National Institute of Technology, Rourkela

DCCN Lab (CS3072)

6th Semester – 2023 Spring Sem

Evaluation Scheme:-

Day to Day Evaluation: 60 Marks
Viva : 20 Marks
Quiz: 20 Marks

Instructions for the Lab

A. If a student is absent on the day of evaluation, will be awarded ZERO for that evaluation.

B. Turn off your systems before leaving lab. Do not use mobile phone during lab hours.

Lab 3

Q1: Answer the following questions for captured file dns1.pcap (DNS Protocol)

1. Locate the DNS query and response messages. Are they sent over UDP or TCP?
2. What is the destination port for the DNS query message? What is the source port of DNS response message?
3. To what IP address is the DNS query message sent? Use nm-tool command to determine the IP address of your local DNS server. Are these two IP addresses the same?
4. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
5. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?
6. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?
7. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Use the command: nslookup –type=NS mit.edu (Use dns2.pcap file)

8. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

9. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
10. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?

Q2: Answer the following questions for captured file tcp.pcap (TCP Protocol)

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu? To answer this question, it’s probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the “details of the selected packet header window” (refer to Figure 2 in the “Getting Started with Wireshark” Lab if you’re uncertain about the Wireshark windows.
2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?
3. What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?
4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?
5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?
6. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command; you’ll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a “POST” within its DATA field.
7. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What is the length of each of the first six TCP segments?
8. What is the EstimatedRTT value (see Section 3.5.3, page 239 in text from Kurose Book) after the receipt of each ACK? Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment. **[Hint:** Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the “listing of captured packets” window that is being sent from the client to the gaia.cs.umass.edu server. Select as Statistics->TCP Stream Graph->Round Trip Time Graph.]