104年公務人員特種考試外交領事人員及外交行政人員、民航人員、原住民族及稅務人員考試試題　代號：20250　全一張（正面）

考 試 別：外交人員特考
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、說明下列名詞的意涵：（每小題 5 分，共 20 分）
㈠隱私（Privacy）
㈡稽核（Audit）
㈢ Web-Based 網路管理架構
㈣傳輸層安全協議（Transport Layer Security）

二、關於實體安全（physical security）請回答下列問題：（每小題 5 分，共 15 分）
㈠實體安全的涵義為何？
㈡實體安全威脅有那些？
㈢實體安全措施有那些？

三、關於防火牆（firewall）請回答下列問題：（每小題 5 分，共 15 分）
㈠防火牆的涵義為何？
㈡防火牆本身有那些功能型態（types of firewall）？
㈢防火牆架構（firewall configurations）有那些？

乙、測驗題部分：（50 分）　代號：5202
㈠本試題為單一選擇題，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 ISO 27001 中，使用之 PDCA 循環，其中 PDCA 循環是指下列何者？
㈠準備－執行－檢查－稽核　㈡準備－執行－檢查－行動
㈢計劃－執行－檢查－稽核　㈣計劃－執行－檢查－行動

2 下列何種措施屬於實體安全（physical security）範疇？
㈠資訊硬體的置放點　㈡系統防毒軟體　㈢防火牆架構　㈣入侵偵測系統

3 ISO 27000 系列中，所定義之資訊安全的三項基本要素-CIA 原則，是指：
㈠可用性、存取控制、次序　㈡共作、次序、存取控制
㈢可用性、機密性、完整性　㈣存取控制、可用性、次序

4 SSL（Secure Sockets Layer），位於 TCP/IP 模型中的那一層？
㈠傳輸層　㈡網際網路層　㈢應用層　㈣網路存取層

5 利用 TCP 協定的特有攻擊，為下列何者？
㈠SYN flooding attack　㈡Overflow attack
㈢DoS （denial-of-service attack）　㈣Zombie network attack

6 要避免因網站本身的程式設計缺失所造成的資訊安全事件，下列何者敘述不屬於安全程式寫作要點？
㈠檢核所有連線來源　㈡檢查所有輸出資料
㈢分隔使用者與管理者的網頁介面　㈣控管上傳檔案

7 在區域網路中，運用 MAC 位址（MAC address）找出 IP 位址（IP address）的協定為：
㈠ARP　㈡RSVP　㈢RARP　㈣DNS

（請接背面）

104年公務人員特種考試外交領事人員及外交行政人員、民航人員、原住民族及稅務人員考試試題　代號：20250　全一張（背面）

考 試 別：外交人員特考
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

8 有關 IPv6 協定的敘述，下列何者正確？
㈠內建 IPSec ㈡IPv6 網址長度為 96 位元 ㈢內建 VPN ㈣與 IPv4 相容

9 利用人心理、個性弱點，應用溝通和欺騙技倆，以獲取帳號、通行碼或其他機敏資料的攻擊手法，稱為：
㈠Social engineering ㈡Replay attack ㈢Man-in-the-middle attack ㈣Phishing attack

10 下列何者與網路安全技術無關？
㈠PGP ㈡SSH ㈢DSA ㈣SGML

11 下列何者為網際網路上之網路管理協定？
㈠INMP ㈡NMPI ㈢NMPS ㈣SNMP

12 下列何者不屬於網際網路的應用服務？
㈠HTTPS ㈡Telnet ㈢SMTP ㈣PPP

13 若無線網路傳輸速率為 20Mbps，若要傳送 3GB 檔案，假設在無其他虛耗狀況，需要多少時間？
㈠20 分 ㈡150 秒 ㈢1500 秒 ㈣1000 秒

14 HTTPS 協定中使用會議金鑰（Session Key）是為了進行下列那一項功能？
㈠對稱式加密 ㈡非對稱式加密 ㈢資料壓縮 ㈣數位簽章

15 下列何者是國際信用卡發卡機構 Visa 及 Master Card 聯合制定的網路信用卡安全交易標準？
㈠SET ㈡VPN ㈢HTTPS ㈣EDI

16 透過長時間且持續性的潛伏及監控，針對特定的攻擊對象設計一套專屬的攻擊策略，此為下列那一種網路安全危害的型態？
㈠特洛依木馬（Trojan Horse）
㈡邏輯炸彈（Logic Bomb）
㈢非同步攻擊（Asynchronous Attack）
㈣進階持續性滲透攻擊（Advanced Persistent Threat, APT）

17 來源端對目標端傳送大量 TCP SYN 同步封包，這種行為是屬於下列那一種攻擊？
㈠緩衝區溢位（Buffer Overflow） ㈡連線截奪（Session Hijacking）
㈢阻斷服務（Deny of Service） ㈣網路監看（Sniffing）

18 關於 AES（Advance Encryption Standard）密碼演算法，下列敘述何者錯誤？
㈠AES 演算法是改良自 Rijndael 演算法
㈡AES 是利用有限場（Finite Field）數學模型所推論出來的演算法
㈢AES 是一種非對稱式加密演算法
㈣AES 是由美國國家標準與技術局（NIST）公開甄選出來的

19 企業網路欲防止內部資料的不合法進出，最好的因應方式應是安裝下列何者？
㈠入侵偵測系統 ㈡防毒軟體 ㈢資料備援系統 ㈣防火牆

20 關於 TCP（Transmission Control Protocol）與 UDP（User Datagram Protocol），下列敘述何者正確？
㈠TCP 會分割及重新組合資料，但 UDP 不會
㈡TCP 可以選擇路由(Routing)，UDP 則以廣播方式傳送
㈢TCP 屬於非連線導向，UDP 則屬於連線導向
㈣TCP 有擁塞控制（Congestion control）機制，UDP 有流量控制（Flow control）機制

21 下列何者是路由器之間用來交換路由資訊的通訊協定？
㈠OSPF ㈡ICMP ㈢IP ㈣SNMP

22 下列何者可以提供動態 IP 位址配置及網路設定參數？
㈠FTP ㈡DHCP ㈢NAT ㈣DNS

23 請問 IPv6 的 IP 位址比 IPv4 的 IP 位址多使用多少個位元組（Bytes）？
㈠4 ㈡6 ㈢8 ㈣12

24 TCP 利用下列何者來進行流量控制（Flow Control）？
㈠Handshaking ㈡序號
㈢接收視窗（Receiver Window） ㈣送方自行控制

25 有關無線網路與 ADSL，下列敘述何者正確？
㈠無線網路的傳輸速率通常高於 ADSL
㈡ADSL 是運用電話線當傳輸電路，而無線網路不需實體傳輸電路，所以 ADSL 安全性較無線網路低
㈢ADSL 的頻寬為獨享式，無線網路的頻寬為共享式
㈣無線網路傳輸資料錯誤率低於 ADSL