

注意：考試開始鈴響前，不得翻閱試題，
並不得書寫、畫記、作答。


國立清華大學 113 學年度碩士班考試入學試題

系所班組別：資訊安全研究所

科目代碼：2401

考試科目：資訊安全

—作答注意事項—

1. 請核對答案卷（卡）上之准考證號、科目名稱是否正確。
2. 考試開始後，請於作答前先翻閱整份試題，是否有污損或試題印刷不清，得舉手請監試人員處理，但不得要求解釋題意。
3. 考生限在答案卷上標記「由此開始作答」區內作答，且不可書寫姓名、准考證號或與作答無關之其他文字或符號。
4. 答案卷用盡不得要求加頁。
5. 答案卷可用任何書寫工具作答，惟為方便閱卷辨識，請儘量使用藍色或黑色書寫；答案卡限用 2B 鉛筆畫記；如畫記不清（含未依範例畫記）致光學閱讀機無法辨識答案者，其後果一律由考生自行負責。
6. 其他應考規則、違規處理及扣分方式，請自行詳閱准考證明上「國立清華大學試場規則及違規處理辦法」，無法因本試題封面作答注意事項中未列明而稱未知悉。

國立清華大學 113 學年度碩士班考試入學試題

系所班組別：資訊安全研究所

考試科目（代碼）：資訊安全（2401）

共 8 頁，第 1 頁

*請在【答案卷、卡】作答

Part I (80%) Please select one correct answer according to the question (2 points/each).

1. Which of the three security goals is most concerned with ensuring that data is not subject to unauthorized modification or alteration?
A. Availability
B. Integrity
C. Confidentiality
D. Non-repudiation
2. Which of the following supporting elements concerns the inability of the user to deny that he or she has performed an action with regard to data or on the system?
A. Confidentiality
B. Authentication
C. Authorization
D. Non-repudiation
3. Mark is attempting to log on to a computer system. He successfully presents his user credentials, but the system continually denies his logon attempts and will not allow him to access the system. Which of the following steps in the logon process is failing?
A. Identification
B. Authorization
C. Authentication
D. Auditing
4. Which of the following supporting elements of security relates to the correct level of permissions, rights, and privileges that a person may have with respect to what actions they may take with data or on a system?
A. Non-repudiation
B. Authorization
C. Confidentiality
D. Authentication
5. An organization decides to split the ability to perform security-related tasks among several different people. Which of the following concepts is the organization practicing?
A. Non-repudiation
B. Administrative control
C. Job rotation
D. Separation of duties

國立清華大學 113 學年度碩士班考試入學試題

系所班組別：資訊安全研究所

考試科目（代碼）：資訊安全（2401）

共 8 頁，第 2 頁

*請在【答案卷、卡】作答

6. The company policy requires that two people be present in order to witness and verify that highly sensitive information that is no longer needed has been properly destroyed. What practice is the company adhering to by requiring two people to perform this task?
 - A. Multi-person control
 - B. Separation of duties
 - C. Non-repudiation
 - D. Job rotation
7. The company suspects that Mike, a system administrator, is performing unauthorized actions on the network. Mike has not taken any significant time off in several years. Which of the following practices should the company consider in order to audit the activities Mike has performed while in his position?
 - A. Separation of duties
 - B. Job rotation
 - C. Mandatory vacation
 - D. Multi-person control
8. Jessica, who works in the accounting department, was discovered to have been performing administrative level actions on the accounting servers during a recent audit. While these actions were not malicious in nature, Jessica does not work at a level that would typically require server administration duties. Which of the following is not being properly implemented in the scenario?
 - A. Separation of duties.
 - B. Principle of least privilege
 - C. Technical control
 - D. Accountability
9. The company was recently subject to a hacking attack that resulted in the breach of several thousand records containing consumer financial data. All the following are examples of actions the company took to prevent such an attack, demonstrating due care, *except*:
 - A. Allowing all employees, regardless of duties, to access the data
 - B. Installing and securely configuring a firewall
 - C. Enabling encryption for all data
 - D. Requiring strong authentication methods
10. Data that is said to be easily readable by humans or machines is called _____.
 - A. ciphertext
 - B. plaintext
 - C. coded text
 - D. encrypted text

國立清華大學 113 學年度碩士班考試入學試題

系所班組別：資訊安全研究所

考試科目（代碼）：資訊安全（2401）

共 8 頁，第 3 頁

*請在【答案卷、卡】作答

11. Which of the following is the process used to convert ciphertext to plaintext?
- A. Decryption
 - B. Encryption
 - C. Encoding
 - D. Enciphering
12. Which of the following terms describes data that is stored on media, usually in the form of files?
- A. Data-in-RAM
 - B. Data-in-process
 - C. Data-in-transit
 - D. Data-at-rest
13. Which of the following terms refers to the output that comes from hashing a piece of text?
- A. Cipher
 - B. Code
 - C. Message digest
 - D. Key
14. How is hashing unlike the encryption and decryption processes?
- A. Hashes are not normally reversed or decrypted.
 - B. Hashes are encoded but not enciphered.
 - C. Hashes must be decrypted by a key different from the one that was used to encrypt them.
 - D. Hashes use the same key to encrypt and decrypt.
15. Which of the following terms describes a crypto-variable?
- A. Key
 - B. Algorithm
 - C. Cipher
 - D. Hash
16. Which of the following components of cryptography are typically publicly known and tested?
- A. Key
 - B. Algorithm
 - C. Crypto-variable
 - D. Cryptosystem

國立清華大學 113 學年度碩士班考試入學試題

系所班組別：資訊安全研究所

考試科目（代碼）：資訊安全（2401）

共 8 頁，第 4 頁

*請在【答案卷、卡】作答

17. Which of the following types of algorithms encrypts specified sizes of groups of text at a time?
- A. Asymmetric
 - B. Symmetric
 - C. Streaming
 - D. Block
18. You must implement a cryptography system in your organization. You need to be able to send large amounts of data, quickly, over the network. The system will be used by a very small group of users only, and key exchange is not a problem. Which of the following should you consider?
- A. Asymmetric cryptography
 - B. Symmetric cryptography
 - C. Hybrid cryptography
 - D. Key escrow
19. Which of the following standards dictates digital certificate file format, as well as use and information contained in the file?
- A. X.509
 - B. PKCS #12
 - C. X.500
 - D. PKCS #
20. If an individual encrypts a message with his own private key, what does this assure?
- A. Confidentiality
 - B. Message authenticity
 - C. Integrity
 - D. Availability
21. Which of the following entities can help distribute the workload of the CA by performing identification and authentication of individual certificate requestors?
- A. Subordinate CA
 - B. Root CA server
 - C. Authentication Authority
 - D. Registration Authority

國立清華大學 113 學年度碩士班考試入學試題

系所班組別：資訊安全研究所

考試科目（代碼）：資訊安全（2401）

共 8 頁，第 5 頁

*請在【答案卷、卡】作答

22. Which of the following authentication factors would require that you input a piece of information from memory in addition to using a smart card?
- A. Possession
 - B. Knowledge
 - C. Inherence
 - D. Temporal
23. All of the following are examples of single-factor authentication, *except*:
- A. Using a username and password combination to log on to a computer system
 - B. Answering security questions to reset a password
 - C. Use of a magnetic-strip security card to enter a secure door
 - D. Use of a smart card and PIN to log on to a computer system
24. Which of the following is the error rate at which biometric systems should be calibrated?
- A. False positive rate
 - B. False rejection rate
 - C. False acceptance rate
 - D. Crossover error rate
25. Which of the following terms describes the process of allowing access to different resources?
- A. Authorization
 - B. Authentication
 - C. Accountability
 - D. Identification
26. Which of the following states that users should be given only the level of access needed to perform their duties?
- A. Separation of duties
 - B. Accountability
 - C. Principle of least privilege
 - D. Authorization
27. The ability to write to a particular file is an example of a _____.
- A. right
 - B. privilege
 - C. discretionary access control model
 - D. permission

國立清華大學 113 學年度碩士班考試入學試題

系所班組別：資訊安全研究所

考試科目（代碼）：資訊安全（2401）

共 8 頁，第 6 頁

*請在【答案卷、卡】作答

28. Which of the following types of malware appears to be a useful piece of software, but in fact is malicious in nature?
- A. Worm
 - B. Trojan
 - C. Adware
 - D. Logic bomb
29. Which of the following types of malware infects critical operating system files, often replacing them with malicious ones?
- A. Rootkit
 - B. Trojan
 - C. Boot sector virus
 - D. Ransomware
30. One of your users calls you in a panic because he has just seen a pop-up message on his computer screen that states that all of the files on the system are encrypted, and that he must pay to have them decrypted or lose them forever. You back up the user's files on a daily basis and update the antivirus signatures every other day. What is the best course of action to take in this case?
- A. Pay the fee the ransomware is asking for.
 - B. Notify the authorities at once and attempt to update the antivirus signature with the latest release.
 - C. Wipe the computer's hard drives and restore the user's files from backup.
 - D. Reboot the computer.
31. Which of the following attacks involves sending false IP-to-MAC address mappings to a host, causing it to communicate with the attacker's machine instead of the legitimate one?
- A. XMAS attack
 - B. Pharming
 - C. DNS poisoning
 - D. ARP poisoning
32. In a watering hole type of attack, which web site is an attacker most likely to compromise?
- A. An organization's official web site
 - B. A site with a name very similar to the victim's web site
 - C. A user's social media site
 - D. A site frequented by the users of a victim organization

國立清華大學 113 學年度碩士班考試入學試題

系所班組別：資訊安全研究所

考試科目（代碼）：資訊安全（2401）

共 8 頁，第 7 頁

*請在【答案卷、卡】作答

33. All of the following are characteristics of host hardening, *except*:
- A. Minimum needed functionality
 - B. Maximum level of privileges for each user
 - C. Patched and updated
 - D. Removal of unnecessary applications
34. Which of the following should always be considered when configuring a host?
- A. Allowing access to configuration of management interfaces and configuration utilities
 - B. Maximum functionality for user accounts
 - C. Principle of least privilege
 - D. Shared passwords for administrative groups of users
35. You have an external DNS server that has been the target of a lot of traffic directed at SMTP lately. The server is required to make and respond to name resolution queries only. You examine the configuration of the server and find that the *sendmail* utility is configured and running on the host, and the server is also listening for inbound connections on TCP port 25. Which of the following actions should you take?
- A. Disable sendmail and any other program using TCP port 25.
 - B. Configure sendmail to send and receive e-mail from designated hosts only.
 - C. Disable the name resolution services on the host.
 - D. Configure DNS service to block inbound e-mail into the host.
36. Which of the following systems is normally required in high-security environments, and is used to address multilevel security requirements?
- A. 256-bit encryption
 - B. Biometric authentication
 - C. Single Sign-On capability
 - D. Trusted operating system
37. To prevent an application from being installed or executed on a host, _____ be implemented.
- A. blacklisting
 - B. greylisting
 - C. whitelisting
 - D. protected memory execution

國立清華大學 113 學年度碩士班考試入學試題

系所班組別：資訊安全研究所

考試科目（代碼）：資訊安全（2401）

共 8 頁，第 8 頁

*請在【答案卷、卡】作答

38. Which of the following should you do before installing a patch on a production host in an enterprise environment?
- A. Install host-based firewall and IDS applications.
 - B. Test the patch.
 - C. Determine the urgency of the patch and install it immediately if it is a critical security update.
 - D. Get approval from the end user.
39. Different groups in your organization require certain applications and security configuration settings that are unique to each group. You install a standard baseline image to the host computers for all the different groups. A developer group now complains that their applications do not work as they require, and that the security settings are too restrictive for them. They are able to document and show the necessity for less-restrictive security settings. Which of the following is your best course of action?
- A. Make changes to each individual host within the developer group to accommodate their needs.
 - B. Withdraw the requirement for a standard baseline since it cannot be enforced without impacting productivity.
 - C. Require that the developer group change their procedures and applications to fit with the new standard baseline image.
 - D. Create a specialized baseline image that applies only to the developer group, and ensure that everyone else gets the standard baseline image.
40. All of the following are reasons to implement a continuous monitoring solution, *except*:
- A. Ensure that any changes made are included in the updated standard security baseline.
 - B. Detect changes to the configuration baseline.
 - C. Detect security incidents.
 - D. Ensure that unauthorized changes are reversed.

Part II (20%) Please answer the following question in Chinese or English.

41. You are a leader of the Red Team in a cybersecurity company, currently engaged in a Red Team exercise with a manufacturing company. Please outline your Red Team exercise plan. (20 points)