UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2023/2024

COURSE NAME	:	FUNDAMENTALS OF INFORMATION SECURITY
COURSE CODE	:	BIT 21403
PROGRAMME CODE	:	BIT
EXAMINATION DATE	:	JULY 2024
DURATION	:	3 HOURS
INSTRUCTIONS	:	1. ANSWER ALL QUESTIONS 2. THIS FINAL EXAMINATION IS CONDUCTED VIA ☐ Open book ☒ Closed book 3. STUDENTS ARE **PROHIBITED** TO CONSULT THEIR OWN MATERIAL OR ANY EXTERNAL RESOURCES DURING THE EXAMINATION CONDUCTED VIA CLOSED BOOK

THIS QUESTION PAPER CONSISTS OF **NINE (9)** PAGES.

PART A

Choose the **BEST** answer.

Q1 What is the primary goal of encryption in computer security?

(a) Ensuring data availability.

(b) Protecting against malware.

(c) Securing data transmission.

(d) Hiding data from unauthorized access.

(2 marks)

Q2 Which of the following is a characteristic of a strong password?

(a) Short length.

(b) Easily guessable.

(c) Contains a combination of letters, numbers, and special characters.

(d) Written down and shared with others.

(2 marks)

Q3 What is the primary goal of message authentication?

(a) Ensuring data confidentiality.

(b) Ensuring data integrity.

(c) Protecting against malware.

(d) Providing access control.

(2 marks)

Q4 Which cryptographic technique involves combining a message with a secret key to generate a fixed-size hash value?

(a) Digital signatures.

(b) Hash-based Message Authentication Codes (HMACs).

(c) Symmetric encryption.

(d) Asymmetric encryption.

(2 marks)

Q5 Which security mechanism verifies the identity of a user or process?

(a) Identification.

(b) Authentication.

(c) Authorization.

(d) Encryption.

(2 marks)

Q6 What type of attack involves overwhelming a system with excessive traffic to disrupt normal operations?

(a) Brute-force attack.

(b) Denial-of-service attack.

(c) Man-in-the-middle attack.

(d) Phishing attack.

(2 marks)

Q7 Which of the following is **NOT** a requirement for attacking symmetric encryption?

(a) Knowledge of the algorithm.

(b) Knowledge of the key.

(c) Analysis of encrypted data.

(d) Availability of computational resources.

(2 marks)

Q8 What is a common type of malware that disguises itself as legitimate software but contains malicious code?

(a) Worm.

(b) Virus.

(c) Trojan.

(d) Spyware.

(2 marks)

Q9 Determine the **BEST** method for securely distributing public keys in a public-key cryptosystem.

(a) Use digital certificates issued by a trusted Certificate Authority (CA).

(b) Share public keys via email.

(c) Post public keys on social media.

(d) Publish public keys on public forums.

(2 marks)

Q10 Choose the **BEST** plan for implementing Role Based Access Control (RBAC) in an organization's network infrastructure.

(a) Assign roles to users based on job functions and responsibilities.

(b) Use Access Control Lists (ACLs) to restrict access to resources.

(c) Implement role-based policies to govern access permissions.

(d) Regularly review and update access privileges based on changes in user roles.

(2 marks)

Q11 Which of the following is the **CORRECT** statement?

(a) Symmetric encryption requires a single key for both encryption and decryption, while asymmetric encryption uses a pair of keys. Symmetric encryption has lower computational complexity but requires secure key distribution. Asymmetric encryption offers key exchange without requiring a secure channel but is computationally more intensive.

(b) Symmetric encryption uses two keys, while asymmetric encryption uses a single key. Symmetric encryption is more computationally complex but offers better security. Asymmetric encryption is less secure but more efficient.

(c) Symmetric encryption requires a single key for both encryption and decryption, while asymmetric encryption uses a pair of keys. Symmetric encryption is computationally more intensive and requires secure key exchange. Asymmetric encryption offers key exchange without requiring a secure channel but is less computationally complex.

(d) Symmetric encryption uses a pair of keys, while asymmetric encryption uses a single key. Symmetric encryption is less secure but more efficient. Asymmetric encryption is more secure but less efficient.

(2 marks)

Q12 Choose the **CORRECT** statement describing Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).

(a) IDS monitors network traffic and alerts administrators to potential security threats, while IPS actively blocks and prevents suspicious traffic. IDS is more passive and reactive, while IPS is more proactive in preventing attacks. Both systems have their advantages and limitations, and a combination of IDS and IPS may provide comprehensive network security.

(b) IDS and IPS both monitor network traffic for suspicious activity, but IDS only alerts administrators to potential threats, while IPS actively blocks and prevents malicious traffic. IDS is more proactive than IPS in preventing attacks. However, IPS may generate false positives and inadvertently block legitimate traffic.

(c) IDS and IPS both monitor network traffic for suspicious activity, but IDS only alerts administrators to potential threats, while IPS actively blocks and prevents malicious traffic. IPS is more proactive and effective in preventing attacks. However, IDS may be more suitable for environments where blocking traffic is not feasible or desirable.

(d) IDS monitors network traffic and actively blocks and prevents suspicious activity, while IPS only alerts administrators to potential threats. IDS is more proactive and effective in preventing attacks. However, IPS may generate false positives and inadvertently block legitimate traffic.

(2 marks)

Q13 Choose the **CORRECT** statement describing two-factor authentication (2FA) for remote access to an organization's network resources.

(a) Require users to enter a username and password, and then send a one-time passcode to their registered mobile device for verification.

(b) Use biometric authentication methods, such as fingerprint or facial recognition, in addition to a password.

(c) Implement hardware tokens that generate one-time passcodes for users to enter along with their passwords.

(d) Require users to answer security questions in addition to entering their passwords.

(2 marks)

Q14 Choose the **CORRECT** statement describing the effectiveness of using encryption to protect sensitive data stored on mobile devices.

(a) Encryption can significantly improve the security of sensitive data stored on mobile devices by preventing unauthorized access in case of loss or theft. However, encryption may impact performance and usability, especially on older devices with limited processing power. It is essential to strike a balance between security requirements and user experience.

(b) Encryption is not effective for protecting sensitive data stored on mobile devices, as it may impact performance and usability without providing significant security benefits. Alternative security measures, such as remote wipe and device tracking, may be more suitable for protecting data on mobile devices.

(c) Encryption is effective for protecting sensitive data stored on mobile devices, as it prevents unauthorized access in case of loss or theft. Although encryption may impact performance and usability to some extent, the security benefits outweigh these concerns. It is crucial to ensure proper key management and encryption implementation to maximize security.

(d) Encryption can improve the security of sensitive data stored on mobile devices, but it may not be effective against all threats. Performance and usability may be impacted, especially on older devices. Organizations should supplement encryption with additional security measures, such as remote wipe and device tracking, for comprehensive protection.

(2 marks)

Q15 Which cryptographic technique involves using a pair of keys for encryption and decryption?

(a) Symmetric encryption.

(b) Asymmetric encryption.

(c) Hashing.

(d) Digital signatures.

(2 marks)

Q16 What type of attack involves an attacker intercepting and modifying communication between two parties?

(a) Brute-force attack.

(b) Denial-of-service attack.

(c) Man-in-the-middle attack.

(d) Phishing attack.

(2 marks)

Q17 ____________ controls the actions of an authenticated user.

(a) Identification

(b) Authentication

(c) Authorization

(d) Encryption

(2 marks)

Q18 How can steganography be applied in cybersecurity?

(a) To monitor network traffic for potential security threats.

(b) To conceal sensitive information within innocent-looking files.

(c) To encrypt data to protect it from unauthorized access.

(d) To analyse patterns of behaviour to detect anomalies in system activity.

(2 marks)

Q19 A company wants to improve the security of its network by implementing a Virtual Private Network (VPN). Which security principle does this action primarily address?

(a) Confidentiality.

(b) Integrity.

(c) Availability.

(d) Authentication.

(2 marks)

Q20 You are investigating a security breach in your organization's network. Which type of analysis involves reconstructing the sequence of events leading up to the breach?

(a) Vulnerability analysis.

(b) Risk analysis.

(c) Forensic analysis.

(d) Penetration testing.

(2 marks)

PART B

Q21 In a multinational corporation, the cybersecurity team has been alerted to a potential insider threat. Emily, a disgruntled employee, is suspected of planning to steal sensitive company information. She is known to have access to various digital assets, including images, documents, and audio files. The team suspects that Emily may be using steganography to hide her activities. They decide to investigate further to determine if she is indeed using steganography to exfiltrate data.

Based on given scenario, answer the following questions.

(a) Explain a reason why an insider threat like Emily might choose steganography over traditional encryption methods.

(2 marks)

(b) Outline **THREE (3)** steps the cybersecurity team can take to detect the use of steganography in Emily's activities.

(6 marks)

(c) If Emily is indeed using steganography to hide sensitive data within images, discuss how can the cybersecurity team recover the hidden information.

(2 marks)

Q22 In a bustling media production company, there's a constant flow of multimedia content being created, edited, and shared among employees. With the increasing concerns about digital piracy and unauthorized distribution, the company's security team has been tasked with ensuring the integrity, confidentiality, and authenticity of their multimedia assets.

Based on given scenario, answer the following questions.

(a) Explain the concept of multimedia security and its importance in the context of a media production company.

(3 marks)

(b) Discuss **TWO (2)** roles of Digital Rights Management (DRM) in safeguarding multimedia content.

(4 marks)

(c) State **THREE (3)** techniques in forensic analysis that can be used to trace the source of unauthorized access or distribution.

(3 marks)

Q23 A digital payment platform enables users to make online purchases, transfer funds, and manage their finances through a mobile app and website. The platform is committed to ensuring the security and privacy of its users' financial information. The platform's security team regularly reviews and updates its security measures to protect against evolving threats.

Based on given scenario, answer the following questions.

(a) Discuss **THREE (3)** benefits of secure online payment processing for both the platform and its users.

(6 marks)

(b) Explain how tokenization and encryption can enhance online payment security.

(4 marks)

Q24 A prominent financial institution handles a vast amount of sensitive data, including customer financial information, transaction records, and employee details. With the increasing frequency of cyber threats targeting databases, the institution recognizes the critical importance of enhancing database security to protect its assets and maintain regulatory compliance.

Based on given scenario, answer the following questions.

(a) Discuss **TWO (2)** potential security risks and threats faced by the financial institution's database infrastructure.

(4 marks)

(b) Based on **Q24(a)**, discuss **TWO (2)** impacts to the confidentiality, integrity, and availability of the institution's data.

(4 marks)

(c) Describe the role of access control mechanisms in ensuring database security.

(2 marks)

- END OF QUESTIONS -