初級資訊安全工程師能力鑑定樣題

單選題 50 題（佔 100%）

C	1. IP 之間的傳輸，屬 OSI 模型哪一層次？ (A) 應用層（Application Layer） (B) 表達層（Presentation Layer） (C) 網路層（Network Layer） (D) 傳輸層（Transport Layer）
C	2. 下列哪種攻擊可以用來繞過實體（Physical）和邏輯（Logical）主機安全機制？ (A) 暴力攻擊（Brute-Force Attack） (B) 阻斷服務攻擊（Denial-of-Service Attack） (C) 社交工程（Social Engineering） (D) 通訊埠掃描（Port Scan）
A	3. SMURF Attack 是利用何種協定進行攻擊？ (A) ICMP (B) UDP (C) RIP (D) ARP
A	4. 公司對外的網站放置於下列何處？ (A) DMZ（Demilitarized Zone） (B) Internet (C) Intranet (D) Extranet
C	5. 某管理員監控網路上的 IP 封包時，發現封包標頭包含了一個協定欄位（Protocol Number），而此欄位的值為 1，請問此封包是屬於何種協定的封包？ (A) TCP (B) UDP (C) ICMP (D) IGMP
C	6. 請問下列何種網路攻擊行為會使目標主機系統超出其工作負荷量，甚至導致系統癱瘓？ (A) 社交攻擊（Social Engineering） (B) 流量分析（Traffic Analysis） (C) 阻斷式服務攻擊（Denial-of-Service Attack） (D) 竊聽（Sniffing）
C	7. 下列設備中，何者是可避免內外直接連線並隱藏內部 IP 位址？

	(A) 封包過濾防火牆（Packet-Filtering Firewall） (B) 狀態檢視防火牆（Stateful Inspection Firewall） (C) 代理伺服器（Proxy Server） (D) 網站應用程式防火牆（Web Application Firewall）
B	8. 在寄送電子郵件時，可以運用安全電子郵件簽章/密碼技術，以確保資訊的哪些特性？ (1) 機密性 (2) 完整性 (3) 可用性 (4) 鑑別性 (A) (1), (2), (3) (B) (1), (2), (4) (C) (1), (3), (4) (D) (2), (3), (4)
D	9. 關於「SSL 協定」，下列敘述何者不正確？ (A) 提供伺服器(Server)驗證 (B) 提供客戶端(Client)安全傳輸 (C) 提供伺服器(Server)與客戶(Client)之間的通訊加密 (D) 可絕對確保買賣交易的安全
A	10. 關於 TCP 協定的特性，下列敘述何者正確？ (A) 確保資料傳送之正確性 (B) 資料開始傳送時不需進行交握(Hand shaking) (C) 傳送發生錯誤時不會要求重新傳送 (D) 傳送時所進行之檢查與偵錯機制較 UDP 簡單
C	11. 請問下列何者非為應用層服務？ (A) HTTP (B) SMTP (C) IPX (D) FTP
B	12. 下列哪一項網路技術可以降低廣播領域（Broadcast Domain）範圍？ (A) Network Address Translate（NAT） (B) VLAN (C) Dynamic Trunking Protocol (D) Inter-Switch Link（ISL）
C	13. 下列敘述何者不正確？ (A) 木馬後門程式常偽裝成提供便利或實用的免費軟體，吸引使用者

	下載使用 (B) 電腦病毒具有散播、隱藏、感染、潛伏及破壞等特性 (C) 阻絕服務攻擊（DoS）通常指攻擊者與通訊的兩端分別建立獨立的聯繫，並交換所收到的資料 (D) 蠕蟲（Worm）會不斷複製，並利用網路感染其他主機
C	14. 雙因認證（Two-Way Factor）可以防止下列何者攻擊？ (A) 阻斷式服務攻擊 (B) SQL 資料隱碼攻擊 (C) 密碼側錄攻擊 (D) 中間人攻擊
C	15. 請問此 cat ~/.bash_history 指令的目的為？ (A) 列出使用者目錄 (B) 列出系統目錄 (C) 列出使用者曾經下過的指令 (D) 列出系統安裝歷史
C	16. 下列何者實務做法對於強化作業系統本身保護，降低被攻擊風險並沒有太大的效益？ (A) 定期自動更新 (B) 啟用預設拒絕政策的系統防火牆 (C) 啟用 IPSec 服務 (D) 安裝並更新防毒軟體
D	17. 下列何者不屬於作業系統安全預防(Preventive)機制？ (A) 實施密碼原則 (B) 安裝防毒軟體 (C) 定期套用安全性更新 (D) 定期檢視安全記錄檔（Log）
A	18. 黑帽駭客（Black Hats）入侵前，收集資訊常用的指令 nslookup，下列何者不是其目的？ (A) 可以用來掃描已開啟的 TCP/UDP Port (B) 可以用來診斷 DNS 的架構 (C) 可以用來查詢網路網域名稱伺服器 (D) 如果以 DNS 的名稱，尋找主機 IP 位址
D	19. 請問下列何者「並非」作業系統中毒的可能徵狀？ (A) 檔案無故遭加密 (B) 上網速度變慢或無法連線 (C) 無故出現對話框，且無法關閉

	(D) 資料讀取速度變快
C	20. 請問下列何者不是 XSS（Cross-Site Scripting）攻擊語法？ (A) <script>alert('xss');</script> (B) +alert('xss')+ (C) ' or 1=1-- (D) <IMG SRC=javascript:alert('XSS')>
B	21. SQL 資料隱碼攻擊（SQL Injection）的攻擊技術主要會發生的原因，是利用下列何者？ (A) 利用系統漏洞對系統造成危害 (B) 程式開發者的疏忽，未對使用者的輸入進行過濾與檢查 (C) 資料庫存取權限設定錯誤所造成 (D) 遭受到駭客運用社交工程及惡意程式攻擊
C	22. 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，該導入哪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
C	23. 安全的系統發展生命週期（Secure Software Development Life Cycle，SSDLC）意指發展一套安全系統的順序，用以開發完善安全的資訊系統。以下哪個不是安全的系統發展生命週期階段？ (A) 設計 (B) 需求 (C) 估價 (D) 開發
A	24. Android 系統的核心層級應用程式沙箱(Sandbox)是以何種方式來提供安全性？ (A) 每個應用程序指定唯一的使用者識別碼（UID），並執行於獨立的處理程序中 (B) 於非特權群組識別碼（GID）下執行所有應用程式 (C) 限制核心處理程序進行非法讀取 (D) 防止任何未經授權的核心處理程序執行
C	25. 程式碼簽署（Code Signing）無法提供以下哪一項功能？ (A) 確認軟體開發者的身份 (B) 防止程式碼被篡改 (C) 用戶端認證 (D) 程式碼執行時期的合法性識別

B	26. 下列何者為目前撰寫安全程式碼的知名的業界參考指引？ (A) NIST SP 800 系列 (B) OWASP 指南 (C) FIPS 系列 (D) ISO22301 相關標準
B	27. 關於逆向工程，下列敘述何者正確？ (A) 從組合語言恢復高階語言的結構與語法過程 (B) 從機器語言恢復高階語言的結構與語法過程 (C) 從高階語言恢復組合語言的結構與語法過程 (D) 從高階語言恢復機器語言的結構與語法過程
A	28. 關於原始碼漏洞修補，下列敘述何者不正確？ (A) 所有類型的原始碼漏洞，均可找到對應的弱點掃描方法 (B) 未經驗證的使用者參數，均應加以驗證 (C) SQL Injection 的源頭可能來自於 Web 頁面，亦可能來自資料庫本身資料 (D) XSS 的源頭可能來自於瀏覽器的 Document Object Model
D	29. 關於弱點掃描（Vulnerability Assessment）的描述，下列敘述何者不正確？ (A) 弱點掃描屬於一種網路探測技術 (B) 弱點掃描主要是偵測並掃描位於主機上的各個端口或節點的弱點資訊後，與自身的弱點資料庫進行比對 (C) 若防火牆和入侵偵測系統是屬於被動的防禦方法，則弱點掃描就屬於一種主動的防禦方法 (D) 弱點掃描與原碼檢測（Source Code Analysis）應擇一使用，以避免檢測數據相互干擾
D	30. 下列對行動碼（Mobile code），下列敘述何者不正確？ (A) 通常不具傷害性 (B) 可在不同作業系統之間執行 (C) 可在不同瀏覽器上順利執行 (D) 無法從遠端系統傳到本地端執行
B	31. 關於病毒（Virus）與蠕蟲（Worm）之比較，下列何者最正確？ (A) 病毒通常為惡意程式，蠕蟲則通常不是 (B) 病毒通常透過使用者操作傳播，蠕蟲則會自行擴散 (C) 病毒檔案通常比蠕蟲大 (D) 病毒可自行存在，但蠕蟲無法自行存在

D	32. 資訊安全管理人員經常接收到資安狀況的回報，需要作出判斷進行相關處置。請問下列哪一現象比較不像遭受到惡意程式的攻擊狀況？ (A) 使用者電腦自動發送出大量電子郵件 (B) 使用者電腦系統突然變慢，硬碟大量執行運作 (C) 使用者防毒軟體突然被關閉，失去即時防禦 (D) 使用者電腦收到電子垃圾廣告郵件
B	33. 關於個人資料電子檔案管理，下列敘述何者不正確？ (A) 非業務所需，個人電腦、公用資料夾、公用 PC 不得存放含有個人資料之電子檔案；且存放公用資料夾及公用 PC 之個人資料檔案應依保存期限刪除 (B) 臨時性之個人資料檔案存放於個人電腦、公用資料夾、公用 PC 之暫存資料夾中時，其存放天數不可限制 (C) 個人資料檔案備份應考量備份資料加密之必要 (D) 儲存備份資料之媒體亦應以適當方式保管，且依組織相關規定定期進行備份資料之還原測試，以確保備份之有效性
A	34. 關於資訊回復點（Recovery Point Objective, RPO），下列敘述何者不正確？ (A) RPO 意指當災害發生後，資訊系統恢復基本或必要服務的所需時間 (B) RPO 的定義與組織執行備份的頻率與方式息息相關 (C) RPO 定義的時間愈短，組織所需投入的成本就愈高 (D) RPO 屬持續營運計畫中需被考量與定義的項目之一
B	35. 下列何者技術可保護資料傳輸過程安全？ (A) 身分驗證 (B) 加密 (C) 電子簽章 (D) 雜湊函數
A	36. 請問可恢復系統功能或檔案資料，但其缺點是耗時較久之資料備份方式是指下列哪一種？ (A) 完全備份（Full Backup） (B) 巨量備份（Bigdata Backup） (C) 差異備份（Differential Backup） (D) 增量備份（Incremental Backup）

C	37. 請問下列哪個議題非屬保護資料安全範圍？ (A) 某報名網站因 SQL Injection 弱點導致遭駭客取得會員資料 (B) 線上購物系統因駭客入侵導致客戶資料外洩 (C) 訂票系統因大量訂單湧入而當機 (D) 某學校教學系統遭人竄改分數
D	38. 在一個組織或安全網域內，相關的資訊系統須有一致性的同步時脈（鐘訊同步），其主要的目的為何？ (A) 確保作業系統的完整性 (B) 防範資料的漏失 (C) 為了系統作業的方便 (D) 確保稽核日誌的準確性，以便紀錄事件與生成證據
A	39. 請問主要記錄系統程式所有活動行為，例如主機或伺服器發生異常活動狀況等，是指下列哪個紀錄檔之功能？ (A) 系統日誌檔 (B) 應用程式日誌檔 (C) 安全性日誌檔 (D) 網路日誌檔
C	40. 請問若某公司的系統管理員，將所有稽核日誌存放於另一台獨立的日誌伺服器（Log Server），並指派非管理系統之專人管理該伺服器，其最重要的目的為？ (A) 方便加密 (B) 確保機密不外洩 (C) 保護日誌 (D) 降低資安事件發生時的處理時間
A	41. 許多公司會將不同設備的日誌（Log）蒐集到同一個平台進行管理，但因為不同設備之日誌格式、命名方式不盡相同，此時為了方便分析，通常會對這些日誌進行什麼處理？ (A) 正規化（Normalization） (B) 去識別化（De-identification） (C) 最佳化（Optimization） (D) 初始化（Initialization）
D	42. 關於雙因素認證常見的媒介，下列敘述何者不正確？ (A) Email (B) 簡訊 (C) 智慧卡 (D) 密碼

D	43. 在建立雲端服務所需資料庫時，從資訊安全的角度來看，以下事項何者較不需要被注意？ (A) 資料加密 (B) 資料庫使用者角色控管 (C) 對連線來源控管 (D) 使用正規化規劃資料庫
B	44. 在建置雲端資訊系統時，常會對系統進行一系列的安全分析，請問下列何者不屬於安全分析？ (A) 弱點分析（Vulnerability Analysis） (B) 可行性分析（Feasibility Analysis） (C) 威脅分析（Threat Analysis） (D) 風險評估（Risk Analysis）
A	45. 請問在行動裝置上，下列何種的使用者驗證方式安全性最低？ (A) 圖形軌跡鎖 (B) 人臉辨識鎖 (C) 指紋辨識鎖 (D) 虹膜辨識鎖
B	46. 在使用行動裝置時，下列何者攻擊手法主要是針對人與人的互動形成的？ (A) 重送攻擊（Replaying Attack） (B) 社交攻擊（Social Engineering） (C) 中間人攻擊（Man in the Middle Attack） (D) 阻斷式服務攻擊（Denial-of-Service Attack）
D	47. 在行動裝置使用上，為避免使用者遭受網路釣魚攻擊（Phishing）所需注意的事項。下列敘述何者不正確？ (A) 輸入重要資訊時須觀察網址是否異常 (B) 勿胡亂開啟來路不明的信件連結 (C) 不隨意連接不信賴的 Wi-Fi 熱點 (D) 用無痕跡的瀏覽器開啟網頁
C	48. 為了確保「物聯網」的使用安全，使用者應該採取哪些防範措施？ (1) 啟用智慧型設備上建議的安全功能 (2) 採用 WiFi 通訊技術就可以確保資料傳輸的安全 (3) 購買會定期更新產品韌體的廠商所推出的物聯網產品 (4) 使用安全的密碼 (A) (1), (2), (3) (B) (1), (2), (4)

	(C) (1), (3), (4) (D) (2), (3), (4)
C	49. 關於 IoT 安全設計開發階段之安全建議，下列敘述何者不正確？ (A) 開發設計階段，將 IoT 採用高強度的密碼，並且強制啟用 (B) 開發設計階段，採用最新安全的作業系統，確保漏洞已經修補 (C) 開發設計階段，採用經濟實惠的硬體裝置節省成本 (D) 開發設計階段，製造商須提供系統故障中斷的應變機制
D	50. 在多個物聯網裝置組成的網路中，攻擊者控制了其中一個節點並將傳送至此節點的所有封包全部丟棄，請問以上敘述屬於下列哪種攻擊手法？ (A) 黑函攻擊 (B) 分割攻擊 (C) 蟲洞攻擊 (D) 黑洞攻擊