This question paper consists of TWO (2) sections. Answer ALL questions in the answer booklet provided. [100 MARKS]

SECTION A (40 Marks)

There are TWENTY (20) questions in this section. Answer ALL questions in the answer booklet.

1. What is the primary objective of digital forensics?

   A. Recovering lost data
   B. Enhancing computer performance
   C. Investigating crimes involving digital devices
   D. Maintaining network security

2. Which of the following is a cybercrime involving sending unwanted and unsolicited emails?

   A. Malware Distribution
   B. Hacking
   C. Spamming
   D. Email Bombing

3. Which of the following characteristics is commonly examined to understand the behavior of a piece of malware without executing it?

   A. Dynamic API calls
   B. Code execution flow
   C. Memory dumps
   D. File structure and metadata

4. What is the term used to describe acquiring digital evidence while preserving its integrity for admissibility in court?

   A. Digital Forensics Soundness
   B. Digital Evidence Preservation
   C. Forensically Sound Evidence Acquisition
   D. Cybercrime Evidence Collection

5. What is the primary goal of malware?

   A. Encrypting user files and demanding a ransom
   B. Displaying unwanted advertisements on the user's screen
   C. Corrupting files or stealing saved login information
   D. All the above

6. Which of the following is a technique used for attacking the security vulnerabilities of a database?

   A. Brute-Force Attack
   B. Buffer Overflow Attack
   C. SQL Injection
   D. Pharming

7. What is included in the category of user-created data in digital forensics?

   A. System files and operating system logs
   B. Metadata and file attributes
   C. Audio and video files
   D. Temporary internet files and browser cache

8. Why is the investigation of metadata emphasized in digital forensics?

   A. To identify the type of digital artifacts.
   B. To determine the authenticity of user-created data.
   C. To assess the encryption level of hidden files.
   D. To analyze the contents of email attachments.

9. What is the significance of "chain of custody" during a cyber incident in the forensic investigation process?

   A. It ensures that all employees know the incident and follow proper reporting procedures.
   B. It establishes a chronological record of events and actions taken, maintaining the integrity of evidence for potential legal proceedings.
   C. It refers to identifying the origin of a security incident to determine the responsible party.
   D. It outlines the sequence of security controls in place to prevent future incidents.

10. When conducting a post-incident review, what is the significance of a "lessons learned" session, and how does it improve future incident response?

    A. It focuses on assigning blame for the incident and ensuring accountability among the involved teams.
    B. A lessons-learned session is an opportunity to identify and document successes, failures, and areas for improvement in the incident response process.
    C. It is only relevant for major incidents and does not apply to routine cybersecurity events.
    D. Lessons-learned sessions are conducted before an incident occurs to prepare teams for potential challenges.

11. What is the role of "asset identification" in the threat modeling process, and how does it contribute to enhancing security measures?

    A. Asset identification involves determining the financial value of each asset within the organization, aiding in risk assessment.
    B. It categorizes assets based on physical size and location, helping prioritize security measures.
    C. Asset identification is crucial for recognizing and documenting the organization's critical assets and facilitating targeted protection efforts.
    D. It primarily identifies software assets to ensure proper patch management.

12. What is the primary purpose of using a sandbox environment?

    A. To execute the malware in a controlled environment and observe its behavior in real time.
    B. To extract static indicators of compromise (IoCs) from the malware code.
    C. To conduct signature-based detection of known malware patterns.
    D. To create a backup of the infected system for forensic analysis.

13. What is the primary purpose of a firewall in a network security infrastructure?

    A. To encrypt data transmitted over the network.
    B. To monitor and control incoming and outgoing network traffic based on predetermined security rules.
    C. To physically isolate critical network components.
    D. To provide secure authentication for users accessing the network.

14. In the context of penetration testing, what is the primary purpose of the "post-exploitation" phase?

    A. To identify vulnerabilities in the target system.
    B. To exploit discovered vulnerabilities and gain unauthorized access.
    C. To document the findings and prepare a detailed penetration test report.
    D. To maintain access, escalate privileges, and explore the extent of compromise after an initial successful exploitation.

15. During a web application penetration test, you discover a Cross-Site Scripting (XSS) vulnerability that allows for the injection of malicious scripts. What is the potential impact of this vulnerability, and how would you classify it in terms of severity?

    A. The impact is minimal, as XSS vulnerabilities only affect the appearance of web pages. It is classified as low severity.
    B. The impact is significant, allowing an attacker to execute malicious scripts in the context of the victim's browser. It is classified as high severity.
    C. XSS vulnerabilities are not a concern in web application security. It is classified as informational.
    D. The impact depends on the browser used and is classified as moderate severity.

16. Why is it crucial to create a forensic image of a suspect system rather than conduct analysis directly on the live system?

    A. Creating a forensic image allows for faster analysis since it is a snapshot of the live system.
    B. A forensic image provides a read-only copy of the system, preserving the original state and preventing unintentional alterations or data loss.
    C. Live system analysis is more reliable and captures real-time data changes than static forensic images.
    D. Forensic imaging is only necessary for network-based forensics, not for host-based investigations.

17. An organization is implementing a key management strategy for its cryptographic systems. The security policy mandates regular key rotation to mitigate the impact of potential key compromises. However, frequent key changes can also introduce operational challenges. What approach would you recommend for an effective and practical key rotation strategy?

    A. Implement a time-based key rotation schedule, where keys are changed on a fixed schedule, regardless of usage patterns.
    B. Use a combination of event-driven rotation triggered by security incidents and periodic time-based rotation to balance security and operational concerns.
    C. Rotate keys based on the system's uptime, ensuring that keys are changed after a specific number of hours of continuous operation.
    D. Adopt a one-time key strategy, where a unique key is generated for each cryptographic operation, eliminating the need for regular rotations.

18. You found a system where a suspicious program is running in the background. Your objective is to analyze the program's behavior and interactions with the operating system. What host-based forensic technique would be most suitable for this task?

    A. Memory analysis
    B. Disk imaging
    C. Network packet capture
    D. Registry analysis

19. In a multinational corporation, a senior executive receives an email claiming to be from the IT department, instructing them to download and install a software update immediately. The email appears authentic and urgent. The executive complies, unknowingly introducing malware into the corporate network. What type of attack does this represent?

    A. Social Engineering
    B. Insider Threat
    C. Advanced Persistent Threat (APT)
    D. Physical Security Breach

20. An organization processes a large volume of sensitive customer data, the employees use weak passwords, and the network lacks adequate encryption protocols. What are the most possible issues they will encounter?

A. DDoS Attack
B. Insider Threat
C. Data Breach
D. Ransomware

SECTION B **(60 Marks)**

There are THREE (3) questions in this part. Answer ALL questions in the answer booklet.

Question 1 (20 marks)

A multinational corporation known for its cutting-edge technology recently fell victim to a substantial data breach. Sensitive intellectual property, proprietary algorithms, and confidential business plans were stolen, prompting a digital forensics investigation. The stolen data is encrypted using a post-quantum cryptographic algorithm, raising concerns about industrial espionage. The organization seeks to understand the breach's extent and gather evidence for potential legal actions.

i. Discuss the challenges and implications of dealing with a highly complex encryption algorithm in the forensic analysis of stolen data. How does the advanced nature of the algorithm impact the ability to recover evidence? (6 marks)

ii. Propose and elaborate on advanced forensic techniques that could be employed to analyze data encrypted with a sophisticated post-quantum cryptographic algorithm. (8 marks)

iii. Outline the legal and ethical considerations the organization should be mindful of when attempting to decrypt the stolen data. How might the organization approach obtaining decryption keys legally and ethically, considering the sensitive nature of the stolen information? (6 marks)

Question 2 (20 marks)

A small healthcare provider has fallen victim to a sophisticated ransomware attack, compromising sensitive patient records and causing widespread disruption to critical services. The attackers demand a substantial ransom for the decryption keys.

i. Given an unknown and sophisticated ransomware variant employing advanced evasion techniques, outline the technical steps you would take to conduct a comprehensive analysis. Include both static and dynamic analysis methods, as well as collaboration with external threat intelligence platforms. (6 marks)

ii. Develop a comprehensive incident containment and recovery plan, considering the criticality of healthcare services. Address the coordination with external healthcare providers, regulatory bodies, and law enforcement. (9 marks)

iii. Propose a nuanced communication strategy that balances transparency about the incident with patient privacy considerations. Include plans for managing the reputational fallout and potential legal implications. (5 marks)

Question 3 (20 marks)

A messaging app is considering the implementation of end-to-end encryption to enhance user privacy. The company wants to balance security and usability while maintaining the ability to comply with legal requests for specific user data.

i. Select an algorithm suitable for end-to-end encryption in a messaging app, considering factors such as security and performance. (4 marks)

ii. Outline a key management strategy that ensures secure encryption key generation, distribution, and storage. (6 marks)

iii. Outline a secure backup and recovery mechanism for user messages in the context of end-to-end encryption. Consider scenarios where users switch devices, lose their devices, or need to recover messages after reinstalling the app.

Ensure that the mechanism maintains the confidentiality of messages while providing a seamless user experience. (10 marks)

***** END OF QUESTION PAPER *****