CS408 – Computer Networks

Homework #3 (Related to Lab #2)

Deadline: 05.05.2022, 18.00

Network Packet Capture & Analysis

Introduction

In this homework, you will use Wireshark packet sniffer, which allows us to display the contents of packets being sent/received from/by protocols at different levels of the TCP/IP protocol stack. Answer the questions in each section below. Clearly indicate what your answer is, how you obtained the answer, and (if applicable) discuss implications regarding your answers. We also ask you to save the captured network traffic into a *pcap* file. You are required to submit a *pcap* file together with the .pdf document where you provide your answers! Submission policy is described at the end of this document. Failure to submit any of the required files will result in getting 0 points for the assignmnet.

Steps

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/~fdc/sample.html" using your web browser (please use just *http*!).
5. Browse "http://www.columbia.edu" using your web browser.
6. Send ICMP Echo packet to "example.com" domain using *ping* tool.
7. Send ICMP Echo packet to "your default gateway IP address" using *ping* tool (in order to find your default gateway IP address, you can use ipconfig /all output).
8. Do an nslookup on www.sabanciuniv.edu.
9. 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/~fdc/sample.html website?
2. What are the source port and destination port of the HTTP request to http://www.columbia.edu/~fdc/sample.html ?
3. What is the IP address of *example.com* domain?
4. What is the IP address of your default gateway?
5. What are the *type numbers* of your ICMP Echo request and ICMP Echo reply?

6. What is the *length of the Data* field of ICMP Echo reply packet from “example.com”?
7. Write a *Wireshark filter* for showing packets with destination IP address 192.168.19.15 and destination port 5656?
8. What is the *Target IP Address* of your ARP Request packet?
9. What is the value of the *User-Agent* header field of HTTP requests sent by your browser?
10. What is the *Content-Length* header field of HTTP response for “http://www.columbia.edu/~fdc/sample.html”?
11. What is the *HTTP Status Code* of HTTP response for “http://www.columbia.edu” ?
12. Locate the DNS query and response messages for “www.sabanciuniv.edu”. Are they sent over UDP or TCP?
13. Examine the DNS query message for “www.sabanciuniv.edu”. What “Type” of DNS query is it? Does the query message contain any “answers”?
14. Examine the DNS response message. How many “answers” are provided for IPv4? If you obtain more than one answer, what do each of these answers contain, what is the data length of the answers?

Submission

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

For questions and support, you should exclusively send an email to your TA Begüm Arslanhan (arslanhanbegum@sabanciuniv.edu) or you can use office hours (preferred).

CS408 Team (Begüm Arslanhan, Artrim Kjamilji)

Good luck!