59.24 and TCP destination port 1334?
7. What is the value of the *User-Agent* header field of HTTP requests sent by your browser?
8. What is the *Content Length* header field of HTTP response for http://www.columbia.edu/history/ ?
9. What is the *HTTP Status Code* of HTTP response for http://www.columbia.edu/history/ ?

Submission

- Create a folder named ***XXXX_surname_name***, where XXXX is your SUNet username (e.g. begumarslanhan_arslanhan_begum)
- Convert your answer document to pdf format with name ***XXXX_surname_name.pdf***, where XXXX is your SUNet username (e.g. begumarslanhan_arslanhan_begum.pdf)
- Put your ***pcap file*** in this folder as well.
- Compress your ***XXX_surname_name*** folder using any compression tool (e.g begumarslanhan_arslanhan_begum.zip).

For questions and support, you can send an email to me (arslanhanbegum@sabanciuniv.edu) or you can use office hours.

Good luck!