111 年度 資訊安全工程師能力鑑定 初級試題

科目 1：I12 資訊安全技術概論

考試日期： 111 年 11 月 19 日

單選題 50 題（佔 100%）

C	1. 請問面對日益嚴重的「電腦犯罪」，下列預防措施何者較「不」正確？ (A) 建立資安管理制度 (B) 技術性管制 (C) 拔掉網路線 (D) 警衛、門禁
A	2. 請問下列何者為常見的 SNMP（Simple Network Management Protocol）安全問題？ (A) 使用 public community string (B) 使用 SNMP v3 (C) 使用 UDP (D) 使用 161 作為服務 Port
B	3. 下列何者攻擊是透過 UDP（User Datagram Protocol）協定送出假造來源的廣播封包至目標網路，以便產生擴大資料流量效果的阻絕服務攻擊？ (A) Smurf (B) Fraggle (C) Land (D) Teardrop

A	4. 下列何者為遠端使用者撥入驗證服務（Remote Authentication Dial In User Service,RADIUS）常使用之通訊埠（Port）？ (A) 1812 (B) 123 (C) 389 (D) 390
B	5. 在網際網路的世界中，每台主機都需要使用 IP 位址協定，才能相互溝通並傳送資料。請問下列哪一個 IP 位址為公用 IP 位址（非私人 IP）？ (A) 10.10.10.10 (B) 100.100.100.100 (C) 172.16.172.16 (D) 192.168.192.168
B C 皆 給 分	6. 通訊埠（Port）是應用層每種服務皆有的唯一埠號碼，其範圍介於 0~65536。其中 1024 之前為公認通訊埠（Well-Known Port），關於通訊埠用途的敘述，下列何項錯誤？ (A) Port:53/TCP 用途：DNS 域名解析服務 (B) Port:123/UDP 用途：LDAP 輕型目錄存取協定 (C) Port:445/UDP 用途：Microsoft-DS SMB 檔案分享 (D) Port:995/TCP 用途：基於 SSL 的 POP3 收發電子郵件加密傳輸

B	7. 網路上有許多駭客組織，都會介紹不同的攻擊方式，每種方式都會有不同的攻擊效果。關於攻擊的敘述，下列何項錯誤？ (A) 阻斷服務攻擊：利用網路通訊協定的弱點，傳送大量的封包使系統負荷過重、發生錯誤或是系統當機無法服務 (B) 網路監看：利用人際關係上溝通疏誤，取得特殊的存取帳號密碼或是重要資訊 (C) 系統漏洞：利用系統程式設計、維護時，所留下的錯誤或漏洞進行入侵 (D) 緩衝區溢位：利用寫入資料超過原本分配緩衝區的大小，造成執行錯誤指令
C	8. 面對組織化、多變化的駭客攻擊，建立資訊安全監控維運中心（Security Operation Center, SOC）以加強資訊安全系統安全，下列何者是 SOC 的較主要運作功能？ (A) 決定風險處理方法 (B) 進行資安弱點管理 (C) 即時監看資安事件 (D) 處理資安事故原因
C	9. 請問可以將網際網路封包加密的是下列何項通訊協定？ (A) SMTP (B) HTTP (C) HTTPS (D) FTP

A	10. TCP 三向交握（Three-way Handshake）的順序為下列何項？ (A) SYN，SYN/ACK，ACK (B) SYN，ACK，SYN (C) SYN，SYN，SYN (D) ACK，SYN，SYN
B	11. 請問要重送 TCP 封包需要使用下列何項工具？ (A) Wireshark (B) Tcpreplay (C) ngrep (D) hping
A	12. 請問下列哪個 SSL Cipher Suite「不」安全應停用？ (A) RC4 (B) AES256 (C) AES512 (D) AES128
B	13. 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，而此安全協定的使用亦可防止哪一種攻擊？ (A) 使用 SSH 協定、防止 DNS 攻擊 (B) 使用 SSH 協定、防止中間人攻擊 (C) 使用 HTTPS 協定、防止 DNS 攻擊 (D) 使用 HTTPS 協定、防止 DDoS 攻擊

C D 皆 給 分	14. 關於雙因子認證（Two-Factor Authentication）的敘述，下列何者錯誤？ (A) 雙因子指的是「你知／Something you know」「你有／Something you have」「你是／Something you are」任兩者 (B) 兩重的密碼認證，不算雙因子認證方式 (C) 可以有效防禦資料隱碼攻擊 (D) 可以有效防禦中間人攻擊
B	15. 關於 Linux 的權限設定敘述，下列何者錯誤？ (A) R 權限對應的數值為 4 (B) E 權限對應的數值為 3 (C) W 權限對應的數值為 2 (D) X 權限對應的數值為 1
A	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
D	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

D	18. 公司高階主管近日購買一部 Macbook Pro，內含新版的 MacOS，由於業務上的關係，此主管經常攜帶筆電外出商談開會，因此公司的資安顧問建議他啟用某一項功能以防範筆電遺失被偷時，仍能夠避免資料外洩，請問該高階主管需要啟用下列何項系統功能？ (A) Bitlocker (B) TrueCrypt (C) EncFs (D) FileVault
B	19. 系統管理人員於網站日誌中看見大量訊息含有類似字串「..%2F..%2F..%2F..%2Fetc%2Fpasswd」，請問可能為以下何種攻擊？ (A) SQL Injection (B) Directory Traversal (C) Cross-Site Scripting (D) Insecure Deserialization
A	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

C	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 (D) 資料庫掃描
B	22. 下列何者「不」是評估應用程式安全性的檢測方法？ (A) Penetration Testing (B) Ransomware Testing (C) Threat Modeling (D) Source Code Review
D	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）

A	24. 如附圖所示，攻擊者透過修改查詢參數「account」為任意帳號即可存取資訊，關於此應用程式缺陷的敘述，下列何者正確？ https://vulnerable.site/app/profile?account=victim (A) 存取控制失效（Broken Access Control） (B) 密碼機制失效（Cryptographic Failures） (C) 注入攻擊（Injection） (D) 安全日誌與監控失效（Security Logging and Monitoring Failures）
A	25. 下列何者「不」是因為開發過程中，未留意程式安全造成的問題？ (A) 魚叉式網路釣魚（Spear Phishing） (B) SQL 資料隱碼攻擊（SQL Injection） (C) 跨站指令碼攻擊（Cross-Site Scripting, XSS） (D) 跨站請求偽造（Cross-Site Request Forgery, CSRF）
A	26. 下列何者為防禦跨站請求偽造（Cross-Site Request Forgery, CSRF）攻擊的最佳方式？ (A) 使用驗證碼（CAPTCHA） (B) 輸入參數黑名單過濾 (C) 輸入參數白名單過濾 (D) 輸入參數長度過濾

A	27. 安全性測試人員可以使用反組譯器（Disassemblers）、除錯器（Debuggers）和反編譯器（Decompilers）來判斷與檢查，是否存在何種程式碼的弱點？ (A) 缺乏逆向工程（Reverse Engineering）保護 (B) 注入缺失（注射缺陷） (C) 跨網站指令碼（Cross-Site Scripting） (D) 不安全的物件參考（Insecure Direct Object Reference）
D	28. 針對網站常見的跨站指令碼攻擊（Cross-site scripting, XSS），請問攻擊成功的常見原因是資通系統未過濾或防範以下何種程式語言的注入攻擊？ (A) Python (B) ASP.NET (C) ShellScript (D) JavaScript
B	29. 請問 CWE（Common Weakness Enumeration）是指下列何項？ (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. 利用社交工程的概念，將惡意程式或是惡意連結等隱藏在電郵件中，看似好友所寄的，誘騙使用者打開郵件。下列何項「不」是有效防止惡意郵件社交工程的方案？ (A) 定期舉辦資訊安全教育訓練，建立對惡意程式的認知 (B) 資訊部門導入防毒及郵件過濾解決方案 (C) 定期進行社交工程演練測試 (D) 導入封包過濾防火牆進行防禦
D	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 List（GVL） (D) Common Vulnerabilities and Exposures（CVE）
B	32. 電腦主機的作業系統及應用程式，關於有效的弱點管理，下列敘述何者較正確？ (A) 對外服務的商務主機，發現了作業系統及應用程式上的弱點，為了運作正常持續不中斷，不需更新修正其弱點 (B) 關閉或是移除不需要使用的服務，只提供最小使用權限給操作使用者 (C) 採用三年一次委外技術顧問的檢測報告說明 (D) 總經理的電腦為了有效運作，必須給予最高系統管理員（Administrator）的權限

A	33. 防毒軟體使用「啟發/探索方法（Heuristic Method）」最主要優點為下列何項？ (A) 偵測全新病毒 (B) 偵測已知病毒 (C) 避免誤隔離 (D) 可更快速偵測已知惡意程式
B	34. 關於儲存媒體管制作業的敘述，下列何者最正確？ (A) 儲存設備維修應以就地維修為優先，無需將硬碟拔除以利維修測試 (B) 儲存媒體如需送修，應填寫設備攜出單，並將存放機密性資料之硬碟予以拔除或徹底刪除其內容。若無法執行硬碟拔除或刪除其內容，則應取得維修人員之個人保密切結書 (C) 含有個資或機敏資料之儲存媒體應存放於具門禁管制之資訊機房門口，以利監視錄影監控 (D) 資料庫、重要伺服器主機之作業系統與應用系統之程式庫、執行碼、原始程式碼等，應交付資安主管或資訊長統一保管

C	35. 若公司營運系統伺服器內有三顆硬碟作 RAID 5，並且備份機制中規劃每週五 23:00 進行完整備份（Full Backup），其餘每天 23:00 進行增量備份（Incremental Backup）已持續運行半年狀況很好，無奈於本週一 11:00 時伺服器其中一顆硬碟發生故障，請問應採取下列何種處理方式？ (A) 將上週五的 Full Backup 磁帶回存，再將六、日的增量備份磁帶回存 (B) 將上週五的 Full Backup 磁帶回存，再將週日的備份磁帶回存 (C) 更換有問題的硬碟即可 (D) 更換有問題的硬碟，並將上週五的 Full Backup 磁帶回存，再將六、日的增量備份磁帶回存
A	36. 關於 MS-SQL Server 內建備份方式的敘述，下列何者錯誤？ (A) 完整備份會截斷交易記錄 (B) 要做任何差異備份或交易記錄備份之前，一定要做一次完整備份 (C) 差異備份不會備份任何交易記錄檔 (D) 交易記錄檔備份透過 SSMS 操作，在預設的情況下會自動截斷交易記錄
B	37. 請問利用磁帶進行資料備份時，執行備份時耗時較久，但回復時需要的磁帶數通常最少的是下列何者？ (A) 巨量備份（Bigdata Backup） (B) 完全備份（Full Backup） (C) 差異備份（Differential Backup） (D) 增量備份（Incremental Backup）

B	38. 資料備份的最主要目的，是保護資料的哪一個特性？ (A) 機密性 (B) 可用性 (C) 鑑別度 (D) 完整性
B	39. 因應個人資料保護法之要求，許多公司在處理和個人資料有關的日誌時，會將敏感資訊進行處理，例如將姓名改成陳〇〇，請問這樣的處理，通常稱下列何項？ (A) 正規化 (B) 去識別化 (C) 最佳化 (D) 初始化
B	40. 請問對公司內的不同網路、系統的時間同步（Clock Synchronization）機制，下列敘述何者最正確？ (A) 系統才需進行時間同步，網路設備不需要 (B) 由單一主機對外部時間源進行校正後，所有系統、設備與該主機同步 (C) 同網段的所有系統設備，應向同一外部主機進行時間校正，不同網段則分別對外部不同時間源進行校正 (D) 不同系統、設備，應分別向外部不同時間源進行時間校正，以分散風險並做比較

D	41. 請問存錄系統管理者或操作者操作系統的紀錄，並予以適當的保護，其主要的目的是要確保下列對於系統管理者或操作者的何項特性？ (A) 機密性（Confidentiality） (B) 完整性（Integrity） (C) 可用性（Availability） (D) 可歸責性（Accountability）
C	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
B	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
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

A	45. 關於雲服務安全，下列敘述何者最為正確？ (A) 資料先加密再儲存於雲服務中，可降低外洩之危害 (B) 雲服務安全為供應商（CSP）之責任，非與使用者相關 (C) 服務皆具備高可用特性與災難復原功能，服務遷移其上即可有效避免中斷風險 (D) 多因子驗證機制（Multi-factor Authentication）設置，可避免儲存於雲服務之資料受駭與外洩風險
C	46. 為強化行動裝置（如手機）的資料安全，下列何者措施無法達到此一效果或目的？ (A) 安裝手機防毒軟體 (B) 將手機資料備份 (C) 減少玩手機遊戲的時間 (D) 不執行手機越獄（Jailbreak, JB）
D	47. 手機的使用者驗證方式，下列何項安全性最低？ (A) 人臉辨識 (B) 指紋辨識 (C) 虹膜辨識 (D) 4 位字元密碼

D	48. 下列何種對使用行動裝置的攻擊，主要是利用人與人的互動？ (A) 中間人攻擊（Man in the Middle Attack） (B) 重送攻擊（Replaying Attack） (C) 阻斷式服務攻擊（Denial-of-Service Attack） (D) 社交工程（Social Engineering）
D	49. 關於 WPA（Wi-Fi Protected Access），下列敘述何者「不」正確？ (A) 初始向量（Initialization Vector，IV）長度：48 位元 (B) WPA 支援 TKIP（Temporal Key Integrity Protocol）加密方式 (C) 封包驗證方式：CRC（Cyclic Redundancy Check） (D) 加密方法：3DES
A	50. 下列何者「不」是因物聯網所衍生的安全問題？ (A) 手機因故障送修，手機內的隱私照片遭維修人員竊取 (B) 駭客入侵您的健身手環，用來追蹤您日常生活的路線與習慣 (C) 交通號誌遭駭客入侵，數位顯示板的內容遭到竄改 (D) 車輛遭到駭客操控，從遠端操控車輛讓引擎熄火並猛踩煞車