弱點管理

**弱點管理方法：**

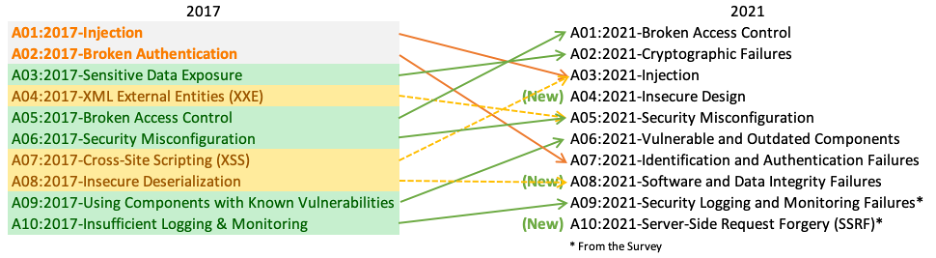
* 資安健診 (Information Security Diagnostic)
  + 說明：由第三方顧問廠商每年定期進行全面的安全檢查，屬於預防性資安措施，找出潛在的安全弱點。
  + 檢視項目：
    - 網路架構檢視、網路惡意活動檢視。
    - 使用者端電腦與伺服器主機的惡意活動檢視。
    - 目錄伺服器設定檢視、防火牆連線設定檢視。
    - 政府組態基準(GCB)檢視、資料庫安全檢視。
* SOC服務 (Security Operation Center)
  + 說明：由外部或內部建立 SOC 團隊，透過集中式監控與管理系統日誌來主動偵測與處理安全事件。SOC團隊通常由資安分析師、事件處理人員、威脅情報人員等角色所組成。
  + 問題單工作流程：查看可疑系統日誌 → 建立事件通報單 → 分派至相關經辦人處理並追蹤到解決。
  + 常用工具
    - 安全資訊與事件管理(SIEM)
      * 用途： 集中蒐集系統日誌、網路活動，進行事件關聯分析、告警及報告。
      * 常用軟體： OSSIM、ArcSight、Splunk。
    - 端點偵測與回應(EDR)
      * 用途：安裝於終端設備，偵測惡意軟體、未授權存取、異常行為，進行事件調查、隔離或封鎖威脅。
      * 常用軟體：CrowdStrike、SentinelOne。
    - 威脅情報平台(TIP)
      * 用途： 提供最新威脅情報、威脅指標 (Indicators of Compromise, IoCs)，協助分析師快速比對、識別威脅來源及性質。
      * 常用軟體：MISP、Recorded Future。
    - 安全自動化與協調回應(SOAR)
      * 用途： 自動化事件處理流程（如隔離主機、封鎖 IP），降低分析人員負擔、提升回應速度與效率。
      * 常用軟體：Splunk Phantom、Cortex XSOAR。
  + 應用：
    - 快速偵測並應對異常行為 (如未授權存取、惡意流量等) 。
    - 強化事件回溯分析能力。
* 原始碼掃描(Source Code Analysis)
  + 說明：對應用程式的原始碼進行安全掃描，找出潛在漏洞 (如未檢查的輸入、寫在程式中的密碼等) 。
  + 執行方式：
    - 通常由內部自行使用工具掃描。
    - 遇到無法修補的漏洞，會詢問廠商顧問協助。
  + 特性：
    - 適用階段：程式開發過程中即可進行，無須等到系統上線後執行。
    - 支持多語言：大多數原始碼掃描工具支持多種程式語言的混合分析 (如 Java、Python、C++ 等) 。
    - 優勢：能早期發現程式漏洞，降低修復成本。
    - 限制：無法全面檢測邏輯瑕疵、業務漏洞或駭客刻意植入的惡意程式碼。
  + 常見軟體：SonarQube、Checkmarx、Fortify。
* 弱點掃描 (Vulnerability Assessment)
  + 說明：利用掃描工具檢查主機、系統或應用程式的已知漏洞。快速找出已知漏洞，但無法模擬實際攻擊行為。
  + 執行方式：可自行安裝軟體掃描，或交由第三方廠商協助。
  + 類型：
    - 主機系統弱點掃描：檢查伺服器和工作站的系統漏洞。
      * 常見軟體：Nessus、OpenVAS、Nexpose。
    - 網頁應用程式弱點掃描：檢查網站與 API 的潛在安全問題。
      * 常見軟體：Burp Suite、OWASP ZAP。
  + 相關標準：
    - 重點整理：
      * CWE 定義軟體開發中的常見弱點類型。
      * CVE 具體標識已發生的漏洞。
      * CVSS 為漏洞的嚴重程度打分。
      * NVD 是詳述漏洞資訊與修補建議的資料庫。
      * CPE 指出漏洞可能影響的軟硬體平台。
    - CVE(Common Vulnerabilities and Exposures)：
      * 全球統一漏洞編號系統，用於識別和追蹤已知漏洞。
      * 範例：CVE-2017-0144，永恆之藍 (EternalBlue) 漏洞，利用 SMBv1 通訊協議的遠端代碼執行 (RCE) 漏洞，曾被用於 WannaCry 勒索病毒攻擊。
    - CWE (Common Weakness Enumeration)：
      * 公開的弱點分類系統，用於識別和標註軟體開發過程中的常見弱點。
      * 範例：CWE-119 - 特定語言容許直接取得記憶體區域 (Improper Restriction of Operations within the Bounds of a Memory Buffer)，永恆之藍的核心弱點。
    - CVSS(Common Vulnerability Scoring System)：
      * 漏洞評分標準，量化漏洞的嚴重程度 (範圍 0–10)。
      * 範例：CVSS v3.1 總分 8.5 (高危漏洞)，攻擊難度低，無需用戶交互，可遠端觸發。
    - NVD(National Vulnerability Database)：
      * 美國國家漏洞資料庫，基於 CVE 提供漏洞詳細資訊與 CVSS 評分。
      * NVD 詳細描述 CVE-2017-0144 的攻擊場景，影響的系統包括 Windows 7、Windows Server 2008，並建議用戶安裝相關安全更新 (MS17-010) 以修補漏洞。
    - CPE (Common Platform Enumeration)：
      * 通用平台枚舉，用於標識漏洞影響的特定軟體或硬體版本。
      * 範例：CPE 編碼範例 - "cpe:2.3:o:microsoft:windows\_7"，代表 CVE-2017-0144 對 Windows 7 作業系統的影響。
* 滲透測試 (Penetration Test)
  + 說明：模擬攻擊者行為，利用弱點的串聯找出進入系統的路徑。
  + 特性：
    - 具破壞性，可能導致服務中斷或資料損毀。
    - 測試前後需詳盡溝通，以免造成誤解或事故，需要明確界定測試範圍與時間，並簽署賠償條款。
  + 類型：
    - 一般性滲透測試：針對單一目標或範圍 (如網站、伺服器) 。
    - 紅隊演練
      * 說明：檢測整體系統的防禦能力，模擬真實攻擊場景。角色定義為紅隊：模擬攻擊者進行滲透。藍隊：負責防禦，應對紅隊攻擊。紫隊：中立第三方，協助紅藍隊溝通與協作。
  + 白箱 vs 黑箱 vs 灰箱 vs 雙黑箱演練
    - 白箱演練
      * 測試者了解內部系統結構與資訊 (如程式碼、網路配置)。
      * 應用場景：內部安全測試，檢測內部邏輯與權限管理弱點。
    - 灰箱演練
      * 測試者擁有部分關於目標系統的內部資訊，例如架構圖、API 文件、部分程式碼片段或有限權限的帳戶。
      * 應用場景：更貼近現實的滲透測試，針對特定系統或功能的安全性評估、資安事件應變演練，通常最能有效率地發現潛在漏洞並模擬真實攻擊。
    - 黑箱演練
      * 測試方式：測試者對系統完全不了解，僅基於外部公開資訊 (如域名、IP) 進行攻擊。
      * 應用場景：外部滲透測試，模擬外部攻擊者的真實行為。
    - 雙黑箱
      * 攻防雙方在測試過程中都不知道對方的具體情況。
      * 應用場景：模擬真實的攻擊和防禦場景，測試藍隊的響應能力與檢測能力。
  + 常見指令：Nmap、CURL、SQLmap、Netcat、John the Ripper、HashCat、Aircrack-ng、Hydra。
  + 常見軟體：Wireshark、Metasploit、Burp Suite、OWASP ZAP、Mimikatz、Nikto。
* 社交工程演練
  + 說明：模擬社交工程攻擊來測試人員的安全意識。通常由第三方顧問廠商每年定期辦理。提升員工的安全意識，減少因人為疏忽造成的安全事故，故通常搭配教育訓練，以強化員工的資安意識。
  + 測試項目：
    - 最常見是釣魚郵件和簡訊演練，但不限於電話或真人實體測試。
    - 統計測試成功和失敗的比例，查看員工的整理資安意識。
  + 後續措施：
    - 被發現弱點的員工需參加教育訓練。
    - 定期測試提高組織防範社交工程的能力。
* 軟體組成分析 (Software Composition Analysis)
  + 說明：用來掃描軟體中引用的第三方元件（尤其是開源套件），並分析其版本、安全漏洞、授權合規性及潛在風險。現今軟體開發很少從零開始，大多是引用第三方套件，套件若有弱點便會一併繼承到自己的軟體中。舉例：Apache Log4j 安全漏洞 (CVE-2021-44228) 爆發時，公司若有上百套系統，要如何在第一時間掌握哪些系統引用了該版本並存在漏洞？因此必須透過軟體材料表(Software Bill of Material, SBOM)是詳細列出軟體中所有組件名稱、版本、依賴關係、供應鏈來源等資訊的結構化清單，可視為「軟體成分說明書」。
    - 步驟 1：使用 SCA 工具掃描原始碼或二進位檔，生成 SBOM（列出所有組件）。
    - 步驟 2：SCA 工具進一步分析 SBOM 中的組件，標示出有安全漏洞或授權風險的項目。
    - 步驟 3：開發人員根據 SCA 的報告進行組件更新或修補，SBOM 則自動同步至最新版本與風險狀態。

**事件處理與調查方法**

* 數位鑑識 (Digital Forensics)
  + 說明：透過系統化的蒐證與分析電子證據，還原資安事件發生過程，確認攻擊來源與影響範圍，作為法律程序或內部調查依據。
  + 執行方式：
    - 蒐集系統日誌、記憶體、網路封包等電子證據。
    - 分析證據以重建事件經過。
    - 提供正式報告供法律或管理決策使用。
  + 常用工具：
    - FTK Imager、Autopsy、Volatility、Wireshark。
  + 特性：
    - 需符合法律程序與證據保全原則，維持完整的證物證據鏈和監管鏈（Chain Of Custody）。
    - 因為需要專業的數位鑑識軟體和通過ISO / IEC 17025資安檢測實驗室，通常由具專業認證外部人員執行。

**OWASP Top 10 常見十大漏洞：**

* 為網路應用程式漏洞的指南，每年統計最常見的十個WEB應用伺服器漏洞，目前最新版為2021年版。
  + **A01:2021-權限控制失效**：直接在網址改 ID 從 /user/1 改成 /user/2 就能查到別人的資料。
  + **A02:2021-加密機制失效**：使用明文或簡單 MD5 儲存密碼。
  + **A03:2021-注入式攻擊**：輸入 ‘admin' or ‘1’=’1’ 繞過登入驗證繞過登入驗證。
  + **A04:2021-不安全設計**：網站未限制登入次數，可以暴力破解密碼。
  + **A05:2021-安全設定缺陷**：使用預設的管理者帳號密碼 admin/admin，或是錯誤網頁顯示太多資訊。
  + **A06:2021-危險或過舊的元件**：使用有漏洞的舊版 Log4j 套件。
  + **A07:2021-認證及驗證機制失效**：密碼重設連結可以直接從 email 網址看到重設 token。
  + **A08:2021-軟體及資料完整性失效**：未驗證更新程式的數位簽章就直接安裝。
  + **A09:2021-資安記錄及監控失效**：系統未記錄登入失敗紀錄。
  + **A10:2021-伺服端請求偽造**：未驗證來源網站，可偽造請求從其他網站發送交易。



**考古題：**

1. 目前有一個大企業，員工超過5000人、系統超過500個，想要定期對內部進行弱點掃描，請問在實務考量下（人力、資源、時間都有限），下列觀念何者較為正確？

(A) 無論弱點的風險等級是重大、高、中、低，無論弱點數量有多少個，無論資訊部門的人力是否足夠，都應該在一天之內把所有弱點都修補完畢，才能確保企業是安全的

(B) 只要掃描出來的弱點類型屬於OWASP Top 10其中之一，就應該立刻進行修補，不需要對弱點進行任何評估

(C) 掃描結果出爐後，應先針對每個弱點的風險等級、實際影響程度、有無出現攻擊利用程式（Exploit）進行評估，同時也要考慮重開機或停機對企業服務的影響程度，最後再來規劃每個弱點的修補時程

(D) 當某台伺服器的弱點掃描結果出現作業系統弱點時，如果該作業系統的官方網站沒有釋出任何修補更新檔（patch），維運人員就不需要對該伺服器做任何處置

防護 114-1 答案C

(在大企業環境中，弱點掃描結果往往數量龐大，無法在一天內修補所有弱點（(A) 不切實際），而且僅根據OWASP Top 10 的標準進行修補也不夠全面（(B) 太過簡單）。此外，當作業系統沒有釋出更新時，仍需評估是否有其他替代控管措施，不能完全不處置（(D) 不正確）。因此，正確的做法是先根據每個弱點的風險等級、實際影響、是否有利用程式（Exploit）等進行詳細評估，並考慮修補過程中可能對企業服務造成的影響，再根據評估結果來制定合理的修補時程，這正是選項 (C) 的做法。)

4. 關於知名密碼破解工具Hashcat的說明，下列哪些描述正確？（複選）

(A) 可以破解的密碼種類超過10種 (Hashcat 支援多種雜湊算法，遠超過10種)

(B) 可以使用 ?u?l?d?d?d?d?d?d這種Mask Attack Mode來進行暴力破解，破解出來的密碼內容範例是aB123456 (提供的 mask 為 ?u?l?d?d?d?d?d?d，要求第一個字元為大寫、第二個為小寫，後面跟著6位數字；然而範例密碼 "aB123456" 的第一個字元為小寫，不符合規定，因此此敘述不正確)

(C) 如果使用參數 -a 1的話，可以同時使用兩個字典檔一起組合破解 (-a 1 是 combinator 模式，允許結合兩個字典檔來生成候選密碼)

(D) 進行 -a 0字典檔攻擊時，如果使用參數 -r的話，可以載入一組規則以便進行Rule-based Attack，例如在所有字典的後面加上1234組合成新的密碼 (在 -a 0 模式下，-r 參數可載入規則檔，依據規則對字典中的每個詞彙進行變化（例如在詞彙後面加上 1234）

防護 114-1 答案ACD

32. 漏洞是指因開發過程中不慎製造而導致安全性風險的弱點，依照2024 SANS / CWE TOP 25所指出的前25最危險的程式設計錯誤，下列那些是排名前五的項目？（複選）

(A) CWE-352 Cross-Site Request Forgery（CSRF）

(B) CWE-125 Out-of-bounds Read

(C) CWE-416 Use After Free

(D) CWE-787 Out-of-bounds Write  
  
防護 114-1 答案AD

(根據針對「2024 CWE Top 25 最危險的軟體弱點」的搜尋結果（由 MITRE 提供），排名前五的項目是：

CWE-79： 網頁產生期間輸入的不當中和處理 ('跨網站指令碼')

CWE-787： 越界寫入

CWE-89： SQL 指令中使用的特殊元素的不當中和處理 ('SQL 注入')

CWE-352： 跨網站請求偽造 (CSRF)

CWE-22： 對受限目錄的路徑名稱的不當限制 ('路徑遍歷')

現在我們檢查使用者提供的選項哪些在前五名內：

(A) CWE-352 Cross-Site Request Forgery（CSRF）： 這個在排名前五，名列第四。

(B) CWE-125 Out-of-bounds Read： 這個在排名第六，不在前五名內。

(C) CWE-416 Use After Free： 這個在排名第八，不在前五名內。

(D) CWE-787 Out-of-bounds Write： 這個在排名前五，名列第二。

因此，排名前五的項目是 (A) CWE-352 Cross-Site Request Forgery（CSRF） 和 (D) CWE-787 Out-of-bounds Write。)

3. 下列哪幾種方式是檢測人員執行紅隊演練過程中可能會使用的攻擊手法？（複選）

(A) 在 DMZ網頁伺服器找到 RCE漏洞並取得系統控制權，然後在內網進行橫向移動，嘗試取得（Windows Server Active Directory，AD）的控制權

(B) 透過釣魚信件對企業的海外分公司員工進行社交工程，取得員工電腦控制權，然後讀取員工電子郵件信箱，尋找可以拿來利用的機敏資料

(C) 移動到企業所在的樓層，側錄Wi-Fi然後嘗試破解密碼，取得企業 Wi-Fi的存取方式，入侵企業內部網路

(D) 註冊成為企業的供應商，並且利用供應商專用網站造假資料、竄改商品金額，驗證攻擊者可以用更低的價格買進商品 (**不完全正確**。雖然這也屬於安全測試的範疇，但更偏向於**應用程式安全測試或業務邏輯測試**，主要針對供應商網站本身的安全性進行測試。而紅隊演練更注重於模擬真實攻擊者的**入侵路徑和手法**，通常不會花費大量時間去註冊成為供應商。這種手法更像是針對特定業務流程的測試)

防護 113-2 答案ABCD、ABC

12. 對於一家正準備進行採購網站應用程式的公司來說，為什麼應該以自動化漏洞評估系統（Automated Vulnerability Assessment System AVAS）作為驗收基礎，而不是根據開放式網路應用安全項目（ Open Web Application Security Project，OWASP Top 10）的10大弱點項目作為驗收要件？

(A) OWASP Top 10僅涵蓋最常見的安全漏洞，而不是所有可能的安全問題 (OWASP Top 10 雖然是重要的安全參考指標，但它只列出了最常見、影響最大的 10 類 Web 應用程式安全風險。實際上，Web 應用程式面臨的安全威脅遠不止這些，還有許多其他類型的漏洞也可能被攻擊者利用。AVAS 可以更全面地掃描和檢測各種已知漏洞，提供更廣泛的安全保障)

(B) OWASP Top 10較易於實施且成本更低

(C) AVAS獲得領導者向象中的指標意義

(D) AVAS僅針對網站應用程式，而 OWASP Top 10 適用於所有類型的軟體

防護 113-2 答案A

28. 網路安全滲透測試的目標包括一切與網路相關的基礎設施，包含網路裝置、作業系統、實體安全、應用程式、管理制度等。下列敘述哪些錯誤？ （複選）

(A) 網路裝置是包含所有能夠連接到網路的各種實體，像是路由器、交換機、防火牆、個人電腦等

(B) 實體安全主要指的是機房環境、通訊設備等，是資訊安全中最重要的目標 (實體安全固然重要，但並非資訊安全中「最重要」的目標。實體安全主要指的是保護資訊資產免受物理上的威脅，例如未經授權的存取、盜竊、破壞、自然災害等。機房環境、通訊設備、門禁系統、監視系統等都屬於實體安全的範疇。資訊安全的目標應該是**全面性的**，包括保護資訊的機密性 (Confidentiality)、完整性 (Integrity) 和可用性 (Availability)，實體安全只是其中的一環。過度強調實體安全而忽略其他方面的安全，例如網路安全、應用程式安全等，同樣會導致安全風險)

(C) 應用程式是管理與控制電腦軟硬體資源的電腦程式 (這個敘述是**作業系統**的定義。應用程式是指為了完成特定任務而設計的電腦程式，例如文書處理軟體、網頁瀏覽器、電子郵件客戶端等。應用程式運行在作業系統之上，利用作業系統提供的資源來執行任務。而作業系統才是負責管理和控制電腦軟硬體資源的系統軟體)

(D) 管理制度指的是為了保障網路安全對使用者提出的要求與限制

防護 113-2 答案B、C

29. 關於滲透測試工具的敘述，下列何者正確？

(A) John the Ripper和 Hashcat，主要用在社交工程 (John the Ripper 和 Hashcat 是密碼破解工具)

(B) Aircrack-ng和 Kismet用在有線網路刺探分析 (Aircrack-ng 和 Kismet 是用於 無線網路 (Wi-Fi) 的安全工具。)

(C) Nmap和 Wireshark用於識別網路中的設備，以及他們開放的端口和服務

(D) OWASP ZAP和 Burp Suite用在作業系統漏洞分析 (OWASP ZAP 和 Burp Suite 是用於 Web 應用程式安全測試 的工具)

防護 113-2 答案C

30. Metasploit框架最主要是用於下列何種情境？

(A) 防火牆配置

(B) 網路封包分析

(C) 漏洞利用和測試

(D) 垃圾郵件過濾

防護 113-2 答案C

(Metasploit 是一個開源的滲透測試框架，它提供了一個龐大的漏洞利用程式碼庫 (Exploits)、Payloads、輔助模組 (Auxiliary Modules) 等，可以用於測試系統和應用程式的安全性，驗證漏洞是否存在，以及評估漏洞的影響。Metasploit 經常被安全研究人員、滲透測試人員和紅隊用於模擬攻擊者的行為，以發現和修復安全漏洞)

1. 有關防止OWASP Top 10的A02:2021-Cryptographic Failures漏洞之敘述，下列何者錯誤？

(A) 確保將所有的機敏資料加密

(B) 使用最新版且標準的強加密演算法

(C) 使用適當的金鑰管理

(D) 使用HTTP的協定加密傳輸中的資料

技術 113-1 答案D

(HTTP為沒有傳輸加密協定)

2. 下列何項行為最容易導致 OWASP Top 10的 A01:2021-Broken Access Control 漏洞發生？

(A) 使用強密碼進行身份驗證

(B) 未在頁面上實施權限控制

(C) 在密碼重置流程中使用多重身份驗證

(D) 定期進行安全漏洞掃描與修復

技術 113-1 答案B

2. 關於弱點掃描，下列敘述何者錯誤？

(A) 網路弱點掃描用在尋找網路環境中的脆弱點，舉凡開放的通訊埠及所代表之服務，其服務是否透過未經加密的進行傳輸，或服務未更新漏洞

(B) 應用程式弱點掃描主要針對特定應用程式（尤其是網頁伺服器及其資料庫）的程式及應用環境（例如： Apache版本漏洞），但主要是尋如 SQL注入、跨站腳本、敏感目錄外洩…等可被攻擊之漏洞

(C) 主機弱點掃描用在檢查個別主機的脆弱點，例如主機效能負載對外服務能力，或是識別主機防毒系統是否更新 (主機弱點掃描主要檢查主機的**作業系統、已安裝的軟體是否存在已知漏洞、配置是否安全 (例如：密碼強度、權限設定)、系統服務是否正確配置等等**。雖然防毒系統是否更新也屬於主機安全的範疇，但**主機效能負載對外服務能力** 並非主機弱點掃描的主要目標，這更偏向效能監控的範疇)

(D) 常見工具，有 OWASP ZAP, OpenVAS, Nessus…等

防護 113-1 答案C

19. 依據OWASP Top 10有關安全配置錯誤風險之敘述，當應用程式處於以下何種狀態時，該應用程式可能容易受到攻擊？

(A) 啟用或安裝了必要的功能

(B) 預設帳號及密碼仍處於啟用狀態

(C) 系統最新的安全功能被啟用

(D) 伺服器發送安全標頭或指令

技術 113-1 答案B

(預設帳號及密碼仍處於啟用狀態是常見的弱點)

22. 依據 OWASP Top 10有關應用程式未驗證或過濾使用者所提供資料而產生風險之敘述，下列何者有誤？

(A) 常見的攻擊手法包含 Cross-site Scripting攻擊

(B) 常見的攻擊手法包含 SQL Injection攻擊

(C) 需要將命令與查詢資料合併，以防止注入式攻擊

(D) 屬 OWASP Top 10的 Injection風險

技術 113-1 答案C

(命令與查詢資料合併就是Injection的主因)

27. 下列何項「不」是程式碼開發所使用的原始碼檢測工具

（Static Code Analysis，SCA）？

(A) Fortify

(B) Checkmarx

(C) Nessus (弱點掃描)

(D) SonarQube

技術 113-1 答案C

29. 關於滲透測試的敘述，下列何者錯誤？

(A) 模擬駭客手法，在不需要系統管理者或公司同意下，進行漏洞驗證 (測透測試需要公司同意，因為有風險)

(B) 模擬駭客手法或惡意使用者的行為，試圖找出和利用系統的弱點

(C) 滲透測試要確保不會影響正常的業務運作和資料的完整性

(D) 滲透測試（Penetration Testing，簡稱 Pen Testing）是一種安全測試方法

防護 113-1 答案A

30. 在進行資安健診時， 檢測作業最關鍵的活動是下列何項？

(A) 更新所有辦公軟體至最新版本

(B) 監控社交媒體上員工的活動

(C) 評估和識別系統中的潛在安全漏洞

(D) 部署最新的防毒軟體

防護 113-1 答案C

31. 關於源碼檢測，下列哪些正確描述了 DLL Side Loading？（複選）

(A) DLL Side Loading 涉及到替換正常的 DLL文件

(B) 通常被用來繞過安全措施並執行惡意程式碼 (攻擊者利用 DLL Side Loading 可以將惡意程式碼注入到合法應用程式的執行過程中，從而繞過某些安全措施，例如應用程式白名單)

(C) 此技術概念僅可以在 Linux系統上實現 (DLL Side Loading 主要發生在 **Windows** 系統上，因為 Windows 有其特定的 DLL 載入機制。雖然類 Unix 系統也有類似的共享函式庫概念（例如 .so 檔案），但其載入機制與 Windows 的 DLL 不同，所以 "DLL Side Loading" 這個特定名詞通常指的是 Windows 平台上的攻擊技術)

(D) DLL Side Loading可以利用合法軟體的加載行為來隱藏惡意活動 (**可以利用合法軟體的加載行為來隱藏惡意活動**：正確。由於惡意 DLL 是被合法應用程式載入的，因此可以利用合法軟體的行為來掩蓋惡意活動，使惡意行為更難被偵測)

防護 113-1 答案ABD

(DLL Side Loading (也稱為 DLL 劫持) 是一種攻擊技術，它利用 Windows 應用程式載入動態連結程式庫 (DLL) 的方式來執行惡意程式碼。攻擊者會將惡意的 DLL 放置在特定的目錄中，誘使應用程式載入惡意的 DLL，而不是原本應該載入的合法 DLL。)

32. 關於資安測試工具用途的敘述，下列哪些正確？（複選）

(A) Acunetix為 Web漏洞掃描程式

(B) Wireshark提供網路協定、 封包等資訊

(C) Sqlmap用於檢測和利用應用程式SQL注入及對資料

庫的攻擊

(D) Canvas社交攻擊用工具 (Canvas 是一款商用的滲透測試工具)

防護 113-1 答案ABC

4. 有關 OWASP Top 10之敘述，下列何者正確？

(A) 為網路安全的法律規範

(B) 為網路攻擊的報告

(C) 為 ISO發布的網路安全標準

(D) 為網路應用程式漏洞的指南

技術 112-2 答案D

5. 有關 OWASP Top 10的 A03:2021-Injection漏洞之敘述，下列何者錯誤？

(A) 將命令與查詢資料分開防止注入攻擊漏洞的發生

(B) 使用安全的應用程式界面（API）防止注入攻擊漏洞的發生

(C) 應用程式相互驗證時容易發生

(D) 使用正向表列或白名單可有效避免此注入攻擊

技術 112-2 答案C

(注入攻擊主要發生在使用者輸入直接拼接到 SQL 查詢，非應用程式相互驗證時)

12. 在我們使用網路掃描工具 nmap進行網路探勘時，nmap通常會先透過 ping來確認目標伺服器是否可以連線，如果目標伺服器關閉 ping回應功能，可能會導致nmap誤判目標伺服器並未上線。請問下列何項 nmap指令可以跳過 ping功能直接開始掃 port？

(A) -sL (List Scan，只列出掃描目標，不會實際進行掃描，相當於 DNS 解析)

(B) -Pn

(C) -p- (掃描所有 port (1-65535)，只是指定 port 範圍，不影響 ping 行為)

(D) -sn (No port scan，只做 ping 掃描，只確認主機是否存活，不掃描 port)

技術 112-2 答案B

19. 關於滲透測試（Penetration Test）的敘述，下列何者錯誤？

(A) 滲透測試的工作由一群對網路及系統安全有完整知識與豐富經驗的成員組成，為確保組織資訊安全，不可能委託由第三方負責

(B) 滲透測試是藉由對企業網路採取各種攻擊的手段以便找出系統可能存在的漏洞

(C) 雙黑箱滲透測試主要對內部人員保密下進行 (測試團隊不了解目標的內部資訊)

(D) 滲透測試主要考驗系統的安全防護能力

112-2 答案A

(滲透測試可以委託由第三方執行，但是攻擊範圍、時間和權責在合約上要說明清楚)

25. 網站應用程式伺服器允許顯示錯誤訊息給使用者，如：Stack traces，將可能導致機敏資訊外洩或底層元件的弱點被發現，關於此應用程式缺陷的描述，下列何者較正確？

(A) 跨站請求偽造（Cross-Site Request Forgery）

(B) 安全設定錯誤（Security Misconfiguration）

(C) 認證和驗證失效（Identification and Authentication Failures）

(D) 伺服器端請求偽造（Server-Side Request Forgery）

技術 112-2 答案B

(此題考的是OWASP top 10 2021年版 A05 安全設定錯誤，錯誤網頁顯示太多資訊)

26. 關於應用程式軟體與資料完整性的敘述，下列何者錯誤？

(A) 使用數位簽章（Digital Signature）來驗證軟體未被竄改

(B) 僅於信任的儲存庫（Repository）取得應用程式套件

(C) 整合測試流程（CI/CD）應適當隔離與存取控制以確保安全

(D) 源碼掃描可有效檢查是否遭植入惡意程式碼（如：後門程式）

技術 112-2 答案D

(源碼掃描雖然可以檢測一些已知的惡意程式碼模式，但不能完全有效地檢測所有類型的後門程式，特別是經過精心偽裝的後門程式可能難以被靜態掃描工具發現，需要結合其他安全措施，如動態分析、人工審查等)

28. 與滲透測試及弱點掃描相關議題的敘述，下列何者較為正確？

(A) 若使用滲透測試工具來測試系統安全性，測試期間宜謹慎規劃不要危及系統運作

(B) 滲透測試會影響系統可用性之稽核測試，宜於正常營運時間執行，可確認實際結果 (實際上，為了最小化對業務運作的影響，滲透測試通常應在非高峰時段或維護窗口期間進行，而不是在正常營運時間。這樣可以減少對用戶和業務流程的干擾。)

(C) ISO 27005 為提供關於技術遵循性審查之特定國際指引 (ISO/IEC 27005 是針對資訊安全風險管理的國際標準，主要提供風險評估和風險處理的指引，而不是專門針對技術遵循性審查。)

(D) 滲透測試或源碼檢測之結果，若有風險需判斷修補，可於下次再檢測時，確認實施結果 (發現安全風險後，應該**儘快進行修補**，並在**修補後立即進行驗證測試**，以確認漏洞已被修復。僅在下次再檢測時才確認修補結果存在很大的安全隱患，可能使系統長時間暴露於風險之中。 理想的做法是建立一個持續性的安全測試流程，定期進行安全評估和修補)

防護 112-2 答案A

29. 關於網路安全滲透測試的敘述，下列何者錯誤？

(A) 網路安全滲透測試是找出駭客實現攻擊目的的所有途徑，而駭客入侵只是要實現某一特地目的

(B) 逆向工程是網路安全滲透測試的一部分，目的是發掘系統的漏洞

(C) 網路安全滲透測試就是一般普遍認知的漏洞掃描 (這是最常見的誤解。**漏洞掃描**通常是指使用自動化工具掃描系統中已知的漏洞，例如軟體版本過舊、設定錯誤等，它是一種自動化的、非侵入性的安全評估方法。**滲透測試**則是一種更深入、更複雜的安全評估方法，它模擬真實的攻擊行為，嘗試利用漏洞入侵系統，並評估系統的整體安全狀況。滲透測試通常包含漏洞掃描，但遠不止於漏洞掃描。滲透測試還會利用如密碼猜解、社交工程等手法，並且嘗試橫向移動、提權等進階的攻擊行為，漏洞掃描只是滲透測試的一個步驟。)

(D) 網路安全滲透測試方法可以分成黑盒測試、灰盒測試、白盒測試等三種

防護 112-2 答案C

30. 關於源碼檢測的敘述，下列何者錯誤？

(A) 又稱靜態應用程式安全測試（Static Application Security Testing，SAST）

(B) 在安全系統發展生命週期（SSDLC）中，源碼檢測也是其中一項重要安全設計流程之一

(C) 主要目的是找出軟體程式碼中的安全問題或漏洞，這種測試通常在軟體的開發和維護階段進行

(D) OWASP ZAP 是常見源碼檢測工具之一 (OWASP ZAP (Zed Attack Proxy) 是一個常用的 **動態應用程式安全測試 (DAST)** 工具，而非靜態的源碼檢測工具。ZAP 主要用於在 Web 應用程式執行時，對其進行滲透測試和漏洞掃描)

防護 112-2 答案D

31. 關於資安健診的敘述，下列何者較「不」正確？

(A) 一種對組織的資訊系統與網路環境進行全面普查的過程，以評估其對各種威脅的抵禦能力

(B) 可以幫助企業或組織發現安全漏洞，增強企業對內外部威脅的抵禦能力

(C) 國際知名的SecurityScorecard 公司，通過完成對網路威脅情報探測的評分分析來評估公司實體的網絡安全狀況，也是一種資安健診

(D) 僅透過弱點掃描手法完成資安健檢

防護 112-2 答案D

(資安健診（資安健康檢查）通常包含多種評估方法，不僅僅是弱點掃描。除了弱點掃描，資安健診還可能包括滲透測試、配置檢查、政策和程序評估、社會工程測試等多種方法，以提供全面的安全評估。因此，僅依賴弱點掃描無法全面反映系統的整體安全狀況，這使得選項 D 描述不夠完整和準確。)

33. 企業為了檢查自己是否會被已知的弱點攻擊，通常會定期安排弱點掃描，以便檢查是否有應用程式或作業系統的漏洞出現在企業的環境中。下列何項「不」是常見的弱點掃描工具？

(A) OSV-Scanner

(B) Nessus

(C) OpenVAS

(D) Masscan

技術 112-2 答案D

(**Masscan** - **不是**弱點掃描工具，而是一個**網路埠掃描器**。Masscan 是一個非常快速的網路掃描工具，可以快速掃描大量 IP 位址和埠，用於發現網路上開放的服務。雖然 Masscan 的結果可以間接幫助識別可能存在漏洞的主機，但它本身並不進行漏洞檢查。)

2. 以下何者為通用型的弱點掃描工具（Vulnerability Scanner）？

(A) Nmap

(B) OpenVAS

(C) OWASP

(D) SCAP

技術 112-1 答案B

4. 下列哪些是目前 2021版 OWASP Top 10中所包含的前10種常見風險類別？（複選）

(A) 權限控制失效（Broken Access Control）(A01:2021)

(B) 跨站請求偽造（Cross-Site Request Forgery） (A05:2017)

(C) 注入式攻擊（Injection）(A03:2021)

(D) 加密機制失效（Cryptographic Failures）(A02:2021)

防護 112-1 答案A、C、D

19. 請問 Metasploit 是下列何種用途的工具或平台？

(A) SQL Injection工具

(B) XSS工具

(C) 滲透測試平台

(D) 原始碼掃描工具

技術 112-1 答案C

27. 關於程式原碼檢測（Code review）的敘述，下列何者錯誤？

(A) 通過檢查軟件程式的源代碼，發現和解決其中存在的潛在問題和漏洞

(B) 無助於開發人員在軟體開發及時發現並修復問題，從而提高軟體的質量和可靠性

(C) 可以查找內存泄漏、緩衝區溢出、程式碼注入等問題

(D) 代碼審查一般會分為三類：正式的代碼審查、結對程式，以及輕量型的非正式代碼審查

技術 112-1 答案B

(有助於開發人員在軟體開發及時發現並修復問題，從而提高軟體的品質和可靠性

正式代碼審查（如 Fagan Inspection）：結構化流程，需會議記錄與檢查表。

結對程式（Pair Programming）：兩人實時協作，邊寫邊審查。

輕量型非正式審查（如 Pull Request 審查）：透過工具（如 GitHub）進行簡易審查。

)

29. 請問 CVSS（The Common Vulnerability Scoring System）是指下列何項？

(A) 常見漏洞和風險編號 (CVE)

(B) 弱點種類 (CWE)

(C) 弱點計分系統 (CVSS)

(D) 漏洞修補建議 (NVD)

技術 112-1 答案C

30. 下面何項「不」是源碼檢測工具？

(A) SonarQube

(B) Checkmarx

(C) Fortify

(D) Nexpose (漏洞掃描工具)

防護 112-1 答案D

33. 關於「弱點掃描」的描述，下列何者最「不」正確？

(A) 此作業可能會觸發入侵偵測系統的警告

(B) 可部署 Web應用程式防火牆，來避免弱點掃描的探測

(C) 是滲透測試（Penetration Test）常見的前置作業之一

(D) Ping工具的使用，是弱點掃描常用前置作業之一

技術 112-1 答案B

(弱點掃描通常是針對主機型的，部署 Web應用程式防火牆只能對Web應用進行防禦)

17. 下列何者「不」是攻擊者常見用來下載外部後門的指令？

(A) WGET

(B) CURL

(C) FTP

(D) PING

技術 111-2 答案D

(PING是偵測對方主機有無在線上指令)

20. 下列何項駭客工具可以傾倒（dump）記憶體裡登入過的帳號密碼？

(A) mimikatz

(B) SQLmap

(C) Burp Suite

(D) AppScan

技術 111-2 答案A

29. 請問 CWE（Common Weakness Enumeration）是指下列何項？

(A) 常見漏洞和風險編號 (CVE)

(B) 弱點種類 (CWE)

(C) Exploit Code (攻擊者用來利用特定漏洞的程式碼，如Metasploit模組)

(D) 漏洞修補建議 (NVD)

技術 111-2 答案B

31. 資安管理人員可以利用下列何種資訊來源來尋找設備裝置、作業系統與應用程式的弱點（Vulnerabilities）相關資訊？

(A) OWASP（Open Web Application Security Project）

(B) Bugtraq

(C) Global Vulnerabilities Lis（GVL）

(D) Common Vulnerabilities and Exposures（CVE）

技術 111-2 答案D

1. 關於Nmap工具之指令操作，下列敘述何者正確？

(A) Nmap的 SYN掃描可以掃描 UDP埠 (SYN 掃描不適用於 UDP 埠)

(B) Nmap使用 -T1參數較 -T4參數的掃描速度快 (Nmap 的計時模板（-T）參數從 0 到 5數字越大掃描速度越快)

(C) Nmap使用 -sO參數可檢測標的主機的作業系統版本 (-sO 是 IP protocol scan，用於協議掃描，檢測作業系統版本應使用 -O 參數)

(D) Nmap使用 -D參數為誘騙掃描（decoy scan） (這個功能通過添加假冒的來源 IP 地址來隱藏實際的掃描來源，增加掃描的匿名性)

防護 111-1 答案D

4. 下列何者為探測通訊埠（Port）的軟體？

(A) Appscan

(B) Nmap

(C) Burp Suite

(D) Telnet

技術 111-1 答案B

5. 請問下列何種工具常被用來建立 Backdoor

(A) telent

(B) ipconfig

(C) NC (NetCat)

(D) cat

技術 111-1 答案C

(NC (Netcat)：因其靈活性，常被用來監聽埠口、建立反向Shell，是典型的後門工具)

10. 在網站平台開發時弱點管理的範疇中時常需要進行源碼檢測、弱點掃描、滲透測試；源碼檢測目的是透過對原始碼的檢查，挖掘已知或未

知的網頁問題，而進行弱點掃描的目的為何？

(A) 驗證所知弱點的可行性 (滲透測試目的)

(B) 以駭客或惡意使用者的角度對目標進行驗證 (滲透測試目的)

(C) 檢測程式中的商業邏輯問題 (手動審查代碼)

(D) 檢測在環境與系統上的錯誤

防護 111-1 答案D

15. 關於軟體組成分析（Software Composition Analysis），下列敘述何者「不」正確？

(A) 可透過分析來識別所使用第三方/開源軟體，其所存在的風險或

威脅

(B) 「軟體組成分析」為源碼檢測其一類型， 主要分析軟體是否存在

開發語法缺陷 (軟體組成分析（SCA）並不專注於檢測源碼中的開發語法缺陷，而是專注於第三方和開源組件的安全性和合規性)

(C) 所分析的風險因子包括，如：元件過期、已知弱點、程式庫信

任、軟體授權等

(D) 「軟體透明度」能提升分析準確性，可透過如 SBOM 標準來發

佈與交換資訊

防護 111-1 答案B

26. 在 OWASP Top 10 2021中，其A6項目說明使用含有已知漏洞的元

件。而在軟體開發時，為減少A6項目的發生，下列何種作法較佳？

(A) 限制可以使用的元件

(B) 使用強的加密演算法

(C) 使用入侵防禦系統

(D) 限制使用的網路埠

技術 111-1 答案A

(在OWASP Top 10 2021中，A6項目（使用含有已知漏洞的元件）的防範重點在於管理和控制軟體元件的安全性)

27. 下列何者「不」屬於滲透測試之手段？

(A) 社交攻擊

(B) 密碼破解

(C) 弱點掃描

(D) 分散式服務阻斷攻擊

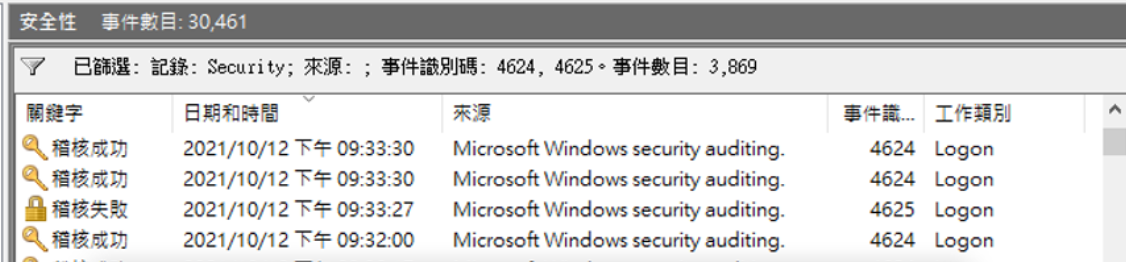
技術 111-1 答案 D

(滲透測試重點是潛入系統偷取資料，而非破壞可用性)

日誌管理

**日誌管理：**

* 日誌保存基本原則
  + 異地備份：日誌應存放於本機以外，防止竄改與遺失
  + 即時監控：使用 SIEM 工具進行分析(如 Splunk)
  + 必要資訊：裝置的來源、時間、使用者、來源/目的、動作、結果
  + 使用目的：故障排除、合規性記錄、支援威脅檢測、安全性問題確認等目的
  + 傳輸加密：由於日誌通常會傳輸到日誌伺服器，因此傳輸當中應該要加密處理
  + 容量控管：是否有容量控管的機制，比方說硬碟滿了從最後一筆開始寫入
* Windows 事件管理(Event Viewer)
  + 預設位置：%SystemRoot%\System32\winevt\Logs\
    - 系統日誌：系統運作相關（驅動程式、服務狀態）
    - 應用程式日誌：應用程式錯誤與警告資訊
    - 安全性日誌：重要安全事件（登入登出、權限變更）
    - 設定日誌：系統設定變更（軟體安裝、系統更新）
  + 常見事件 ID：4624(登入成功)、4625(登入失敗)
  + 可擴充性：可自行擴充其他類型



* Linux事件管理
  + /var/log/lastlog：所有用戶「最後一次登入」時間。指令lastlog(二進制檔案，不可用 vi 看)
  + /var/log/wtmp：成功登入記錄。指令 last(二進制檔案，不可用 vi 看)
  + /var/log/btmp：失敗登入記錄。指令 lastb(二進制檔案，不可用 vi 看)
  + /var/log/messages (RHEL) 或 syslog (Debian)：通用系統訊息（核心、服務、硬體）
  + /var/log/secure (RHEL) 或 auth.log (Debian)：認證與安全事件（SSH、SUDO、PAM）
  + /var/log/audit/audit.log：系統稽核記錄
* Apache vs. IIS 日誌格式筆記
  + Apache範例：192.168.1.1 - - [10/Dec/2023:14:30:45 +0800] "GET /index.html HTTP/1.1" 200 1234 "https://example.com" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
    - 解讀：IP 192.168.1.1在 2023年12月20日+8時區請求 /index.html，狀態碼 200，傳輸 1234 位元組。來自 https://example.com，使用 Windows 的 Firefox 瀏覽器。
  + IIS範例：
    - 2023-12-10 06:30:45 203.0.113.45 GET /products/item1 - 80 - 192.168.1.2 Mozilla/5.0+(Windows+NT+10.0) 200 0 0 234
    - 解讀：客戶端 192.168.1.2 於 2023-12-10 06:30:45（UTC）請求埠號80的資源 /products/item1。狀態碼 200，耗時 234 毫秒，使用 Windows 瀏覽器。

**資通安全管理法要求**

* 管理重點
  + 保存期限：按照業務需求和法規，例如：資通安全法規定保留 6 個月
  + 存取控制：限制日誌讀取與修改權限
  + 時間同步：確保所有系統時間一致 (NTP)
  + 定期備份：建立日誌備份機制
  + 異常監控：注意異常登入與存取行為

**考古題：**

21. 某「安全性資訊與事件管理」（簡稱SIEM）系統依照The Syslog Protocol（RFC5424）標準設計，因事件眾多，希望只顯示必須立即採取行動或系統無法使用，這類極為嚴重的訊息在特定的畫面上，請問其篩選條件下列何者最為合適？

(A) Severity <= 1

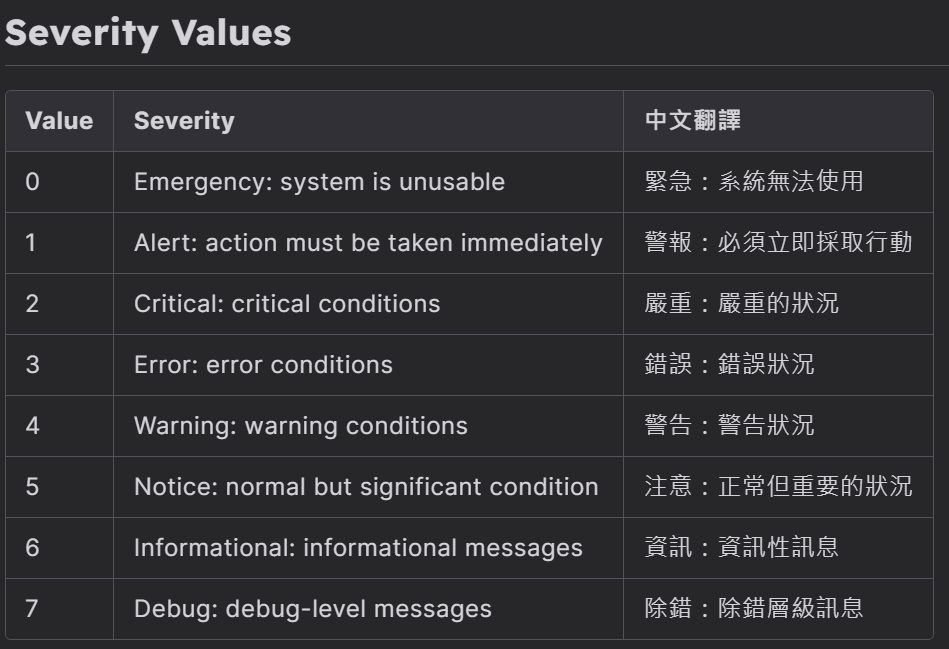
(B) Severity <= 3

(C) Severity <= 5

(D) Severity <= 7

114-1 防護 答案A

(根據 RFC5424 定義，Syslog 的嚴重性等級從 0（Emergency，系統無法使用）到 7（Debug，除錯資訊）。我們希望只顯示必須立即採取行動或系統無法使用的訊息，這對應於 0（Emergency）和 1（Alert）的等級。使用篩選條件 "Severity <= 1" 能夠確保只顯示這兩個最嚴重的等級，而其他較低嚴重性的訊息則被排除。因此，選項 (A) 最為合適。)



36. 資料庫伺服器時間校正功能發生狀況的風險問題，最應加強下列哪幾項控制措施？（複選）

(A) 事件分析 (當資料庫伺服器時間校正出現問題時，進行事件分析能夠協助追蹤並辨識異常狀況，以便迅速釐清問題根源)

(B) 時間同步 (這是直接針對時間校正功能的控制措施，確保系統內各項操作與記錄皆能維持正確的時間一致性)

(C) 網路連通監控 (由於時間同步通常依賴網路連線與外部時間伺服器，因此監控網路連通性有助於及早發現連線異常，進而防止時間同步失效)

(D) 存取控制 (雖然也是重要的安全措施，但與資料庫伺服器的時間校正問題並無直接關聯)

規劃 114-1 答案ABC

15. 關於Linux檔案的敘述下列何者錯誤？

(A) /etc/shadow：儲存使用者密碼的Hash值

(B) /bash\_history：使用者登入的歷史紀錄

(C) /var/log/secure：檔案用於記錄與安全相關的所有事件，包含使用者登入紀錄

(D) /.ssh/known\_hosts：記錄對方連線主機的指紋資訊

技術 113-2 答案B

(~/.bash\_history (注意開頭的波浪號 ~ 代表家目錄) 記錄的是**使用者在 Bash shell 中執行過的指令歷史**，而不是登入歷史。每個使用者在其家目錄下都有一個自己的 .bash\_history 檔案。登入歷史通常存於 /var/log/wtmp、lastlog 或 /var/log/auth.log（依系統而定）)

39. 關於Linux日誌的相關描述，下列何者錯誤？

(A) /var/log/boot.log記錄開機時系統核心偵測與啟動硬體，及各種核心支援的功能啟動等，只存放當次開機的資訊

(B) /var/log/cron記錄crontab排程有沒有實際被進行

(C) /var/log/dmesg記錄系統在開機的時候核心偵測過程所產生的各項資訊

(D) /var/log/messages記錄系統上面所有的帳號最近一次登入系統時的相關資訊

技術 113-2 答案D

(而最近一次登入資訊可以使用 lastlog 命令查看，該資訊儲存在 /var/log/lastlog 檔案中)

40. 關於日誌管理會收攏許多Log記錄的敘述，下列何者正確？

(A) Web網站日誌只收集網站流量和使用者活動的資訊，無法用在效能調教或是駭客入侵鑑識

(B) 網頁應用程式防火牆安全日誌，可以收到駭客惡意攻擊的訊息，無法探測潛在的漏洞攻擊活動

(C) 應用程式日誌，除可以記錄應用程式的錯誤訊息，也有機會用於除錯與效能的調校

(D) 作業系統日誌，以Windows Event Log類型來說，只可以收集安全、應用程式、系統等三類型記錄，無法自定義相關日誌

技術 113-2 答案C

(選項ABD最後一句都錯了)

41. 有效管理來自伺服器、網路設備及應用程式等各種來源的日誌資訊可以提升資料的安全性並檢測威脅。請問下列有關日誌管理的描述何者有誤？

(A) 不同網路設備的日誌格式不同，Windows Event Viewer就沒辦法直接開啟Linux系統的日誌

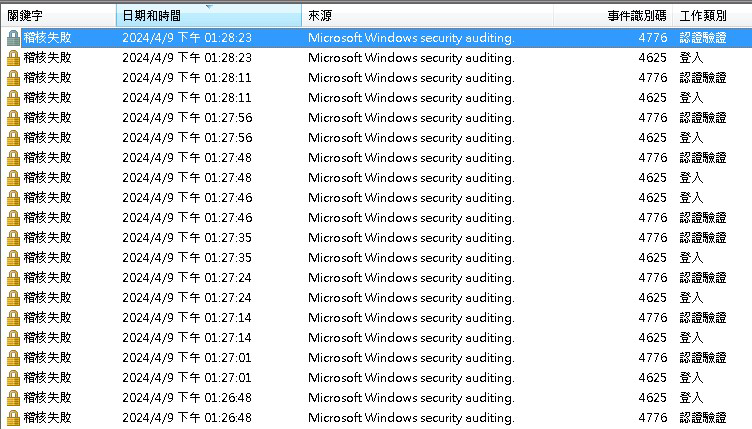
(B) 依據「資通系統防護基準驗證實務」規定，日誌的保存期限至少為3個月 (6個月)

(C) 任何發生在機關資通系統中可觀察到行為之結果稱為資通系統事件，應當具備有記錄特定事件之功能，並決定應記錄之特定資通系統事件

(D) 日誌應記錄資通系統管理者帳號所執行之各項功能

技術 113-2 答案B

42. 最近某工程師發現他的電腦十分緩慢，當其查看事件檢視器如附圖，請問從附圖中的資料，可以確認的結論為下列何項？



(A) 該電腦已經被入侵成功

(B) 有人嘗試登入該電腦，但都失敗

(C) 該電腦應該沒有問題

(D) 電腦中了木馬

技術 113-2 答案B

(Event ID 4625 為登入失敗的紀錄)

43. 在日誌管理中，為了確保操作行為能被追蹤並歸責到特定使用者，下列哪一項做法較「不」適當？

(A) 使用唯一識別符碼，以確保使用者身份唯一

(B) 記錄每次操作的時間、使用者ID和具體動作

(C) 對所有事件，包括正常與異常行為，均進行詳細記錄

(D) 系統日誌的存取應妥善保護，並由最高權限的管理員帳戶維護管理

技術 113-2 答案D

(應將日誌存取權限與管理職責分離（如設置唯讀權限、獨立稽核角色或異地備份），而非僅由單一高權限帳戶控制。)

23. 在勒索軟體事件中，下列哪些日誌的來源可能找到入侵的紀錄或警訊？（複選）

(A) 網路面資安防護設備

(B) 重要主機之作業系統事件

(C) 防毒軟體告警

(D) 門禁進出紀錄 (雖然門禁進出紀錄可以反映人員的實體進出，但在勒索軟體事件中，通常與網路入侵的關聯性較低。除非有證據表明攻擊者是透過實體入侵的方式植入勒索軟體，否則門禁紀錄不太可能提供直接的入侵線索)

防護 113-1 答案 ABC

40. 公司的官網受到駭客入侵，必須從官網 IIS Log File來追蹤駭客來源以及手法，關於 IIS Log File的敘述，下列何者錯誤？

(A) IIS預設 log路徑為%SystemDrive%\inetpub\logs\LogFiles\

(B) IIS如果有多個網站網站的 log會在資料夾中以u\_exyymmdd.log的 log檔呈現

(C) 在預設狀態下， IIS預設的日誌時間與台灣時間是一致的

(D) IIS提供了4種日誌檔格式（1）IIS紀錄檔格式、（2）NCSA紀錄檔案格式、（3）W3C紀錄檔格式、（4）自定義日誌檔案格式

技術 113-1 答案C

(預設的 W3C 格式 IIS 日誌檔案時間是 UTC 時間，而不是台灣時間)

42. 下列何項為應用系統日誌管理的主要目的？

(A) 加速系統的運作

(B) 用於故障排除、合規性記錄、支援威脅檢測、安全性問題確認等目的

(C) 監控系統用戶的操作

(D) 監督系統運用的效能

技術 113-1 答案B

42. 關於系統稽核日誌的保護機制敘述，下列何者正確？

(A) 稽核日誌紀錄留存的時間，應以設備硬體空間能儲存多久的時間而制定

(B) 系統管理與使用者，需要參考稽核日誌的結果，所以存取權限設定可予以開放

(C) 因應系統稽核日誌也是資訊安全事故的有效證據，所以控管存取權限是最重要的議題

(D) 當保留稽核日誌紀錄受到防毒軟體的限制時，可考量不予以留存

管理 113-1 答案C

(A錯在不應以硬體空間決定保存時間，還需考慮法規和公司政策

B錯在不應開放存取權限，避免被修改和刪除

D錯在不能因防毒軟體限制就不留存)

22. 請問Windows作業系統中，若需記錄使用者於本機登入失敗的相關記錄，下項描述何者正確？

(A) 無需設定可以直接透過事件檢視器（Windows Event Viewer）查看 (送分原因應該是因為部分會開啟)

(B) 需要事先透過稽核原則（登出/登入）設定確認啟用 ( 要記錄使用者在本機登入失敗的相關記錄，必須在「本機安全性原則」或「群組原則」中啟用「稽核登入事件」的「失敗」選項。路徑通常是： 電腦設定 -> Windows 設定 -> 安全性設定 -> 本機原則 -> 稽核原則 -> 稽核登入事件，選擇 失敗。)

(C) 當使用者輸入不正確的密碼時，會在金鑰發佈中心（KDC）上產生672 事件 (事件 ID **672** 與 Kerberos 的金鑰發佈中心（KDC）相關，主要用於記錄 Kerberos 預認證失敗的事件。然而，對於一般的本機登入失敗，應該是事件 ID **4625** 來記錄。因此，這個選項不完全正確。)

(D) 可以透用事件4634來查看登入失敗的事件 ( 事件 ID 4634 表示帳戶已登出，是用來記錄成功登出的事件。登入失敗的事件 ID 是 **4625**。)

防護 112-2 答案A、B

39. 企業透過日誌管理，處理大量且複雜的日誌資訊（例如：logs & events）IT部門或是資安部門將這些記錄使用在容量監控管制、故障排除、合規性記錄留存、資安威脅檢測與鑑識…等目的，關於日誌管理的敘述，下列何者錯誤？

(A) 可用於事件取證，日誌資訊對於原因的判別是關鍵點，而在還不確定原因之前，則需要全面性的收集日誌資訊

(B) 為了滿足不同的法規規範，日誌成為稽核重要的參考資料 (資通安全法要求日誌保留六個月)

(C) 日誌管理，可以用在事件警示，卻不適用在 SOC（Security Operation Center）管理

(D) 沙賓法案（SOX）或是醫療保險相關法案（HIPAA）這一類的法遵，都會要求讓日誌成為重要稽核軌跡（audit trail）

技術 112-2 答案C

(日誌管理是 SOC 運營的核心組成部分。SOC 團隊依賴日誌資料來進行安全監控、威脅檢測、事件響應和調查等工作。日誌管理系統（如 SIEM）是 SOC 的關鍵工具，用於收集、分析和關聯來自各種來源的日誌資料，以識別安全威脅和異常行為。)

40. 關於Linux系統日誌資料的敘述，下列何者正確？

(A) /var/log/lastlog記錄系統中所有用戶最後一次的登錄時間。可直接用 vi查閱，但需搭配使用 lastlog命令進行 (/var/log/lastlog 確實記錄用戶最後一次的登錄時間，但該文件為二進制格式，無法直接用 vi 查看，必須透過 lastlog 命令讀取。因此描述中「可直接用 vi 查閱」是錯誤的)

(B) /var/log/cron記錄與系統設定任務相關的日誌

(C) /var/log/dmesg記錄系統關機時，內核自我檢查資訊，也可以使用 dmesg命令直接查看內核自檢資訊 (/var/log/dmesg（或部分系統中的 /var/log/boot.log）主要記錄系統啟動時的內核訊息，而非關機時的自我檢查資訊。雖然 dmesg 命令可用於查看內核緩衝區的訊息，但前半段關於「關機時」的描述錯誤。)

(D) /var/log/secure記錄郵件資訊的日誌 (記錄與系統安全相關的日誌（如 SSH 登入、sudo 操作），而非郵件資訊。郵件日誌通常存放於 /var/log/maillog)

技術 112-2 答案B

41. Windows Event Log是重要稽核與資安鑑識記錄檔，關於 Windows Event Log的敘述，下列何者錯誤？

(A) windows event log預設位置為：%SystemRoot%\System32\winevt\Logs\

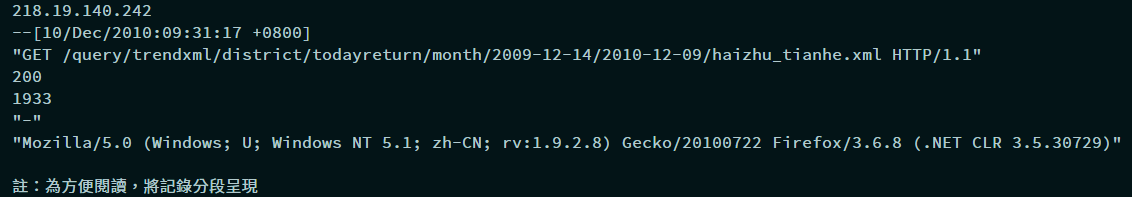
(B) 關於 windows event log相關設定與調整在：HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog

(C) windows event log只有三類，無法再擴充其他類型 event log (從 Windows Vista/Server 2008 開始，支援自定義事件日誌)

(D) 以Security.evtx為例， 包含主機的 Login/Logout資訊，還有其他 安全事件相關的log

技術 112-2 答案C

42. 如附圖所示，關於此筆 Apache記錄的敘述，下列何者錯誤？



(A) 218.19.140.242這是一個apache伺服器的local端 IP (Remote端IP)

(B) [10/Dec/2010:09:31:17 +0800]格式為[day/month/year:hour:minute:second zone]，最後的 +0800表示伺服器所處的時區

(C) 1933表示伺服器向客戶端傳送多少位元組，把這些位元組加起來得知伺服器在某點時間內總的傳送資料量

(D) "Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9.2.8) Gecko/20100722 Firefox/3.6.8 (.NET CLR 3.5.30729)" 這項主要記錄客戶端的瀏覽器資訊

技術 112-2 答案A

43. 關於「日誌管理」的敘述，下列何者錯誤？

(A) 日誌管理不會與法律合規性有任何關連性 (資通安全法要求日誌除了保留六個月外還要有一定的控管機制)

(B) 日誌未安全存放，很有可能被駭客或惡意破壞者刪除或修改

(C) 安全資訊和事件管理（Security Information and Event Management，SIEM）其中功能是達成降低資安威脅

(D) 透過日誌管理系統統一分析，可以用在鑑識攻擊事件追蹤分析

技術 112-2 答案A

25. 關於應用程式日誌管理保存的敘述，下列何者最「不」適當？

(A) 日誌必須儲存於本機以避免資料外流

(B) 日誌格式須確保被能被所使用之日誌管理方案支援

(C) 日誌須定期分析與監控，以即時發現可疑活動

(D) 日誌須留存足夠資訊以有效識別，如：時間、來源 /目的、動作 ..等

技術 112-1 答案A

(日誌應存放於本機以外，防止竄改與遺失)

31. 為避免人員舞弊與資訊安全系統監控相關議題的敘述，下列何項「不」正確？

(A) 資訊安全監控時，系統留存稽核日誌應保存完整，以防止未經授權的存取

(B) 資訊安全事故發生時，應由責任負責同仁盡速通報

(C) 資訊系統日誌都會包含大量資訊，且內容多數與資訊安全監視無關。宜考量以工具識別重要事件作為審查資訊

(D) 由系統或網路管理者管理稽核日誌 (為了防止舞弊和確保稽核日誌的客觀性，應該將稽核日誌的管理權限與系統或網路管理者的權限分開。系統或網路管理者可能有能力修改或刪除自己的操作記錄，這會破壞稽核日誌的可靠性。最佳實務是由獨立的安全團隊或稽核人員來管理稽核日誌)

防護 112-1 答案D

40. 若某公司以 UDP port 514的方式，遠端蒐集 Syslog進行日誌留存，請問下列敘述何者最正確？

(A) 遠端蒐集之日誌，無法作為有效證據 (只要能證明證據監管鏈就可以)

(B) 網路流量大時，有可能遺失封包（資料）(因為UDP是屬於一種非可靠的傳輸方式)

(C) Syslog無須考量加密即可保護資料傳輸之安全 (可以使用替代的TLS/SSL Syslog (通常使用 TCP Port 6514)達到傳輸加密)

(D) 遠端蒐集之日誌，存放時不應加密，以免破壞資料的正確性 (要使用加密保證儲存資料的機密性)

技術 112-1 答案B

42. 下列何項為應用系統日誌管理的主要目的？

(A) 加速系統的運作

(B) 用於故障排除、合規性記錄、支援威脅檢測、安全性問題確認等目的

(C) 監控系統用戶的操作

(D) 監督系統運用的效能

技術 112-1 答案B

43. 日誌的功能是幫助資訊安全維運人員進行系統除錯、稽核取證與行為歸責的重要依據。請問下列描述何者錯誤？

(A) 記錄的內容包括設備的作業系統、發生的日期與時間、資料流量、使用者身份資料等

(B) 不同的資安設備可能產生不同的日誌格式，增加即時追蹤的困難度

(C) 將日誌存放在公開的儲存空間，可以提高判讀的速度

(D) 透過系統設定，系統可以根據日誌得到的資訊向監控者傳送警報訊息。

技術 112-1 答案C

(日誌需要設定特定的存取權限，以保持機密性)

16. 在現行 Fedora/CentOS/RHEL Linux中記錄登入系統如SSH （Secure Shell）等遠端連線登入紀錄為下列何者？

(A) /var/log/secure

(B) /var/log/messages

(C) /var/log/wtmp

(D) /var/log/null

技術 111-2 答案A

42. 關於Syslog的敘述，下列何者錯誤？

(A) 可以被以UDP協定及TCP協定來傳送

(B) 通常被用於資訊系統管理及資安稽核

(C) 無法透過SSL或TLS方式加密

(D) 是一種用來在TCP/IP網路中傳遞記錄檔訊息的標準

技術 111-2 答案C

(雖然傳統的 Syslog 預設使用明文傳輸（基於 UDP 或 TCP），但現代 Syslog 已支持透過 TLS（Transport Layer Security）加密，例如 RFC 5425 明確規範了 Syslog 使用 TLS 加密的標準（稱為 Syslog-TLS）)

43. 關於「系統日誌」 的敘述下列何者錯誤？

(A) 防止系統日誌被未經授權的存取

(B) 防止侵害個人隱私，不儲存可識別使用者的資訊

(C) 需防範日誌記錄檔被修改或刪除

(D) 需留意不超過儲存媒體的最大容量

技術 111-2 答案B

(系統日誌需記錄使用者操作（如登入紀錄、操作行為）以進行稽核或追蹤問題，因此需儲存可識別資訊（如使用者ID）。但需注意隱私保護（如存取控制、匿名化、最小蒐集原則或加密），而非完全「不儲存」)

26. 關於日誌與監控作業，下列敘述何者較「不」正確？

(A) 日誌應記錄使用者活動、異常，並且依法定要求的時間保存

(B) 系統日誌為避免外洩，應在發生資安事件時才查詢，平日不應存

取

(C) 日誌應避免可被該系統管理人員修改

(D) 資訊處理系統、網路設備的鐘訊，應與議定的準確時間來源同步

管理 111-1 答案B

(平時就要主動監控異常行為)

19. 請問若某公司，將存有機密性資料系統的日誌，以 Syslog的方式透

過網際網路（Internet）傳輸到30公里之外的異地備援機房，請問就安全的考量上來說，下列議題，何者最需優先處理？

(A) 備援機房的進出管理

(B) 日誌審查（Log Review）的頻率

(C) 傳輸過程的加密/保護

(D) 30公里的距離過遠

技術 111-1 答案C

31. 「系統管理員將所有稽核日誌存放於另一台獨立的日誌伺服器（ Log Server），並由非管理系統之人員管理該伺服器。」下列何者為其最重要的目的？

(A) 強化機密性

(B) 保護日誌

(C) 避免 SQL Injection攻擊

(D) 降低分析資安事故的時間

技術 111-1 答案B

42. 在Linux系統中，下列何檔案存放了「使用者的登入歷史紀錄」？

(A) /var/log/wtmp

(B) /var/log/messages

(C) /etc/login.defs

(D) /var/log/dmesg

技術 111-1 答案A

資料庫

情境背景

某醫院資料庫儲存患者就診紀錄，包含以下欄位：

* 非機密資料：年齡、性別、就診日期、診療科別、藥物名稱、檢查項目
* 機密資料：患者姓名、身分證字號、確診疾病名稱

---

案例一：資料庫聚合（Aggregation）

操作方式

攻擊者執行以下查詢：

1. 統計「2023年1月」於「腫瘤科」就診的「30-40歲女性」人數 → 得到 50人
2. 查詢同一時段腫瘤科開立的「標靶藥物A」總數量 → 得到45份

結果與機密性

* 單一查詢結果：人數或藥物數量均為非機密資料。
* 組合後推導：

「50名患者 vs. 45份藥物」→ 推論出90%患者使用標靶藥物A

→ 可能揭露「該科別主要治療癌症類型」（如乳癌），屬機密資訊。

關鍵特徵

* 直接組合現有資料，無需外部知識或複雜推理。
* 資料的「加總」或「比例」直接產生敏感性。

---

案例二：資料庫推論（Inference）\*\*

操作方式

攻擊者執行以下查詢：

1. 查詢「患者X」的檢查項目 → 包含 BRCA1基因檢測（非機密）。
2. 結合外部知識：
   * BRCA1基因突變與「乳癌、卵巢癌」高度相關（公開醫學研究）。
   * 患者X近期於「婦科」有密集就診紀錄（非機密）。

結果與機密性

* 間接推導：患者X可能確診乳癌或卵巢癌（機密診斷）。

關鍵特徵

* 需依賴外部知識（BRCA1的醫學意義）。
* 透過邏輯連結非機密資料（檢查項目 + 就診科別）推論機密結果。

---

| 特性 | 聚合（Aggregation） | 推論（Inference） |
| --- | --- | --- |
| 資料來源 | 直接組合資料庫內多筆非機密資料 | 結合資料庫內非機密資料 + 外部知識或統計推理 |
| 機密性產生方式 | 資料「加總」或「比例」直接揭露敏感性 | 需邏輯推理或跨領域知識連結才能推導機密結果 |
| 防禦手段 | 限制統計查詢（如設定最小查詢閾值） | 模糊化資料粒度（如合併年齡區間、隱藏細節） |

23. 要管理好資料庫系統，除了對資料庫系統有深度認知之外，仍需要了解資料庫系統所面臨的安全威脅。下列何項較「不」屬於資料庫系統所面臨的安全威脅？

(A) 資料庫內資料外洩

(B) 資料庫內的資料遭非法篡改與偽造

(C) 資料庫推論（Database Inference）

(D) 資料庫管理人員不具有作業系統操作認證 (此選項涉及管理人員的資質或權限認證問題。若管理員缺乏操作系統的認證，可能導致配置錯誤或維護不當，但這更偏向「管理流程」或「人員訓練」的範疇，而非技術性的直接威脅。安全威脅通常指外部攻擊或內部濫用權限等具體行為，而非人員是否具備認證資格。)

113-2 技術 答案D

20. 為避免資料庫被入侵攻擊，下列何種處理方式最適合？

(A) 應用系統採用多因素身份驗證機制進行設計，可確保應用程式對資料庫存取身分

(B) 不用定期更新資料庫軟體版本，因為會影響程式相容性 (不更新軟體 會保留已知漏洞，使攻擊者可利用公開漏洞入侵系統。更新修補程式是基本防禦手段，此選項明顯錯誤。)

(C) 資料庫中的敏感資料不用加密，以提升效能 (未加密的敏感資料 一旦遭竊即直接暴露，加密雖可能輕微影響效能，但安全性優先。此選項忽略資料洩漏的風險，屬錯誤做法。)

(D) 資料庫多在內網，十分安全不需監視資料庫活動 (內網並非絕對安全，內部威脅（如員工濫用權限）或橫向移動攻擊（如APT攻擊）仍可能發生。缺乏監控將無法偵測異常行為（如大量資料讀取），此選項過度依賴網路邊界防護，風險極高。)

113-1 技術 答案A

34. 下列何項「不」是資料庫的資料加密方式？

(A) 資料遮罩（ Data Masking） (料遮罩是一種「脫敏」技術，通過遮蔽或替換敏感數據（如用\*\*\*\*隱藏部分數字），使數據無法被直接識別。其關鍵在於「不可逆性」，遮蔽後的數據通常無法還原，因此不屬於加密（加密需可逆）。此為匿名化手段，非加密方式。)

(B) 透明資料加密（Transparent Data Encryption，TDE） (TDE在存儲層自動加密整個資料庫（如數據文件、備份），無需應用層修改，且解密對用戶透明。屬於標準的資料庫加密技術。)

(C) 資料欄位加密

(D) 資料庫檔案加密

113-1 管理 答案A

35. 針對資料庫內外威脅所提出保護措施，下列敘述何者正確？

(A) 定期對存取資料庫的應用程式，進行源碼檢測以及Web黑箱檢測，降低駭客入侵風險

(B) MS-SQL資料庫其檔案格式一定是.bak的副檔名 (MS-SQL的備份檔案預設為.bak，但其他核心檔案如主資料檔（.mdf）、日誌檔（.ldf）並非此格式。此敘述錯誤，因混淆備份檔與其他檔案類型。)

(C) 企業資訊系統 MS-SQL資料庫，可以採用系統管理者帳號進行管理，不需要為個別資料庫獨立帳號密碼 (使用單一高權限帳號（如sa）管理所有資料庫，違反「最小權限原則」。若該帳號遭竊取或濫用，將導致全面性資料外洩或破壞。正確做法是為不同資料庫或角色建立獨立帳號，並限制權限範圍。)

(D) 身為多個 MS-SQL資料庫管理者，可採用同一組密碼，便於管控使用 (密碼重複使用會擴大單點失效風險（一組密碼外洩即危及所有資料庫），且違反「職責分離」原則。應為每個管理者分配獨立帳號與強密碼，並啟用多因素驗證（MFA）。)

112-1 技術 答案A

41. 資料庫類型很多，常見 MS-SQL資料庫，就有其日誌記錄，下列針對 MS-SQL資料庫日誌敘述何者錯誤？

(A) 錯誤記錄檔是位於 Program Files\Microsoft SQL Server\MSSQL. n \MSSQL\LOG\ERRORLOG和ERRORLOG

(B) MS-SQL資料庫仍需要定期 TRANSACT清除日誌

(C) MS-SQL交易記錄檔過大，透過 SQL Query來清除其語法 DBCC SHRINKFILE （'資料庫名稱 \_log ', 0, TRUNCATEONLY）

(D) MS-SQL記錄檔無法變更位置，因此我們必須預留相關磁碟空間，以及定期清理

112-1 技術 答案D

(MS-SQL 允許透過以下步驟變更日誌檔位置：

1. 使用 ALTER DATABASE 修改日誌檔路徑。
2. 重新啟動服務或離線移動檔案。

此選項明顯違反實際操作，屬錯誤敘述。)

21. 針對資料庫要進行事前告警、及時發現，以及事後分析追查可能的異常存取資安事件， 應導入下列何種資料庫安全防護措施？

(A) 資料庫加密

(B) 資料庫叢集

(C) 資料庫稽核 (稽核機制能全面覆蓋「事前監控告警、事中即時偵測、事後分析追蹤」的資安需求，是應對異常存取的核心防護措施。)

(D) 資料庫掃描

111-2 技術 答案C

23. 資料庫是企業內最重要的資產，身為資安人員該如何確保資料庫的安全，是一件非常重要的任務與責任。若是在存取資料庫中個別資料雖不具機密性，但連結數筆資料後卻可獲得機密資訊，是 下列 哪一種資料庫安全威脅？

(A) 資料庫管理系統（Database Management System）

(B) 資料庫分析（Database Analysis）

(C) 資料庫推論（Database Inference）

(D) 資料庫聚合（Database Aggregation） (題幹描述「連結數筆非機密資料後獲得機密資訊」屬於聚合（Aggregation），因直接組合資料即產生敏感性。若需透過推理或外部知識，則為推論（Inference）。因此答案為 (D)。)

111-2 技術 答案D

(資料庫推論（Database Inference）與資料庫聚合（Database Aggregation）的區別：

* 資料庫聚合（Aggregation）
  + 定義：通過組合多個非機密或低敏感度的資料項（如欄位、記錄、統計值等），直接形成具有機密性或高敏感度的資訊。
  + 特點：
    - 資料的「組合」本身直接導致敏感性提升，無需複雜推理。
    - 例如：單一員工的薪資非機密，但部門薪資總和與人數結合後可推算出平均薪資（機密）。
* 資料庫推論（Inference）
  + 定義：透過間接方式（如多次查詢、統計分析或結合外部知識），從非機密資料中推導出未授權的機密資訊。
  + 特點：
    - 需要邏輯推理或外部資訊的輔助，而非單純組合資料。
    - 例如：透過員工的職位、入職年份及公開薪資標準，推論出個人薪資。)

9. 某中小企業資訊部門之業務執掌包含程式開發、程式上線、應用程式管理以及資料庫管理等，該公司因故必須縮減資訊部門人力，若您是該企業之資訊部門主管，下列何種處理較無法降低資安風險的發生？

(A) 將部分資安工作移轉至其他業務單位 (將資安工作移交給其他業務單位看似能減輕資訊部門的負擔，但這可能帶來潛在的問題。其他業務單位通常專注於自身的業務目標，不一定具備資訊部門在資安方面的專業知識和技能。例如，若將資料庫管理或應用程式安全的任務移轉給不熟悉相關安全規範的部門，他們可能會因為缺乏經驗而誤設權限或忽略漏洞，進而增加資料外洩或系統被攻擊的風險。因此，這種做法不僅無法有效降低資安風險，反而可能因為責任分散和專業性不足而使其升高。)

(B) 增加業務活動之監視紀錄

(C) 增加資安稽核頻率

(D) 導入自動化資料庫稽核管理工具

111-1 規劃 答案A