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 110 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. 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 110 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)

Part I (90%) Please select one correct answer according to the question (3 points/each).

1. Which protocol can create a security vulnerability in switches, firewalls, and routers because it authenticates using a cleartext password?
   (A) SNMP
   (B) SSH
   (C) SMTP
   (D) NAT

2. Your company has a policy to not allow any connection from overseas addresses to its network. Which security mechanism is best to employ to accomplish this goal?
   (A) VLAN management
   (B) Access control lists
   (C) Implicit deny
   (D) Network separation

3. A company adopting an Infrastructure as a Service (IaaS) model would typically:
   (A) Own the infrastructure equipment
   (B) Be responsible for housing and maintaining equipment
   (C) Only support networking infrastructure
   (D) Pay on a per-use basis

4. What is the primary enhancement WPA2 has over WEP?
   (A) WPA2 uses longer keys than WEP.
   (B) AES and CCMP.
   (C) Temporary WEP keys using TKIP.
   (D) WPA2 supports the 802.1x protocol for secure client authentication.

5. What is the definition of privacy?
   (A) Business secrets protected through trade laws
   (B) The right to control information about you and what others can do with that information
   (C) Government information protected through laws concerning national security
   (D) Information used to identify a specific individual

6. Which of the following represents two simple rules a good SLA should satisfy?
   (A) Web standards and coding practices
   (B) Technology and processes
   (C) Services provided and level of performance
   (D) Duration and protection

7. Network separation is used primarily to:
   (A) Maximize performance
   (B) Limit the required number of SPAN ports
   (C) Separate networks for security reasons
   (D) Facilitate logging of suspicious traffic

8. During your investigation of a security breach, you discover the corporate fileserver is connected to a VLAN that is accessible to systems in the development environment. This violates which security principle?
   (A) VLAN management
   (B) Least privilege
   (C) Network separation
   (D) Loop protection

9. Which of the following servers would you be least likely to place in a DMZ?
   (A) Web server
   (B) DNS server
   (C) SMTP server
   (D) File Server

10. Which of the following is not a remote-access method?
    (A) Remote desktop software
    (B) Terminal emulation
    (C) SaaS
    (D) Secure Shell

11. An organization wanting to create a restricted-access, Internet-accessible resource for processing sensitive data might consider using?
(A) Software as a Service
(B) A private cloud
(C) A public cloud
(D) A community cloud

12. To achieve reliability and speed improvements through the use of RAID, which form would you use?
(A) RAID 0
(B) RAID 1
(C) RAID 10
(D) RAID 5

13. In which of the following areas is evidence most likely to be lost if a compromised system is shut down before evidence collection is complete?
(A) Raw disk blocks
(B) Memory contents
(C) File system information
(D) USB drivers

14. When examining your network logs, you notice a large amount of TCP traffic coming from an external IP address directed at the web server in your DMZ. The destination TCP ports seems to be different for each packet you examine. What type of traffic are you likely seeing in your logs?
(A) Smurf attack
(B) Port scan
(C) Ping sweep
(D) DNS transfer

15. You suspect a user's workstation is infected with malware and are about to begin an investigation. If you want to reduce the likelihood that this workstation will infect other systems on your network, but you still want to preserve as much evidence as possible, which of the following should you do?
(A) Shut down the workstation
(B) Remove the power cord from the workstation
(C) Remove the network cable from the workstation
(D) Remove all USB devices and peripherals

16. What type of network attack uses repetition or delay of valid data transmissions?
(A) Bonet
(B) Cross-site scripting
(C) Token hijacking
(D) Replay attack

17. You've noticed some strange behavior today on your organization's system. This morning things were working fine, but now when you enter the URL for your company's main web page, you get a web page written in a foreign language. Which of the following attacks is occurring at your organization?
(A) Man-in-the-middle
(B) Watering hole attack
(C) DNS poisoning
(D) Spam

18. What change should you make to prevent session hijacking?
(A) Encrypt cookie files.
(B) Sanitize all the input fields.
(C) Outsource your site to the cloud.
(D) Apply SSL to the entire site, instead of just the login page.

19. Your site survey has discovered hidden in the ceiling a rough access point resembling one of the fire detectors. What type of device is this likely to be?
(A) An AP bought at the office supply store to boost the Wi-Fi signal near the sales department cubes
(B) Part of the normal corporate wireless LAN that is simply designed to blend in with the office
(C) A custom wireless evil twin that is attempting to gather user information
(D) A bluesnarfer

20. Your boss wants a network device that will detect malicious network traffic as it happens and stop it from reaching systems inside your network. She has asked you to come up with several different options and present them to her in the morning. You should researching which of the following?
(A) Intrusion detection systems
(B) Intrusion prevention systems
(C) Firewalls
(D) Continuous auditing systems

21. Which of the following is not a step you'd perform when hardening a production system?
(A) Disable unnecessary services
(B) Disable unnecessary accounts
(C) Enable simple TCP services
(D) Configure auditing

22. You want to hire someone to test an application your company just developed. The app handles sensitive data, so you want to limit the amount of information you release about the application to people outside your company. Which of the following testing types are you looking for?
(A) White-box testing
(B) Gray-box testing
(C) Closed-box testing
(D) Black-box testing

23. Your organization wants someone to examine your intranet portal to assess the threat from a malicious insider. What kind of testing is the most appropriate for this situation?
(A) Credentialed testing
(B) Code review
(C) Active testing
(D) Risk assessment

24. Which of the following is one of the most common web attack methodologies?
(A) Cross-site scripting
(B) Cross-site request forgery
(C) Buffer overflows
(D) RPC errors

25. Error and excepting handling should be performed in what fashion?
(A) All errors/exceptions should be trapped and handled in the main program.
(B) All errors/exceptions should be trapped and handled in the generating routine.
(C) Errors and exceptions should only be handled if they exceed a given severity.
(D) Errors and exceptions should be logged; handling is optional.

26. What would you use to create an HMAC?
(A) TLS
(B) SHA-256
(C) AES
(D) RSA

27. When a PKI system is used in conjunction with file and folder encryption, what is a potential risk?
(A) A lost or damaged key can lock data away permanently.
(B) Encryption prevents backups from being run.
(C) Once the root key of the PKI is compromised, all the encrypted data can be read.
(D) Encryption never has risks.

28. The CIO asks you to ensure that all e-mails have strict non-repudiation. How can a PKI system solve this issue?
(A) Managing symmetric keys for e-mail encryption
(B) Forcing all users to use two-factor authentication when accessing the e-mail server
(C) Using PKI to support TLS on the SMTP delivery
(D) Issuing a digit certificate to all users for signing e-mails

29. Why is it important to disable geo-tagging on your mobile device?
(A) Geo-tagging makes it so your friends can confirm you took the photos.
(B) Geo-tagging can inadvertently expose the location where photos were taken.
(C) Geo-tagging is a great hobby.
(D) Geo-tagging can enable correlation of photos and locations.

30. Your boss wants you to order her a new laptop, one with a special chip that will allow her to store encryption keys using BilLocker to protect her drive. What special chip is your boss talking about?
(A) Trusted Platform Module
(B) PKI Module
(C) BitLocker Encryption Module
(D) FIPS 140 Chip

國立清華大學 110 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)

Part II (10%) Please answer the following question.

31. 對公開金鑰加密器 RSA 而言，選擇一個隨機的大質數一直是基本的問題，在過去是先選擇一個隨機大整數，然後使用 Miller-Rabin primality testing 演算法去測試此整數是否為質數。在 2002 年 Agrawal, Kayal, and Saxena 提出了另一個演算法(簡稱 AKS 演算法) for primality testing。請問若有兩個隨機大整數各自通過這兩個質數測試演算法，在意義上有何不同(請說明理由)? (5 分)。另請寫出 Miller-Rabin primality testing 演算法 (Pseudocode)。(5 分)