

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 114 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：2601

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 114 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（2601）

共__10__頁，第__1__頁 *請在【答案卡】作答

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

1. Which protocol offers guaranteed delivery and is connection oriented?

- (A) UDP
- (B) IP
- (C) TCP
- (D) TFTP

2. What protocol is used for reporting or informational purposes?

- (A) IGMP
- (B) TCP
- (C) ICMP
- (D) IP

3. What port, other than port 110, is used to retrieve e-mail?

- (A) Port 25
- (B) Port 143
- (C) Port 80
- (D) Port 135

4. What port does DNS use?

- (A) Port 80
- (B) Port 69
- (C) Port 25
- (D) Port 53

5. What command is used to log on to a remote server, computer, or router?

- (A) ping
- (B) traceroute
- (C) telnet
- (D) netstat

國立清華大學 114 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（2601）

共__10__頁，第__2__頁

*請在【答案卡】作答

6. Which of the following exploits might hide its destructive payload in a legitimate application or game?
- (A) Trojan program
 - (B) Macro virus
 - (C) Worm
 - (D) Buffer overflow
7. Which of the following doesn't attach itself to a host but can replicate itself?
- (A) Worm
 - (B) Virus
 - (C) Trojan program
 - (D) Buffer overflow
8. A software or hardware component that records each keystroke a user enters is called which of the following?
- (A) Key sniffer
 - (B) Keylogger
 - (C) Trojan program
 - (D) Buffer overflow
9. What type of network attack relies on multiple servers participating in an attack on one host system?
- (A) Trojan attack
 - (B) Buffer overflow
 - (C) Denial-of-service attack
 - (D) Distributed denial-of-service attack
10. Which of the following enables you to view all host computers on a network?
- (A) SOA
 - (B) ipconfig
 - (C) Zone transfers
 - (D) HTTP HEAD method

國立清華大學 114 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（2601）

共__10__頁，第__3__頁

*請在【答案卡】作答

11. Many social engineers begin gathering the information they need by using which of the following?

- (A) The Internet
- (B) The telephone
- (C) A company Intranet
- (D) E-mail

12. Discovering a user's password by observing the keys he or she presses is called which of the following?

- (A) Password hashing
- (B) Password crunching
- (C) Piggybacking
- (D) Shoulder surfing

13. Entering a company's restricted area by following closely behind an authorized person is referred to as which of the following?

- (A) Shoulder surfing
- (B) Piggybacking
- (C) False entering
- (D) Social engineering

14. Before conducting a security test by using social-engineering tactics, what should you do?

- (A) Set up an appointment.
- (B) Document all findings.
- (C) Get written permission from the person who hired you to conduct the security test.
- (D) Get written permission from the department head.

15. Security testers and hackers use which of the following to determine the services running on a host and the vulnerabilities associated with these services?

- (A) Zone transfers
- (B) Zone scanning
- (C) Encryption algorithms
- (D) Port scanning

國立清華大學 114 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（2601）

共__10__頁，第__4__頁

*請在【答案卡】作答

16. To find extensive Nmap information and examples of the correct syntax to use in Linux, which of the following commands should you type?

- (A) Nmap -h
- (B). nmap -help
- (C) nmap?
- (D) man nmap

17. To see a brief summary of Nmap commands in a Linux shell, which of the following should you do?

- (A) Type nmap -h.
- (B) Type nmap -summary.
- (C) Type help nmap.
- (D) Press the F1 key.

18. Which of the following is a program for extracting Windows password hash tables?

- (A) Nmap
- (B) Fgdump
- (C) John the Ripper
- (D) Lophecrack

19. Advanced Encryption Standard (AES) replaced DES with which algorithm?

- (A) Rijndael
- (B) Blowfish
- (C) DEA
- (D) Twofish

20. Asymmetric cryptography systems are which of the following?

- (A) Faster than symmetric cryptography systems
- (B) Slower than symmetric cryptography systems
- (C) The same speed as symmetric cryptography systems
- (D) Practical only on systems with multiple processors

國立清華大學 114 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（2601）

共__10__頁，第__5__頁

*請在【答案卡】作答

21. Hiding data in a photograph is an example of which of the following?

- (A) Steganography
- (B) Stenography
- (C) Ciphertext
- (D) Cryptology

22. Which of the following is an asymmetric algorithm?

- (A) DES
- (B) AES
- (C) RSA
- (D) Blowfish

23. Intruders can perform which kind of attack if they have possession of a company's password hash file?

- (A) Dictionary
- (B) Scan
- (C) Ciphertext
- (D) Buffer overflow

24. Intercepting messages destined for another computer and sending back messages while pretending to be the other computer is an example of what type of attack?

- (A) Man-in-the-middle
- (B) Smurf
- (C) Buffer overflow
- (D) Mathematical

25. Why did the NSA decide to drop support for DES?

- (A) The cost was too high.
- (B) The encryption algorithm was too slow.
- (C) The processing power of computers had increased.
- (D) It was too difficult for government agencies to use.

國立清華大學 114 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（2601）

共__10__頁，第__6__頁

*請在【答案卡】作答

26. Which of the following describes a chosen-plaintext attack?

- (A) The attacker has ciphertext and algorithm.
- (B) The attacker has plaintext and algorithm.
- (C) The attacker has plaintext, can choose what part of the text gets encrypted, and has access to the ciphertext.
- (D) The attacker has plaintext, ciphertext, and the password file.

27. Two different messages producing the same hash value results in which of the following?

- (A) Duplicate key
- (B) Corrupt key
- (C) Collision
- (D) Message digest

28. Digital signatures are used to do which of the following?

- (A) Verify that a message was received
- (B) Ensure that repudiation is provided
- (C) Provide authentication and nonrepudiation
- (D) Encrypt sensitive messages

29. What is the standard for PKI certificates?

- (A) X.500
- (B) X.400
- (C) X.509
- (D) MySQL.409

30. OpenPGP is focused on protecting which of the following?

- (A) Web content
- (B) E-mail messages
- (C) Database systems
- (D) IPSec traffic

國立清華大學 114 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（2601）

共__10__頁，第__7__頁

*請在【答案卡】作答

31. Wi-Fi Protected Access (WPA) was introduced in which IEEE 802 standard?
- (A) 802.11a
 - (B) 802.11b
 - (C) 802.11i
 - (D) 802.11
32. What is a known weakness of wireless network SSIDs?
- (A) They're broadcast in cleartext.
 - (B) They're difficult to configure.
 - (C) They use large amounts of bandwidth.
 - (D) They consume an excessive amount of computer memory.
33. An access point provides which of the following?
- (A) Access to the BSS
 - (B) Access to the DS
 - (C) Access to a remote station
 - (D) Access to a secure node
34. Which EAP method requires installing digital certificates on both the server and client?
- (A) EAP-TLS
 - (B) PEAP
 - (C) EAP-SSL
 - (D) EAP-CA
35. Which wireless encryption standard offers the best security?
- (A) WPA2
 - (B) WEP
 - (C) WPS
 - (D) WPA

國立清華大學 114 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（2601）

共__10__頁，第__8__頁

*請在【答案卡】作答

36. What protocol was added to 802.11i to address WEP's encryption vulnerability?

- (A) MIC
- (B) TKIP
- (C) TTL
- (D) EAP-TLS

37. What IEEE standard defines wireless technology?

- (A) 802.3
- (B) 802.5
- (C) 802.11
- (D) All 802 standards

38. What TKIP enhancement addressed the WEP vulnerability of forging packets?

- (A) Extended Initialization Vector (IV) with sequencing rules
- (B) Per-packet key mixing
- (C) Rekeying mechanism
- (D) Message Integrity Check (MIC)

39. Which IEEE standard defines authentication and authorization in wireless networks?

- (A) 802.11
- (B) 802.11a
- (C) 802.11b
- (D) 802.1X

40. Entering the value OR 1=1 in a Web application that has an "Enter Your PIN" field is most likely an example of which attack?

- (A) SQL injection
- (B) Code injection
- (C) Buffer overflow
- (D) Ethernet flaw

國立清華大學 114 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（2601）

共__10__頁，第__9__頁

*請在【答案卡】作答

41. The AccessFileName directive in Apache, along with a configuration file (such as .htaccess), can be used to perform which of the following on a Web site?
- (A) Run malicious code in the browser.
 - (B) Protect against XSS worms.
 - (C) Scan for CGI vulnerabilities.
 - (D) Restrict directory access to those with authorized user credentials.
42. Which of the following is an open-source technology for creating dynamic HTML Web pages?
- (A) ASP
 - (B) PHP
 - (C) Java
 - (D) Oracle
43. What tags identify ColdFusion as the scripting language?
- (A) <# #>
 - (B) <% %>
 - (C) The letters CF
 - (D) <! /!>
44. Which of the following HTML tags is used to create a hyperlink to a remote Web site?
- (A)
 - (B)
 - (C)
 - (D) <A HREF/>
45. Which of the following tags enables an HTML programmer to create a loop?
- (A) <LOOP>
 - (B) <NEST>
 - (C) <WHILE>
 - (D) HTML doesn't have a looping function or tag.

國立清華大學 114 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（2601）

共__10__頁，第__10__頁

*請在【答案卡】作答

46. Which of the following C statements has the highest risk of creating an infinite loop?

- (A) while (a > 10)
- (B) while (a < 10)
- (C) for (a = 1; a < 100; ++a)
- (D) for (; ;)

47. Which organization offers free benchmark tools for Windows and Linux?

- (A) PacketStorm Security
- (B) CVE
- (C) Center for Internet Security
- (D) Trusted Security Solutions

48. Which of the following is an OS security mechanism that enforces access rules based on privileges for interactions between processes, files, and users?

- (A) MBSA
- (B) Mandatory Access Control
- (C) Server Message Block
- (D) Systems Management Server

49. Which of the following is a major challenge of securing embedded OSs?

- (A) Training users
- (B) Configuration
- (C) Patching
- (D) Backup and recovery

50. SCADA systems are used for which of the following?

- (A) Monitoring embedded OSs
- (B) Monitoring ATM access codes
- (C) Monitoring equipment in large-scale industries
- (D) Protecting embedded OSs from remote attacks