



ITE 資訊專業人員鑑定

資訊安全類-資訊與網路安全管理概論試題

試卷編號：ISN103

學科 100% (為單複選題，每題 2.5 分，共 100 分)

1. 下列何種傳輸媒介發生串音干擾 (crosstalk) 的可能性最低？
- (A) Shielded twisted pair
 - (B) Unshielded twisted pair
 - (C) Coaxial
 - (D) Fiber optic

Ans : D

2. 下列哪些程式語言具有產生物件 (object) 的能力？(複選)
- (A) Java
 - (B) C
 - (C) Objective-C
 - (D) SQL

Ans : AC

3. 假設 h 為一個單向雜湊函數 (one-way hash function)，如 h 滿足最佳的抗碰撞性質，意指下列哪兩種情況應該成立？(請參閱附圖作答)
(複選)
- (A) 對於已知訊息 x 而言，無法找出一個訊息 y ，使得 $h(y) = x$
 - (B) 對於已知訊息 x 而言，無法找出一個訊息 y ，使得 $h(x) = y$
 - (C) 對於已知訊息 x 而言，無法找出另一訊息 $y(y \neq x)$ ，使得 $h(x) = h(y)$
 - (D) 無法找出一組訊息 y_1 與 y_2 ，使得 $h(y_1) = h(y_2)$

Ans : CD



4. 連線到某網站首頁時，瀏覽器端最不可能發出的網路封包類型為何？
- (A) TCP
 - (B) HTTP
 - (C) DNS
 - (D) SMTP

Ans : D

5. 由 ISO/IEC 17799 改變而來，內容包含資訊安全最佳實務做法的是？
- (A) ISO/IEC 27000
 - (B) ISO/IEC 27001
 - (C) ISO/IEC 27002
 - (D) ISO/IEC 27004

Ans : C

6. Microsoft Access 屬於下列何種類型的資料庫管理系統？
- (A) 關聯式 (relational)
 - (B) 物件導向式 (object-oriented)
 - (C) 階層式 (hierarchical)
 - (D) 網路式 (network)

Ans : A

7. 依據 ISO/IEC 27005，高層次風險評鑑 (high-level risk assessment) 的優點，不包括下列哪一項？
- (A) 增加風險評鑑計畫的接受度
 - (B) 輔助策略性的資訊安全規劃
 - (C) 優化組織資源的運用
 - (D) 針對所有的資產進行更精細的風險評估

Ans : D

8. 依據「個人資料保護法」，非公務機關如未訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法，且經中央目的事業主管機關要求限期改正，但屆期仍未改正者，最高可處罰鍰金額為多少？

(A) 5 萬元
(B) 10 萬元
(C) 15 萬元
(D) 20 萬元

Ans : D

9. 關於 SYN 洪水攻擊 (flood attack)，下列描述何者正確？

(A) 此攻擊針對 UDP 協定
(B) 直接損害是導致被攻擊主機的檔案外洩
(C) 屬於服務阻斷 (denial of service) 攻擊的一種
(D) 攻擊者必須持續發出 SYN/ACK 封包

Ans : C

10. 假設 SQL 指令注入 (SQL injection) 攻擊某主機甲成功，則在攻擊發生時，哪個情況最不可能發生？

(A) 甲的主記憶體同時發生緩衝區溢位 (buffer overflow)
(B) 甲正執行一個未檢查輸入資料的網頁程式
(C) 甲正執行一個透過 SQL 存取資料庫的程式
(D) 甲正在執行網站伺服器軟體

Ans : A

11. 依據日常活動理論 (routine activities theory)，網路侵權行為的發生與下列哪三個因素較為相關？(複選)

(A) 科技的發展過快
(B) 侵權意圖的存在
(C) 缺乏有效的保護或防範機制
(D) 軟體或數位資料容易複製

Ans : BCD



12. 處理程序位址空間 (process address space) 的哪個區域，是因應 C 語言 malloc() 函數或 Java 語言的 new 運算子呼叫時的動態空間配置而設計？

(A) 程式本文 (text)
(B) 堆 (heap)
(C) 堆疊 (stack)
(D) 分段表 (segmentation table)

Ans : B

13. 關於 RSA 演算法，下列哪些描述不正確？(複選)

(A) 其安全性植基於離散對數 (discrete logarithm) 難題
(B) 可支援 SSL 進行金鑰交換
(C) 屬於對稱式密碼方法的一種
(D) 演算過程用到的模數 (modulus) N 必須是質數

Ans : ACD

14. 下列何者可以透過網路回送 html 檔案內容，供前端使用者瀏覽網頁？

(A) Microsoft Office
(B) Microsoft Publisher
(C) Microsoft Visio
(D) Microsoft Internet Information Services

Ans : D

15. 李四破解王五電腦的密碼之後，成功登入該電腦系統。依據刑法妨害電腦使用罪，下列描述哪些正確？(複選)

(A) 李四最高可處五年有期徒刑或拘役
(B) 王五須提出告訴，法院才會受理本案
(C) 本案非告訴乃論
(D) 本案可科或併科十萬元以下罰金

Ans : BD



16. 下列何種存取控制模型最適合達成責任分工 (separation of duties) ?
- (A) 強制存取控制 (mandatory access control, MAC)
 - (B) 隨意存取控制 (discretionary access control, DAC)
 - (C) 角色基礎存取控制 (role-based access control, RBAC)
 - (D) 存取控制串列 (access control list, ACL)

Ans : C

17. Google App Engine 讓開發者將程式放到 Google 所提供的雲端環境，其所提供的雲端服務類型為何？
- (A) Software-as-a-service
 - (B) Platform-as-a-service
 - (C) Infrastructure-as-a-service
 - (D) Big Data Service

Ans : B

18. 根據刑法妨害電腦使用罪的規定，哪個行為非屬告訴乃論？
- (A) 入侵同事的 gmail 帳戶
 - (B) 發送大量封包攻擊私立大學主機
 - (C) 私人企業員工藉職務之便刪除企業營運關鍵資料
 - (D) 製作病毒程式供他人犯了妨害電腦使用罪，並且損害公共利益

Ans : D

19. 涉及通電中之電氣設備，如電器、變壓器、電線、配電盤等引起之火災，屬於哪一類？
- (A) A 類
 - (B) B 類
 - (C) C 類
 - (D) D 類

Ans : C



20. 關於資料倉儲 (data warehouse) 的敘述，下列哪些正確？(複選)
- (A) 支援資料探勘 (data mining) 的應用
 - (B) 包含特定主題的資料市集 (data mart)
 - (C) 作為即時線上交易處理 (on-line transaction processing) 的資料庫
 - (D) 可支援線上分析處理 (on-line analytical processing)
- Ans : ABD
21. 下列哪些與資訊倫理為較相關的議題？(複選)
- (A) 探討如何維護個人對於資訊使用的適當權利
 - (B) 探討提供錯誤資訊的行為所應負起的責任
 - (C) 探討資訊免費使用與付費使用的條件
 - (D) 探討資訊科技應該如何增加速度
- Ans : ABC
22. 關於系統開發過程中的可行性研究 (feasibility study)，下列敘述何者錯誤？
- (A) 大多於開發晚期執行，確定系統執行是否正確可行
 - (B) 研究範圍包括成本 / 效益分析
 - (C) 目標是提出最值得採用的解決方案
 - (D) 應評估系統是否可能產生侵犯智財權等法律問題
- Ans : A
23. 關於傳輸層安全 (Transport Layer Security, TLS)，下列描述哪些錯誤？(複選)
- (A) 前身為 SSL (Secure Sockets Layer)
 - (B) 應用公開金鑰密碼學 (public key cryptography) 驗證伺服器身分
 - (C) 可視為網路層的安全協定
 - (D) 其 1.2 版本可能遭受一種 chosen plaintext attack，稱為 BEAST (browser exploit against SSL/TLS) 攻擊

Ans : CD



24. 以下哪個案例最可能破壞資料的完整性 (integrity) ?

- (A) 竊取他人電腦內的機密資料
- (B) 卸除他人電腦中的服務程式
- (C) 未經授權修改他人資料庫
- (D) 竊取他人電腦內的紀錄檔

Ans : C

25. 依據刑法妨害電腦使用罪，如無故取得、刪除或變更私人企業電腦內電磁紀錄，並導致該企業的損害，最高可處幾年有期徒刑？

- (A) 兩年
- (B) 三年
- (C) 五年
- (D) 七年

Ans : C

26. 下列哪個不是 TCP/IP 連線劫持 (session hijacking) 攻擊成功的必要前提？

- (A) 與受害主機位於同一網段
- (B) 取得要劫持連線的 TCP 序號 (sequence number)
- (C) 偽裝成受害主機，發送特定 TCP 序號的封包
- (D) 入侵受害主機並奪取執行權限

Ans : D

27. 關於「個人資料保護法」，哪些敘述是正確的？(複選)

- (A) 主要保護標的為人格權
- (B) 婚姻與家庭應視為自然人的個人資料
- (C) 健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用，符合合理使用原則者不在此限
- (D) 中央目的事業主管機關認為有可能違反規定之虞時，得派員攜帶執行職務證明文件，進入處理個資的非公務機關進行檢查

Ans : ABD



28. 為了管理伺服器服務中斷的風險，建置負載平衡器屬於下列何種管理策略？

- (A) 風險避免 (risk avoidance)
- (B) 風險抑減 (risk reduction)
- (C) 風險消除 (risk elimination)
- (D) 風險接受 (risk acceptance)

Ans : B

29. 下列哪兩個方法能夠有效因應終端使用者對於新科技的抗拒？(複選)

- (A) 自行開發系統
- (B) 適當的教育訓練
- (C) 邀請使用者參與系統開發過程
- (D) 採用開放原始碼 (open source) 程式

Ans : BC

30. 中央處理器通常包含下列哪些組件？(複選)

- (A) 控制單元 (control unit)
- (B) 算術邏輯單元 (arithmetic logic unit)
- (C) 暫存器 (register)
- (D) 主記憶體 (main memory)

Ans : ABC

31. 在詳盡的風險分析過程中，哪個步驟發生的時間點最早？

- (A) 資產識別
- (B) 弱點識別
- (C) 營運衝擊分析
- (D) 風險評估

Ans : A

32. 下列何者平均效能落在 $O(n \log n)$ 等級的排序演算法？

- (A) 插入排序法 (insertion sort)
- (B) 合併排序法 (merge sort)
- (C) 氣泡排序法 (bubble sort)
- (D) 選擇排序法 (selection sort)

Ans : B



33. 下列哪個作業系統以 Linux 為基礎，廣為智慧型手機所採用？
- (A) Android
 - (B) Windows 7
 - (C) Symbian
 - (D) Windows Phone

Ans : A

34. 著作權法對於著作權的保護，僅包含下列何者？
- (A) 著作之表達
 - (B) 著作背後的思想
 - (C) 著作表達的基礎原理
 - (D) 著作表達的原始概念

Ans : A

35. 在 Windows 7 系統中，哪個工具可以檢視執行中的處理程序及可用記憶體動態容量？
- (A) 裝置管理員
 - (B) Windows 防火牆
 - (C) Windows 檔案總管
 - (D) 工作管理員

Ans : D

36. 下列哪些與緩衝區溢位 (buffer overflow) 攻擊成功直接相關？(複選)
- (A) 作業系統未檢查執行位址的合理性
 - (B) 程式沒有仔細檢查資料輸入
 - (C) 程式宣告過多區域變數
 - (D) 作業系統宣告過多區域變數

Ans : AB

37. 附圖中的 Java 程式片段執行之後， $i+j$ 的值=？（請參閱附圖作答）

```
int i = 0, j = 0;
    for(i = 0; i < 5; i++)
        for(j = 10; i < j; --j)
            i += 2;
```

- (A) 0
- (B) 14
- (C) 15
- (D) 16

Ans : C

38. 關於網際網路協定安全（Internet Protocol Security, IPsec）之敘述，下列何者正確？

- (A) 以每個 TCP 連線為加密單位
- (B) 以每個 IP 封包為加密單位
- (C) 以每個網頁作為加密單位
- (D) 依據伺服器的設定決定加密單位

Ans : B

39. 有鑑於安隆有限公司（Enron）等財務欺詐事件所暴露的公司和證券監管問題，美國制定了哪個法案？

- (A) Sarbanes-Oxley Act
- (B) Health Insurance Portability and Accountability Act
- (C) Federal Information Security Management Act
- (D) International Financial Reporting Standards

Ans : A

40. 憑證機構針對金鑰生成參數與參數品質的安全控管，依法應於何種文件中載明？

- (A) 風險評鑑報告（risk assessment report）
- (B) 資產清單（inventory of assets）
- (C) 憑證實務作業基準（certification practice statement）
- (D) 適用性聲明書（statement of applicability）

Ans : C