Family Name:..... **First Name:**.....

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

CYBR 171: TEST 1

May 1, 2023

GROUP

A

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. What is the difference between a vulnerability and a threat? [1 mark]

A. A vulnerability is a hypothetical scenario that could potentially harm an information system, while a threat is a known weakness that can be exploited.

B. A vulnerability is a known weakness that can be exploited, while a threat is a hypothetical scenario that could potentially harm an information system.

C. A vulnerability is a software or hardware component that has a known weakness, while a threat is a person or group that is actively attempting to exploit that weakness.

D. There is no difference between a vulnerability and a threat in cybersecurity.

Question 2. Who is a white-hat hacker? [1 mark]

A. A hacker who attacks systems with the intention of causing harm or damage.

B. A hacker who has malicious intent and engages in illegal activities.

C. A hacker who uses a combination of both legal and illegal methods to achieve their objectives.

D. A hacker who works for a company to find vulnerabilities in their system and improve security.

Question 3. What is the purpose of authenticity in a messaging system? [1 mark]

A. To ensure the confidentiality of messages.

B. To establish trust between parties.

C. To prevent unauthorised access to messages.

D. To trace the actions of an entity.

Question 4. How does non-repudiation help to prevent fraud in financial transactions? [1 mark]

A. It ensures that messages cannot be modified.

B. It ensures the confidentiality of messages.

C. It prevents a party from denying sending or receiving a message.

D. It prevents unauthorised access to messages.

Question 5. Which of the following is an example of two-factor authentication? [1 mark]

A. Entering a username and password.

B. Scanning a fingerprint and entering a password.

C. Typing in a PIN code.

D. Using a password manager.

Question 6. What is encryption? **[1 mark]**

A. A countermeasure against polymorphic malware.
B. A function that produces a fixed-size output for an input.
C. A technique used to prevent unauthorised access to data.
D. A type of malware that locks down a system.

Question 7. What is the range of the Caesar cipher shift values? **[1 mark]**

A. 0–25.
B. 0–26.
C. 1–25.
D. any positive integer value.

Question 8. What is the MAIN purpose of a penetration test? **[1 mark]**

A. To test the effectiveness of a company's antivirus software.
B. To test the effectiveness of a company's backup strategy.
C. To test the effectiveness of a company's cybersecurity defenses.
D. To test the effectiveness of a company's physical security measures.

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

A. It cannot encrypt large files.
B. It is slower than other modes.
C. It is vulnerable to pattern recognition attacks.
D. It requires more memory than other modes.

Question 10. What is the MAIN problem solved by the Diffie-Hellman key exchange? **[1 mark]**

A. Ensuring the confidentiality and integrity of transmitted data.
B. Generating a shared secret key between two parties without prior communication.
C. Generating a unique session key for each communication session.
D. Securely transmitting a private key over an insecure channel.

Question 11. Which of the following is a FALSE statement about *cryptographic* hash functions? **[1 mark]**

A. They can be used for digital signatures.
B. They are commonly used for password storage.
C. They are reversible functions.
D. They are used for message integrity.

Question 12. What is a man-in-the-middle attack? [1 mark]

A. A type of attack that intercepts communication between two parties.

B. A type of intrusion that exploits a vulnerability in a system.

C. A type of malware that spreads through email attachments.

D. A type of social engineering attack that tricks users into revealing sensitive information.

Question 13. Which of the following is NOT a benefit of using password salting? [1 mark]

A. It adds a layer of security to password storage.

B. It makes it easier to recover lost passwords.

C. It makes it harder for attackers to guess the password.

D. It makes it harder for attackers to use precomputed hash values.

Question 14. Which of the following cryptography algorithms is considered the most secure against brute force attacks? [1 mark]

A. AES.

B. DES.

C. 3DES.

D. MD5.

Question 15. How does password spraying differ from a brute force attack? [1 mark]

A. Password spraying is faster than brute force attacks.

B. Password spraying is less effective than brute force attacks.

C. Password spraying uses a large number of passwords across many user accounts, whereas brute force attacks try a small number of passwords on a single user account.

D. Password spraying uses a single password across many user accounts, whereas brute force attacks try a large number of passwords on a single user account.

Question 16. Which of the following type of authentication is the BEST description of a *Google Titan* key? [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 a not enrolled user presents a biometric to an authentication system and it does recognise them? [1 mark]

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

Question 18. What is the PRIMARY defense against credential-stuffing attacks? [1 mark]

A. Blocking IP addresses that show signs of suspicious activity.
B. Implementing multi-factor authentication.
C. Regularly changing passwords for user accounts.
D. Requiring strong passwords for user accounts.

Question 19. Which of the following security threats is most likely to be MISSED by a *signature-based* antivirus system? [1 mark]

A. A logic bomb.
B. A rootkit.
C. A Trojan horse.
D. A zero-day exploit.

Question 20. How does a patch protect a system from an *zero-day exploit*? [1 mark]

A. By alerting system administrators to any suspicious activity.
B. By blocking the vulnerability and preventing it from being exploited.
C. By detecting and removing any malware that exploits the vulnerability.
D. By encrypting sensitive data to prevent it from being stolen.

Question 21. What is the MAIN aim of a switched packet network with multiple paths? [1 mark]

A. Allowing for faster transmission of data between nodes.
B. Providing redundancy and resiliency in case of partial network failures.
C. Reducing network congestion and improving network performance.
D. Simplifying network management and configuration.

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

A. To identify the application or service using a network connection.

B. To identify the physical location of a device on a network.

C. To identify the type of network cable used to connect devices.

D. To identify the type of network protocol used to transmit data.

Question 23. You are using a Wi-Fi network that employs WPA2 encryption. Which of the following statements is MOST CORRECT? [1 mark]

A. Each client on the network is assigned a unique encryption key, which provides additional security.

B. The network is protected by a signature-based anti-malware that blocks all malicious traffic.

C. The pre-shared key used for encryption is transmitted in plaintext and can be easily intercepted by attackers.

D. The same encryption key is used for all clients on the network, which makes it vulnerable to attacks.

Question 24. How can you check the authenticity of a *digital certificate*? [1 mark]

A. By checking the encryption strength of the certificate and ensuring it meets industry standards.

B. By checking the expiration date of the certificate and ensuring it is still valid.

C. By checking the public key of the certificate and ensuring it matches the private key of the website or server.

D. By verifying the issuer of the certificate and ensuring it is a trusted certificate authority.

Question 25. Which of the following is BEST defining an *evil twin* attack? [1 mark]

A. An attack where an attacker floods a network with traffic to cause a denial of service.

B. An attack where an attacker gains unauthorised access to a network by exploiting a vulnerability in the system.

C. An attack where an attacker impersonates a legitimate network access point to intercept network traffic.

D. An attack where an attacker steals sensitive information by tricking users into providing it.

SECTION B - APPLYING CONCEPTS

Question 26. A white-hat hacker has discovered a vulnerability in a company's computer system and has informed the system owner. However, the system owner has not taken any action to fix the vulnerability. A black-hat hacker has also discovered the same vulnerability and is attempting to exploit it for personal gain. Which of the following actions is MOST appropriate for the white-hat hacker? [2 marks]

A. Continuing to inform the system owner and urging them to take action to fix the vulnerability.

B. Exploiting the vulnerability themselves to demonstrate the severity of the issue to the system owner.

C. Launching a counter-attack against the black-hat hacker to prevent them from exploiting the vulnerability.

D. Notifying law enforcement and taking legal action against the black-hat hacker.

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

A. GUFN.

B. HVGO.

C. IWHP.

D. ZDYW.

Question 28. An unemployed hacker uses a bank customer's Internet banking credentials to transfer $1,000 to their own account. Which of the following best describes this type of attack? [2 marks]

A. Insider active attack.

B. Insider passive attack.

C. Outsider active attack.

D. Outsider passive attack.

Question 29. Alice decides to use RSA to maintain the confidentiality and authenticity of a message she sends to Bob. Which of the following is the CORRECT combination? [2 marks]

A. She uses her private key to encrypt the message, and Bob's public key to encrypt the hash.

B. She uses her private key to encrypt the hash, and Bob's public key to encrypt the message.

C. She uses her public key to encrypt the message, and Bob's public key to encrypt the hash.

D. She uses her public key to encrypt the hash, and Bob's public key to encrypt the message.

Question 30. Calculate the number of rainbow tables an attacker would have to create for a system with a hash size of 4 bits and a salt of 6 bits. [2 marks]

This table will help you do the calculation.

N	0	1	2	3	4	5	6	7	8	9	10
2 ^ N	1	2	4	8	16	32	64	128	256	512	1024

A. 4.

B. 16.

C. 64.

D. 1024.

Question 31. What is the MAIN difference between *Polymorphic* and *Metamorphic* viruses? [2 marks]

A. Polymorphic viruses are harder to detect than Metamorphic viruses.

B. Polymorphic viruses change their code with each infection, while Metamorphic viruses change their appearance.

C. Polymorphic viruses only infect specific file types, while Metamorphic viruses infect any file type.

D. Polymorphic viruses use encryption to hide their code, while Metamorphic viruses do not.

Question 32. A user downloads a software program from an untrusted website, and their computer becomes infected with malware. The malware is able to replicate itself and spread to other computers on the network. Based on your analysis, which of the following BEST describes the type of malware? [2 marks]

A. Logic bomb.

B. Polymorphic virus.

C. Trojan horse.

D. Worm.

Question 33. You are connected to a WPA2-encrypted Wi-Fi network using a preshared key. Assuming the attacker knows the preshared key, which of the following statements is MOST CORRECT? [2 marks]

A. It is safe to check your email on the HTTP web.

B. The attacker can still intercept and decrypt your traffic.

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

D. You should only access websites that use HTTPS encryption.

SECTION C- SHORT ANSWERS

Question 34. A company discovers that one of its employees has fallen victim to a *password spraying* attack due to using a weak password that was easily guessed by the attacker. BRIEFLY discuss if two-factor authentication would be effective against such types of attacks and why? [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 the *double-spend* problem in cryptocurrency and how is it solved? [3 marks]

Student ID: .....

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