

**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 109 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

—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. 作答中如有發現試題印刷不清，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 109 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）

共_6_頁，第_1_頁 *請在【答案卷、卡】作答

Part I (75%) Please select one correct answer according to the question (3 points/each).

1. What is the primary different between a proxy and a firewall?
 - (a) A proxy allows access, while a firewall denies access.
 - (b) A firewall uses a hardened operating system, while a proxy does not.
 - (c) A proxy makes application-level requests on behalf of internal users, while a firewall typically just passes through authorized traffic.
 - (d) A firewall is capable of successfully performing Network Address Transaction for internal clients, while a proxy is forced to reveal internal addressing schemes.

2. Why is it important for a web application firewall to perform SSL inspection?
 - (a) A lack of SSL inspection would allow a channel of threats past the firewall.
 - (b) SSL is only used when you know you are under attack.
 - (c) Inspecting the SSL traffic assists with load balancing.
 - (d) None of the above.

3. Why is delay-based filtering effective against spam?
 - (a) Spam generators will not send spam if they cannot do it immediately.
 - (b) Spam generators do not wait for the SMTP banner.
 - (c) Spam generators are poorly behaved and will quickly move on to the next server.
 - (d) Spam generators has a very short TTL value.

4. 802.1x defines the encapsulation of EAP. What is EAP?
 - (a) Extensible Autonomous Protocol
 - (b) Extensible Authentication Protocol
 - (c) Extended Authentication Protocol
 - (d) Encapsulation Authentication Protocol

5. In ACLs, an implicit deny will apply to network traffic that:
 - (a) Matches two or more rules in the ACL.
 - (b) Does not match any entry in the ACL.
 - (c) Originates from inside the DMZ.
 - (d) Comes from a spoofed source address.

國立清華大學 109 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)

共 6 頁，第 2 頁 *請在【答案卷、卡】作答

6. What is a threat to VPN over open wireless?
 - (a) Hackers can sniff all the VPN packets and decrypt them.
 - (b) The user must connect to the open wireless before starting VPN, allowing an attacker a potential window of time to compromise the machine.
 - (c) A certificate could be faked, allowing access into the corporate server.
 - (d) All of the above.

7. Which of the following is not a commonly used file-hashing algorithm?
 - (a) SHA-224
 - (b) SHA-256
 - (c) SHA-512
 - (d) TLS

8. Which of the following techniques is most likely to be employed by a credit card company looking for fraudulent transactions?
 - (a) Big data analysis
 - (b) Network forensics
 - (c) Script mining
 - (d) Drive imaging

9. What is a zero-day exploit?
 - (a) A piece of malicious code that attaches itself to another piece of code in order to replicate.
 - (b) An attack that exploits a previously unknown vulnerability.
 - (c) A piece of software that appears to avoid one service but that also hides another purpose.
 - (d) Malware specifically designed to modify the operation of the operating system.

10. Which of the following correctly defines phishing?
 - (a) The use of social engineering to trick a user into responding to an e-mail to initiate a malware-based attack.
 - (b) The use of social engineering to talk someone into revealing credentials.
 - (c) The hacking of computer systems and networks associated with the phone company.
 - (d) Looking over the shoulder or using a camera to view a user entering sensitive data.

國立清華大學 109 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)

共 6 頁，第 3 頁 *請在【答案卷、卡】作答

11. Which of the following best defines social engineering?
 - (a) An attempt by an attacker to discover unprotected wireless networks.
 - (b) The targeting of high-value individuals.
 - (c) The art of deceiving another person to reveal confidential information.
 - (d) An attempt by an attack to gain unauthorized access through the telephone system.

12. What is the primary benefit of steganography over encryption?
 - (a) Can hold more data securely
 - (b) Harder to brute force the key
 - (c) Difficulty in detecting it
 - (d) Ease of Implementation

13. A message digest provides integrity by:
 - (a) Providing encryption that cannot be unlocked
 - (b) Providing a value that can be independently verified to show if the message changed.
 - (c) Providing message confidentiality so other users cannot see the message
 - (d) Applying a signature to the message

14. Which is an example of fault tolerance in a computer system?
 - (a) Dual power supplies
 - (b) RAID 5 configured disks.
 - (c) Multiple network interface controllers
 - (d) All of the above

15. If an attack is able to insert himself into an encrypted conversation between you and a secure web server, he has successfully executed what type of attack?
 - (a) A Smurf attack
 - (b) Replay attack
 - (c) Clickjacking attack
 - (d) Man-in-the-middle attack

國立清華大學 109 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)

共 6 頁，第 4 頁 *請在【答案卷、卡】作答

16. Your entire office is passing around a PowerPoint presentation of dancing and singing hamsters. Everyone thinks it's great until the next morning when everyone's hard drives appear to have been erased. The dancing hamster file is an example of a:
- (a) Virus
 - (b) Trojan
 - (c) Rootkit
 - (d) Exploit
17. How is near field communication like Ethernet?
- (a) It does not enforce security itself, but relies on higher-level protocols such as SSL.
 - (b) It forces each endpoint to communicate through a switch.
 - (c) It provides collision avoidance.
 - (d) All of the above.
18. Why is free Wi-Fi, such as in coffee shops, a popular target for session hijacking?
- (a) The unsecured Wi-Fi allows an attacker to place malicious files on the user's machine.
 - (b) The site uses a captive portal.
 - (c) Unsecured Wi-Fi allows the attacker to sniff the wireless session for a user's session cookie.
 - (d) The user does not engage VPN over wireless.
19. What makes rouge access points a threat?
- (a) They are loaded with malware.
 - (b) They potentially allow any person access to the corporate network.
 - (c) They only support WEP, which is easily broken.
 - (d) Wireless signals are short range, so extra access points are not a threat.
20. Your boss is trying to find more information about port-based network access controls. Which of the following IEEE standards should she be looking at?
- (a) 802.1x
 - (b) 802.11x
 - (c) 802.x
 - (d) 801.2x

國立清華大學 109 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)

共 6 頁，第 5 頁 *請在【答案卷、卡】作答

21. A buffer overflow attack was launched against one of your Windows-based web servers. You'd like to know what process was affected on the server itself. Where might you look for clues as to what process was affected?
- (a) Access log
 - (b) Application log
 - (c) Security log
 - (d) Setup log
22. Which of the following correctly describes the relationship between SSL and TLS?
- (a) TLS is the open-community version of SSL.
 - (b) SSL can be modified by developers to expand the protocol's capabilities.
 - (c) TLS is a proprietary protocol, while SSL is an open-community protocol.
 - (d) SSL is more extensible and backward compatible with TLS.
23. Which of the following correctly describes a drawback of symmetric key system?
- (a) Computationally less intensive than asymmetric systems.
 - (b) Work much more slowly than asymmetric systems.
 - (c) Carry out mathematically intensive tasks.
 - (d) Key must be delivered via secure courier.
24. Which of the following occurs in a PKI environment?
- (a) The RA creates the certificate, and the CA signs it.
 - (b) The CA signs the certificate.
 - (c) The RA sign the certificate.
 - (d) The user signs the certificate.
25. Which of the following best describes how a digit signature is created?
- (a) The sender encrypts a message digest with his private key.
 - (b) The sender encrypts a message digest with his public key.
 - (c) The receiver encrypts a message digest with his private key.
 - (d) The receiver encrypts a message digest with his public key.

國立清華大學 109 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)

共__6__頁，第__6__頁 *請在【答案卷、卡】作答

Part II (25%) Please answer the following questions.

26. (5%) What is Double DES?

27. (10%) What is the most effective method to break Double DES? How about the cost (efforts) for this method?

28. (10%) What is one-time pad? Please explain how it works clearly and list its requirements for key.