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：ISN106

學科 100 % （為單複選題，每題 2.5 分，共 100 分）

1. 中央處理器通常包含下列哪些組件？

（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

2. 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

3. 考慮任一節點可能失效的前提下，哪種網路拓樸的穩定性最高？

（A）匯流排（bus）
（B）輻射狀（star）
（C）網格狀（mesh）
（D）環狀（ring）

Ans：C

4. 關於資料倉儲（data warehouse）的敘述，下列哪些正確？

（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

5. 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

6. 關於網際網路協定安全（Internet Protocol Security, IPsec），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

7. 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

8. 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，屬於何類？

（A）A 類
（B）B 類
（C）C 類
（D）D 類

Ans：C

9. 為了管理伺服器服務中斷的風險，建置負載平衡器屬於何種管理策略？

（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

10. 以下何項技術是用來確保員工從外部連線回公司時確認連線安全的技術？

（A）VPN
（B）SSL
（C）虛擬主機
（D）防毒軟體

Ans：A

11. 在安全軟體開發生命週期（Secure SDLC）中，源碼檢測（Source Code Analysis）應在哪一個階段導入，可以節省整體成本？

（A）安全軟體需求
（B）安全軟體設計
（C）安全軟體開發
（D）安全軟體測試

Ans：C

12. 在系統開發過程中，資料庫的結構可進行正規化與反正規化的調整，正規化最主要的優點在於？

（A）提升資料加密效率
（B）避免浪費儲存空間
（C）避免資料有不一致的狀況
（D）保護資料免於未經授權的存取

Ans：C

13. 關於 ISO/IEC 27005 對風險識別的描述，下列何者不正確？

（A）第一階段是資產識別（asset identification）
（B）第二階段是威脅識別（threat identification）
（C）第三階段是現有控制措施識別（existing controls indentification）
（D）第四階段是潛在控制措施識別（potential controls indentification）

Ans：D

14. 在 IPv4 的協定下，是由 4 個 8 位元數字組成來表達一個 IP 位址，如 192.168.0.0，若看到 192.168.0.0/28.，子網路遮罩為何？

（A）255.255.255.240
（B）255.255.255.128
（C）255.255.255.255
（D）255.255.255.64

Ans：A

15. 使用單引號（'） 等特殊字元或關鍵字以達到查詢語句邏輯的攻擊手法為以下何種？

（A）隱藏欄位攻擊法
（B）混淆攻擊法（URL Obfuscation）
（C）搜尋引擎攻擊法
（D）資料隱碼攻擊法（SQL Injection）

Ans：D

16. 關於差異備份（Differential Backup）的說明，下列何者正確？

（A）把全部檔案進行備份，並把已備份的檔案標示為已備份
（B）只備份經修改的檔案，或新建立但沒有標示為已備份的檔案，並把備份後的檔案標示為已備份
（C）只備份經修改的檔案， 或新建立但沒有標示為已備份的檔案，但不會把已備份的檔案標示為已備
（D）差異備份的備份時間比增量備份快

Ans：C

17. 關於勒索軟體（Ransomware）的描述，下列哪些正確？

（A） 要避免感染勒索軟體，主要應注意不要存取來路不明的網站、郵件或檔案，但有的勒索軟體來自惡意廣告，實務上不易預防
（B） 勒索軟體主要會竊取電腦上的機敏資料，並寄發勒索信件給受害者索取贖金
（C） 勒索軟體的贖金支付方式多半透過彼特幣（Bitcoin）等虛擬貨幣
（D） 勒索軟體會利用 Tor 網路來隱匿攻擊者行蹤

Ans：ACD

18. 下列何選項不屬於 IPv4 裡面的私有 IP（Private IP）？

（A）A Class：10.0.0.0 - 10.255.255.255
（B）B Class：172.16.0.0 - 172.31.255.255
（C）C Class：192.168.0.0 - 192.168.255.255
（D）D Class：224.0.0.0 - 239.255.255.255

Ans：D

19. 使用瀏覽器上網過程中，下列何種不是可能的加密選項？

（A）HTTPS
（B）TLS
（C）SSL
（D）SMTP

Ans：D

20. 關於 RSA 演算法，哪些描述正確？

（A）是美國麻省理工學院一位天才教授 Rivest S. Adleman（RSA）所發明的
（B）RSA 加密演算法中，明文加密使用區塊為每次加密的範圍，使用對方公開金鑰（Public Key）將明文加密
（C）RSA 之安全性取決於質因數分解之困難度
（D）是非對稱式密碼系統的一種

Ans：BCD

21. 關於 ISO/IEC 27005 對風險管理的描述，下列何者不正確？

（A）第一階段應建立前後環節（establishing the context）
（B）第二階段應進行風險評鑑（risk assessment）
（C）第三階段應著手風險處理（risk treatment）
（D）第四階段應彙整可行方案（risk recommendations）

Ans：D

22. 下列何者與會議連線劫持（session hijacking）無關？

（A）登入 Cookie 必須是唯一的，每個用戶均不相同
（B）跨站腳本攻擊（Cross-site Scripting）可造成連線劫持
（C）連線劫持跟偽冒的回應封包及檔頭有關
（D）入侵受害主機並提權後竄改所有連線封包

Ans：D

23. 下列關於跨站腳本攻擊（Cross-site Scripting）的描述，哪些正確？

（A）惡意腳本可能來自於使用者端的網址列 URL
（B）惡意腳本可能來自於伺服器端的資料庫
（C）惡意腳本可能來自於使用者端瀏覽器的 DOM（Document Object Model）
（D）惡意腳本可能來自於檔案輸入，即使是純文字檔（.txt）

Ans：ABCD

24. 關於 VPN 虛擬私有網路（Virtual Private Network），下列哪些是客戶端設備 VPN 常見的協定之一？

（A）L2TP 協定
（B）PPTP 協定
（C）IPSec 協定
（D）MPLS 技術

Ans：ABC

25. 關於雜湊函數（hash function）的描述，下列何者有誤？

（A）又被稱為訊息指紋（message fingerprint）演算法
（B）SHA256 已被中國山東大學的王小雲教授等學者於 2004 年所破解
（C）任意長度的輸入訊息透過單向雜湊函數的計算後必定是一個固定長度的輸出
（D）可利用所謂的生日攻擊法評估單向雜湊函數的強碰撞抵抗性

Ans：B

26. 以下哪個案例最可能破壞資料的機密性（confidentiality）？

（A）複製他人電腦內的機密資料
（B）清空他人電腦中的資源回收桶
（C）修改他人電腦中的文件內容
（D）隱藏他人電腦中的重要檔案

Ans：A

27. 關於雜湊函數的攻擊方法描述，下列哪些正確？

（A）「彩虹表」是字典攻擊法的一種，它針對各種可能的字母組合，預先計算好其雜湊值
（B）雜湊函數應用很廣，主要用來保證文件的機密性（confidentiality）
（C）雜湊函數是一種「雙向函數（two-way function）」，意即攻擊方需取得金鑰才能從雜湊值反推出訊息原文
（D）雜湊值的長度固定，所以不同原文可能產生相同的雜湊值，這個現象叫做「碰撞（collision）」

Ans：AD

28. 根據 ISO/IEC 27005 對於風險（Risk）的定義，風險與下列何者無關？

（A）威脅（Threat）
（B）脆弱性（Vulnerability）
（C）後果（Consequence）
（D）根因（Root Cause）

Ans：D

29. 計算機中心的助理甲蒐集同學們的電話號碼，目的是「如實習時間有變更須要，會打電話給同學們變更時間」，甲將所蒐集的同學們的電話號碼 Key 成 Excel，根據個人資料保護法，請問此動作是屬於下列何步驟？

（A）告知
（B）蒐集
（C）處理
（D）利用

Ans：C

30. 網路上透過問卷來蒐集個人資料，且未經同意轉賣給他人圖利，請問這會觸犯下列何種法令？

（A）通訊保障及監察法電子簽章法
（B）個人資料保護法
（C）電子簽章法
（D）刑法妨礙電腦使用專章

Ans：B

31. 在安全軟體開發生命週期（Secure SDLC）中，滲透測試（Penetration Testing）應在哪一個階段進行？

（A）安全軟體部署與維運
（B）安全軟體設計
（C）安全軟體開發
（D）安全軟體測試

Ans：D

32. 關於 OWASP Top 10 常見弱點風險之描述，下列何者有誤？

（A）OWASP Top 10 以檢視 Web 應用程式風險為主
（B）OWASP Top 10 每 3~5 年會更新一次排序
（C）OWASP 所列舉的風險並定能對應到 CVE （Common Vulnerabilities and Exposures）弱點編號
（D）Injection 類別的風險係威脅伺服器端，XSS （Cross-site Scripting）類別的風險係威脅使用者端

Ans：C

33. 根據著作權法，對於網路上的文章或照片之描述，下列哪些正確？

（A）網際網路上經常出現的文章或照片，除了極少數的例外，絕大多數都是受到著作權法保護的
（B）未具名或以別名表示著作人的著作，仍受著作權法保障
（C）公開傳輸行為的「合理使用」情形非常有限，我們如果未經授權，就擅自將他人的文章或照片，隨意轉寄或轉貼給家人或朋友以外的眾人欣賞，將有可能侵害作者的公開傳輸權
（D）單純為傳達事實之新聞報導所作成之語文著作，仍受著作權法保障

Ans：ABC

34. 關於 SQL 資料隱碼（SQL injection）的描述，下列何者有誤？

（A）SQL Injection 的惡意字串不一定會出現'單引號的特殊字元
（B）' OR 'a'='a 是一種 SQL Injection 惡意字串
（C）有 SQL Injection 漏洞的程式碼可改寫為預存式查詢（Prepared Statement）或參數化查詢（Parameterized Queries）來做補強
（D）Hibernate 程式語言已經在框架層補強 SQL Injection 風險，開發人員可專注在邏輯面瑕疵

Ans：D

35. 關於 ISO/IEC 27005 對風險評鑑的描述，下列何者不正確？

（A）第一階段是風險識別（risk identification）
（B）第二階段是風險分析（risk analysis）
（C）第三階段是風險評估（risk evaluation）
（D）第四階段是風險接受（risk acceptance）

Ans：D

36. 以下哪些功能可以利用數位簽章憑證達到？

（A）加密資料
（B）確保資料完整性
（C）不可否認
（D）確認對方身份

Ans：ABCD

37. 關於 APT（Advanced Persistent Threat）的描述，下列哪些正確？

（A）0-day 零時差漏洞係指尚該弱點無有效的官方更新檔 http://blogs.technet.com/b/technet_taiwan/archive/2016/03/29/pass-the-hash-pth-and-pass-the-ticket-ptt-01.aspx
（B）OFFICE 文件或 PDF 文件可夾帶可執行的惡意程式
（C）社交工程攻擊的手法之一是反轉字元攻擊，其係利用微軟漏洞，即 Unicode 特殊字元，須立即進行更新修復
（D）網管在遠端登入協助故障排除時，可能會遭受 Pass-the-hash 或 Pass-the-ticket 攻擊

Ans：ABD

38. 關於 Unicode 反轉字元偽裝攻擊的描述，下列哪些不正確？

（A）slx.sc r 係 Excel 表單偽裝成螢幕保護程式
（B）rcs.xls 係螢幕保護程式偽裝成 Excel 表單
（C）在中文語系環境進行攻擊需使用到 RTLO（Right to Left Override）轉碼字元
（D）在英文語系環境進行攻擊需使用到 LTRO（Left to Right Override）轉碼字元

Ans：AD

39. 關於行政院的安全軟體測試參考指引，下列描述哪些不正確？

（A）靜態分析通常採用「源碼檢測」
（B）動態分析通常採用「滲透測試」或「弱點掃描」
（C）軟體式的應用層防火牆可過濾程式的邏輯瑕疵
（D）OWASP Top 10 指的是十大 C/C++ 常見撰寫錯誤

Ans：CD

40. 關於 Cryptolocker 等勒索軟體/病毒（綁架病毒）的描述，下列哪些不正確？

（A）贖金交付多半需以彼特幣（bitcoin）支付
（B）惡意程式的連線網路可能使用 TOR 匿名網路
（C）中毒現象多半為全硬碟加密無法開啟
（D）加密演算使用至少 2048-bit 對稱式金鑰，難以暴力破解

Ans：CD