CS 408 - Computer Networks - Fall 2024
Homework #2 (Related to Lab #2)
Network Package Capture & Analysis using Wireshark

Deadline: 15.11.2024 Time: 23:55

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 must apply the steps mentioned below to generate and save a pcap file. After that, answer the following questions. Clearly write what your answer and show how you obtained the answer by referring to the pcap file (you MUST provide screenshots from the submitted pcap file for each answer). In addition, you are required to submit the pcap file that you generated 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).
3. Clear the DNS cache (using `ipconfig /flushdns` command in cmd.exe window)
4. Open an incognito/private tab of a web browser and browse http://www.faqs.org (please use http, not https).
5. Send ICMP Echo packet to github.com 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).
6. Stop sniffing and save packets into a pcap file.

Questions (read everything up to here before answering the questions)

1. What is the IP address of http://www.faqs.org website?
2. What are the source port and destination port numbers of the HTTP request used to get http://www.faqs.org ?
3. What is the IP address of github.com domain?
4. What are the type numbers of the ICMP Echo request and ICMP Echo reply (used for ping)?
5. What is the range of sequence numbers in the ICMP Echo request and ICMP Echo reply packets captured when github.com was pinged? The range should start with the first request sent and end with the last reply received.
6. What is the value of the User-Agent header field of HTTP requests sent by your browser?
7. How many .js files has/have been downloaded from http://www.faqs.org? What is/are the name(s) of these file(s)?
8. What is the Status Code of HTTP response for http://www.faqs.org?
9. Locate an ARP request and reply pair. What are the Sender and Target MAC addresses, and Sender and Target IP addresses in the ARP request and reply packets?

10. Write a Wireshark filter for showing packets where your IP address is the source and UDP is used. What is the application layer protocol that appears the most when you apply this filter?

Submission

- Create a folder named XXXX_surname_othernames, where XXXX is your SUNet username (e.g. johndoe_doe_john)
- Convert your answer document to pdf and name the file as XXXX_surname_othernames.pdf, where XXXX is your SUNet username (e.g. johndoe_doe_john.pdf)
- Put your pcap file in this folder as well. Use the same file naming format for the pcap file as well.
- Compress your folder using any compression tool and create the compressed file to be submitted to SUCourse. Make sure that the name of the compressed file should use the same format as others. (e.g. johndoe_doe_john.zip).

For questions and support, you can send an email to Saleh Alshurafa (saleh@sabanciuniv.edu) or any of the other TAs. You can also visit office hours.

Good luck!