112 年度第 1 次 資訊安全工程師能力鑑定 中級試題

科目 1：I22 資訊安全防護實務

考試日期： 112 年 4 月 8 日

單選題 15 題，複選題 5 題，題組題 5 題（佔 100%）

B	1. 下列的弱點應對修補方式，何者較「不」適當？ (A) 緩衝區溢位要用記憶體防護（DEP） (B) 遠端執行安全漏洞（RCE）可以透過防火牆阻擋 (C) Command Injection 用過濾方式即可防護 (D) Resource Injection 可以用白名單方式過濾
B	2. 試問運用網頁文字輸入欄位中，以輸入「' or 1=1」訊息內容的方式，讓該網頁顯示出所有的資料內容，這種攻擊型態屬於下列那種攻擊手法？ (A) XSS (B) SQL Injection (C) CSRF (D) DDoS
B	3. 駭客為了追求最大利益，將亂槍打鳥的隨機攻擊轉換成目標式攻擊，進階持續性威脅（Advanced Persistent Threats, APT）即是最難防禦的目標式攻擊。關於 APT 攻擊的敘述，下列何者錯誤？ (A) 具有隱匿性高且長期潛伏於目標系統的特性 (B) APT 攻擊的模式通常都是透過老舊的網路設備進行攻擊 (C) 潛伏期可以只是幾天，也可能長達一年半載 (D) 遭受攻擊後，被害者多數只能盡快修補漏洞並設定災害停損點，無法有效根除攻擊
A C D	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？ (A) 權限控制失效（Broken Access Control） (B) 跨站請求偽造（Cross-Site Request Forgery） (C) 注入式攻擊（Injection） (D) 加密機制失效（Cryptographic Failures）
	【題組 1】 組織內部正在導入相關以技術來審查脆弱性補強的工具，包含作業

	系統弱點掃描、滲透測試、社交工程等，以下描述是針對這些工具實施之後，相關後續處理的議題。
B	5. 【題組 1 背景描述如附圖】系統弱點掃描後的修補處理方式，下列何者是「不」可以接受補償措施的替代方案？ (A) 工具誤判的風險，須予以審查確認並由主管核可 (B) 目前更新系統需要長期計畫，故風險先予以接受 (C) 因系統老舊風險無法修補，但已將對外連線皆予以關閉，無其他風險漏洞 (D) 優先安排時間予以更新作業系統，並事前測試確認
C	6. 【題組 1 背景描述如附圖】下列何者「不」是利用工具技術偵測應用系統弱點的機制？ (A) 弱點掃描 (B) 滲透測試 (C) 社交工程 (D) 源碼檢測
D	7. 【題組 1 背景描述如附圖】下列何種資產不會產生資訊系統安全弱點暴露的風險，被外界所利用攻擊？ (A) 電腦硬體資產 (B) 電腦軟體資產 (C) 電腦資料資產 (D) 人員資產
A B C D	8. 【題組 1 背景描述如附圖】下列哪些是資訊安全管理系統實施中須考量的系統弱點？ (A) 源碼掃描後的高風險結果 (B) 滲透測試後的高風險結果 (C) Microsoft 定期發布的 Windows Update 檔案 (D) 網路供應商定期提供的網路防火牆韌體更新資訊
A	9. 零時差攻擊（Zero-day Attack）是指駭客利用開發商尚未釋出修補程式的安全漏洞進行攻擊。下列敘述何者錯誤？ (A) 零時差攻擊不會出現在已停止支援之作業系統中

	(B) 面對零時差攻擊，入侵防禦系統（Intrusion Prevention System, IPS）或是網頁應用程式防火牆可進行有限度的防護 (C) 虛擬修補概念可以降低零時差攻擊的風險 (D) 迅速與確實進行弱點修補才是零時差攻擊的根本解決之道
B	10. 社交工程是利用人性弱點誘騙受害者透漏機敏性資料或是允許授權等行為，下列敘述何者錯誤？ (A) 網路釣魚是最常見的社交工程的攻擊手法 (B) 社交工程演練的目的是要培養員工反擊的能力，進而破壞駭客的攻擊手法 (C) 駭客會利用偽造網站網址誘騙使用者上當也是屬於社交工程的攻擊手法之一 (D) 企業組織會透過教育訓練宣導資安觀念，並委託廠商設計測試的釣魚郵件進行檢視員工點擊郵件與連結的行為是否違法資安規定
A	11. 路由協定（Routing Protocol）是一種指定封包轉送方式的網路協定，請問關於路由協定之敘述，下列何者錯誤？ (A) 路由資訊協定（Route Information Protocol, RIP）是最簡單的路由協定，主要傳遞路由資訊，透過每隔 5 秒廣播一次路由表來維護相鄰路由器的位置關係 (B) 路由資訊協定（Route Information Protocol, RIP）是一個距離向量路由協定，最大 hop 數為 15，超過 15 hop 的網路則認為目標網路不可到達 (C) 開放式最短路徑優先（Open Shortest Path First, OSPF）協定是屬於鏈路狀態路由協定，係利用所維護的網路狀態資料庫，透過最短路徑優先演算法（SPF 演算法）計算來得到路由表 (D) 開放式最短路徑優先（Open Shortest Path First, OSPF）協定是屬於動態路由協定 0

B	12. 當網路防火牆受到偵測攻擊時，下列何者最「不」適宜？ (A) 對外管理 Port 應該關閉 (B) 最高權限應該提供給維護廠商 (C) 定期檢視規則是否過期 (D) 告警應該有專人確認與處置
A	13. 關於 MITRE ATT&CK 中的網路服務阻斷（Network Denial of Service）技術（Technique）對策，下列何項錯誤？ (A) 可分析應用程式日誌（Application Log）內容來偵測此技術 (B) 可觀察網路流量（Network Traffic）狀態來偵測此技術 (C) 可觀察感應器健康（Sensor Health）狀態來偵測此技術 (D) 可透過網路流量過濾（Filter Network Traffic）來緩解此技術
B	14. 關於 MITRE ATT&CK 中的資料加密衝擊（Data Encrypted for Impact）技術對策，下列何項錯誤？ (A) 可透過資料備份（Data Backup）來緩解此技術 (B) 可觀察感應器健康狀態（Sensor Health）來偵測此技術 (C) 可透過端點行為預防（Behavior Prevention on Endpoint）來緩解此技術 (D) 可觀察檔案建立（File Creation）與修改（File Modification）狀態偵測此技術
A C D	15. 身分驗證機制是利用帳戶密碼進行作為識別使用者的機制，是多數資訊系統驗證使用者身分的基礎。關於身分驗證機制的敘述，下列哪些正確？ (A) 設定「最小密碼長度」的原則主要是要產生更多的密碼組合，提高被破解的難度。美國國家標準暨技術研究院（National Institute of Standards and

	Technology, NIST）建議最小長度為 8 個字元 (B) 設定「密碼歷程記錄」的原則為了方便使用者自己找到以前使用過的密碼 (C) 設定「密碼最短使用效期」的原則是指該密碼必須使用一段時間後才能再次進行變更，通常是配合密碼歷程機制啟用 (D) 「圖形驗證碼」是設計一組對人類能夠輕易回答而對電腦是困難的題目，以作為區分執行動作的是電腦還是人類的行為
A B C	16. NIST 網路安全框架（Cybersecurity Framework, CSF）有關「框架核心（Framework Core）」係由識別（Identify）、保護（Protect）、偵測（Detect）、回應（Respond）與復原（Recover）等功能所組成。請問關於「保護（Protect）」功能的敘述，下列哪些正確？ (A) 包含身份管理與存取控制（Identity Management and Access Control）與意識和訓練（Awareness and Training） (B) 包含資料安全（Data Security）與資訊保護流程與程序（Information Protection Processes and Procedures） (C) 包含維護（Maintenance）與保護技術（Protective Technology） (D) 包含資產管理（Asset Management）與風險評估（Risk Assessment）
	【題組 2】 駭客勒索集團入侵年收五百億上市公司，對其重要資料庫系統與研發系統破壞勒索加密，經過相關緊急應變後，費時近半個月才恢復公司正常運營，事後總經理召開檢討會議進行檢討。
D	17. 【題組 2 背景描述如附圖】發現公司並未依照法規（資安法與上市上櫃資通安全管控指引）定期進行相關作為，請問下列敘

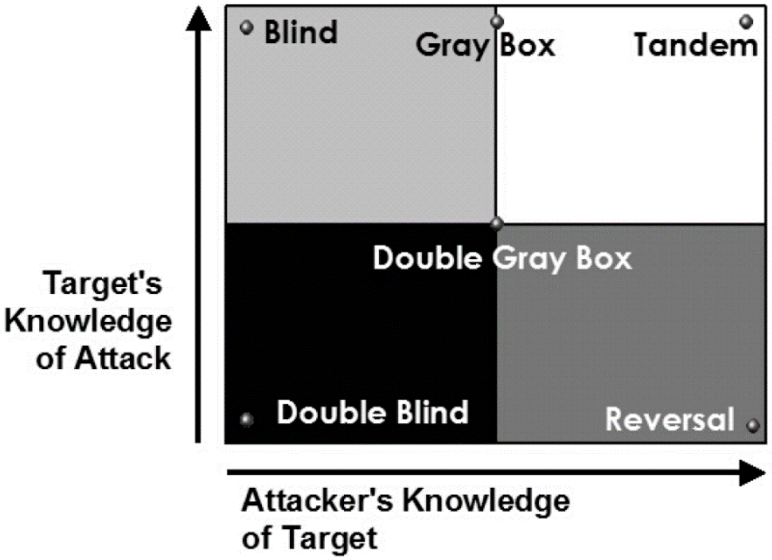
	述何者正確？ (A) 公司可以不需配置資安長，只需配置設適當資安人力 (B) 公司遭受重大資安事件，不需揭露相關資安事件重大訊息 (C) 強制公司加入台灣電腦網路危機處理暨協調中心 (D) 資安納入內部控制，以及資安納入公司治理評鑑
C	18. 【題組 2 背景描述如附圖】國際勒索集團公司勒索 5000 萬美金，不然公開該公司機密資料。該勒索集團手法竟是透過公司郵件系統以釣魚郵件方式，讓內部員工執行惡意程式所造成，針對郵件安全防護的技術與手段，下列何項是「非必要」之措施？ (A) 加強員工郵件安全的教育訓練，定期進行社交攻防演練 (B) 採用 CDR 產品進行郵件清洗，並禁止執行檔下載，執行檔下載須依規定申請 (C) 對外部郵件一律進行隔離 (D) 檢查郵件內容中的惡意 URL 連結
A	19. 【題組 2 背景描述如附圖】勒索集團對公司機密資料進行加密，公司 IT 或是資安團隊應採取的應變措施，下列何項較「不」適當？ (A) 聯繫駭客勒索集團，進行贖金交易取回解密密碼 (B) 查核相關資料庫備份機制是否可以回復 (C) 查核虛擬備份環境可否快速復原相關系統，加速恢復運營 (D) 查核相關備援備份資料是否也受到汙染或破壞
A B C	20. 【題組 2 背景描述如附圖】從這次員工電腦因釣魚郵件感染而擴散到不同網段與主機系統，下列哪些是在資安管理制度或防護技術最適宜的措施？ (A) ISO27001:2022 版本在其控制項 8.22 網路隔離，達

	成降低駭客入侵橫向擴散的危害 (B) 在員工電腦規劃端點偵測與回應（Endpoint Detection and Response, EDR）解決方案，建立有效偵測 IOA（Indicator of Attack）與 IOC（Indicator of Compromise）警告偵測機制 (C) 員工電腦應該建立軟體白名單系統，嚴格管控執行程式的安裝執行 (D) 員工所配發個人電腦，相關資料備份工作由員工自備外接儲存媒體自行備份處置
A	21. ISO/IEC 27001 是資訊安全管理的國際標準，ISO 27001 認證是在確保公司擁有一套安全穩固的資訊管理系統來保護公司內部重要的資訊財產。下列敘述何者錯誤？ (A) ISO/IEC 27001 設計是針對 IT 部門進行管理 (B) 建構資訊安全管理系統（Information Security Management System, ISMS）是以具系統性的方法來保護資訊安全。取得 ISMS 的認證也能增加企業或組織的可信度，並且為公司帶來正面的影響及信任 (C) 組織應架構一項風險處理計畫以鑑別適當管理措施、資源、職責及優先順序，以便管理資訊安全風險 (D) 組織應依規劃之期間施行內部稽核，以提供資訊安全管理系統相關資訊，最後階段必須保存文件化資訊作為稽核計畫及稽核結果之證據
A	22. 依照我國「資通安全事件通報及應變辦法」的規定，公務機關知悉資通安全事件後，應於多少時間之內，依主管機關指定之方式及對象，進行資通安全事件之通報？ (A) 1 小時內 (B) 8 小時內 (C) 24 小時內 (D) 72 小時內

A	23. 關於備份 3-2-1 原則的敘述，下列何者正確？ (A) 以儲存媒體而言，分開存放在兩種不同儲存媒體 (B) 至少三份，分別放到硬碟的 C 槽跟 D 槽 (C) 資料分別存放在辦公室不同樓層 (D) 備份資料不需備份加密金鑰
A B	24. 在組織 ISMS 制度中之服務級別協定（Service-Level Agreement, SLA）要求妥善率達到 5 個 9 的標準下，請問在一年中，下列哪些停機時間在容許的範圍內？ (A) 30 秒 (B) 5 分鐘 (C) 1 小時 (D) 1 天
	【題組 3】 王大明剛接下某製造業資安工作，於本週發生了勒索軟體將公司資料加密，並收到歹徒所指示的付款要求。
D	25. 【題組 3 背景描述如附圖】勒索軟體除了加密資料進行勒索之外，還可能有許多危害，請問下列何項「不」是勒索軟體可能造成的危害？ (A) 資料外洩 (B) 系統入侵造成供應鏈破口 (C) 再被利用去攻擊他人 (D) 自動完成備份及更新
A	26. 【題組 3 背景描述如附圖】本事件可能遭成的後續影響，針對資料被加密，請問主要是破壞了下列哪一項的資安原則？ (A) 可用性 (B) 機密性 (C) 完整性 (D) 可歸責性
A	27. 【題組 3 背景描述如附圖】經過調查後，最「不」可能取得網域伺服器的最高權限為下列何項？ (A) 防火牆本身的漏洞

	(B) 郵件伺服器漏洞 (C) 社交工程 (D) 入侵供應鏈廠商
A B C	28. 【題組 3 背景描述如附圖】請問下列哪些是組織可掌握的復原或處理方式？ (A) 還原關鍵系統與其資料 (B) 確認是否還有潛藏惡意程式 (C) 調查攻擊手法及路徑 (D) 直接付款取回加密金鑰
B	29. 資訊系統常透過組態檔案提供初始參數或是預設功能設定值，當系統組態被不當或是錯誤的設定就容易產生安全漏洞。下列敘述何者錯誤？ (A) 啟用預設帳號密碼是最常見的設定缺陷，像是有些軟體元件為了設定上的方便，允許使用空白密碼或是預設密碼進行登入，故駭客容易藉此入侵系統 (B) 站台目錄列表（Directory Listing）功能除了像是檔案伺服器等特定需求以外，建議將此項功能開放，方便使用者檢索目錄列表 (C) 當系統發生異常時，盡量避免將相關詳細的錯誤訊息直接呈現在頁面上 (D) 充分掌握環境中的各項元件與組態，隨時進行維護與改善以確保資訊系統部屬與運作的安全與持續
D	30. 下面何項「不」是源碼檢測工具？ (A) SonarQube (B) Checkmarx (C) Fortify (D) Nexpose
D	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
B C	32. 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？ (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 (C) 應用程式是管理與控制電腦軟硬體資源的電腦程式 (D) 管理制度指的是為了保障資訊安全對使用者提出的要求與限制
C	33. 【題組 4】OSSTMM 開源安全測試方法手冊（The Open Source Security Testing Methodology Manual）其中所述，於測試安全性前應適當定義安全測試（Security Test）以妥善管理複雜性。關於範圍（Scope）的敘述，下列何項錯誤？ (A) PHYSSEC 實體安全（Physical Security）包含人員（Human）管道 (B) PHYSSEC 實體安全（Physical Security）包含實體（Physical）管道 (C) SPECSEC 頻譜安全（Spectrum Security）包含有線（Wired）管道 (D) COMSEC 通訊安全（Communications Security）包含資料網路（Data Networks）管道
A	34. 【題組 4】如附圖所示，OSSTMM 開源安全測試方法手冊（The Open Source Security Testing Methodology Manual）其中所

	述，於測試安全性前應適當定義安全測試（Security Test）以妥善管理複雜性。關於常見的安全測試類型，下列敘述何項錯誤？  (A) 盲測（Blind Test）通常也稱為藍隊演練（Blue Team Exercise） (B) 雙盲測試（Double Blind Test）通常也稱為滲透測試（Penetration Test） (C) 灰箱測試（Gray Box Test）常被稱為弱點測試（Vulnerability Test） (D) 反向測試（Reversal Test）通常也稱為紅隊演練（Red Team Exercise）
D	35. 【題組 4】OSSTMM 開源安全測試方法手冊（The Open Source Security Testing Methodology Manual）其中所述，於測試安全性前應適當定義安全測試（Security Test）以妥善管理複雜性。關於錯誤類型（Error Type）之描述，下列何項錯誤？ (A) 假陽性（False Positive）：測試結果被判斷為真實，但實際證明其為虛假 (B) 假陰性（False Negative）：測試結果被判斷為虛假，但實際證明其為真實

	(C) 抽樣誤差（Sampling Error）：測試結果不具代表性，因為範圍被改變 (D) 人為錯誤（Human Error）：測試結果因受測者的行為舉止而受到改變
A B C D	36. 【題組 4】OSSTMM 開源安全測試方法手冊(The Open Source Security Testing Methodology Manual）其中所述，於測試安全性前應適當定義安全測試（Security Test）以妥善管理複雜性。關於定義安全測試（Defining a Security Test）的描述，下列哪些正確？ (A) 定義所需保護的資產，找出其控制（Control）機制之侷限（Limitations） (B) 識別資產所處區域（Engagement Zone），包含相關保護機制、程序與服務 (C) 定義測試範圍媒介（Vectors）如何內外交互，如：內到內、內到外、A 到 B 單位 (D) 確保安全測試定義符合教戰守則（Role of Engagement）以避免誤解或錯誤期待
	【題組 5】 網站滲透攻擊是紅隊滲透重要基本課題，而善用網路資源與工具，可以達到事半功倍之效果，身為資安滲透團隊成員，以下相關網路資源與工具，事必須要掌握的技術與技巧。
A	37. 【題組 5 背景描述如附圖】關於網路資源的敘述，下列何者錯誤？ (A) FOFA 是覆蓋全球資料頗為完整的 IT 設備搜尋引擎，非中國創立資料庫 (B) Shodan 是世界上第一個用於聯網與 IoT 設備的搜尋引擎，可以查找到電子門鎖相關資訊 (C) ZoomEye 是由中國創宇 404 實驗室所搭建網路空間搜尋引擎 (D) Censys 也是蒐集全球最新的 Internet 掃描數據源

C	38. 【題組 5 背景描述如附圖】子網域資訊的取得是滲透前重要的 Footprint 程序，下列何項「不」是子網域查找工具？ (A) subfinder (B) SubDomainizer (C) Virustotal (D) SubBrute
B	39. 【題組 5 背景描述如附圖】身為一個滲透測試人員，必須善用網際網路有用資料庫或搜尋引擎，下列各類資料庫系統的敘述，何者錯誤？ (A) shodan.io 是世界上用於聯網設備查找的搜索引擎 (B) censys.io 是一個免費資料庫，累積許多無線網路重要刺探資訊 (C) pulsedive.com 蒐集許多威脅情報 (D) intelx.io 可處理加密貨幣搜尋與暗網搜尋
A B C	40. 【題組 5 背景描述如附圖】成功滲透到某個網站後，為了避免觸發相關警示而通知 IT 人員，於是採用「免殺（迴避防毒軟體的偵測）」的手法。發現該主機為一台 Windows 10 所搭建網站系統，決定使用 Windows 作業系統中相關工具程式來進行 Command & Control，下面哪些 Windows 作業系統「原生」指令可以使用在遠端下載？ (A) Bitsadmin.exe (B) Certutil.exe (C) HH.exe (D) Update.exe