Nova Southeastern University
College of Computing and Engineering

Assignment 2

ISEC 660 Advanced Network Security
Winter 2021
Due date: 2/14/2021
Total Points: 100

Notes:
1. Please include your name in EVERY document you submit.
2. Please sign and submit the "*Certification of Authorship*" form (located in Canvas) along with your solutions.

Section I. Reading

1. PowerPoint Slides (accessed in Canvas)

2. (Suggested textbook)
ISBN: 978-0133594140
Computer Networking: A Top-Down Approach
Author: James F. Kurose & Keith W. Ross
Edition: 7th
Publisher: Prentice Hall
Year Published: 2016
(Chapters 1 – 5 of the textbook, okay to use the previous editions of the textbook)

Alternatively, you can refer to the following online materials by focusing on the Application Layer, the Transport Layer, the Network Layer (layer 3), and the Datalink layer (layer 2) of the protocol stack.

https://www.geeksforgeeks.org/computer-network-tutorials/
https://www.javatpoint.com/computer-network-tutorial

Section II. Questions (80 points, all questions are equally weighted)

Q1. What is a network protocol?

Q2. Why does the HTTP protocol run on top of TCP rather than on UDP?

Q3. What are the two major services provided at the transport layer? What are their differences?

Q4. Suppose Client A initiates a SSL session with server S. Provide possible source and destination port numbers for:

a. The segment sent from S to A.

b. The segment sent from A to S.

Q5. Describe two major network-layer (layer 3) functions in a datagram network.

Forwarding and routing. Forwarding is about moving a packet from a router's input link to the appropriate output link. Routing is about determining the end-to-routes between sources and destinations.

Q6. Briefly compare and contrast IPv4 and IPv6.

Q7. Suppose an application generates chunks of 1960 bytes of data every 20 millisecond, and each chunk gets encapsulated in a TCP segment and then an IPv4 datagram. Assuming that all TCP segments and IPv4 datagrams use default structures for headers. What percentage of each datagram will be overhead, and what percentage will be application data?

Q8. Why the Ethernet is called a multiple access protocol? Is it a reliable protocol or not? Why?

Q9. What is the major networking device at the network layer (layer 3)? What is the major networking device at the datalink layer (layer 2)?

Q10. Why are acknowledgements (i.e. receivers acknowledging the recipient of messages) used in 802.11 but not in a wired Ethernet?

Section III. Practical assignment (20 points)

In this Wireshark lab, you'll get acquainted with Wireshark, and make some simple packet captures and observations. A brief introduction of the Wireshark tool, its installation, and initial experiments can be found in the file "Wireshark_Intro.pdf".

You are required to install the latest version of Wireshark, run the tool, and capture network traffic by accessing http://www.mit.edu/index.html. It is recommended that you disable other background networking applications to make the traffic easy to identify. Answer the following questions:

1. What is the IP address (IPv4 or IPv6, depending on the platform you used) and TCP port number used by the client computer (source) to communicate with www.mit.edu? What is the IP address (IPv4 or IPv6) and TCP port number used by the server (destination) www.mit.edu?
2. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and nsu.nova.edu? What is it in the segment that identifies the segment as a SYN segment?
3. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

4. Print the two HTTP messages (GET and OK) referred to in question 3 above. To do so, select Print from the Wireshark File command menu, and select the "Selected Packet Only" and "Print as displayed" radial buttons, and then click OK.
5. Print the two TCP messages (SYN and SYNACK) referred to in question 2 above.
6. Is the connection to nsu.nova.edu secure or not? Why? Justify your answer based on the captured network traffic.