Cybersecurity Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Quiz 6 – Network Traffic Analysis

Points: \_\_\_\_\_\_\_\_\_\_ / 21

You may only use your notes for the following questions.

1. What is a packet? (1 point)

2. What are the layers in the TCP/IP model from top to bottom? (4 point)

Top

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Bottom

3. What is the difference between TCP and UDP? When should each be used? (2 points)

4. What is the difference between the well-known, registered, and dynamic ports? (3 points)

5. Match the protocol to its well-known port number.

a. FTP \_\_\_\_\_\_\_\_\_\_ (1 point)

b. HTTP \_\_\_\_\_\_\_\_\_\_ (1 point)

c. HTTPS \_\_\_\_\_\_\_\_\_\_ (1 point)

d. Telnet \_\_\_\_\_\_\_\_\_\_ (1 point)

e. DNS \_\_\_\_\_\_\_\_\_\_ (1 point)

A. 20/21

B. 23

C. 53

D. 80

E. 443

You may use your notes, any online resources, and/or any software resources on the following questions.

8. Download the provided .pcap file. Analyze the packets to answer the following questions…

a. What website did the client request? (1 point)

b. What is the client’s IP address? (1 point)

c. What is the server's IP address? (1 point)

d. Who owns the server’s IP address (HINT: Use Google *whois* followed by the IP address)? (1 point)

e. True/False – The data for the requested website has been encrypted. (1 point)

f. BONUS – What Cipher Suite has been used to encrypt the data? (1 point)