

112 年度第 2 次 資訊安全工程師能力鑑定 中級試題

科目 2：I22 資訊安全防護實務

考試日期：112 年 8 月 12 日

第 1 頁，共 14 頁

單選題 15 題，複選題 5 題，題組題 5 題（佔 100%）

D	1. 關於 MITRE ATT&CK 中的橫向移動（Lateral Movement）戰術（Tactic），下列何項錯誤？ (A) 遠端服務破解（Exploitation of Remote Services）屬於此類戰術 (B) 內部魚叉釣魚（Internal Spearphishing）屬於此類戰術 (C) 橫移工具傳輸（Lateral Tool Transfer）屬於此類戰術 (D) 本地資料取得（Data from Local System）屬於此類戰術
C	2. 2022 年 8 月美國眾議院議長裴洛西（Nancy Pelosi）日前來台訪問，造成台灣有些公私部門遭受分散式阻斷服務攻擊（Distributed Denial-of-Service Attack，DDoS）。關於 DDoS 攻擊與當時事件的敘述，下列何者錯誤？ (A) 當時我國行政院數位發展部部長唐鳳提出的防禦方式是採取以 Web3 為主的不對稱防禦架構 (B) 當時我國政府為了解決此問題，利用「流量清洗」的方式去對抗，投入大量資源與成本多設專線去阻擋 (C) DDoS 攻擊可以分成消耗網路頻寬與擷取網路上傳輸封包資訊兩種動作 (D) 目前市面上有販售 DDoS 攻擊的服務，更加難以有效偵查 DDoS 攻擊
A B	3. 下列哪些攻擊手法可以透過遠端攻擊網路伺服器？（複選） (A) Ping Flooding (B) DDoS (C) 簡單配對攻擊（Secure Simple Pairing Attacks） (D) Wi-Fi MITM
	【題組 1】 <div>現在你是一間企業的資安專責人員。最近，你發現一個未被掌握的內部系統漏洞，而且發現了來自不明來源的異常網路流量。你的任務是分析這個威脅，並提出適當的回應策略。</div>
C	4. 【題組 1】 情境如附圖所示。針對這個不明的異常流量，第一

112 年度第 2 次 資訊安全工程師能力鑑定 中級試題

科目 2：I22 資訊安全防護實務

考試日期：112 年 8 月 12 日

第 2 頁，共 14 頁

	步你該如何確認本項威脅來源？ (A) 關閉所有的內部網路 (B) 通知所有員工有潛在的威脅 (C) 進行詳細的威脅與風險分析 (D) 立即去法院按鈴申告
B	5. 【題組 1】情境如附圖所示。在瞭解詳細的威脅情況後，第一步你需要與哪一個組織內部團隊合作？ (A) 市場行銷團隊 (B) 事件回應團隊 (C) 威脅分析團隊 (D) 行銷風險評估團隊
C	6. 【題組 1】情境如附圖所示。經過分析這個威脅來源是透過郵件附件進行攻擊的，這個攻擊手法對應到 Cyber Kill Chain 的哪一個階段？ (A) Weaponization (B) Installation (C) Delivery (D) Exploitation
A B C	7. 【題組 1】情境如附圖所示。承上題，在這樣的情況下，為了提高你的資訊安全防護並防止未來的攻擊，你可以採取下列哪些措施？（複選） (A) 增強員工的資訊安全意識，如定期的資訊安全訓練 (B) 強化網路監控以偵測不尋常的活動 (C) 建立並維護一個更新的災難恢復計畫 (D) 不斷地升級電腦硬體，即使沒有發現任何威脅
A	8. 當使用者利用帳號密碼登入系統時，密碼的儲存基本原則是不可以直接用明文方式存放於資料庫中，因此密碼通常利用加密（Encryption）或是雜湊（Hash）的方式進行編碼轉換。關於雜湊函數的敘述，下列何者錯誤？ (A) 雜湊原理是限制輸入長度為 8 字元以上並透過雜湊函數進行計算，計算後會得到一樣長度的密文

112 年度第 2 次 資訊安全工程師能力鑑定 中級試題

科目 2：I22 資訊安全防護實務

考試日期：112 年 8 月 12 日

第 3 頁，共 14 頁

	<p>(B) 常見的雜湊函數有 MD5、SHA-1 及 SHA-2 等</p> <p>(C) 輸入的原始字串只差一個字元，透過雜湊函數得到的結果會差異很大</p> <p>(D) 雜湊函數具有不可逆的特性，無法利用雜湊值計算取得原始資料</p>
A	<p>9. 根據常見的弱點類型，下列何種是 Web 應用程式最常見的安全弱點？</p> <p>(A) SQL Injection: SQL 注入攻擊</p> <p>(B) Distributed Denial-Of-Service: DDoS 攻擊</p> <p>(C) Local File Inclusion: LFI 本地端檔案內容揭露</p> <p>(D) Cross Site Request Forgery: CSRF 跨站請求偽造</p>
B	<p>10. 關於 MITRE ATT&CK 中的輸入擷取 (Input Capture) 技術，下列何項錯誤？</p> <p>(A) 無法使用預防控制 (Preventive Controls) 輕易緩解此技術</p> <p>(B) 無法透過觀察驅動程式載入 (Driver Load) 活動來偵測此技術</p> <p>(C) 可觀察系統註冊機碼 (Windows Registry) 活動來偵測此技術</p> <p>(D) 可觀察程序建立 (Process Creation) 活動與元資料 (Process Metadata) 來偵測此技術</p>
C	<p>11. 關於進行網路架構設計的敘述，下列何者較「不」適當？</p> <p>(A) 應區分內外網</p> <p>(B) 網站跟資料庫最好在不同網段</p> <p>(C) 目錄伺服器 AD 應該放在辦公網段</p> <p>(D) 可以透過 VLAN 切割網段</p>
C	<p>12. 在 Cyber Kill Chain 模型中，Delivery 階段通常包括下列何項攻擊手法？</p> <p>(A) 惡意軟體安裝</p> <p>(B) 網站水坑攻擊</p>

112 年度第 2 次 資訊安全工程師能力鑑定 中級試題

科目 2：I22 資訊安全防護實務

考試日期：112 年 8 月 12 日

第 4 頁，共 14 頁

	<p>(C) 電子郵件附件或內文 URL 連結</p> <p>(D) 帳號密碼填充攻擊</p>
<p>A</p> <p>B</p> <p>D</p>	<p>13. 為了進行有效的弱點管理並減少組織風險，下列哪些是必要的措施？（複選）</p> <p>(A) 定期進行弱點掃描</p> <p>(B) 使用最新的防毒軟體</p> <p>(C) 仔細研讀所有的軟體使用條款</p> <p>(D) 實施弱點修補管理流程</p>
<p>A</p> <p>B</p> <p>C</p>	<p>14. 關於 MITRE ATT&CK 中的瀏覽器會話劫持（Browser Session Hijacking）技術，下列哪些正確？（複選）</p> <p>(A) 可透過資安認知訓練（Awareness Training）來緩解此技術</p> <p>(B) 可分析登入會話（Logon Session）的產生狀態來偵測此技術</p> <p>(C) 可透過使用者帳戶管理（User Account Management）來緩解此技術</p> <p>(D) 僅能透過分析程序存取（Process Access）與程序修改（Process Modification）狀態來偵測此技術</p>
	<p>【題組 2】</p> <p>你是公司資安當責人員，今年度開始公司執行導入 ISO 27001 的管理制度，預計於今年 12 月通過認證，目前已經擬定了相關的政策、程序書，正在執行資產盤點及風險評估的階段。在資源有限的前提下，你發現了多個內部議題，而相關議題的提出者是公司內部主要的利害關係人，身為資安當責人員的你身兼多職，你必須以符合 ISO 27001 的分工組織來進行工作分配，在剛完成第二階文件的你，面對的挑戰有…</p>
<p>C</p>	<p>15. 【題組 2】情境如附圖所示，總經理提出當公司的核心資訊系統受到攻擊時，首先執行的步驟是下列何項？</p> <p>(A) 修復受影響的系統</p> <p>(B) 報告給執法機關</p> <p>(C) 確認並評估攻擊的範圍和影響</p>

112 年度第 2 次 資訊安全工程師能力鑑定 中級試題

科目 2：I22 資訊安全防護實務

考試日期：112 年 8 月 12 日

第 5 頁，共 14 頁

	(D) 通知所有受影響的客戶和使用者
C	16. 【題組 2】情境如附圖所示，承上題，資訊室同仁在導入 ISO 27001 的過程中，目前已經完成「風險評估」，而同仁正在啟動「實施控制」施行對策，你發現同仁跳過了一個管理流程，這個流程是下列何項？ (A) 建立風險接受準則 (B) 訂定資訊安全政策 (C) 建立風險處理框架 (D) 監控和檢查控制效果
A	17. 【題組 2】情境如附圖所示，承上題，負責作業安全的同事(OP)，在實施資訊安全防護機制時，下列何項你必須提醒該同仁考慮的因素？ (A) 組織的業務需求和目標 (B) 組織的市場競爭優勢 (C) 組織的企業形象 (D) 組織的投資組合
B C	18. 【題組 2】情境如附圖所示，承上題，資安小組在設定災難恢復目標時，負責資料備份與事件回應小組無法正確的擬定 RTO (Recovery Time Objective)，看來是負責資料備份的同仁誤解了 RTO 的定義，下列哪些是正確的？（複選） (A) RTO 決定了備份政策 (B) RTO 決定了復原政策 (C) 業務流程中斷到恢復到可接受的服務水平所需要的最大時間 (D) 資料備份從啟動到備份完成所需要的最短時間
B	19. 某廠商其日誌服務採用 syslog，該伺服器 A 另有透過防火牆強化保護，公司的伺服器 B 要傳輸日誌給伺服器 A 時，發現無法正常傳輸，但伺服器 B 透過 ping 確認其與伺服器 A 可以正常連線並取得回應，請問下列那項方案最合適解決此項狀況？ (A) 重新安裝伺服器 A 的 syslog (B) 於該防火牆放行目的埠號 514 的 UDP 流量

112 年度第 2 次 資訊安全工程師能力鑑定 中級試題

科目 2：I22 資訊安全防護實務

考試日期：112 年 8 月 12 日

第 6 頁，共 14 頁

	(C) 移除保護伺服器 A 的防火牆設備 (D) 將伺服器 B 移至與伺服器 A 相同的網段
C	20. 依照我國「資通安全事件通報及應變辦法」的規定，當發現一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改之情事時，公務機關知悉資通安全事件後，應依規定在多少時間之內完成損害控制或復原作業，並依主管機關指定之方式及對象辦理通知事宜？ (A) 12 小時 (B) 24 小時 (C) 36 小時 (D) 72 小時
D	21. 就勒索軟體事件而言，最有可能降低事件衝擊的控制措施為下列何項？ (A) 原始碼檢測 (B) 日誌分析 (C) 社交工程演練 (D) 離線資料備份
B	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 (B) 需要事先透過稽核原則（登出/登入）設定確認啟用 (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 (D) 可以透用事件 4634 來查看登入失敗的事件
A C D	23. 請問關於「安全性資訊與事件管理」（簡稱 SIEM）的描述，下列哪些較正確？（複選） (A) 可協助組織在威脅傷害企業營運之前，先進行偵測、分析和回應安全性威脅 (B) 缺乏記錄管理的功能

112 年度第 2 次 資訊安全工程師能力鑑定 中級試題

科目 2：I22 資訊安全防護實務

考試日期：112 年 8 月 12 日

第 7 頁，共 14 頁

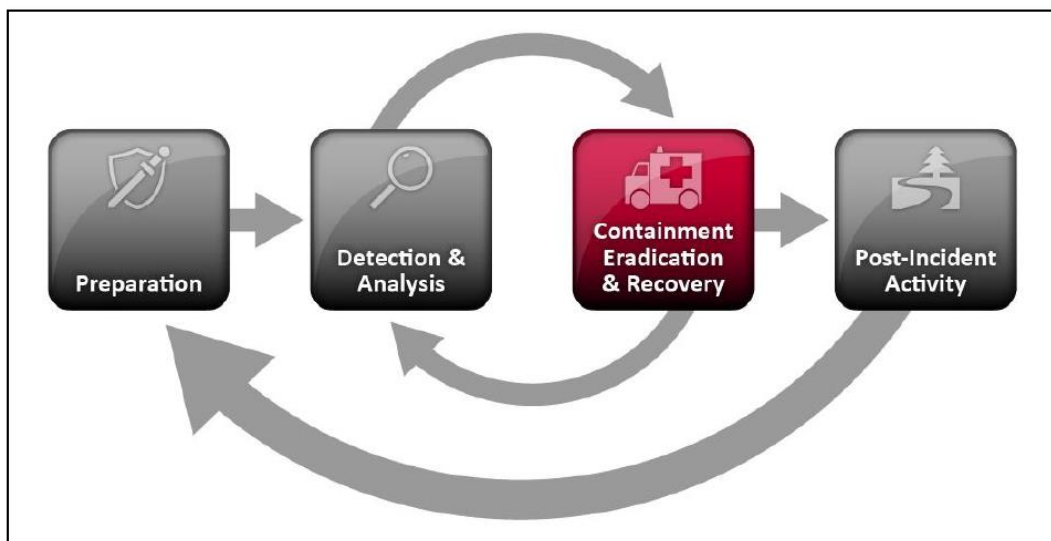
	<p>(C) 讓組織就可以迅速回應潛在的網路攻擊，並滿足合規性要求</p> <p>(D) 結合了安全性資訊管理 (SIM) 和安全性事件管理 (SEM)</p>
A	<p>24. 【題組 3】情境如附圖所示，關於 NIST SP 800-61 資安事故處理指引 (Computer Security Incident Handling Guide) 其事故處置生命週期 (Incident Response Life Cycle)，而偵測與分析 (Detection & Analysis) 中事故優先序 (Incident Prioritization) 所需考量的因素，下列哪一項最「不」合適？</p> <div data-bbox="295 779 1355 1290"><pre>graph LR; A[Preparation] --> B[Detection & Analysis]; B --> C[Containment Eradication & Recovery]; C --> D[Post-Incident Activity]; D --> A;</pre></div> <p>(A) 資安事故的可稽核性 (Auditability)</p> <p>(B) 資安事故的可復原性 (Recoverability)</p> <p>(C) 資安事故造成的功能影響 (Functional Impact)</p> <p>(D) 資安事故造成的資訊影響 (Information Impact)</p>
C	<p>25. 【題組 3】情境如附圖所示，關於 NIST SP 800-61 資安事故處理指引 (Computer Security Incident Handling Guide) 其事故處置生命週期 (Incident Response Life Cycle)，而控制、清除與復原 (Containment, Eradication & Recovery) 中最常被用於識別來源攻擊主機之方法，下列哪一項最「不」正確？</p>

112 年度第 2 次 資訊安全工程師能力鑑定 中級試題

科目 2：I22 資訊安全防護實務

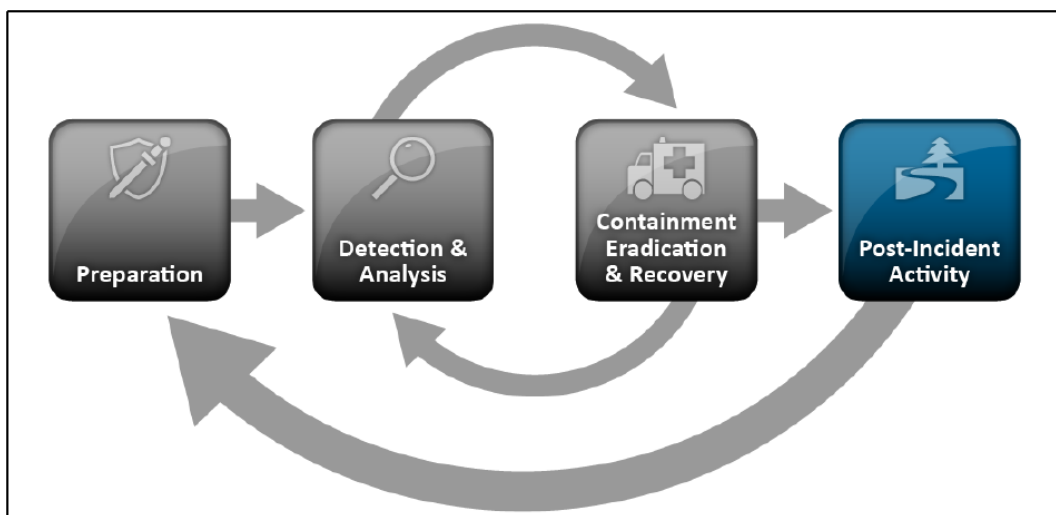
考試日期： 112 年 8 月 12 日

第 8 頁，共 14 頁



- (A) 驗證來源攻擊主機是否偽造 IP 位置 (IP Address)
- (B) 使用搜尋引擎 (Search Engine) 調查來源攻擊主機
- (C) 以服務阻斷攻擊 (Deny of Service) 觀察來源攻擊主機反應
- (D) 觀察攻擊者所可能使用的通信管道 (Communication Channels)

- D 26. 【題組 3】情境如附圖所示，關於 NIST SP 800-61 資安事故處理指引 (Computer Security Incident Handling Guide) 其事故處置生命週期 (Incident Response Life Cycle)，而事故後活動 (Post-Incident Activity) 的證據留存 (Evidence Retention) 程序所需考量的因素，下列哪一項最「不」正確？



112 年度第 2 次 資訊安全工程師能力鑑定 中級試題

科目 2：I22 資訊安全防護實務

考試日期：112 年 8 月 12 日

第 9 頁，共 14 頁

	<p>(A) 訴訟 (Prosecution)</p> <p>(B) 資料保留 (Data Retention)</p> <p>(C) 費用 (Cost)</p> <p>(D) 效率 (Efficiency)</p>
B C D	<p>27. 【題組 3】情境如附圖所示，關於 NIST SP 800-61 資安事故處理指引 (Computer Security Incident Handling Guide) 其事故處置生命週期 (Incident Response Life Cycle) 之敘述，下列何項正確？ (複選)</p> <div data-bbox="296 719 1321 1234"> <pre> graph LR A[Preparation] --> B[Detection & Analysis] B --> C[Containment Eradication & Recovery] C --> D[Post-Incident Activity] D --> A </pre> </div> <p>(A) 準備 (Preparation) 階段：確保事故處置生命週期其所需資源皆已完備，但不包含事前降低資安事故發生機率或避免其產生</p> <p>(B) 偵測與分析 (Detection & Analysis) 階段：準確偵測和評估所可能發生的資安事故為其此階段最具挑戰性之工作，若發生還須確認其類型、範圍與嚴重程度</p> <p>(C) 控制、清除與復原 (Containment, Eradication & Recovery) 階段：若有預先定義用於控制事件之策略與程序，會更容易決策所需採取的行動</p> <p>(D) 事故後活動 (Post-Incident Activity) 階段：包含整個事故處置生命週期中，最重要也最常被忽略的項目 – 案例分析 (Case Study) 和改進</p>
A	<p>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？</p>

112 年度第 2 次 資訊安全工程師能力鑑定 中級試題

科目 2：I22 資訊安全防護實務

考試日期：112 年 8 月 12 日

第 10 頁，共 14 頁

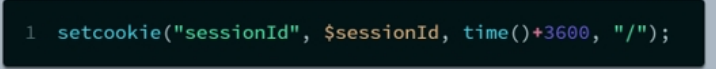
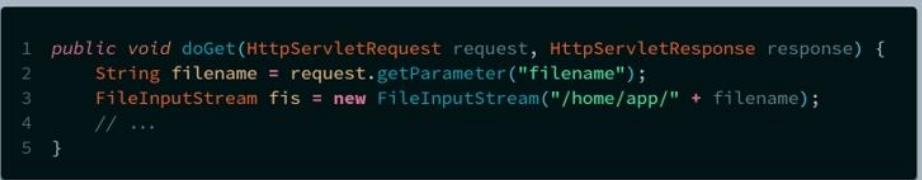
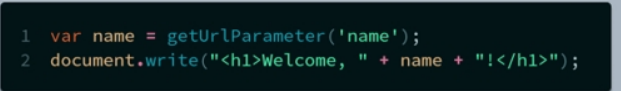
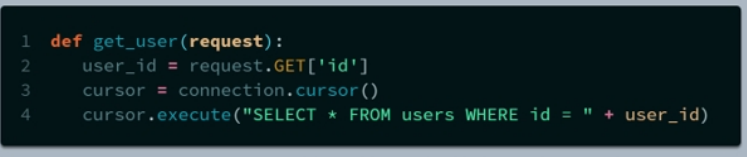
	<ul style="list-style-type: none">(A) 若使用滲透測試工具來測試系統安全性，測試期間宜謹慎規劃不要危及系統運作(B) 滲透測試會影響系統可用性之稽核測試，宜於正常營運時間執行，可確認實際結果(C) ISO 27005 為提供關於技術遵循性審查之特定國際指引(D) 滲透測試或源碼檢測之結果，若有風險需判斷修補，可於下次再檢測時，確認實施結果
C	<p>29. 關於網路安全滲透測試的敘述，下列何者錯誤？</p> <ul style="list-style-type: none">(A) 網路安全滲透測試是找出駭客實現攻擊目的的所有途徑，而駭客入侵只是要實現某一特地目的(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(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
D	<p>30. 關於源碼檢測的敘述，下列何者錯誤？</p> <ul style="list-style-type: none">(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
D	<p>31. 關於資安健診的敘述，下列何者較「不」正確？</p> <ul style="list-style-type: none">(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

112 年度第 2 次 資訊安全工程師能力鑑定 中級試題

科目 2：I22 資訊安全防護實務

考試日期：112 年 8 月 12 日

第 11 頁，共 14 頁

	<p>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</p> <p>(D) 僅透過弱點掃描手法完成資安健檢</p>
B C D	<p>32. 關於源碼檢測分析的敘述，下列何者正確？（複選）</p> <p>在 PHP 源碼中</p> <p>(A) </p> <p>存在Cookies安全性問題，即便設置Secure和HttpOnly標籤，Cookies還是會被竊取或被JavaScript存取</p> <p>在 JAVA 程式語言中</p> <p>(B) </p> <p>此範例中的程式碼存在路徑穿透風險。提供輸入被用作文件路徑的一部分，如果攻擊者提供包含 ./ 的輸入，可能導致應用程式讀取到應該被保護的系統文件。</p> <p>在 JavaScript 範例中</p> <p>(C) </p> <p>存在跨站腳本攻擊（XSS）的風險。用戶提供的輸入直接被插入到網頁中，如果攻擊者提供包含惡意 JavaScript 的輸入。</p> <p>在 python 範例中</p> <p>(D) </p> <p>代碼存在 SQL 注入的風險。用戶提供的輸入直接被拼接到 SQL 查詢中，如果攻擊者提供包含惡意 SQL 語句的輸入，可能導致資料庫被攻擊者控制。</p>
	<p>【題組 4】</p> <p>A 企業推出長照媒合線上服務，其資訊架構包含 Web 及 mobile app 等，後端採用 MySQL 資料庫。其架構有切割出 API 伺服器及資料庫伺服器。</p>

112 年度第 2 次 資訊安全工程師能力鑑定 中級試題

科目 2：I22 資訊安全防護實務

考試日期：112 年 8 月 12 日

第 12 頁，共 14 頁

C	33. 【題組 4】情境如附圖所示。上線前可以進行滲透測試、弱點掃描、源碼檢測，三者發現的弱點數量與誤判率比較的敘述，下列何者較為正確？ (A) 發現率最高的是滲透測試 (B) 誤判率最高的是滲透測試 (C) 通常發現數量以原始碼檢測最高 (D) 原始碼檢測可以找出商業邏輯問題
B	34. 【題組 4】情境如附圖所示。API 伺服器上線前可以進行滲透測試、弱點掃描、源碼檢測的敘述，下列何者正確？ (A) 原始碼檢測應該每季執行 (B) 滲透測試有機會找出商業邏輯漏洞 (C) 弱點掃描應該在開發階段進行 (D) 弱點掃描不應定期執行
A	35. 【題組 4】情境如附圖所示。在檢測後發現命令注入弱點 (Command Injection)，請問應採用下列何項進行修復？ (A) 過濾特殊字元及允許命令之白名單 (B) 不允許大寫字元 (C) 過濾 Unicode 字元 (D) 使用防毒軟體
A B D	36. 【題組 4】情境如附圖所示。資通安全健診除了網路架構檢視外，還包含下列哪些項目？（複選） (A) 網路惡意活動檢視（有線）封包監聽分析 (B) 使用者電腦更新檢視 (C) 外部廠商資安稽核 (D) 目錄伺服器（AD）組態設定檢視

112 年度第 2 次 資訊安全工程師能力鑑定 中級試題

科目 2：I22 資訊安全防護實務

考試日期：112 年 8 月 12 日

第 13 頁，共 14 頁

	<p>【題組 5】</p> <p>您是 XYZ 公司的資訊安全負責人，公司正在進行滲透測試。在測試過程中，滲透測試者通報了一些嚴重的 Web 安全弱點，包括可以遠端執行指令的弱點和能夠讀取本地文件的弱點。並且成功的利用 auth.log 檔案的本地讀取及透過 SSH 驗證注入網站的應用程式達成遠端執行指令稿，使用測試人員可以透過 GitHub 下載 Reverse Shell 和各種編碼或編譯套件，透過這台主機上，發現了管理人員在 root 目錄下放置了帳號密碼檔，且這組帳號密碼經過測試，有大量的使用者可以用相同密碼登入。</p>
C	<p>37. 【題組 5】 情境如附圖所示。當滲透測試者通報可以遠端執行指令的弱點時，尚在內部封閉測試期間，您應該首先採取的行動是下列何項？</p> <p>(A) 關閉受影響的 web 應用程式</p> <p>(B) 馬上通知公司的所有員工</p> <p>(C) 聯繫滲透測試者進行進一步的詳情討論</p> <p>(D) 通報網路安全當局</p>
A	<p>38. 【題組 5】 情境如附圖所示。滲透測試者在報告中提及的本地文件讀取弱點，可能導致下列何項的安全風險？</p> <p>(A) 使攻擊者可以讀取到機密資訊</p> <p>(B) 使攻擊者可以關閉系統</p> <p>(C) 使攻擊者可以獲得系統管理員的權限</p> <p>(D) 使攻擊者可以對網路流量進行監控</p>
C	<p>39. 【題組 5】 情境如附圖所示。這個網站是第三方開源套件，以下哪種策略能最有效地防止遠端執行指令的攻擊？</p> <p>(A) 定期更新應用程式功能組件 (Plug-in)</p> <p>(B) 轉為使用客製開發軟體</p> <p>(C) 定期檢查並安裝安全更新和修補程式</p> <p>(D) 總是使用最新的軟體版本</p>
B C D	<p>40. 【題組 5】 情境如附圖所示。以下哪些安全實踐可以避免當開源的第三方套件存在遠端執行指令稿攻擊？（複選）</p> <p>(A) 回收一般使用者權限</p>

112 年度第 2 次 資訊安全工程師能力鑑定 中級試題

科目 2：I22 資訊安全防護實務

考試日期：112 年 8 月 12 日

第 14 頁，共 14 頁

	<p>(B) 禁用不必要的服務連出</p> <p>(C) 定期更新軟體和作業系統</p> <p>(D) 實施最小權限原則</p>
--	--

機密