代號：20250
頁次：4－1

109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：外交人員考試
等　　別：四等考試
類科組別：外交行政人員類科資訊組
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請以藍、黑色鋼筆或原子筆在申論試卷上作答。
㈢本科目除專門名詞或數理公式外，應使用本國文字作答。

一、網路的媒體存取（Media Access）機制主要有 CSMA/CA 與 CSMA/CD 兩種協定，有關這兩個協定請回答下面問題：
㈠請分別說明這兩者的運作原理與機制。（16 分）
㈡說明何者適用於有線網路？（2 分）
㈢說明何者適用於無線網路？（2 分）

二、在公開金鑰加密系統（Public Key Cryptosystem）中，公鑰（Public Key）是不需要保密的，譬如：A 可以透過網路收到 B 傳送過來的公鑰，但此時 A 要如何確認並驗證這個公鑰是 B 的，是一個很重要的問題。公開金鑰基礎建設（Public Key Infrastructure）標準中，使用數位憑證（Digital Certificate）來解決這問題。對此，請回答：
㈠請先舉例說明公鑰的用途。（3 分）
㈡請說明數位憑證（Digital Certificate）與公鑰的關係。（3 分）
㈢請說明解決此問題的整個機制。（需說明到憑證管理機構與數位簽章技術）（12 分）

三、請詳細解釋下列專有名詞：（每小題 4 分，共 12 分）
㈠ FDMA
㈡ TCP SYN flood attack
㈢ VPN

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 對資料進行加密是要確保那一項的資安要求？

㈠機密性（Confidentiality）　　㈡完整性（Integrity）

㈢鑑別性（Authenticity）　　㈣可用性（Availability）

2 在實務應用上，使用公開金鑰密碼系統（Public Key Cryptosystem）的公鑰時，常用那一種方法來確保公鑰的有效性（Validation）？

㈠驗證該公鑰的憑證（Certificate）　　㈡驗證該公鑰的雜湊值（Hashed Value）

㈢測試該公鑰的亂度（Randomness）　　㈣測試該公鑰的加密（Encryption）功能

3 為避免使用 SQL 結構化查詢語言（Structured Query Language）而發生隱碼注入攻擊（SQL Injection Attack）的防禦方法，下列敘述何者錯誤？

㈠限制輸入字串的長度　　㈡排除輸入字串是否隱藏 SQL 指令

㈢不以系統管理員的帳號連結資料庫　　㈣開啟防火牆或防毒軟體加以阻擋

4 採用單一簽入（Single Sign-on）技術的系統登入方法，下列敘述何者錯誤？

㈠使用者不須使用多組不同的帳號及通行密碼來分別登入多種應用系統

㈡使用者只要登入一次，就可以使用該帳號授權使用的其他系統資源

㈢若駭客竊取到使用者的帳號及通行密碼，仍無法取得該帳號授權使用的其他系統資源

㈣可以有效簡化系統管理者對使用者的權限控管問題

5 有關導入 ISO 27001 資訊安全管理系統（Information Security Management System, 簡稱 ISMS）的標準驗證，營運持續管理程序書是屬於那一階文件？

㈠第一階　　㈡第二階　　㈢第三階　　㈣第四階

6 利用 Ping 指令進行 Ping of Death 攻擊，主要源自於下列那一項網路協定的安全弱點？

㈠ TCP（Transmission Control Protocol）

㈡ UDP（User Datagram Protocol）

㈢ ICMP（Internet Control Management Protocol）

㈣ SMTP（Simple Mail Transfer Protocol）

7 封包過濾防火牆（Packet Filter Firewall）是部署在 OSI（Open System Interconnection）七層模型中的那一層？

㈠應用層（Application Layer）　　㈡交談層（Session Layer）

㈢網路層（Network Layer）　　㈣資料連接層（Data Link Layer）

8 依據 OSI（Open System Interconnection）定義的七層模型，路由器（Router）是部署在那一層？

㈠網路層（Network Layer）　　㈡傳輸層（Transport Layer）

㈢應用層（Application Layer）　　㈣交談層（Session Layer）

9 有關雲端服務（Cloud Services），下列敘述何者錯誤？
㈠採用虛擬化技術（Virtualization）
㈡採用集中式架構（Centralized Architecture）
㈢可提供使用者隨選服務（Service on Demand）
㈣可提供動態擴充的資源共享服務

10 下列那一個網路協定可以同時提供在線（On-line）與離線（Off-line）的瀏覽模式，並可允許多個裝置同步讀取電子郵件？
㈠ POP（Post Office Protocol）　㈡ SMTP（Simple Mail Transfer Protocol）
㈢ UDP（User Datagram Protocol）　㈣ IMAP（Internet Message Access Protocol）

11 在兼顧安全考量及服務品質要求的前提之下，當監控到單位內部的網路流量突然持續暴增時，下列那一種緊急應變處理方式最適宜？
㈠立即關閉網路伺服器的電源　㈡立即關閉網路伺服器的外網連接埠
㈢立即啟動流量清洗及導流措施　㈣立即啟動入侵偵測系統更新

12 下列那種使用個人電腦的行為，會增加感染惡意程式的風險？
㈠安裝防毒軟體並定期進行掃描　㈡瀏覽不明網站上的免費影音檔案
㈢更新系統程式　㈣更新病毒特徵碼

13 下列關於社交工程攻擊之敘述中何者錯誤？
㈠社交工程是利用非技術性手段，取得系統存取的資訊
㈡偽裝成服務人員或管理人員，藉機騙取密碼
㈢攻擊目的在於誘使被害人安裝具有破壞性之惡意程式，達到非法存取或對系統之破壞行為
㈣可透過安裝防毒軟體阻擋社交工程攻擊，並定期更新病毒碼

14 下列關於 HTTPS 與 HTTP 敘述何者錯誤？
㈠ HTTPS 協定，可確保傳輸資料的完整性與機密性，使用 SSL 加密封包
㈡透過協定上的加密機制，HTTP 網站可防止資料竊取者直接瀏覽傳輸資料
㈢在 HTTP 協定中，網頁與電腦瀏覽器直接以明文形式傳輸資料
㈣使用加密協定，可能因加密額外消耗運算資源，也可能佔用比較多的傳輸頻寬

15 IP 位址可分為虛擬 IP 與實體 IP 兩種，可解決 IP 位址不敷使用之情況，下列關於虛擬 IP 敘述何者錯誤？
㈠虛擬 IP 封包需轉送時，路由器便會直接將其轉送至目的地
㈡當虛擬 IP 封包需要進入外部網路傳輸時，需進行網路位址轉換 NAT（Network Address Translation）轉換 IP 位址
㈢虛擬 IP 僅能使用於區域網路內，而無法直接與外部的網路進行資料傳遞
㈣虛擬 IP 的主機通常處於內部網路

16 單向雜湊函數（One-Way Hash Function）常用於產製資料串的數位指紋（Digital Fingerprint）。有關單向雜湊函數的特性，下列敘述何者錯誤？
㈠資料串被雜湊後，可從雜湊值還原出原來的資料串
㈡可接受輸入任意長度的資料串，輸出固定長度的雜湊值
㈢輸入不同資料串會產生相同雜湊值的機率非常低
㈣比對接收到的傳輸資料串及其雜湊值，可驗證該資料串在傳輸過程中是否有遭受更改

17 下列何種是客戶端與伺服器之間進行檔案傳輸的協定？
㈠ HTTP(Hyper Text Transfer Protocol)　㈡ SMTP(Simple Mail Transfer Protocol)
㈢ FTP(File Transfer Protocol)　㈣ PPP(Point to Point Protocol)

18 下列何者為網域名稱系統 DNS（Domain Name System）之功能？
㈠用於暫存先前存取過的資料　㈡將完整網域名稱轉換為其所對應的 IP 位址
㈢解讀網域名稱所在地區及網頁內容　㈣檢查兩端連線狀態是否正常

19 知名的勒索病毒 WannaCry 是透過 Windows 漏洞入侵電腦進行攻擊，下列關於勒索病毒敘述何者正確？
㈠讓使用者失去對系統或資料的控制，使系統或資料成為人質，強迫使用者支付贖金
㈡中了勒索病毒後，只需要換一台未中毒的電腦，即可復原中毒檔案
㈢勒索病毒幾乎都選擇「比特幣」作為贖金的工具，是因為比特幣交易方便
㈣將存在 C 槽資料備份到 D 槽是最有助於防止勒索病毒的方式

20 下列關於加密與雜湊的敘述何者錯誤？
㈠加密需要秘密金鑰，並且可以透過解密得到原文
㈡雜湊不需秘密金鑰，無法逆向解出原始輸入
㈢雜湊演算法通常被拿來檢驗傳送的訊息是否有被更改過
㈣相同的內容作為同一個雜湊演算法的輸入，得到的輸出一定不相同

21 駭客會在程式中置放常用的單字，方便猜測使用者密碼時大幅縮短破解密碼的時間，此種方式屬於下列何種攻擊方法？
㈠字典攻擊法　㈡網路釣魚　㈢殭屍網路攻擊　㈣阻斷服務攻擊

22 下列何者不是發生分散式阻斷服務攻擊（Distributed Denial-of-Service Attack）可能發生的問題？
㈠網路異常緩慢
㈡垃圾郵件的數量急遽增加
㈢嘗試存取網站或任何網際網路服務時被拒絕
㈣會在電腦上留下後門入口，供惡意使用者或程式可盜取機密或個人資訊

23 為了確保個人隱私以及傳遞資料時的安全性，在公共區域使用免費 WiFi 時，下列何者能夠降低中間人攻擊發生機率？
㈠關閉分享功能　㈡尋找較強的 WiFi 訊號
㈢使用 VPN（Virtual Private Network）　㈣將具有隱私的檔案放置於雲端

24 下列何者為資料隱碼攻擊 SQL Injection？
㈠一種惡意軟體，駭客能透過它長時間隱藏於用戶電腦中，進行資料竊取
㈡網路罪犯經由遠端遙控一群已被惡意軟體控制的電腦進行各種惡意行為
㈢將用戶電腦內的檔案資料鎖住或加密
㈣設計不良的程式因忽略字元檢查所衍生的問題，造成惡意指令得以入侵資料庫伺服器

25 電腦網絡中非軍事區 DMZ（Demilitarized Zone）是一個作為緩衝區域的小型網域。下列何者不是存放在 DMZ 中的伺服器所具備的特性？
㈠能夠提供服務給外界存取
㈡區內的伺服器不包含機密資料
㈢提供的服務可能包含 Web、FTP、DNS 等
㈣是一個屬於內部網域，但不屬於外部網域的特殊區域