109 年度初級資訊安全工程師能力鑑定試題

科目 2：資訊安全技術概論

考試日期：109 年 5 月 30 日　　第 1 頁，共 9 頁

單選題 50 題（佔 100%）

C	1. 關於安全管控，下列何者較「不」安全？ (A) 定期檢視網路架構 (B) 定期針對重要設備進行設定檔備份 (C) 針對網路設備之存取不限制存取來源 IP (D) 建立防火牆連線規則管理政策
D	2. SQL 資料隱碼攻擊（SQL Injection Attack），是發生在應用程式之資料庫層的安全漏洞，下列何者「不」是其所造成的影響？ (A) 造成個人機敏資料、帳戶資料、密碼等資料外洩 (B) 資料結構被駭客得知弱點，得以做進一步攻擊 (C) 資料庫伺服器被攻擊，系統管理員帳戶被竄改 (D) 允許惡意使用者將程式碼注入到網頁上
B	3. 傳輸協定中，下列何者是「較」安全的加密傳送協定？ (A) smtp (B) https (C) telnet (D) ftp
A	4. 在分散式阻斷服務（Distributed Denial-of-Service, DDoS）攻擊中，攻擊者發送 HTTP POST 請求時，設定 Content-Length 為很大的值與 HTTP BODY 的傳輸速率非常緩慢，造成連線持續佔用而耗盡網站伺服器的連接資源，此為下列何種攻擊方法？ (A) 慢速 POST 請求攻擊 (B) Slowloris 攻擊 (C) HTTP 洪水攻擊 (D) 資料處理過程攻擊
C	5. 關於網路安全的防護方法，下列敘述何者「不」正確？ (A) 定期更新病毒碼 (B) 定期更新核心版本與套件 (C) 定期重灌系統 (D) 設置防火牆
A	6. 下列何者為防禦 ARP 欺騙（ARP spoofing）的最佳方式？ (A) 使用固定 IP 並綁定 MAC (B) 使用 DHCP (C) 使用防火牆 (D) 使用 WAF
A	7. 國際標準化組織(ISO)所提出的 OSI 模型(Open System Interconnection

	Reference Model）總共分成幾層？ (A) 7 層 (B) 6 層 (C) 5 層 (D) 4 層
B	8. 關於無線網路安全，下列敘述何者「不」正確？ (A) 無線路由器之韌體應即時更新，可避免已知弱點遭利用 (B) 無線網路 SSID 設定為隱藏，可完全避免遭受駭客探測 (C) 無線路由器後台禁止透過網際網路存取，可降低受駭風險 (D) 禁用已知有瑕疵之無線加密協議，可降低傳輸內容遭受竊聽攻擊
B	9. 為了確保電子郵件使用的安全性，應該要注意遵循下列哪些事項？(1)機密公文不得以電子郵件傳送、(2)敏感性的資訊，應該加密處理之後再傳送、(3)電子郵件的附檔，不需掃毒即可傳送、(4)可以運用電子簽章來確保身份辨識及達成不可否認性 (A) (1), (2), (3) (B) (1), (2), (4) (C) (1), (3), (4) (D) (2), (3), (4)
B	10. 網際網路所使用之 TCP/IP 通訊協定共區分為下列哪幾層？ (A) 會議層（Session Layer）、傳輸層（Transport Layer）、網路層（Internet Layer）、連結層（Link Layer） (B) 應用層（Application Layer）、傳輸層（Transport Layer）、網路層（Internet Layer）、連結層（Link Layer） (C) 應用層（Application Layer）、傳輸層（Transport Layer）、網路層（Internet Layer）、資料連結層（Data Layer） (D) 應用層（Application Layer）、傳輸層（Transport Layer）、網路層（Internet Layer）、實體層（Physical Layer）
B	11. 某甲欲使用檔案傳輸軟體將一敏感檔案傳給某乙，某甲除了將敏感檔案加密之外，在傳輸過程中，某甲可以使用下列何種安全協定，另此一安全協定的使用亦可防止何種攻擊？ (A) SSH、DNS 攻擊 (B) SSH、中間人攻擊 (C) HTTPS、DNS 攻擊 (D) HTTPS、中間人攻擊
B	12. TCP 三向交握（Three-way Handshake）過程中的封包使用了下列哪些旗標（Flags）？

	(A) SYN and RST (B) SYN and ACK (C) SYN and FIN (D) FIN and ACK
C	13. 行動通訊網路到哪一代之後，語音與數據通訊皆採用 IP 架構運作？ (A) 2G 通訊 (B) 3G 通訊 (C) 4G 通訊 (D) 5G 通訊
D	14. 關於作業系統主要的功能，下列敘述何者最「不」適當？ (A) 做為使用者之介面 (B) 分配與管理系統資源 (C) 提供系統服務與保護 (D) 提供影像處理服務
C	15. 下列何者因為每次程式執行時的記憶體配置的位址均「不」同，能夠讓攻擊者難以猜測程式的記憶體地址？ (A) 資料執行保護（Data Execution Prevention, DEP） (B) 可執行空間保護（Executable Space Protection, ESP） (C) 位址空間配置隨機化（Address Space Layout Randomization, ASLR） (D) 安全例外狀況處理常式（Safe Security Exception Handler, SAFESEH）
D	16. Intel X86 作業系統之核心模式（Kernel Mode），被設計於中央處理器（CPU）的何種特權等級中執行？ (A) Ring 3 (B) Ring 2 (C) Ring 1 (D) Ring 0
C	17. 關於主機之安全性措施，下列敘述何者正確？ (A) 所有重大安全性更新，應於服務主機直接安裝以提升安全性 (B) 防毒軟體可完全避免惡意軟體與木馬程式運行 (C) 無需使用之主機服務，應進行關閉以降低受駭風險 (D) 作業系統內建之防火牆功能，應進行關閉以確保網路服務正常運行
C	18. WannaCry 勒索病毒植入電腦後會將該電腦之檔案進行加密，請問該勒索病毒是利用微軟的何種漏洞來執行？

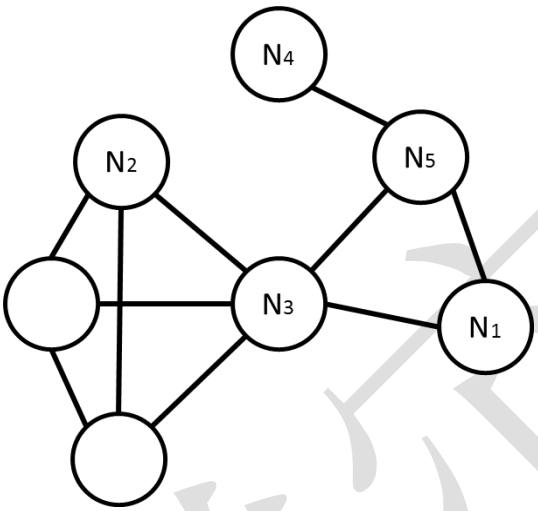
	(A) Microsoft XML Core Services (B) Shellshock 漏洞 (C) 伺服器訊息區塊（SMB）漏洞 (D) Local Security Authority Subsystem Service（LSASS）
C	19. 黑帽駭客（Black Hats）是指惡意攻擊電腦系統及網路的人，下列何者「不」是其行為？ (A) 誘騙使用者上當並植入木馬程式 (B) 利用電腦裝置的漏洞進行入侵 (C) 通知網站客戶該網站有漏洞 (D) 釣魚式攻擊
D	20. 關於電子郵件社交工程的防範作為，下列何者「不」適當？ (A) 不要自動回覆讀信回條 (B) 關閉自動下載圖片 (C) 不隨意點擊郵件中的附加檔案或及超連結 (D) 收到免費咖啡訊息，可以打開連結看看，再聯繫寄件者確認
A	21. 下列何者為 Cmd Injection 語法？ (A) http://127.0.0.1/delete.php?filename=bob.txt;ls (B) alert(0); (C) or 1=1 (D) <script>alert(0);</script>
D	22. 下列何者「不」是用於撰寫動態網頁的程式語言？ (A) PHP (B) JSP (C) ASP.NET (D) PostScript
C	23. 系統管理人員於網站日誌中看見大量訊息含有類似字串「%3E%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E」，可能為下列何種攻擊？ (A) SQL 資料隱碼攻擊（SQL Injection Attack） (B) 阻斷服務攻擊（Denial of Service Attack） (C) 跨網站指令碼攻擊（Cross Site Scripting Attack） (D) 不安全的反序列化漏洞（Insecure Deserialization）
C	24. 在軟體開發生命週期（System Development Life Cycle, SDLC）中，修正軟體中同一個安全性問題，於下列何者階段的成本最高？ (A) 設計階段 (B) 需求階段

	(C) 產品階段 (D) 測試階段
C	25. 下列何者攻擊有可能異動資料庫內的資料？ (A) 跨站請求攻擊（Cross Site Request Forgery, CSRF） (B) 跨網站指令碼攻擊（Cross Site Scripting Attack, XSS） (C) SQL 資料隱碼攻擊（SQL Injection Attack） (D) 輕型目錄存取協定注入（Lightweight Directory Access Protocol Injection, LDAP Injection）
C	26. 下列何者「不」是強化伺服器安全的機制？ (A) 使用防毒軟體 (B) 關閉不需要的服務並遵照最小權限原則 (C) 關閉防火牆 (D) 進行滲透測試
C	27. 關於應用系統安全部署，下列敘述何者「較」為正確？ (A) 建立維護用後門 (B) 以最高權限執行軟體 (C) 移除除錯用的原始程式碼 (D) 開啟所有的底層服務
B	28. 關於系統開發測試中白箱測試與黑箱測試，下列敘述何者較「不」正確？ (A) 白箱測試主要測試內部邏輯架構的正確性 (B) 黑箱測試主要運用機器掃描原始程式碼 (C) 滲透測試屬於黑箱測試 (D) 原碼掃描屬於白箱測試
A	29. 請問 CVE（Common Vulnerabilities and Exposures）是指下列何者？ (A) 常見漏洞和風險編號 (B) 弱點種類 (C) Exploit Code (D) 漏洞修補建議
D	30. 關於原始碼掃描，下列敘述何者「較」正確？ (A) 原始碼掃描作業必須提供完整的程式原始碼才能進行分析 (B) 原始碼掃描作業必須區隔個別程式語言，不可將多種語言混合在一起 (C) 原始碼掃描擅長分析邏輯瑕疵 (D) 原始碼掃描可在程式開發過程中進行，無須等到系統上線後執行
C	31. 關於網路防火牆，下列敘述何者較「不」正確？

	(A) 阻擋外部人員對內部網路的掃瞄 (B) 透過封包過濾，阻擋來自特定來源 IP 的連線 (C) 能避免員工對外傳送機密文件 (D) 應用層的防火牆可針對連線的類型、檔案的大小等條件進行過濾
A	32. 下列何種病毒會使用「不」同金鑰加密來改變自身外形？ (A) Polymorphism (B) Scripting viruses (C) Macro Viruses (D) Visual Basic Script
C	33. 關於網站應用程式弱點修補，下列何種方式較「不」能確保安全性？ (A) 於官網下載無弱點之網站應用程式，並進行更新 (B) 停止使用或尋找替代無弱點之網站應用程式 (C) 使用 Layer 4 防火牆進行防護 (D) 若更新檔未釋出，可於 WAF 透過攻擊特徵碼進行阻擋
D	34. 為避免當發生災害或儲存媒體失效時，確保資料之安全並可以迅速回復正常作業，讓衝擊之影響減至最低，下列敘述「較」何者正確？ (A) 定期執行資料之加密作業 (B) 定期執行資料之掃描作業 (C) 定期執行資料之掃毒作業 (D) 定期執行資料之備份作業
D	35. 下列何者較「不」是影響備份執行時間長短之主要因素？ (A) 備份範圍主機的多寡 (B) 備份設備所使用的儲存媒體類型（如：磁帶、硬式磁碟機） (C) 備份機制的設定（如：完整備份、差異備份或增量備份） (D) 所需備份的檔案類型（如：PPT、XLS、WMV）
B	36. 關於差異備份（Differential Backups）與增量備份（Incremental Backup），下列敘述何者正確？ (A) 差異備份是指每一次備份都是將所有檔案資料重新備份一次 (B) 每次差異備份所備份之資料量會大於等於（>=）增量備份所備份的資料量 (C) 初次差異備份須先針對所有資料進行一次完整備份，但增量備份不用 (D) 增量備份在進行資料復原時，只需要使用最後一次的備份資料即可
C	37. 關於資料加密採用 DES，下列敘述何者較「不」正確？ (A) DES 英文全名是 Data Encryption Standard

	(B) 一種對稱密鑰加密演算法 (C) DES 已經不是安全加密法，因使用的 128 位金鑰過短 (D) 安全性較 AES 低
A	38. 下列何種措施「不」能強化資料的機密性？ (A) 備份（Backup） (B) 加密（Encryption） (C) 去識別化（De-identification） (D) 存取控制（Access Control）
A	39. 系統作業日誌應該予以定期審查，請問下列何種系統日誌較需設定高審查頻率？ (A) 高風險的資訊系統 (B) 中風險的資訊系統 (C) 低風險的資訊系統 (D) 極低風險的資訊系統
B	40. 下列何種記錄檔之功能目的在於記錄系統上的應用程式所有安裝行為，包含在何時安裝、何時執行了什麼程式等？ (A) 系統日誌檔 (B) 應用程式日誌檔 (C) 使用者登出入日誌檔 (D) 網路日誌檔
C	41. 平時必須記錄使用者活動、異常、錯誤及資訊安全事件之事件日誌，以便建立系統稽核軌跡。請問下列何者並「不」需要納入系統安全稽核軌跡？ (A) 使用者登入及登出系統之日期及時間 (B) 存取系統成功與失敗情形的記錄 (C) 佔用的頻寬及所需的費用金額 (D) 系統公用程式與應用程式的使用
D	42. 各種設備所產生的日誌格式可能不一樣，為了讓接收端的軟體能夠辨識與讀懂不同型態的日誌，日誌格式應該進行下列何種處理，以方便分析？ (A) 格式化（Formatting） (B) 標準化（Standardization） (C) 最佳化（Optimization） (D) 正規化（Normalization）
A	43. 關於日誌（Log）事件存錄與日誌保護，下列敘述何者較「不」正確？ (A) 日誌應詳細紀錄所有使用者的帳號、密碼及活動資訊以作為日後

	的佐證 (B) 宜儘可能不讓系統管理者具有日誌存取權限，以避免抹除其本身活動之日誌或停止對其活動之存錄 (C) 日誌紀錄的時間應與標準時間一致，以便往後的調查與佐證 (D) 系統特別權限的使用也是應該要特別記錄的項目，以便提高異常活動的偵測能力
A	44. 下列何者「不」是和雲端安全有關的國際標準？ (A) ISO/IEC 27011 (B) ISO/IEC 27017 (C) ISO/IEC 27018 (D) CSA STAR
C	45. 關於行動裝置通訊軟體，下列敘述何者較「不」正確？ (A) 開啟「阻擋訊息」，阻擋非來自好友之訊息 (B) 只在信譽良好網站或官方 APP 市集中下載使用 (C) 對於聳動的訊息，可直接分享給相關好友 (D) 不在公用電腦登入，並定期更改密碼
A	46. BYOD（Bring Your Own Device）是指帶行動裝置至辦公環境中辦公事，在資安標準作業規範 ISO/IEC 27002:2013 中，針對 BYOD 的指導綱要與安排項目，「不」包含下列何者？ (A) 合理性查核，已測試輸出資料是否合理 (B) 提供適當的通信設備，包括保護遠端存取的方法 (C) 提供軟硬體支援與維護 (D) 稽核與安全監視
C	47. 關於行動裝置可能遭受的安全威脅，下列敘述何者「不」在其中？ (A) 行動裝置遺失資料外洩 (B) 行動裝置感染病毒 (C) 行動裝置因欠費，無法連上網路 (D) 行動裝置因安裝不明軟體，有遭植入後門之風險
B	48. 在物聯網裡，網路犯罪分子可能經由猜測密碼，而入侵網路或連到特定網路的設備，此為下列何種攻擊手法？ (A) 監聽攻擊（Sniffing Attack） (B) 密碼攻擊（Password-Based Attack） (C) 金鑰淪陷攻擊（Compromised-Key Attack） (D) 阻斷服務攻擊（Denial-of-Service Attack）
D	49. 關於物聯網安全，下列敘述何者「不」正確？ (A) 政府與 IoT 開發商應協力降低 IoT 的安全風險問題

	(B) 建立與利益相關人的風險意識 (C) 規劃出提升 IoT 安全的獎勵措施 (D) 不用建立損害侵權、保險補償、安全認證…等措施
C	50. 在附圖中，只有節點 N5 具備有向外連網能力，其他節點皆必須透過節點 N5 才能與外界進行網際網路連結，請問當節點 N5 為絕對安全的情況下，哪個節點消失時對整體網路的影響最大？  (A) N1 (B) N2 (C) N3 (D) N4