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

Quiz 5 – Log Analysis

Points: \_\_\_\_\_\_\_\_\_\_ / 20

You may only use your notes for this page of the quiz.

1. What is a log? (1 point)

2. Why do cybersecurity professionals view logs? (1 point)

3. Why did we use a scripting language (i.e., Python) to process log files? (1 point)

4. What is SQL? (1 point)

5. What is a .JSON file? (1 point)

6. What is UNIX time? When does UNIX time start? (2 points)

7. Match the HTTP status code to its description.

a. 200 \_\_\_\_\_\_\_\_\_\_ (1 point)

b. 400 \_\_\_\_\_\_\_\_\_\_ (1 point)

c. 404 \_\_\_\_\_\_\_\_\_\_ (1 point)

d. 418 \_\_\_\_\_\_\_\_\_\_ (1 point)

A. The server cannot or will not process the request due to something that is perceived to be a client error.

B. The request succeeded.

C. I’m a teapot. The server refuses the attempt to brew coffee with a teapot.

D. The server cannot find the requested resource.

You may use your notes or any online resources on this page.

8. What is the date and time represented by the UNIX timestamp 783615600? Please write the date in our time zone (CST). (1 point)

9. Download the file called quiz\_data.log from the GitHub link on Google Classroom. Using this log, answer the following questions...

a. How many transactions are represented in the file? (1 point)

b. What is the total of all transactions? (1 point)

c. What was the transaction amount purchased by the user bacon23 from the IP address 193.45.22.7 on 5-1-2022? (1 point)

d. What is the username. IP, date, and amount of the largest transaction? (4 points)

d. Which date has the most purchases? (1 point)