103年公務人員特種考試外交領事人員及外交行政人員、國際經濟商務人員、民航人員及原住民族考試試題

考 試 別：外交領事人員及外交行政人員特考
等　　別：四等考試
類 科 組：外交行政人員資訊組
科　　目：資訊安全與網路管理概要
考試時間：1 小時 30 分　　座號：_____

※注意：禁止使用電子計算器。

甲、申論題部分：（50 分）

㈠不必抄題，作答時請將試題題號及答案依照順序寫在申論試卷上，於本試題上作答者，不予計分。
㈡請以黑色鋼筆或原子筆在申論試卷上作答。

一、請說明下列名詞之意涵：（每小題 4 分，共 12 分）

㈠雪崩效應（Avalanche Effect）

㈡異常指引下查詢（Trap-directed Polling）

㈢線性密碼器（Stream Cipher）

二、在密碼學中有「對稱式」與「非對稱式」兩種密碼演算法。請針對此兩種演算法，分別說明其原理與相關應用。（13 分）

三、網際網路（Internet）制訂了一個名為 SNMP（Simple Network Management Protocol）的網路管理標準。SNMP 包含三個重要組成文件，請說明此三個文件制訂了那些相關網路管理標準。（10 分）

四、開發網路管理系統，通常會採用一個稱為三階層（3-tier）的系統架構。何謂三階層架構？如何運用它來建立網路管理系統？請說明之。（15 分）

乙、測驗題部分：（50 分）　　**代號：5202**

㈠本測驗試題為單一選擇題，請選出一個正確或最適當的答案，複選作答者，該題不予計分。
㈡共 25 題，每題 2 分，須用 2B 鉛筆在試卡上依題號清楚劃記，於本試題或申論試卷上作答者，不予計分。

1　使用加密演算法對某資料進行加密，在於確保該資料可滿足何種安全需求？

㈠機密性（confidentiality）　　㈡完整性（integrity）

㈢鑑別性（authenticity）　　㈣不可否認性（non-repudiation）

2　密碼式雜湊函數（cryptographic hash function）可將任意長度的訊息轉換成固定長度的輸出值，此輸出值稱為該訊息的雜湊值。下列敘述何者錯誤？

㈠密碼式雜湊函數具有訊息壓縮的特性，實務使用上應注意不同的輸入訊息可能會產生相同的輸出雜湊值

㈡密碼式雜湊函數具有單向不可逆的特性，無法從某訊息的雜湊值來反推訊息原文

㈢比對某傳輸訊息及其雜湊值，可藉以判定該訊息在傳輸過程中是否被更改

㈣為了增加密碼式雜湊函數的安全強度，實務使用上通常都不能公開該雜湊函數的運算演算法

3 有關數位簽章（digital signature）的運作原理及應用特性，下列敘述何者錯誤？

㈠簽署者使用所持有的私鑰對欲簽署訊息進行簽署

㈡驗證者必須獲得簽署者的公鑰後才能進行簽章驗證

㈢簽署者可重複使用某一訊息的合法簽章作為另一不同訊息的合法簽章

㈣簽署者、欲簽署訊息、簽章三者之間存在唯一的繫連關係，可用以達成簽署者對簽署訊息的不可否認性

4 攻擊者透過網路通訊協定的漏洞，鎖定某目標主機，大量重複傳送封包（packets），試圖讓該主機的系統工作超過其負荷，造成系統癱瘓。此攻擊方式屬於何種類型？

㈠溢位（overflow）攻擊　　㈡拒絕服務（denial of services）攻擊

㈢釣魚（phishing）攻擊　　㈣中間人（man in the middle）攻擊

5 下列何種軟體工具可協助電腦系統管理員用來隱藏不讓一般使用者看到的檔案，但也經常被攻擊者利用這種工具來取得系統管理員的權限，並對受害的電腦系統植入惡意程式？

㈠根目錄工具包（rootkits）　　㈡系統補丁更新（patch update）

㈢鍵盤側錄（keylogger）　　㈣封包過濾（packet filter）

6 網站資料庫系統遭受資料隱碼入侵（SQL injection）攻擊的主要原因為何？

㈠網站管理者採用 8 字元長度的通行密碼

㈡網站管理者未定期更換通行密碼

㈢網站設計者未對系統輸入欄位進行資料屬性查驗

㈣網站設計者未對系統輸出欄位進行資料屬性查驗

7 某企業的員工薪資資料庫系統提供平均值（AVERAGE）、總和（SUM）、變異數（VARIANCE）等統計查詢指令。假設該資料庫系統允許統計查詢某部門的平均月薪或總和月薪，但不允許查詢單一員工的個人月薪。欲使經由統計查詢某部門的平均月薪後仍不會意外洩漏某位員工的個人月薪，該資料庫系統應對統計查詢指令另提供何項安全控管功能？

㈠查詢次數限制　　㈡推論控制　　㈢身分識別　　㈣資料加密

8 為了防止天然災害對儲存資料造成毀損或遺失，應採用下列何種安全措施最為適當？

㈠資料加密　　㈡存取控制　　㈢人力備援　　㈣資料備份

9 若欲隱藏內部網路伺服器的 IP 位址（IP address）及連接埠（port），應採用下列何種類型的防火牆技術？

㈠篩子路由器（Screening Router）

㈡動態封包過濾器（Dynamic Packet Filter）

㈢應用層閘道（Application Level Gateway）

㈣網路位址轉譯（Network Address Translation）

10 依循開放系統互連（Open System Interconnection, OSI）的七層模式下，為了兼顧處理速度及使用彈性，通常會將封包過濾防火牆裝設在何處？

㈠應用層（application layer） ㈡會談層（session layer）

㈢網路層（network layer） ㈣資料連結層（data link layer）

11 經由下列何項國際標準的驗證，可用於評估市售資安產品的安全等級？

㈠全面品質管理（Total Quality Management, TQM）

㈡資訊技術服務管理（Information Technology Service Management, ITSM）

㈢能力成熟度模型整合（Capability Maturity Model Integration, CMMI）

㈣共通準則（Common Criteria, CC）

12 企業組織欲導入 ISO 27001 資訊安全管理系統標準的執行步驟中，第一步驟為何？

㈠制訂資訊安全政策 ㈡制訂適用性聲明

㈢定義資訊安全管理系統的適用範圍 ㈣制訂營運持續計畫

13 企業組織欲符合 ISO 27001 資訊安全管理系統標準的稽核要求，必須建立完整的四階文件。企業組織內相關資訊安全的管理程序文件是屬於第幾階文件？

㈠第一階文件 ㈡第二階文件

㈢第三階文件 ㈣第四階文件

14 Internet 的網路協定之核心為：

㈠ APP ㈡ WWW ㈢ TCP/IP ㈣ Ethernet

15 在 Internet 上傳及下載檔案的協定為：

㈠ TCP/IP ㈡ FTP ㈢ WWW ㈣ APP

16 在 4 個位元組的 IP 位址中，第一個位元組用來區分 IP 等級。下列的第一個位元組，那一個是 B 級的 IP 位址？

㈠ 101 ㈡ 127 ㈢ 191 ㈣ 199

17 建置網路時的網路拓樸（Topology），不包括下列那一項？

㈠ APP ㈡ Star ㈢ Ring ㈣ Bus

18 在網路建設中，將有線網路轉成無線網路的設備，稱為：

㈠ Repeater ㈡ AP ㈢ Bridge ㈣ WAP

19 網路設備中，負責路徑選擇之功能的設備為：

㈠ Router ㈡ Bridge ㈢ Repeater ㈣ Ethernet

20 在正式 IP 與非正式 IP 之間，做 IP 位址轉換的稱作：

㈠ Server ㈡ HTTP ㈢ NAT ㈣ Web

21 在企業內部的私有網路，稱作：

㈠ ISP ㈡ Internet ㈢ Extranet ㈣ Intranet

22 個人電腦上網最主要的有線網路，是下列那一項？

㈠ USB ㈡ Ethernet ㈢ HDMI ㈣ VGA

23 居家上網時，自動為上網電腦分派 IP 位址的協定，是：

㈠ Ethernet ㈡ WAP ㈢ WiFi ㈣ DHCP

24 為個人、家庭、企業連接到 Internet 的服務提供者，稱作：

㈠ Router ㈡ Bridge ㈢ ISP ㈣ Modem

25 下列那一項不屬於 WiFi 的安全協定？

㈠ WAP ㈡ WEP ㈢ WPA ㈣ TKIA