初級資訊安全工程師 能力鑑定樣題

單選題 50 題

B	1. 下列何者非社交工程攻擊方式？ (A) 利用電子郵件誘騙使用者登入偽裝之網站以騙取帳號及通行碼 (B) 利用程式設計缺陷，向程式寫入錯誤的內容 (C) 利用即時通訊軟體如 LINE，偽裝親友來訊，誘騙點選來訊中之連結後中毒 (D) 利用電話佯裝資訊人員，騙取帳號及通行碼
C	2. 下列哪個協定較為安全？ (A) HTTP (B) FTP (C) SSL (D) TELNET
C	3. 短時間內傳送大量的封包給另一部電腦的攻擊方式，稱之為？ (A) 木馬程式或殭屍病毒 (B) 釣魚郵件攻擊 (C) 阻斷服務攻擊 (D) 中間人攻擊
A	4. 請問 SSH 常見的服務 Port 為？ (A) 22 (B) 23 (C) 24 (D) 25
B	5. 公司管理員打算利用 IPSec 來確保封包內容傳輸的私密性（Confidentiality），請問管理員需要使用 IPsec 的哪項協定以達成目的？ (A) AH (B) ESP (C) IKE (D) ISAKMP
B	6. 在未經授權的情況下取得網路傳輸資料，或者針對傳輸網路進行流量分析，請問上述行為屬於下列何者常見的網路威脅？ (A) 截斷（Interruption） (B) 竊取（Interception） (C) 偽造（Fabrication） (D) 篡改（Modification）
C	7. 網際網路中主要的通訊協定模式有兩種 OSI 7 層及 TCP/IP 協定組，請問在這兩個通訊協定模式中，負責傳輸封包（Packet）及選擇路徑

	（Routing），是那一層的工作？ (A) 實體層（Physical Layer） (B) 資料鏈結層（Data-Link Layer） (C) 網路層（Network Layer） (D) 應用層（Application Layer）
A	8. 下列何者不是應用在「虛擬私有網路」（VPN）上的通訊協定？ (A) TFTP (B) PPTP (C) IPSEC (D) SSL
C	9. 請問 TCP/IP 通訊協定中，負責提供分段排序、錯誤控制、流量控制等工作是哪一層之任務？ (A) 應用層 (B) 會議層 (C) 傳輸層 (D) 網路層
D	10. 關於跨站腳本攻擊（Cross-Site Scripting, XSS），下列敘述何者正確？ (A) 過濾雙引號之符號 (B) 使用 URL Encode (C) 使用正規表達式 (D) 使用 HTML Encode
D	11. 請問下列何者非 SYN SCAN 的優點？ (A) 快速及可靠 (B) 雜訊少 (C) 所有平台（不管 TCP 堆疊實作）皆準確 (D) 不會被偵測
D	12. 公司的資安人員想要安全性的監控網路上所有的交換器和路由器的狀態，請問他需要在每個設備上設定哪個協定？ (A) STP (B) VLAN (C) MPLS (D) SNMPv3
D	13. 下列何者不是資料外洩時，短期內所應採取的補救措施？ (A) 評估造成傷害的風險 (B) 立即收集有關外洩事故的重要資料 (C) 採取適當措施，制止資料外洩 (D) 執行資訊事故安全教育訓練

B	14. 當某一作業系統中的兩個程式因互相搶用資源而造成兩個程式均無法完成既定工作之結果，請問此現象稱為？ (A) 碰撞（Collision） (B) 死結（Deadlock） (C) 佇列（Queue） (D) 欺騙（Spoof）
A	15. 請問 ssh 公私鑰存在 Linux 哪個目錄？ (A) /.ssh (B) /home (C) /etc (D) user
B	16. 下列何項 Windows 功能可以封鎖未經授權之應用程式的自動安裝，並防止不小心變更系統的設定。即使系統管理員執行系統管理過程亦須要由管理員主動同意或提供認證資訊才能執行？ (A) 具有進階安全性的 Windows 防火牆 (B) 使用者帳戶控制（User Account Control；UAC） (C) 資源監視器（Resource Monitor） (D) Windows Secondary Logon
D	17. 下列何者非登入作業系統可使用的網路身分驗證服務？ (A) Windows AD（Active Directory）服務 (B) LDAP（Lightweight Directory Access Protocol）服務 (C) NIS（Network Information Service）服務 (D) DHCP（Dynamic Host Configuration Protocol）服務
A	18. 關於資安組織 OWASP(開放 Web 軟體安全計畫—Open Web Application Security Project)，下列敘述何者不正確？ (A) 是一個開放社群、營利性組織 (B) 主要目標是研議協助解決 Web 軟體安全之標準、工具與技術文件 (C) 長期協助政府或企業瞭解並改善網頁應用程式與網頁服務的安全性 (D) 美國聯邦貿易委員會（FTC）強烈建議所有企業需遵循 OWASP 所發佈的十大 Web 弱點防護守則
A	19. 下列何者不是常見的 SQL Injection 自動化工具？ (A) BEEF Framework (B) SQLMAP (C) BSQL (D) Bobcat

D	20. 下列何者不是 Server-side Injection 攻擊手法？ (A) Blind SQL Injection (B) Hibernate Injection (C) Command Injection (D) XSS Injection
A	21. 請問針對作業系統訂定的資訊安全策略中，下列何種安全模式中「檔案持有者」可授權決定「其他使用者」存取該檔案的權限？ (A) 自由存取控制（Discretionary Access Control，DAC） (B) 強制性存取控制（Mandatory Access Control，MAC） (C) 角色存取控制（Role-based Access Control，RBAC） (D) 屬性存取控制（Attribute-based Access Control，ABAC）
B	22. 用在入侵和攻擊他人的電腦系統上，取得系統管理員的權限，具有隱藏和遠端操控的能力；電腦病毒、間諜軟體等也常使用來隱藏蹤跡。該工具軟體為？ (A) Cookie (B) Rootkit (C) Backdoor (D) Phishing
D	23. 我們都知道要防止 XSS 跨網站指令碼攻擊必須過濾特殊字元，請問下列何者不是我們應該過濾的特殊字元？ (A) # (B) & (C) “ (D) ‖
D	24. 請問防禦 SQL Injection 的最佳方式為下列何者？ (A) 黑名單過濾 (B) 參數長度過濾 (C) 輸出過濾 (D) Prepared Statement
C	25. 下列哪種方法可讓開發人員發現其撰寫的網頁程式碼是否存有輸入驗證漏洞（Input Validation Weaknesses）？ (A) 反組譯應用程式執行碼 (B) 迴歸測試（Regression Testing） (C) 模糊測試（Fuzz Testing） (D) 使用除錯器（Debugger）逐步執行檢視
D	26. 網頁中使用驗證碼(CAPTCHA)主要可防禦下列何種攻擊？ (A) SQL 注入攻擊(Injection)。

	(B) 跨站腳本攻擊(XSS)。 (C) 緩衝區易位攻擊(Buffer Overflow)。 (D) 跨站偽造請求攻擊(CSRF)。
C	27. 下列何者屬於開發安全方面需注意的問題？ (A) 部署時必須考量伺服器效能，避免導致應用程式效能低 (B) 應用程式設計必須設計多線程，用戶能對服務隨時存取 (C) 應用程式必須考量是否有 SQL 注入漏洞 (D) 應用程式必須考量 License 限制，避免出現無法部署其他伺服器
A	28. 請問 2017 流行的 wannacry 攻擊是攻擊哪個服務？ (A) SMB (B) SMTP (C) HTTP (D) FTP
C	29. 下列何者不是常見的弱點掃描工具之一？ (A) Open Vulnerability Assessment System (OpenVAS) (B) Nessus (C) MegaSploit (D) Nmap
B	30. 當系統或應用程式上被發現具有弱點，但是在修補程式未發佈之前，或是使用者更新前所進行的惡意攻擊行為，稱之為？ (A) 釣魚(phising) (B) 零時差攻擊(zero day attack) (C) 暴力攻擊(brute-force attack (D) 重送攻擊(replay attack)
A	31. 下列哪個檔案最可能內含巨集型病毒（Macro Virus）？ (A) staff.doc (B) cmd.exe (C) command.dll (D) device.drv
B	32. 認識惡意程式，下列敘述何者不正確？ (A) 邏輯炸彈被設定在特定條件下啟動破壞攻擊行為 (B) 特洛伊木馬會自我複製，也會主動散播到別的電腦裡面 (C) 病毒會感染寄生或附著在別的電腦程式或文件檔案裡面 (D) 蠕蟲的特性是快速的自我繁殖感染其他的主機，發送大量封包，使網路癱瘓
D	33. 關於儲存媒體使用規範，下列敘述何者不正確？ (A) 各式儲存媒體如識別卡、磁碟片、磁帶、光碟片及各式磁碟機等

	如須報廢或不堪使用時，應將內含之資料加以清除，以確保資料安全 (B) 儲存機密資料之儲存媒體，必須遵照組織訂定之作業方式進行標示並妥善保存 (C) 機密資料變動時，媒體標示需即時更新 (D) 備份媒體無需定期更新，僅以抽檢方式驗證其有效性
D	34. 依據資訊安全管理系統 CNS27001、CNS27002 對資料備份的描述與要求，下列敘述何者不正確？ (A) 資料備份主要目的為防範資料漏失 (B) 組織宜建立備份政策，以定義組織對備份的相關要求 (C) 備份資料的存放地點宜於遠端，以避免主要場域發生災難時不被波及 (D) 備份資料測試復原時，應覆寫回原始媒體或系統，以確保資料復原之有效性
C	35. 關於保護公司內部機密性資料的備份，下列何者方式較佳？ (A) 隱藏保護 (B) 防寫保護 (C) 加密保護 (D) 雜湊保護
D	36. 關於備份，下列敘述何者正確？ (A) 差異備份係指與增量備份完成後之索引檔進行比對，只要發生過變化之文件都會再備份一次 (B) 完全備份係指與差異備份完成後之索引檔進行比對，只要發生過變化之文件都會再備份一次 (C) 差異備份係指與增量備份完成後之索引檔進行比對，只要發生過變化之文件都會再備份一次 (D) 差異備份係指與完全備份完成後之索引檔進行比對，只要發生過變化之文件都會再備份一次
B	37. 勒索軟體對於資料安全的傷害極大，請問下列敘述何者不正確？ (A) 勒索軟體感染方式，利用加密方式將電腦資料加密勒索 (B) 勒索軟體是透過網頁瀏覽或郵件感染造成，與網路無關 (C) 勒索軟體會造成備份成本增加 (D) 勒索軟體會感染一般電腦也會感染到網路主機
B	38. 關於系統日誌的管理與分析，下列敘述何者不正確？ (A) 每天不斷產生的日誌，資料量龐大，往往超出人力可以判讀的範圍 (B) 預設的 Syslog 本身沒有加密，但是不會遭到偽冒攻擊

	(C) 混合式攻擊手法普遍，很難從單一設備上解讀出攻擊手法的資訊 (D) 不同設備所產生的日誌格式可能不一樣，會造成彙整上的困難
D	39. Windows 作業系統中的事件檢視器，有三個較為重要之日誌檔，請問此三個日誌檔分別為下列何者？ (A) 連結性日誌、系統日誌、應用程式日誌 (B) 安全性日誌、網路日誌、應用程式日誌 (C) 安全性日誌、系統日誌、本機防毒日誌 (D) 安全性日誌、系統日誌、應用程式日誌
A	40. Bob 過去兩週一直在試圖滲透一個遠端的生產系統。 某一次，他能夠進入系統，並使用該系統三週的時間。 殊不知，執法機構也正在記錄他的每一項活動，並在後來成為證據。 該組織使用一種虛擬環境來捕獲 Bob。 這種虛擬環境是什麼？ (A) 一種用來困住駭客的蜜罐技術 (B) 一種使用特洛伊木馬的命令系統 (C) 一種用來困住登入後使用者的環境 (D) 一種用來困住登入前使用者的環境
C	41. 請問系統管理人員登入成功或失敗，是否需留存相關紀錄？ (A) 登入成功不需要，登入失敗需要 (B) 登入成功需要，登入失敗不需要 (C) 登入成功和失敗都需要 (D) 登入成功和失敗都不需要
D	42. 下列哪種行為可能會威脅雲端帳號的安全？ (A) 使用有公信力的服務 (B) 在不同網站使用不同帳號與密碼 (C) 避免使用陌生電腦登入雲端服務帳號 (D) 使用瀏覽器會記錄帳號密碼的便利功能
B	43. 雲端運算透過許多應用程式來提供服務，如果在身分驗證方面不夠嚴謹或是應用程式存在安全漏洞，可能就會造成使用時的安全問題。下列何者為所描述的安全威脅？ (A) 惡意的內部員工 (B) 不安全的介面與 APIs (C) 資源共享的技術問題 (D) 濫用與非法使用
D	44. 隨雲端服務時代來臨，網路及系統架構逐漸擴張，安全控制議題也被彰顯。請問下列何者不屬於安全控制中的認證方法？ (A) 驗證（Authentication）

	(B) 帳號管理（Accounting） (C) 授權（Authorization） (D) 加密（Encryption）
C	45. 行動裝置經常需要安裝新的 APP，如 Apple Store, Google Play 中下載。請問下列何者不是下載 APP 應注意之安全事項？ (A) 確認欲下載 APP 的評比與權限設定 (B) 只在信譽良好網站或官方 APP 市集中下載 (C) 該 APP 是否需要付費 (D) 觀察使用者對該 APP 之評論
C	46. 關於提高行動裝置（如手機）本身的安全性，下列敘述何者不正確？ (A) 開啟並設定開機密碼 (B) 開啟並設定解鎖密碼 (C) 加大電池容量 (D) 開啟並設定手機自動鎖定功能
D	47. 關於行動裝置上的應用程式軟體安全，下列敘述何者不正確？ (A) 僅安裝可信賴來源之軟體 (B) 定期更新軟體 (C) 安裝防毒軟體 (D) 可安裝破解版軟體節省荷包
A	48. 在物聯網裡，駭客可能會運用監聽程式（Sniffer），截取任何透過網路傳送之未加密的資訊再加以竊取。這是屬於哪一類的攻擊手法？ (A) 監聽攻擊（Sniffing Attack） (B) 密碼攻擊（Password-Based Attack） (C) 金鑰淪陷攻擊（Compromised-Key Attack） (D) 阻斷服務攻擊（Denial-of-Service Attack）
D	49. 在被認可的安全措施上，下列敘述何者不正確？ (A) 建立 IoT 安全設計指導準則 (B) 建立深層防護措施，分層防禦，以及常規性檢測工具 (C) 建立 IoT 安全資訊分享平台 (D) 不同產業可以建立一致的 IoT 安全基礎規範
B	50. 當兩個物聯網裝置在通訊過程中，傳遞的憑證訊息遭攔截並透過此憑證模擬合法身分達到存取特定服務。請問以上描述屬於下列哪種攻擊手法？ (A) 中間人攻擊 (B) 重送攻擊 (C) 冒充攻擊 (D) 監聽攻擊

C	51. 下列哪一項不是阻斷式服務攻擊（Denial-of-Service Attack）？ (E) 利用程式漏洞消耗 100%的 CPU 運算能力 (F) 向系統持續發送惡意封包，導致主機當機 (G) 寄送釣魚郵件給公司所有人員 (H) 向某個電子郵件地址發送成千上萬封電子郵件
A	52. 下列何種安全機制最弱？ (E) WEP (F) WPA (G) WPA2-Personal (H) WPA2-Enterprise
C	53. 下列敘述何者正確？ (E) 巨集病毒只會感染 Excel 檔案，但不會感染 Word 檔案 (F) 開機型病毒藏匿於硬碟非主要開機磁區 (G) 非常駐型病毒將自己寄生在 *.COM、 *.EXE 或是 *.SYS 的檔案中 (H) 檔案型病毒只會感染 .COM 檔
B	54. 請問防火牆的功能為？ (A) 檢核原始碼安全 (B) 保護網路安全 (C) 保護實體安全 (D) 保護人員安全
B	55. 下列何者是一般管理員採用動態路由協定（Dynamic Routing Protocol）以取代靜態路由（Static Routes）的主要理由？ (E) 動態路由的路由器負載較輕 (F) 動態路由能夠延展到較大的網絡 (G) 動態路由較安全 (H) 動態路由有較快的網路傳輸能力
D	56. 下列何種網路攻擊「不會」造成伺服器主機系統處理效率下降或發生錯誤？ (E) 死亡偵測攻擊（Ping-of-Death Attack） (F) 分割重組攻擊（Teardrop Attack） (G) 分散式攻擊（Distributed Attack） (H) 中間人攻擊（Man-In-The-Middle Attack）
C	57. 有一種防火牆的功能如下：「檢查來源端及目的端的 IP 位址、埠號（Port），若有符合網路安全管理人員所設定的安全規則就准許通過，

	否則拒絕其進入。」請問此為何種防火牆的描述？ (E) 應用代理閘道（Application-Proxy）防火牆 (F) 狀態檢查（Stateful inspection）防火牆 (G) 封包過濾（Packet Filter）防火牆 (H) 個人（Personal）防火牆
C	58. 在電子商務的交易過程中，可以運用「電子簽章技術」來確保資訊的哪一種特性？ (E) 可測試性 (F) 可維護性 (G) 不可否認性 (H) 易使用性
A	59. 「虛擬私有網路（VPN）」主要是透過什麼技術來建立網路上的安全通訊連線？ (E) 通道（Tunnel）技術 (F) 資料壓縮技術 (G) 調變與解調變技術 (H) 無線通訊技術
D	60. TCP/IP 通訊協定中，負責提供定址與路由工作的是哪一層之任務？ (E) 應用層 (F) 表達層 (G) 傳輸層 (H) 網路層
D	61. 請問常見的 DNS 資源記錄類型 CNAME 為？ (A) IPv4 主機位址 (B) 文字字串 (C) 郵件交換 (D) 別名
B	62. 公司管理人員正在設定交換器，並且需要確保只有授權的裝置才可以透過交換器存取公司網路。下列何者為最安全的做法？ (E) 設定 MAC 篩選基礎的連接埠安全性（Port Security） (F) 使用 802.1x (G) 創造每個裝置的 VLAN (H) 啟用 BPDU Guard 功能
D	63. 基於系統安全的基礎，系統管理者對所管理的伺服器（包含：應用程式、平台、資料庫等）應進行相關安全性設定，下列敘述何者正確？ (A) 系統上線後仍保留預設帳戶

	(B) 使用系統預設開啟的連接埠 (C) 錯誤訊息應開放詳細資訊以便問題修正 (D) 過期的 OS、Web / App Server、DBMS、API、函式庫等，應評估並進行更新
B	64. 當作業系統安裝好之後，為了避免因為安全因素導致作業系統遭受駭客入侵，應採取下列何項措施較佳？ (E) 更新病毒碼 (F) 更新修補程式 (G) 更新防火牆設定 (H) 更新入侵偵測系統
A	65. 下列何者並非攻擊者入侵主機後，常見使用來下載外部後門的指令？ (E) PING (F) WGET (G) CURL (H) FTP
A	66. 公司某部門有台 Windows 10 的電腦，允許所有部門員工登入使用，但基於安全性考量，除了管理員之外，希望能夠禁止一般員工在此電腦上使用 USB 行動碟，請問管理員應利用何種工具完成此項安全性需求作業？ (E) 本機群組原則 (F) 磁碟重組工具 (G) 行動裝置管理員 (H) 具有進階安全性的 Windows 防火牆
B	67. 下列何者不是微軟 Windows 作業系統中，具特權權限之帳號？ (A) Administrator (B) root (C) 在 Administrators 群組中之一般使用者帳號 (D) Local System
D	68. 有一種資安風險的描述為：「因為開發者暴露了內部檔案、檔案夾、金鑰、或資料庫的紀錄，來作為 URL 或是 Form 的參數，使攻擊者可藉由操作這些參數擅自進入其他 Objects 中」。此為下列何項風險的描述？ (E) 跨站腳本攻擊（Cross-Site Scripting） (F) API 未受防護（Underprotected APIs） (G) 注入攻擊（Injection） (H) 無效的存取控制（Broken Access Control）

A	69. 下列何者不是 Blind SQL Injection 的特性？ (A) SQL 錯誤資訊會顯示在頁面中 (B) SQL 錯誤資訊不會顯示在頁面中 (C) 常利用 wait for delay 語法來測試 (D) 常與 Time base SQL injection 一起發生
C	70. 下列何者不是網頁攻擊手法？ (E) Cross-Site Scripting (F) SQL Injection (G) Parameterized Query (H) Cross-Site Request Forgery
B	71. 請問針對作業系統訂定的資訊安全策略中，下列何種安全模式是統一由管理者進行檔案存取授權後，使用者才可以進行檔案存取？ (E) 自由存取控制（Discretionary Access Control，DAC） (F) 強制存取控制（Mandatory Access Control，MAC） (G) 角色存取控制（Role-based Access Control，RBAC） (H) 屬性存取控制（Attribute-based Access Control，ABAC）
C	72. 攻擊者針對網站應用程式漏洞，將 HTML 或 Script 指令插入網頁中，造成使用者瀏覽網頁時，執行攻擊者惡意製造的網頁程式。以上是說明哪一種攻擊手法？ (A) 資料隱碼攻擊（SQL injection） (B) 跨站請求偽照（Cross-Site Request Forgery, CSRF） (C) 跨網站腳本攻擊（Cross-Site Scripting, XSS） (D) 搜尋引擎攻擊（Google Hacking）
C	73. 關於跨站請求偽造（Cross-Site Request Forgery, CSRF），下列何者是最佳的解決辦法？ (A) 加入 HttpOnly (B) 過濾不必要特殊字元 (C) 加入圖形驗證碼 (D) 使用 HTTPS
B	74. 下列何者為防禦（Cross-Site Scripting, XSS）的最佳方式？ (A) 輸入參數黑名單過濾 (B) 輸入參數白名單過濾 (C) 輸入參數長度過濾 (D) 輸出頁面過濾
A	75. HTTP Cookie 的用途是？

	(A) 在瀏覽器中儲存資訊（如 Session ID 等） (B) 瀏覽器的設定檔 (C) 幫助防禦 XSS 攻擊 (D) 幫助防禦 XML Injection 攻擊
A	76. 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	77. 下列何者不是 Windows 安全開發必須注意的地方？ (A) Socket 設計 (B) 多執行緒設計 (C) 常駐程式設計 (D) 封包流量設計
D	78. 下列何者並非防毒軟體偵測的方式？ (A) 特徵碼掃描 (B) 檔案完整性掃描 (C) 沙箱檢測 (D) 程式碼檢核
D	79. 關於弱點掃描，下列敘述何者不正確？ (E) 弱點掃描工具的使用，可能會觸發入侵偵測系統的警告 (F) 弱點掃描可算是滲透測試的前置作業之一 (G) Ping 工具的使用，可算是弱點掃描的前置作業之一 (H) 部署 Web 應用程式防火牆，即可避免遭受弱點掃描的探測
B	80. 下列哪些是 rootkits 的主要特性？ (1)讓駭客取得最高權限 (2)具隱藏性 (3)在系統內大量自我複製 (4)讓駭客執行遠端控制 (E) (1)(2)(3) (F) (1)(2)(4) (G) (2)(3)(4) (H) (1)(2)(3)(4)

B	81. 你的老闆閱讀了一篇關於新發現嚴重漏洞的文章，而廠商所提供的修復漏洞修正檔也已於今天被釋出，他要求你立即更新所有系統此一修正檔，請問你應該採用下列何種做法？ (E) 立即將修正檔套用到所有系統 (F) 先測試修正檔，無誤後再行修補 (G) 先更新防毒軟體之後再行修補 (H) 先執行漏洞掃描，再進行修正檔套用
C	82. 下列何者不是電腦病毒的傳染途徑？ (E) 經由網路下載的軟體傳染 (F) 經由電子郵件的附加檔案中傳染 (G) 經由應用程式存取資料庫資料 (H) 經由已被感染的可移式媒體（如：USB、CD 等）
D	83. 關於備份管理作業，下列敘述何者不正確？ (E) 資訊系統資料需排定備份計畫，並定期執行備份作業 (F) 系統備份結果之相關作業紀錄須留存備查 (G) 規劃備份作業應包含系統設定、應用程式及資料庫等項目 (H) 備份資料需排定執行資料回復測試，並將測試結果記錄於本機紀錄檔
B	84. 下列哪個資訊儲存媒體，相較於其他選項，不太適合企業作為大量資料備份用途？ (E) LTO Tape (F) SD Memory Card (G) Disk Array（磁碟陣列系統） (H) Tape Library（磁帶櫃）
C	85. 某一個組織針對先前備份的資料進行復原時，發現先前備份的資料無法順利還原，請問這個組織可能是在以下哪個環節上出了問題？ (E) 沒有設定適當的 RTO 時間 (F) 因為備份的時間太長，以致影響了復原的可靠度 (G) 因為先前備份好的媒體，沒有定期進行復原測試 (H) 組織在訂定備份政策時，沒有定義好要執行備份的頻率
C	86. 為確保公司備份資料之完整性，下列何者方式最佳？ (A) 加解密 (B) 身分驗證 (C) 雜湊計算

	(D) 資訊隱藏
B	87. 某組織之上班尖峰時間為上午 9 點至 12 點，下午為 13 至 17 點，該組織為了資料安全，採取備份控制措施，請問該組織的備份控制措施最佳策略，應為下列何者？ (E) 中午 12 點執行完全備份，晚上 20 點進行差異備份 (F) 中午 12 點執行差異備份，晚上 20 點進行完全備份 (G) 上午 10 點執行完全備份，下午 15 點進行差異備份 (H) 上午 10 點執行差異備份，下午 15 點進行完全備份
D	88. 關於 Syslog 系統日誌或系統記錄，下列敘述何者不正確？ (E) Syslog 是一種用來在 TCP/IP 網路中傳遞記錄檔訊息的標準 (F) Syslog 系統日誌訊息可以被以 UDP 協定及 TCP 協定來傳送 (G) Syslog 通常被用於資訊系統管理及資安稽核 (H) Syslog 是以明碼型態被傳送，無法透過 SSL 或 TLS 方式加密
A	89. 關於「系統日誌」應該採取的適當保護措施，下列敘述何者不正確？ (E) 防止侵害個人隱私，不須記錄使用者識別碼 (F) 防止系統日誌被未經授權的存取 (G) 防範日誌記錄檔被修改或刪除 (H) 防範超過媒體記錄容量時所產生的錯誤
C	90. 請問「主要記錄系統本身登入/登出行為，例如系統管理人員透過遠端登入系統等」係下列哪個記錄檔之功能？ (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
D	91. 「留存日誌」是為了達成資訊安全的何種特性？ (A) 機密性（Confidentiality） (B) 可用性（Availability） (C) 可靠性（Reliability） (D) 不可否認性（Non-Repudiation）
B	92. 關於雲端蜜罐（Honeypot）技術，下列敘述何者不正確？ (E) 任何攻擊蜜罐的行為都是可疑的 (F) 通常設置在真正的運作環境之中 (G) 偽裝成有利用價值的網路、資料或電腦系統，並在裡面設置漏洞，誘使駭客攻擊 (H) 為取得電腦病毒樣本的其中一種方法
A	93. 對雲端服務的安全管理而言，實施稽核是一項必要的作法，可確認雲

	端服務提供商是否已符合相關的資安要求。下列何者不是確保雲端服務的安全需考量的事項？ (E) 用戶應選擇單一的雲端服務提供商所提供的服務 (F) 將實施稽核的權利納入合約之中 (G) 用戶應選擇熟悉雲端服務和法規的稽核人員 (H) 用戶可要求雲端服務提供商定期審查、更新、發佈和資安有關的流程與文件
A	94. 使用雲端架設的 Http 服務時，若伺服器回傳 404 的 HTTP 狀態碼，請問是以下何種情況？ (A) Not Found，請求失敗，請求所希望得到的資源未在伺服器上被發現 (B) OK，請求已成功，所請求的回應標頭或資料本體將被送回 (C) Gateway Timeout，伺服器嘗試執行請求時，未能及時從其他伺服器取得回應 (D) I'm a teapot，要求伺服器煮咖啡時應當回傳此狀態碼
D	95. 針對行動裝置的安全防護，下列敘述何者不正確？ (A) 行動裝置充電時應儘量使用變壓器座充，避免連接電腦 (B) 行動裝置應設置密碼或鍵盤鎖等防護措施 (C) 行動裝置應避免下載或安裝來路不明之安裝程式 (D) 行動裝置不會中毒，所以不需安裝防毒 App，以免影響行動裝置安全與效能
B	96. 關於提高行動裝置連線的安全性，下列敘述何者不正確？ (A) 當不需要開啟定位功能（GPS）時，應保持關閉 (B) 當有第三方免費提供 Wi-Fi 服務時就直接用，不需了解服務提供者身份 (C) 應小心使用藍牙功能，無使用需求時應予以關閉 (D) 當使用公眾場合所提供之手機充電功能時，應確保手機相關傳輸功能未被開啟或先手動關閉
D	97. 關於行動裝置上運用 HCE（Host Card Emulation）行動支付方式的安全，下列敘述何者不正確？ (E) 從雲端支付平台取得的金鑰是有時效性的 (F) 無需挑選通過服務平台安全認證的手機 (G) 手機無需具備安全元件來儲存支付資訊 (H) 需更換具備安全防護特殊的 SIM 卡才能支援

D	98. 在物聯網裡，電器設備透過無線通訊協定互聯時，有可能因為外來超強訊號的干擾而產生「蓋臺」的現象，這是屬於哪一類的攻擊手法？ (A) 中間人攻擊（Man-In-The-Middle Attack） (B) 資料隱碼攻擊（SQL Injection Attack） (C) 隱藏欄位攻擊（Hidden-Field-Tampering Attack） (D) 阻斷服務攻擊（Denial-of-Service Attack）
A	99. 目前在物聯網裡，連網的智慧家電多數是採用安全性不高的通訊協定，駭客可以利用這些不安全的通訊協定，進行什麼樣的攻擊？ (1) 中間人攻擊（Man-in-the-Middle） (2) 劫持（TCP/IP Hijacking） (3) 重播攻擊（Replay） (4) 垃圾搜尋攻擊（Dumpster Diving） (E) (1), (2), (3) (F) (1), (2), (4) (G) (1), (3), (4) (H) (2), (3), (4)
D	100. 物聯網安全漏洞有很多因素，下列敘述何者不正確？ (E) 物聯網軟體組件安全性不足，應將安全納入設計程序中 (F) 物聯網需要不斷的更新，並建立漏洞管理 (G) 物聯網安全必須建立在被驗證過的安全機制上 (H) 物聯網技術必須建立在黑盒子內，太透明風險更高