IPAS 證照輔導班

資訊安全技術概論

練習本

目錄

1.網路與通訊安全 2

1.1. 網路安全 Network Security 2

2. 作業系統與應用程式安全 5

2.1. 作業系統安全 5

2.2. 作業系統與應用程式 7

2.3. 程式與開發安全 9

3. 資安維運技術 10

3.1. 惡意程式防護與弱點管理(vulnerability management) ... 10

3.2. 資料安全(data Security)及備份管理(backup) 12

3.3.日誌管理 14

4. 新興科技安全 16

4.1. 雲端安全概論 cloud security 16

4.2. 行動裝置安全概論 Mobile security 17

4.3. 物聯網安全概論 IOT security 18

崑山科技大學資工系 IPAS 證照輔導班 練習

名稱: 1.網路與通訊安全

1.1 網路安全 Network Security

答案	編號	題目
	1.	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）
	2.	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
	3.	請問下列何者非為應用層服務? (A) HTTP (B) SMTP (C) IPX (D) FTP
	4.	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)
	5.	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) 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傳 (D)傳送時進行檢查與偵錯機制較 UDP 簡單
	6.	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
	7.	下列哪個協定較為安全？ (A) HTTP (B) FTP (C) SSL (D) TELNET
	8.	「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? (A)通道(Tunnel)技術 (B)資料壓縮技術 (C)調變與解調變技術 (D)無線通訊技術
	9.	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
	10.	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)

崑山科技大學資工系 IPAS 證照輔導班 練習

名稱: 1.網路與通訊安全

1.1 網路安全 Network Security

答案	編號	題目
	1.	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？ (A) 應用層 (B) 表達層 (C) 傳輸層 (D) 網路層
	2.	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
	3.	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
	4.	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
	5.	請問 SSH 常見的服務 Port 為？ (A) 22 (B) 23 (C) 24 (D) 25
	6.	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？ (A) 動態路由的路由器負載較輕 (B) 動態路由能夠延展到較大的網絡 (C) 動態路由較安全 (D) 動態路由有較快的網路傳輸能力
	7.	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? (A) 可測試性 (B) 可維護性 (C) 不可否認性 (D) 易使用性
	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
	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
	10.	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？ (A)設定 MAC 篩選基礎的連接埠安全性（Port Security） (B)使用 802.1x (C)創造每個裝置的 VLAN (D)啟用 BPDU Guard 功能

崑山科技大學資工系 IPAS 證照輔導班 練習

名稱: 1.網路與通訊安全

1.1 網路安全 Network Security

答案	編號	題目
	1.	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)
	2.	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？ (A) 死亡偵測攻擊（Ping-of-Death Attack） (B) 分割重組攻擊（Teardrop Attack） (C) 分散式攻擊（Distributed Attack）(D) 中間人攻擊（Man-In-The-Middle Attack）
	3.	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？ (A) PING (B) WGET (C) CURL (D) FTP
	4.	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
	5.	SMURF Attack 是利用何種協定進行攻擊? (A) ICMP (B) UDP (C) RIP (D) ARP
	6.	請問下列何者非 SYN SCAN 的優點？ (A) 快速及可靠 (B) 雜訊少 (C) 所有平台皆準確 (D) 不會被偵測
	7.	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
	8.	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)
	9.	下列哪一項不是阻斷式服務攻擊（Denial-of-Service Attack）？ (A) 利用程式漏洞消耗 100%的 CPU 運算能力 (B) 向系統持續發送惡意封包，導致主機當機 (C) 寄送釣魚郵件給公司所有人員 (D) 向某個電子郵件地址發送成千上萬封電子郵件
	10.	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)

崑山科技大學資工系 IPAS 證照輔導班 練習

名稱: 2.作業系統與應用程式安全

2.1 作業系統安全

答案	編號	題目
	1.	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
	2.	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）
	3.	請問 ssh 公私鑰存在 Linux 哪個目錄？ (A) /.ssh (B) /home (C) /etc (D) user
	4.	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
	5.	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
	6.	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
	7.	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)
	8.	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) 列出使用者曾下過的指令 (D) 列出安裝歷史
	9.	請問 2017 流行的 wannacry 攻擊是攻擊哪個服務？ (A) SMB (B) SMTP (C) HTTP (D) FTP
	10.	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

崑山科技大學資工系 IPAS 證照輔導班 練習

名稱: 2.作業系統與應用程式安全

2.1 作業系統安全

答案	編號	題目
	1.	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？ (A) 本機群組原則 (B) 磁碟重組 (C) 裝置管理員 (D) 進階安全性的 Windows 防火牆
	2.	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）
	3.	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
	4.	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？ (A) 自由存取控制（Discretionary Access Control，DAC） (B) 強制存取控制（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）
	5.	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
	6.	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？ (A)更新病毒碼(B)更新修補程式(C)更新防火牆設定(D)更新偵測系統
	7.	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
	8.	下列哪些是 rootkits 的主要特性？ (A) (1)(2)(3) (B) (1)(2)(4) (C) (2)(3)(4) (D) (1)(2)(3)(4) (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
	9.	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
	10.	請問 2017 流行的 wannacry 攻擊是攻擊哪個服務？ (A) SMB (B) SMTP (C) HTTP (D) FTP

崑山科技大學資工系 IPAS 證照輔導班 練習

名稱: 2.作業系統與應用程式安全

2.2.作業系統與應用程式(含資料庫與網頁)攻擊手法

答案	編號	題目
	1.	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
	2.	下列何者不是網頁攻擊手法？ (A) Cross-Site Scripting (B) SQL Injection (C) Parameterized Query (D) Cross-Site Request Forgery
	3.	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
	4.	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
	5.	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
	6.	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
	7.	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
	8.	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
	9.	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。以上是哪種攻擊？ (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）
	10.	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

崑山科技大學資工系 IPAS 證照輔導班 練習

名稱: 2.作業系統與應用程式安全

2.2.作業系統與應用程式(含資料庫與網頁)攻擊手法

答案	編號	題目
	1.	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
	2.	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)‖
	3.	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？ (A) 跨站腳本攻擊（Cross-Site Scripting）(B) API 未受防護（Underprotected APIs） (C) 注入攻擊（Injection） (D) 無效的存取控制（Broken Access Control）
	4.	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
	5.	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
	6.	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
	7.	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
	8.	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')>
	9.	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)
	10.	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

崑山科技大學資工系 IPAS 證照輔導班 練習

名稱: 2.作業系統與應用程式安全

2.3. 程式與開發安全

答案	編號	題目
	1.	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
	2.	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。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
	3.	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
	4.	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
	5.	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
	6.	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)必須設計多線程，用戶能對服務隨時存取 (C)必須考量是否有 SQL 注入漏洞 (D)必須考量 License 限制，避免出現無法部署其他伺服器
	7.	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
	8.	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)
	9.	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)可在不同系統執行(C)可在不同瀏覽器上執行(D)無法從遠端系統傳到本地端執行
	10.	關於逆向工程,下列敘述何者正確?(A)從組語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)從高語恢復組語的結構與語法過程(D)從高階語言恢復機語的結構與語法過程

崑山科技大學資工系 IPAS 證照輔導班 練習

名稱: 3.資安維運技術

3.1.惡意程式防護與弱點管理(vulnerability management)

答案	編號	題目
	1.	當系統或應用程式上被發現具有弱點，但在修補程式未發佈前，或是使用者更新前所進行的惡意攻擊行為，稱之？(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)
	2.	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
	3.	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)指攻擊者與通訊兩端分別建立獨立聯繫,並交換收到的資料 (D)蠕蟲(Worm)會不斷複製,並利用網路感染其他主機
	4.	下列何者不是電腦病毒的傳染途徑? (A) 經由網路下載的軟體傳染 (B) 經由電子郵件的附加檔案中傳染 (C) 經由應用程式存取資料庫資料 (D)經由已被感染的可移式媒體(如:USB、CD)
	5.	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
	6.	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
	7.	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,避免檢測數據相互干擾
	8.	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

	9.	下列敘述何者正確？ (A) 巨集病毒只會感染 Excel 檔案，但不會感染 Word 檔案 (B) 開機型病毒藏匿於硬碟非主要開機磁區 (C) 非常駐型病毒將自己寄生在 *.COM、 *.EXE 或是 *.SYS 的檔案 中 (D) 檔案型病毒只會感染 .COM 檔
	10.	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
	11	關於弱點掃描，下列敘述何者不正確？ (A) 弱點掃描工具的使用，可能會觸發入侵偵測系統的警告 (B) 弱點掃描可算是滲透測試的前置作業之一 (C) Ping 工具的使用，可算是弱點掃描的前置作業之一 (D) 部署 Web 應用程式防火牆，即可避免遭受弱點掃描的探測
	12	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
	13	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？ (A) 立即將修正檔套用到所有系統 (B) 先測試修正檔，無誤後再行修補 (C) 先更新防毒軟體之後再行修補 (D) 先執行漏洞掃描，再進行修正檔套用

崑山科技大學資工系 IPAS 證照輔導班 練習

名稱: 3.資安維運技術

3.2.資料安全(data Security)及備份管理(backup)

答案	編號	題目
	1.	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
	2.	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
	3.	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網路主機
	4.	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
	5.	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
	6.	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
	7.	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

	8.	關於備份管理作業，下列敘述何者不正確？ (A) 資訊系統資料需排定備份計畫，並定期執行備份作業 (B) 系統備份結果之相關作業紀錄須留存備查 (C) 規劃備份作業應包含系統設定、應用程式及資料庫等項目 (D) 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
	9.	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)
	10.	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
	11	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？ (A)沒有設定適當的 RTO 時間 (B)因為備份的時間太長，以致影響了復原的可靠度 (C) 因為先前備份好的媒體，沒有定期進行復原測試 (D) 組織在訂定備份政策時，沒有定義好要執行備份的頻率
	12	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
	13	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？ (A) LTO Tape (B) SD Memory Card (C) Disk Array(磁碟陣列系統) (D) Tape Library(磁帶櫃)
	14	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，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？ (A) 中午 12 點執行完全備份，晚上 20 點進行差異備份 (B) 中午 12 點執行差異備份，晚上 20 點進行完全備份 (C) 上午 10 點執行完全備份，下午 15 點進行差異備份 (D) 上午 10 點執行差異備份，下午 15 點進行完全備份

崑山科技大學資工系 IPAS 證照輔導班 練習

名稱: 3.資安維運技術

3.3.日誌管理

答案	編號	題目
	1.	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
	2.	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
	3.	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
	4.	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
	5.	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
	6.	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
	7.	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)

	8.	關於 Syslog 系統日誌或系統記錄，下列敘述何者不正確？ (A) Syslog 是一種用來在 TCP/IP 網路中傳遞記錄檔訊息的標準 (B) Syslog 系統日誌訊息可以被以 UDP 協定及 TCP 協定來傳送 (C) Syslog 通常被用於資訊系統管理及資安稽核 (D) Syslog 是以明碼型態被傳送，無法透過 SSL 或 TLS 方式加密
	9.	「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）
	10.	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
	11	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？ (A) 防止侵害個人隱私，不須記錄使用者識別碼 (B) 防止系統日誌被未經授權的存取 (C) 防範日誌記錄檔被修改或刪除 (D) 防範超過媒體記錄容量時所產生的錯誤

崑山科技大學資工系 IPAS 證照輔導班 練習

名稱: 4.新興科技安全

4.1.雲端安全概論 cloud security

答案	編號	題目
	1.	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
	2.	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
	3.	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
	4.	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)
	5.	在建立雲端服務所需資料庫時,從資安的角度來看,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
	6.	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
	7.	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？ (A) 用戶應選擇單一的雲端服務提供商所提供的服務 (B) 將實施稽核的權利納入合約之中 (C) 用戶應選擇熟悉雲端服務和法規的稽核人員 (D) 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

崑山科技大學資工系 IPAS 證照輔導班 練習

名稱: 4.新興科技安全

4.2.行動裝置安全概論 Mobile security

答案	編號	題目
	1.	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
	2.	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
	3.	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
	4.	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
	5.	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
	6.	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
	7.	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
	8.	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)

崑山科技大學資工系 IPAS 證照輔導班 練習

名稱: 4.新興科技安全

4.3.物聯網安全概論 IOT security

答案	編號	題目
	1.	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
	2.	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
	3.	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)
	4.	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）
	5.	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）
	6.	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

	7.	物聯網安全漏洞有很多因素，下列敘述何者不正確？ (A) 物聯網軟體組件安全性不足，應將安全納入設計程序中 (B) 物聯網需要不斷的更新，並建立漏洞管理 (C) 物聯網安全必須建立在被驗證過的安全機制上 (D) 物聯網技術必須建立在黑盒子內，太透明風險更高
	8.	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）
	9.	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） (A) (1), (2), (3)　(B) (1), (2), (4)　(C) (1), (3), (4)　(D) (2), (3), (4)
	10.	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