Family Name:..... **Other Names:** .....

Student ID:..... **Signature**.....

CYBR 171: TRIMESTER 1 – TEST 1

May 2, 2022

Instructions

- Time allowed: **60 minutes**
- **CLOSED BOOK**
- **Permitted materials**
  - Only silent non-programmable calculators or silent programmable calculators with their memories cleared are permitted in this test.
  - Printed English to foreign language dictionaries are permitted.
  - No other material is permitted.
- Attempt **ALL** questions in this booklet.
- This test contributes 25% of your final grade.
- Section A on pages 3 to 7 has TWENTY-FIVE multi-choice questions.
- Section B on pages 8 to 9 has EIGHT multi-choice questions.
- Choose your answer for each question in Sections A and B, and mark it on the multi-choice answer sheet provided, NOT in this question booklet. Any answers for Sections A or B in the question booklet WILL NOT BE MARKED.
- Read the instructions given on the answer sheet on how to mark your answers.
- **Hand in the multi-choice answer sheet.**
- Section C on page 10 has THREE written short answer questions.
- Write answers to Section C in the spaces provided in the test booklet.
- **Hand in the test booklet.**

Questions	**Marks**	
1. Section A - CONCEPTS	[25]	
2. Section B - APPLYING CONCEPTS	[16]	
3. Section C - SHORT ANSWERS	[9]	
	TOTAL:	

This page intentionally left blank.

SECTION A - CONCEPTS

Question 1. Which of the following is the BEST definition of *threat*? [1 mark]

A. An attempt to compromise system integrity, availability or confidentiality.
B. An attempt to gain unauthorized access to system services.
C. An event that has adversely impacted the security properties of an information system.
D. An event with the potential to adversely impact the security properties of an information system.

Question 2. Which of the following is the BEST example of an *passive attack*? [1 mark]

A. Attacker guesses my password and uses it to steal money.
B. Attacker misuses their legitimate access to bank system to steal money.
C. Attacker exploits vulnerability in bank system to steal money.
D. Attacker exploits vulnerability in bank system to view bank balances.

Question 3. Which of the following is the CORRECT definition of the acronym CIA? [1 mark]

A. Confidentiality, integrity, accountability
B. Confidentiality, integrity, authenticity
C. Confidentiality, immutability, authenticity
D. Confidentiality, integrity, availability

Question 4. Which of the following is TRUE about the *DES* and *RSA* algorithms? [1 mark]

A. DES encryption is slower than RSA encryption.
B. DES uses two different keys for encryption and decryption.
C. RSA uses a shorter key than DES.
D. RSA uses two different keys for encryption and decryption.

Question 5. According to Claude Shannon, which of the following is MOST important to kept secret? [1 mark]

A. Algorithm.
B. Encryption system.
C. Key.
D. Number of possible keys.

Question 6. Which of following is the BEST description of a *transposition* cipher? [1 mark]

A. Each character of the plaintext is reordered to form the ciphertext.
B. Each character of the plaintext is replaced by a pair of characters to form the ciphertext.
C. Each character of the plaintext is turned into ASCII to form the ciphertext.
D. Each character of the plaintext is turned into binary to form the ciphertext.

Question 7. Which of the following CANNOT be chosen as a key for a Caesar cipher? [1 mark]

A. Alphabetic character.
B. Binary number.
C. Integer number.
D. String of alphabetic characters.

Question 8. Which of the following modern cryptography algorithms is the MOST vulnerable to bruteforcing attacks? [1 mark]

A. AES.
B. DES.
C. 3DES.
D. RSA.

Question 9. Which of the following is the BEST reason to avoid the use of the Electronic Code Book (ECB) mode of operation? [1 mark]

A. A small change in plaintext causes a big change in the ciphertext.
B. Cannot be used with a block cipher.
C. Easy to see the relationship between plaintext and ciphertext.
D. Requires the use of padding.

Question 10. Which of the following is the MAIN problem solved by the Diffie-Hellman method? [1 mark]

A. Authenticity of a key sent between communicating parties.
B. Creating of keys resistant to brute force attacks.
C. Large number of key pairs needed between communicating parties.
D. Third party making a copy of a key sent between communicating parties.

Question 11. Which of the following properties is FALSE for a *hash function*? [1 mark]

A. Different output for the same input.
B. One-way function.
C. Small change to input leads to large change to output.
D. Two different inputs should not produce the same output.

Question 12. Which of the following is the CORRECT definition of a *rainbow table*? [1 mark]

A. Dictionary of encrypted values.
B. Dictionary of hashes.
C. Dictionary of passwords.
D. Dictionary of plaintexts.

Question 13. Which of the following is the CORRECT reason to use password salting? [1 mark]

A. Avoid the need to send the password across the network.
B. Increase the work required to bruteforce a password.
C. Lockout an attacker who tries the wrong password multiple times.
D. Prevent users from using easy to guess passwords.

Question 14. Which of following passwords would be MOST likely to be considered easy for humans to remember but HARD easy for computers to guess using DICTIONARY attacks? [1 mark]

A. apple.
B. cooktrainerbackvictory.
C. XEb@uy=wktj&$4H.
D. 1968.

Question 15. Which of the following is the CORRECT description of *password spraying*? [1 mark]

A. Use same password on many different accounts.
B. Use many different passwords with the same username.
C. Use many different passwords on many different accounts.
D. Use random passwords on many different accounts.

Question 16. Which of the following type of authentication is the BEST description of a smart card? [1 mark]

A. Something you are.
B. Something you can do.
C. Something you know.
D. Something you possess.

Question 17. Which of the following is the CORRECT term for a situation when an enrolled user presents a biometric to an authentication system and it doesn't recognise them? [1 mark]

A. False match.
B. False non-match.
C. True match.
D. True non-match.

Question 18. Which of the following is the FIRST action carried out by a virus according to lectures? [1 mark]

A. Checks for condition that must be met to start looking for a program to infect.
B. Copies instructions into the target program.
C. Jumps to the beginning of the infected program.
D. Performs some action related to the purpose of the virus.

Question 19. Which of the following is the MAIN purpose of a *web shell*? [1 mark]

A. Maintain access.
B. Defacement.
C. Destruction.
D. Financial gain.

Question 20. At what point would a system be considered SAFE from an *zero-day exploit*? [1 mark]

A. Anti-malware detection updated.
B. Malware exploiting vulnerability discovered.
C. Vulnerability discovered by hackers.
D. Vulnerability fixed.

Question 21. Which of the following is the MOST important requirement for a switched packet network? [1 mark]

A. Contents of packet kept confidential.
B. Delivery of packets.
C. Packets belonging to one message take the same route.
D. Packet takes most direct route to destination.

Question 22. Which of the following is the MAIN purpose of including a source port in the header of a packet sent to a server? [1 mark]

A. Identifies which program on client will process the reply.
B. Identifies which program on client will process the request.
C. Indicates which service to process the request.
D. Indicates which service to process the reply.

Question 23. You are connecting to a WPA2 network using a shared key. Which of following statements is FALSE? [1 mark]

A. You can capture any passwords sent to the wireless access point when another client connects.

B. You can protect your web traffic from sniffing by using HTTPS.

C. You can send deauthentication requests to the wireless access point to disconnect any other client.

D. You can sniff any traffic sent by any other client on the same network.

Question 24. Which of the following is NOT found in a *digital certificate*? [1 mark]

A. Issuer's distinguished name.

B. Issuer's digital signature.

C. Owner's distinguished name.

D. Owner's private key.

Question 25. Which of the following is LEAST important for a MiTM attack using an evil twin to succeed? [1 mark]

A. Evil twin has a connection to the Internet.

B. Evil twin has a more powerful radio than the victim wifi access point.

C. Evil twin has the same SSID as the victim wifi access point.

D. Evil twin implements a captive portal.

SECTION B - APPLYING CONCEPTS

Question 26. You are a grey hat hacker targeting a hospital. You easily bruteforce access to the main database and contact them to inform them of the vulnerability. You are arrested and charged under the New Zealand Crimes Act for violating a clause related to unauthorised access. Which of the following arguments regarding your guilt is CORRECT? [2 marks]

A. Guilty because your intention was malicious.

B. Guilty because it is the action rather than the motivation that is important.

C. Not guilty because you actions caused no obvious harm.

D. Not guilty because your intention was to help.

Question 27. You encrypt the plaintext MAXY using the Vigenere cipher. Which of the following options is the CORRECT ciphertext for the given text if the key is BZ? [2 marks]

A. LZWX.

B. MYXW.

C. NYYW.

D. NZYX.

Question 28. You are using a cipher with a blocksize of 16 bits. How MANY bits are required to be added as padding for a 151 bit plaintext? [2 marks]

A. 6.

B. 9.

C. 15.

D. 16.

Question 29. Alice decides to use RSA to authenticate that she encrypted a message being sent to Bob. Which of the following keys is the CORRECT one to use? [2 marks]

A. Bob' public key.

B. Bob's private key.

C. Alice's public key.

D. Alice's private key.

Question 30. Calculate the number of rainbow tables an attacker would have to create for a system with a hash size of 3 bits and a salt of 5 bits. [2 marks]

This table will help you do the calculation.

N	2^N
2	4
3	8
5	32
8	256

A. 4.

B. 8.

C. 32.

D. 256.

Question 31. Your PC has been infected by malware. Your analysis shows that it tried to modify the code used to startup the operating system but failed. It was successfully able to complete the infection process by inserting itself into executable files in your program directory. Based upon your analysis, which of the following BEST describes the type of malware? [2 marks]

A. Metamorphic virus.

B. Multipartite virus.

C. Polymorphic virus.

D. Terminate-and-stay Resident virus.

Question 32. A virus infects a PC, when investigating the incident you discover that the integrity-based anti-malware system did not detect it. Based on your analysis, which of the following BEST describes the type of malware? [2 marks]

A. Metamorphic virus.

B. Multipartite virus.

C. Polymorphic virus.

D. Terminate-and-stay Resident virus.

Question 33. You are connected to a WPA2 wifi router in a public space and access several different websites on the Internet. Which of the following statements is MOST CORRECT? [2 marks]

A. The attacker has to have the network key for the WPA2 router to setup an evil twin and have you connect to it.

B. You do not need to worry because all traffic to the websites is protected by WPA2.

C. You should only access ecommerce and other banking websites using HTTPS.

D. You should watch out for "This Connection is Untrusted" because this always means you are are subject to a MiTM attack.

SECTION C- SHORT ANSWERS

Question 34. OUTLINE the steps in a *credential stuffing* attack. [3 marks]

Question 35. What has to be SYNCHRONISED between a hash-based token and authenticator that use a one-time-password and why is it necessary? [3 marks]

Question 36. BRIEFLY discuss what is *post quantum computing* and how it will help against the quantum threat to cryptography? [3 marks]

Student ID: .....

SPARE PAGE FOR EXTRA ANSWERS

Cross out rough working that you do not want marked.
Specify the question number for work that you do want marked.

* * * * * * * * * * * * * * *