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 112 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：2501

考試科目：資訊安全

一作答注意事項一

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112學年度碩士班考試入學試題

系所班組別：資訊安全研究所碩士班

考試科目（代碼）：資訊安全 (2501)

*請在【答案卷、卡】作答

Part I (94%) Please select one correct answer according to the question (2 points/each).

1. What is the most commonly used technique to protect against virus attacks?
   A. Signature detection
   B. Heuristic detection
   C. Data integrity assurance
   D. Automated reconstruction

2. You are the security administrator for an e-commerce company and are placing a new web server into production. What network zone should you use?
   A. Internet
   B. DMZ
   C. Intranet
   D. Sandbox

3. Which of the following techniques requires that administrators identify appropriate applications for an environment?
   A. Sandboxing
   B. Control signing
   C. Integrity monitoring
   D. Whitelisting

4. What type of application vulnerability most directly allows an attacker to modify the contents of a system's memory?
   A. Rootkit
   B. Back door
   C. TOC/TOU
   D. Buffer overflow

5. What character should always be treated carefully when encountered as user input on a web form?
   A. !
   B. &
   C. *
   D. ’

6. What database technology, if implemented for web forms, can limit the potential for SQL injection attacks?
   A. Triggers
   B. Stored procedures
   C. Column encryption
   D. Concurrency control

7. What condition is necessary on a web page for it to be used in a cross-site scripting attack?

A. Reflected input
B. Database-driven content
C. .NET technology
D. CGI scripts

8. What is the most effective defense against cross-site scripting attacks?

A. Limiting account privileges
B. Input validation
C. User authentication
D. Encryption

9. What worm was the first to cause major physical damage to a facility?

A. Stuxnet
B. Code Red
C. Melissa
D. WannaCry

10. Ben's system was infected by malicious code that modified the operating system to allow the malicious code author to gain access to his files. What type of exploit did this attacker engage in?

A. Escalation of privilege
B. Backdoor
C. Rootkit
D. Buffer overflow

11. What technology does the Java language use to minimize the threat posed by applets?

A. Confidentiality
B. Encryption
C. Stealth
D. Sandbox

12. What HTML tag is often used as part of a cross-site scripting (XSS) attack?

A. <H1>
B. <HEAD>
C. <XSS>
D. <SCRIPT>

13. When designing firewall rules to prevent IP spoofing, which of the following principles should you follow?
   A. Packers with internal source IP addresses don't enter the network from the outside.
   B. Packets with internal source IP addresses don't exit the network from the inside.
   C. Packets with public IP addresses don't pass through the router in either direction.
   D. Packets with external source IP addresses don't enter the network from the outside.

14. Why should you avoid deleting log files on a daily basis?
   A. An incident may not be discovered for several days and valuable evidence could be lost.
   B. Disk space is cheap, and log files are used frequently.
   C. Log files are protected and cannot be altered.
   D. Any information in a log file is useless after it is several hours old.

15. What are ethics?
   A. Mandatory actions required to fulfill job requirements
   B. Laws of professional conduct
   C. Regulations set forth by a professional organization
   D. Rules of personal behavior

16. What is the end goal of disaster recovery planning?
   A. Preventing business interruption
   B. Setting up temporary business operations
   C. Restoring normal business activity
   D. Minimizing the impact of a disaster

17. Which one of the following disaster types is not usually covered by standard business or homeowner's insurance?
   A. Earthquake
   B. Flood
   C. Fire
   D. Theft

18. Which one of the following is not a denial-of-service attack?
   A, Teardrop
   B. Smurf
   C. Ping of death
   D. Spoofing

19. How does a SYN flood attack work?
 A. Exploits a packet processing glitch in Windows systems
 B. Uses an amplification network to flood a victim with packets
 C. Disrupts the three-way handshake used by TCP
 D. Sends oversized ping packets to a victim

20. A web server hosted on the Internet was recently attacked, exploiting a vulnerability in the operating system. The operating system vendor assisted in the incident investigation and verified the vulnerability was not previously known. What type of attack was this?
 A. Botnet
 B. Zero-day exploit
 C. Denial-of-service
 D. Distributed denial-of-service

21. Of the following choices, what indicates the primary purpose of an intrusion detection system (IDS)?
 A. Detect abnormal activity
 B. Diagnose system failures
 C. Rate system performance
 D. Test a system for vulnerabilities

22. Which of the following is true for a host-based intrusion detection system (HIDS)?
 A. It monitors an entire network.
 B. It monitors a single system.
 C. It's invisible to attackers and authorized users.
 D. It cannot detect malicious code.

23. Of the following choices, what is the best form of anti-malware protection?
 A. Multiple solutions on each system
 B. A single solution throughout the organization
 C. Anti-malware protection at several locations
 D. One-hundred-percent content filtering at all border gateways

24. What is the most important rule to follow when collecting evidence?
 A. Do not turn off a computer until you photograph the screen.
 B. List all people present while collecting evidence.
 C. Never modify evidence during the collection process.
 D. Transfer all equipment to a secure storage location.

25. If port scanning does no damage to a system, why is it generally considered an incident?
    A. All port scans indicate adversarial behavior.
    B. Port scans can precede attacks that cause damage and can indicate a future attack.
    C. Scanning a port damages the port.
    D. Port scanning uses system resources that could be put to better uses.

26. What type of incident is characterized by obtaining an increased level of privilege?
    A. Compromise
    B. Denial of service
    C. Malicious code
    D. Scanning

27. Which of the following is most likely to detect DoS attacks?
    A. Host-based IDS
    B. Network-based IDS
    C. Vulnerability scanner
    D. Penetration testing

28. At which layer of the OSI model does a router operate?
    A. Network layer
    B. Layer 1
    C. Transport layer
    D. Layer 5

29. Which type of firewall automatically adjusts its filtering rules based on the content of the traffic of existing sessions?
    A. Static packet filtering
    B. Application-level gateway
    C. Stateful inspection
    D. Dynamic packet filtering

30. A VPN can be established over which of the following?
    A. Wireless LAN connection
    B. Remote access dial-up connection
    C. WAN link
    D. All of the above

31. What type of malware uses social engineering to trick a victim into installing it?
 A. Viruses
 B. Worms
 C. Trojan horse
 D. Logic bomb

32. The CIA Triad comprises what elements?
 A. Contiguousness, interoperable, arranged
 B. Authentication, authorization, accountability
 C. Capable, available, integral
 D. Availability, confidentiality, integrity

33. Which of the following is not a required component in the support of accountability?
 A. Auditing
 B. Privacy
 C. Authentication
 D. Authorization Restricted job resp

34. What is the last phase of the TCP/IP three-way handshake sequence?
 A. SYN packet
 B. ACK packet
 C. NAK packet
 D. SYN/ACK packer

35. In what type of cipher are the letters of the plaintext message rearranged to form the cipher text?
 A. Substitution cipher
 B. Block cipher
 C. Transposition cipher
 D. One-time pad

36. If Renee receives a digitally signed message from Mike, what key does she use to verify that the message truly came from Mike?
 A. Renee's public key
 B. Renee's private key
 C. Mike's public key
 D. Mike's private key

37. Which of the following statements is true?
   A. The less complex a system, the more vulnerabilities it has.
   B. The more complex a system, the less assurance it provides.
   C. The less complex a system, the less trust it provides.
   D. The more complex a system, the less attack surface it generates.

38. Audit trails, logs, CCTV, intrusion detection systems, antivirus software, penetration testing, password crackers, performance monitoring, and cyclic redundancy checks (CRCs) are examples of what?
   A. Directive controls
   B. Detective controls
   C. Corrective controls
   D. Preventive controls

39. Which of the following is a procedure designed to test and perhaps bypass a system's security controls?
   A. Logging usage data
   B. War dialing
   C. Penetration testing
   D. Deploying secured desktop workstations

40. Auditing is a required factor to sustain and enforce what?
   A. Accountability
   B. Confidentiality
   C. Accessibility
   D. Redundancy

41. Spamming attacks occur when numerous unsolicited messages are sent to a victim. Because enough data is sent to the victim to prevent legitimate activity, it is also known as what?
   A. Sniffing
   B. Denial of service
   C. Brute-force attack
   D. Buffer overflow attack

42. John recently received an email message from Bill. What cryptographic goal would need to be met to convince John that Bill was actually the sender of the message?
   A. Nonrepudiation
   B. Confidentiality
   C. Availability
   D. Integrity

國立清華大學112學年度碩士班考試入學試題

系所班組別：資訊安全研究所碩士班

考試科目（代碼）：資訊安全 (2501)

43. How many keys are required to fully implement a symmetric algorithm with 10 participants?
    A. 10
    B. 20
    C. 45
    D. 100

44. How many encryption keys are required to fully implement an asymmetric algorithm with 10 participants?
    A. 10
    B. 20
    C. 45
    D. 100

45. What kind of attack makes the Caesar cipher virtually unusable?
    A. Meet-in-the-middle attack
    B. Escrow attack
    C. Frequency analysis attack
    D. Transposition attack

46. What TCP/IP communications port is used by Transport Layer Security traffic?
    A. 80
    B. 220
    C. 443
    D. 559

47. What type of cryptographic attack rendered Double DES (2DES) no more effective than standard DES encryption?
    A. Birthday attack
    B. Chosen ciphertext attack
    C. Meet-in-the-middle attack
    D. Man-in-the-middle attack

Part II (6%) Please answer the following question.

48. What is Kerckhoffs's principle?