

109 年度初級資訊安全工程師能力鑑定試題

科目 1：資訊安全技術概論

考試日期：109 年 11 月 28 日

第 1 頁，共 9 頁

單選題 50 題 (佔 100%)

A	1. 下列何種傳輸協定會在傳輸的過程中將傳輸資料加密保護？ (A) SSH (B) HTTP (C) FTP (D) SMTP
A	2. 小明在咖啡廳想存取家中電腦所提供的 FTP 服務，請問小明在出門前須先對管理家中電腦連線的防火牆訂定下列何種安全政策？ (A) 開放連接埠 21，TCP 連線 (B) 開放連接埠 21，UDP 連線 (C) 開放連接埠 22，TCP 連線 (D) 開放連接埠 22，UDP 連線
C	3. 防火牆限制外部網際網路使用者，只可存取放置組織公開資訊（對外網站）的區域，不可進入內部網路，其放置組織公開資訊的區域一般被稱為下列何者？ (A) 虛擬區域網路（Virtual Local Area Network, VLAN） (B) 虛擬私人網路（Virtual Private Network, VPN） (C) 非軍事區（Demilitarized Zone, DMZ） (D) 無線區域網路（Wireless LAN, WLAN）
B	4. 關於 Syn Flooding 網路阻斷服務攻擊，下列敘述何者「不」正確？ (A) 用戶端發送 SYN 到伺服器端 (B) 伺服器端回傳 ACK 到用戶端 (C) 用戶端不發送 ACK 到伺服器端 (D) 伺服器端回傳 SYN-ACK 到用戶端
B	5. 下列何者「不」是 TCP/IP 連線劫持（Session Hijacking）攻擊成功的必要前提？ (A) 取得要劫持連線的 TCP 序號（Sequence Number） (B) 入侵受害主機並奪取執行權限 (C) 與受害主機可建立網路連線 (D) 偽裝成受害主機，發送特定 TCP 序號的封包
D	6. 網路應用程式防火牆（Web Application Firewall）用於防禦開放式系統互聯（Open System Interconnection, OSI）模型中第幾層之網路攻擊？ (A) Layer 1 (B) Layer 3 (C) Layer 5 (D) Layer 7

109 年度初級資訊安全工程師能力鑑定試題

科目 1：資訊安全技術概論

考試日期：109 年 11 月 28 日

第 2 頁，共 9 頁

A	7. 下列何種加密方法之強度最弱？ (A) 有線等效加密 (Wired Equivalent Privacy, WEP) (B) Wi-Fi 存取保護 (Wi-Fi Protected Access, WPA) (C) WPA2-Personal (D) WPA2-Enterprise
B	8. 防火牆主要是提供下列何種保護的功能？ (A) 原始碼安全 (B) 網路安全 (C) 實體安全 (D) 人員安全
C	9. 為了確保資訊傳送的安全性，下列敘述何者正確？ (1) 不要在答錄機上遺留敏感資訊的訊息 (2) 機密公文可以使用傳真機傳送 (3) 要注意電子郵件自動轉寄到外部郵件地址的使用規則 (4) 公務往來書信或訊息的保留與作廢，必須符合相關法規的要求 (A) (1), (2), (3) (B) (1), (2), (4) (C) (1), (3), (4) (D) (2), (3), (4)
A	10. 下列何者協定可能避免廣播風暴 (Broadcast Storm) ？ (A) 生成樹協定 (Spanning Tree Protocol, STP) (B) 位址解析協定 (Address Resolution Protocol, ARP) (C) 超文本傳輸協定 (HyperText Transfer Protocol, HTTP) (D) 傳輸控制協定 (Transmission Control Protocol, TCP)
C	11. 在資料進行傳輸過程中所使用的加密協定，下列何者為目前最安全者？ (A) SSL 1.2 (B) SSL 3.0 (C) TLS 1.2 (D) TLS 3.0
C	12. TCP/IP 通訊協定中稱為網路介面層，負責與硬體溝通的是下列何者？ (A) 應用層 (Application Layer) (B) 傳輸層 (Transport Layer) (C) 連結層 (Link Layer) (D) 網路層 (Network Layer)
A	13. 下列何者為 TCP 三向交握 (Three-way Handshake) 的最後步驟？

109 年度初級資訊安全工程師能力鑑定試題

科目 1：資訊安全技術概論

考試日期：109 年 11 月 28 日

第 3 頁，共 9 頁

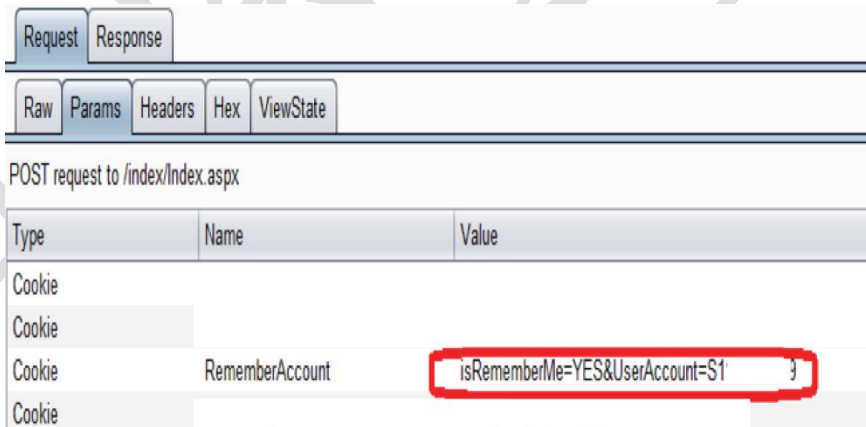
	(A) ACK (B) SYN (C) SYN/ACK (D) ACK/SYN
B	14. 下列何種作業系統透過終端機或是工作站登入，可以供多人共同使用並執行多個程式？ (A) 多人單工系統 (B) 多人多工系統 (C) 單人單工系統 (D) 單人多工系統
A	15. 請問 <code>grep -l -i pass /var/log/*.log 2>/dev/null</code> 指令，是要執行下列何種功能？ (A) 找出/var/log 中關於 pass 關鍵字的 log (B) 找出/var/log 中所有 log (C) 找出/var/log 中關於 2 的 log (D) 找出/var/log 中的密碼
B	16. 某公司基於安全性考量，決定將目前的 802.11 無線網路由原先的 WPA2- Personal 認證方法變更為 WPA-Enterprise，請問管理員需要在網路環境中新增管理下列何種伺服器？ (A) Kerberos 伺服器 (B) RADIUS 伺服器 (C) SNMP 伺服器 (D) NTP 伺服器
B	17. 請問 <code>cat ~/.bash_history</code> 指令，是要執行下列何種功能？ (A) 列出系統使用者 (B) 列出使用者曾經下過的指令 (C) 列出系統目錄 (D) 列出系統內的檔案
D	18. 應用程式執行特定作業結束後，並沒有通知作業系統，故無法向作業系統要求釋放記憶體空間，此狀況稱為下列何者？ (A) 記憶體暫存 (Memory Register) (B) 記憶體注入 (Memory Injection) (C) 記憶體映像 (Memory Mapping) (D) 記憶體洩漏 (Memory Leaks)
A	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「admin%27+OR+%271%27%3D%271%27+--」，請問可能為下列何種

109 年度初級資訊安全工程師能力鑑定試題

科目 1：資訊安全技術概論

考試日期：109 年 11 月 28 日

第 4 頁，共 9 頁

	<p>攻擊？</p> <p>(A) SQL 資料隱碼攻擊 (SQL Injection)</p> <p>(B) 目錄遍歷 (Directory Traversal)</p> <p>(C) 跨網站指令碼 (Cross-Site Scripting, XSS)</p> <p>(D) 不安全的反序列化漏洞 (Insecure Deserialization)</p>
C	<p>20. 下列何者「不」屬於程式弱點可能的利用方式？</p> <p>(A) 暴力破解 (Brute Force)</p> <p>(B) 緩衝區溢位 (Buffer Overflow)</p> <p>(C) 社交工程 (Social Engineering)</p> <p>(D) SQL 資料隱碼攻擊 (SQL Injection)</p>
D	<p>21. M 公司授權進行內部網路的安全活動，相關人員於過程中使用 Nmap 進行掃描，發現有內部主機使用 vsftpd2.3.4，經判斷後發現具備漏洞可利用，後續使用 Msfconsole 成功利用漏洞，此情境為下列何者？</p> <p>(A) 源碼掃描</p> <p>(B) 社交工程</p> <p>(C) 封包竊聽</p> <p>(D) 滲透測試</p>
C	<p>22. 附圖為 OWASP Top 10 – 2017 文件敘述中的何項風險分類？</p>  <p>(A) 跨網站指令碼 (Cross-Site Scripting, XSS)</p> <p>(B) XML 外部實體攻擊 (XML External Entity Attack, XXE)</p> <p>(C) 機敏資料外洩 (Sensitive Data Exposure)</p> <p>(D) 注入攻擊 (Injection)</p>
B	<p>23. 下列何者是被 SQL 資料隱碼攻擊 (SQL Injection) 成功的原因？</p> <p>(A) 作業系統漏洞未即時更新修補程式 (Patch)</p> <p>(B) 未對使用者的輸入資料進行過濾與檢查</p> <p>(C) 資料庫存取權限設定錯誤</p> <p>(D) 遭受大量網路流量攻擊</p>
D	<p>24. 關於跨站指令碼攻擊 (Cross-Site Scripting, XSS)，請問攻擊成功的常</p>

109 年度初級資訊安全工程師能力鑑定試題

科目 1：資訊安全技術概論

考試日期：109 年 11 月 28 日

第 5 頁，共 9 頁

	見原因是資通系統未過濾或防範下列何種程式的注入攻擊？ (A) Python (B) ASP.NET (C) ShellScript (D) JavaScript
D	25. 下列何者是解決跨站請求偽造（Cross-Site Request Forgery, CSRF）的最佳方式？ (A) 加入 HttpOnly (B) 過濾特殊字元 (C) 使用 HTTPS 連線 (D) 使用圖形驗證碼
A	26. 使用 HTTP Cookie 的目的為下列何者？ (A) 在瀏覽器中儲存資訊（如：Session ID） (B) 作為瀏覽器的組態設定檔 (C) 防禦 XSS 攻擊 (D) 防禦 XML Injection 攻擊
A	27. 下列何者最「不」能防範 SQL 資料隱碼攻擊（SQL Injection）？ (A) 對資料庫進行加密 (B) 對查詢字串進行字串過濾 (C) 使用 Prepare Statement (D) 使用 Stored Procedure
A	28. 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）
D	29. 某資安人員想要更進一步了解與比較他在資料中心中利用掃描工具所發現的漏洞，探討每個弱點能否被遠端利用，或是攻擊者是否需要登入才能利用此弱點漏洞利用程度、修復級別與漏洞嚴重程度評分等資訊，請問他應該檢視漏洞報告內的何種指標資訊？ (A) CSV (B) NVD (C) VSS (D) CVSS
D	30. 若網頁瀏覽器的 Cookies 並未使用加密保護機制，網站設計者為圖登入方便性而將使用者帳密儲存在 Cookie 之中，此種安全漏洞可能讓駭

109 年度初級資訊安全工程師能力鑑定試題

科目 1：資訊安全技術概論

考試日期：109 年 11 月 28 日

第 6 頁，共 9 頁

	<p>客使用下列何種網頁攻擊手法取得 Cookie 中的機敏資料？</p> <p>(A) SQL 資料隱碼攻擊 (SQL Injection)</p> <p>(B) XML 外部實體攻擊 (XML External Entity Attack, XXE)</p> <p>(C) Google 駭客 (Google-Hacking)</p> <p>(D) 跨站指令碼攻擊 (Cross-Site Scripting, XSS)</p>
A	<p>31. 下列何者「不」是發動中間人攻擊 (Man-In-The-Middle, MITM) 的必要手段？</p> <p>(A) 阻斷服務 (Denial of Service, DoS) 傳送端的功能</p> <p>(B) 偽造傳送端憑證</p> <p>(C) 竄改傳送端原始資訊</p> <p>(D) 將傳送端傳送的封包導引到駭客的機器</p>
C	<p>32. 某資安管理人員發現企業網路中爆發惡意軟體，該人員使用專門的惡意軟體分析工具從三個不同的系統中截取到惡意程式的樣本，並注意到惡意程式碼每次感染時均會略有變動，因此公司的防毒軟體無法盡早發現，請問這家公司感染了下列何者類型的惡意程式？</p> <p>(A) Multipartite Virus</p> <p>(B) Encrypted Virus</p> <p>(C) Polymorphic Virus</p> <p>(D) Stealth Virus</p>
B	<p>33. 關於滲透測試，下列敘述何者「不」正確？(1)滲透測試只可委由第三方執行、(2)滲透測試只能透過人工進行、(3)滲透測試可以檢測出邏輯瑕疵、(4)滲透測試只能在系統上線後進行，無法在測試區進行</p> <p>(A) (1)(2)(3)</p> <p>(B) (1)(2)(4)</p> <p>(C) (1)(3)(4)</p> <p>(D) (2)(3)(4)</p>
C	<p>34. 關於資料傳輸安全 (含實體資料及電子資料)，下列敘述何者較「不」正確？</p> <p>(A) 含有高風險之個人資料檔案，無論內部傳輸或對外傳送，皆應採用確認送達對方之傳遞方式，如：親送</p> <p>(B) 傳送電子檔案資料可透過專線、加密之 FTP 或其他適當方式進行保護</p> <p>(C) 僅針對高風險之個人資料檔案，採適當之安控機制</p> <p>(D) 個人資料檔案對外傳送時，應遵守資訊揭露的最小化原則 (如：僅呈現姓名及地址等資訊)，其他資訊則應適當彌封或遮蔽</p>
C	<p>35. 為確保公司備份資料之完整性，下列何種處理方式最佳？</p> <p>(A) 加解密</p>

109 年度初級資訊安全工程師能力鑑定試題

科目 1：資訊安全技術概論

考試日期：109 年 11 月 28 日

第 7 頁，共 9 頁

	<p>(B) 身分驗證</p> <p>(C) 雜湊計算</p> <p>(D) 資訊隱藏</p>
C	<p>36. 某組織在資料異動量大以及期望資料復原速度快之前提下，規劃了資料備份策略為週日進行完全備份，週一至週六進行「X」備份。該組織週三因系統問題導致資料毀損，此時資料備份管理員之處理程序為先還原週日完全備份資料後，再加上週二（事故發生前一天）所備份之資料，請問此「X」備份是指下列何者？</p> <p>(A) 完全備份（Full Backup）</p> <p>(B) 選擇式備份（Selective Backup）</p> <p>(C) 差異備份（Different Backup）</p> <p>(D) 增量備份（Incremental Backup）</p>
C	<p>37. 關於復原點目標（Recovery Point Objective, RPO），下列敘述何者正確？</p> <p>(A) RPO 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</p> <p>(B) RPO 的定義與組織執行備份的頻率與方式無相關</p> <p>(C) RPO 定義的時間愈短，組織所需投入的成本通常就愈高</p> <p>(D) RPO 與組織內資料可允許的誤差時間無關</p>
C	<p>38. 下列何者較可保護資料傳輸過程中的機密性？</p> <p>(A) 雙因子驗證</p> <p>(B) 編碼技術</p> <p>(C) 加密技術</p> <p>(D) 雜湊函數</p>
D	<p>39. 關於管理者及操作者日誌，下列敘述何者「不」正確？</p> <p>(A) 宜忠實記錄系統啟動及結束作業時間</p> <p>(B) 宜忠實記錄系統錯誤及更正作業</p> <p>(C) 宜忠實記錄建立日誌條目的人員</p> <p>(D) 系統作業日誌需要妥善保存，但不須交由第三者檢查</p>
C	<p>40. 在調查使用動態主機設定協定（Dynamic Host Configuration Protocol, DHCP）分配 IP 地址的網路時，應在何處查看並確定哪種媒體存取控制位址（Media Access Control Address, MAC）在特定時間具有特定的 IP 位址？</p> <p>(A) 在個人計算機的位址解析協定（Address Resolution Protocol, ARP）緩存上</p> <p>(B) 在 Web 服務器日誌文件中</p> <p>(C) 在 DHCP 服務器日誌文件中</p> <p>(D) 沒有辦法確定具體的 IP 地址</p>

109 年度初級資訊安全工程師能力鑑定試題

科目 1：資訊安全技術概論

考試日期：109 年 11 月 28 日

第 8 頁，共 9 頁

C	41. 關於日誌管理，下列敘述何者較正確？ (A) 日誌應正規化再留存，以利日後分析查閱使用 (B) 日誌不應壓縮留存，確保內容正確未遭受破壞 (C) 日誌應確保其「不可否認性」，透過日誌傳送協議（如：Syslog）至第三方單位即時儲存，可降低竄改風險 (D) 日誌種類繁雜並佔用大量儲存空間，分散儲存於服務主機中為最佳實務
C	42. 事件紀錄檔（Event log）用於蒐集、統計和分析電腦生成的事件紀錄檔消息，對於了解複雜系統的活動軌跡至關重要，它是由用於生成、傳輸、儲存、分析和處理事件紀錄檔數據的硬體、軟體、網路和媒體所組成。關於事件紀錄檔，下列敘述何者較「不」正確？ (A) 事件記錄包含伺服器登入資訊 (B) 事件記錄可以作為調查佐證 (C) 事件記錄包含工單資料 (D) 事件記錄需要至少保存足夠期間可供查詢
D	43. 下列何者「不」是雲端運算服務形式？ (A) SaaS (B) PaaS (C) IaaS (D) QaaS
B	44. 在雲端平台建置過程中常會使用磁碟陣列（Redundant Array of Independent Disks, RAID）當作儲存空間，請問下列何種模式容錯率最高？ (A) RAID 0 (B) RAID 1 (C) RAID 2 (D) RAID 5
A B 皆 給 分	45. 關於雲端蜜罐（Honeypot），下列敘述何者「不」正確？ (A) 通常設置在正式的產品運作環境之中 (B) 任何連線蜜罐的行為都是可疑的 (C) 偽裝成有價值的網路或電腦系統，並設置漏洞，誘使駭客攻擊 (D) 可用來取得電腦病毒樣本
A	46. 關於行動裝置安全，下列何者「不」在保護的面向之中？ (A) 擴充性 (B) 機密性 (C) 完整性 (D) 可用性

109 年度初級資訊安全工程師能力鑑定試題

科目 1：資訊安全技術概論

考試日期：109 年 11 月 28 日

第 9 頁，共 9 頁

C	<p>47. 關於行動裝置連線安全，下列敘述何者正確？(1)不需要開啟定位功能（GPS）時，應保持關閉、(2)有免費提供 Wi-Fi 服務時就直接用，不需了解服務提供者身份、(3)應小心使用藍牙（Bluetooth）功能，無使用需求時應予以關閉、(4)使用公眾場合所提供之手機充電功能時，應關閉手機傳輸功能</p> <p>(A) (1)(2)(3) (B) (1)(2)(4) (C) (1)(3)(4) (D) (2)(3)(4)</p>
C	<p>48. 在物聯網裡，網路犯罪分子可能竊取用來加密通訊的金鑰，並將之用於解譯加密過的資料，屬於下列何種攻擊手法？</p> <p>(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）</p>
B	<p>49. 物聯網時代的來臨，有人提出「預防無用論」（Perfect Prevention is Impossible），此一論點的主要見解為下列何者？(1)企業應永遠假設自身正在遭受攻擊、(2)企業應儘可能地降低攻擊所帶來的衝擊與影響、(3)企業絕對可以成功阻止針對性攻擊的入侵、(4)企業應建立整體性的持續防禦流程</p> <p>(A) (1)(2)(3) (B) (1)(2)(4) (C) (1)(3)(4) (D) (2)(3)(4)</p>
D	<p>50. 攻擊者控制了物聯網其中一個節點，並丟棄（Drop）所有傳送至此節點的封包，此為下列何種攻擊手法？</p> <p>(A) 黑函攻擊 (B) 分割攻擊 (C) 蟲洞攻擊 (D) 黑洞攻擊</p>