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

Final Assessment

Points: \_\_\_\_\_\_\_\_\_\_ / 78

**Part 1** – You may only use your notes for this part of the final.

**Multiple Choice** – For questions 1 through 6, select exactly one answer.

1. What name is given to hackers who hack for a cause? (1 point)

A. white hat

B. hacker

C. hacktivist

D. blue hat

2. What name is given to an amateur hacker? (1 point)

A. red hat

B. black hat

C. script kiddie

D. blue team

3. Which of the following is considered the best for wireless security? (1 point)

A. WEP

B. WPA

C. WPA2

D. WPA 3

4. What is an IV? (1 point)

A. a type of attack in which the communication between two systems is intercepted by a third party

B. a random value used to add randomness into the encryption process

C. a random and unique data fed as an additional input to a hashing algorithm so the hash changes

D. a secret added to an input during hashing

5. What is salt? (1 point)

A. a type of attack in which the communication between two systems is intercepted by a third party

B. a random value used to add randomness into the encryption process

C. a random and unique data fed as an additional input to a hashing algorithm so the hash changes

D. a secret added to an input during hashing

6. What is a dictionary attack? (1 point)

A. a type of brute force attack where hackers try to guess a user’s password by checking it against a predefined list of passwords

b. a type of attack where the hashes are already generated in a table and the hash being cracked is compared to the hashes in the table to see if there is a match

c. a type of brute force attack where hackers try every combination of letter, number, and special character for a given password size

d. a type of attack where the hackers try to guess a user’s password by checking it against every word in the English dictionary

**Multiple Select** – For questions 7 through 0, select the indicated number of answers.

7. Of the following file extension, which two are commonly used for log files? (2 points)

A. .ppt

B. .json

C. .pdf

D. .exe

E. .log

8. Of the following, which three are hashing algorithms? (3 points)

A. MD5

B. ISO

C. SHA-256

D. IEEE 802.11

E. AES

F. LM/NTLM

9. Of the following devices, which three are considered host devices? (3 points)

A. PC

B. Switch

C. Router

D. IP Telephone

E. Printer

F. Access Point

**Classification** – For questions 10 through 15, classify each example of a hacker as either a black hat (B), grey hat (G), or white hat (W). (6 points total)

10. It is my job to identify weaknesses in the network in my company. (1 point) \_\_\_\_\_\_\_\_\_\_\_\_

11. I work with technology companies to fix a flaw with FTP. (1 point) \_\_\_\_\_\_\_\_\_\_\_\_

12. I used a keylogger to get the usernames and passwords of other students, \_\_\_\_\_\_\_\_\_\_\_\_  
and then accessed their accounts to plagiarize work and delete files. (1 point)

13. From my laptop, I transferred $10 million to my bank account using victim \_\_\_\_\_\_\_\_\_\_\_\_  
account numbers and PINs after viewing recordings of victims entering the   
numbers. (1 point)

14. I use malware to compromise company networks to steal credit card \_\_\_\_\_\_\_\_\_\_\_\_  
 information. (1 point)

15. I discovered a vulnerability for a network I am not authorized to enter \_\_\_\_\_\_\_\_\_\_\_\_  
 and worked with the network administrator to fix the vulnerability. (1 point)

**Matching** – For questions 16 through 18, match the term to the description.

16. Match the HTTP status code to its description. (4 points total)

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

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

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

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

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

B. The server cannot find the requested resource.

C. The request succeeded.

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

17. Match the Linux command to its description. (9 points total)

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

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

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

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

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

f. rm \_\_\_\_\_\_\_\_\_\_ (1 point)

g. echo \_\_\_\_\_\_\_\_\_\_ (1 point)

h. pwd \_\_\_\_\_\_\_\_\_\_ (1 point)

i. cd \_\_\_\_\_\_\_\_\_\_ (1 point)

A. Prints an argument to the command line. Commonly used to make .txt files.

B. Changes the current location to a different directory.

C. Prints the contents of one or more files to the command line.

D. Makes a directory.

E. Prints the present working directory.

F. Searches a file or text for a specific pattern.

G. Lists the contents of the current directory.

H. Gets a word count for a file.

I. Removes the specified file or directory. The directory must be empty.

18. Match the protocol to its well-known port number. (5 points total)

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

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

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

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

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

A. 20/21

B. 443

C. 23

D. 53

E. 80

**Fill in the Blank** – For questions 19 and 20, fill in the blanks.

19. Bob needs to send Alice a message and doesn’t want anyone but Alice to be able to read the contents. Bob will use the following steps to accomplish this. (4 points)

1. Bob writes the message.

2. Bob encrypts the message with \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_’s \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ key.

3. Bob sends the encrypted message to Alice.

4. Alice receives the message.

5. Using \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_’s \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ key, Alice decrypts the message.

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

Top

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

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

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

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

Bottom

**Short Response** – For questions 21 and 22, answer the question with a complete sentence.

21. What is the difference between symmetric and asymmetric encryption? (2 points)

22. What is a protocol? (1 point)

**Part 2** – You may use your notes or any online resources on this part of the final.

23. Consider the following cipher text. (2 points total)

Ocdn dn tjpm adivg

a. What cipher was used to encrypt the message? (1 point)

b. What was the plaintext? (1 point)

24. For this question, you will need to download the packet capture called **question\_24\_packets.pcap**. This packet capture is inside a GitHub that is linked on Google Classroom under the assignment called **Final Assessment**. Using the provided packet capture, answer the following questions. (23 points total)

a. What is the IP address of the client? (1 point)

b. What is the IP address of the server? (1 point)

c. What application layer protocol was used to deliver the resource to the client? (1 point)

d. What resource was downloaded by the client? What type of file is it? (2 points)

e. What hash type was used for the usernames and passwords? (1 point)

f. Decrypt the username and passwords. Record each pair in the table below. (16 points)

|  |  |
| --- | --- |
| Username | Password |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

g. Why were the passwords stored as hashes instead of plaintext? (1 point)

25. For this question, you will need to download the packet capture called **question\_25\_packets.cap**. This packet capture is inside a GitHub that is linked on Google Classroom under the assignment called **Final Assessment**. Using the provided packet capture, answer the following questions. (5 points total)

a. What is the MAC address of the wireless router? (1 point)

b. What protocol was used to secure the wireless network? (1 point)

c. What was the ESSID of the Wi-Fi network? (1 point)

d. What was the password for the Wi-Fi network? (1 point)

e. What was the IP address of the connected host? (1 point)