CS408 – Computer Networks – Spring 2024

Homework #3

Deadline: March 29, 2024, Friday, 23:59

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 document that you list your answers! Submission policy is described at the end of this document.

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). (For mac; `sudo arp -a -d` in Terminal)
3. Clear the DNS cache (using `ipconfig /flushdns` command in cmd.exe window) (For mac; `sudo killall -HUP mDNSResponder` in Terminal).
4. Browse "http://info.cern.ch/" using your web browser (please use just *http*).
5. Browse "http://info.cern.ch/cs408" using your web browser (please use just *http*).
6. Send ICMP Echo packet to "example.com" domain using *ping*.
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). (For mac; default gateway address can be found by `netstat -nr | grep default` in Terminal)
8. Stop sniffing and save packets into a *pcap* file.

Questions (to be answered via pcap analysis)

1. What is the IP address of http://info.cern.ch website?
2. What are the source port and destination port of the HTTP request to http://info.cern.ch?
3. What is the IP address of *example.com* domain?

4. What is the IP address of your default gateway?
5. What are the *MAC addresses* of your ICMP Echo request source and destination?
6. What is the *length of the Data* field of ICMP Echo reply packet from "http://example.com"?
7. Write a *Wireshark filter* for showing packets with destination IP address 192.168.19.05 and destination port 1023?
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 *HTTP Status Code* of HTTP response for "http://info.cern.ch/cs408"?

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 any compression tool (e.g simgedemir_demir_simge.zip).

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

Good luck!