代號：20250
頁次：3－1

107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：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。
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、請詳細解釋下列專有名詞。（每小題 5 分，共 20 分）
㈠ Network Address Translation（NAT）
㈡ Software Defined Network（SDN）
㈢ Certificate Authority（CA）
㈣ Business Continuity Plan

二、瞬間大量的網路流量會對網路品質造成封包延遲或封包丟失等問題，面對此情況，網路管理者通常有下列三種策略：Overprovisioning, Priority, Quality of Service Guarantees。請說明此三種策略及各自的優缺點。（15 分）

三、針對網路安全中重要的 IPsec（Internet Protocol Security）協定組，請回答：（每小題 5 分，共 15 分）
㈠ IPsec VPN（Virtual Private Network）和 SSL VPN 主要差別為何？
㈡ IPsec 中的 AH（Authentication Header）協定和 ESP（Encapsulating Security Payload）協定的作用有何不同？
㈢ IPsec 中的 Transport mode 和 Tunnel mode 兩種操作方式有何不同？

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　下列何種網路拓樸的容錯能力最高，當其中一條路徑中斷時，仍然可以使用其他路徑傳輸資料？
㈠網狀網路　㈡環狀網路　㈢星狀網路　㈣匯流排網路

2　下列何者與傳輸層提供的主要功能無關？
㈠編訂序號　㈡控制資料流量　㈢偵錯與錯誤處理　㈣加密資料

3　關於路由器的敘述，下列何者錯誤？
㈠支援動態路由協定　㈡能解讀封包在網路層的資訊
㈢包含有路由表　㈣提供單一網路介面

4 下列何者為網路層之主要功能？
㈠編訂序號 ㈡選擇傳送路徑 ㈢控制資料流量 ㈣偵錯

5 下列關於傳輸媒介之敘述何者錯誤？
㈠使用雙絞線成本較低，但易受電磁波干擾 ㈡同軸電纜安裝及擴充容易，但可靠性差
㈢光纖傳輸速率高、不易受電磁波干擾且成本低廉 ㈣紅外線傳輸距離較短，易受其他物體阻隔

6 傳遞訊息時常需要進行錯誤偵測，若傳送 7 位元資料時，使用奇同位進行錯誤偵測，則下列何者正確？
㈠0000000 ㈡1111000 ㈢1010101 ㈣1100001

7 下列關於加密演算法敘述何者錯誤？
㈠RSA 和 DSA 屬於非對稱式加密系統
㈡DES 和 AES 屬於公開金鑰密碼系統
㈢RSA 之安全性是由於要將乘積分解成兩個大質數極其困難
㈣DSA 之安全性是基於解離散對數的複雜度

8 利用大量的殭屍電腦，對某網站發送大量封包，導致該網站無法提供服務，此方式屬於何種攻擊？
㈠電腦蠕蟲 ㈡分散式阻絕服務 ㈢郵件炸彈 ㈣特洛伊木馬

9 下列何者為 DNS 伺服器提供之服務？
㈠將網路卡位址轉換成 IP 位址 ㈡將 IP 位址轉換成網路卡位址
㈢將網域名稱轉換成 IP 位址 ㈣將訊號進行轉換

10 網路攻擊類型可分為主動式攻擊和被動式攻擊，下列何者屬於被動式攻擊？
㈠重送攻擊 ㈡偽裝攻擊 ㈢通訊分析攻擊 ㈣服務阻絕攻擊

11 下列關於資料隱碼攻擊（SQL Injection）敘述，何者正確？
㈠若使用者輸入資料未經過輸入驗證，便容易發生 ㈡不易造成資料外洩
㈢屬於系統內部人員所進行的攻擊 ㈣預防資料隱碼攻擊，資料庫權限應儘可能開放

12 下列何者與金鑰加密技術有關？
㈠SSL（Secure Socket Layer） ㈡cookie 技術
㈢錯誤控制 ㈣網域名稱轉換

13 下列關於資料交換技術之敘述，何者錯誤？
㈠電路交換在資料傳輸前，必須建立傳送端與接收端之間的連線，未傳輸完成前，其餘節點不可使用其之間的線路
㈡以訊息交換方式傳遞資料，因傳輸路徑上會進行錯誤檢查，因此能降低資料傳輸錯誤率
㈢分封交換技術會將資料切割成固定大小的封包，並依照封包所指定的傳輸路徑傳送
㈣以訊息交換傳遞資料，傳送端須於傳送資料前與接收端建立連線

14 下列何者不是數位簽章（Digital Signature）一定會用到的技術？
㈠訊息摘要（Message-Digest） ㈡非對稱式加密
㈢對稱式加密 ㈣公開金鑰

15 下列那一項是我國個人資料保護法與歐盟資料保護一般規則（GDPR）有較相同的規定？
㈠資料刪除權（被遺忘權）
㈡資料可攜權
㈢引進新科技之個資處理方式時需進行資料保護影響評估
㈣資料保護長制度

16 下列有關跨站腳本（Cross-Site Scripting, XSS）攻擊的描述，何者錯誤？
㈠攻擊的對象是使用者的瀏覽器
㈡XSS 發生於使用者的瀏覽器同時造訪多個網站（跨站）
㈢避免 XSS 的主要方法之一是將使用者所輸入的內容進行過濾
㈣駭客事先將攻擊的語法貼至網站留言板，讓受害者造訪被感染的留言板時，會自動執行攻擊，是一種 Persistent XSS 攻擊

17 下列有關緩衝區溢位（Buffer Overflow）攻擊的描述，何者錯誤？
㈠跟程式語言有關，例如不會發生在以 Java 撰寫的程式
㈡與作業系統執行環境有關，例如不會發生在行動裝置（如手機）或遊戲機（如 PS4）
㈢攻擊發生原因是由於程式未檢查緩衝區的邊界，所以要對某一程式進行緩衝區溢位，需先分析該程式的原始碼或執行碼
㈣目前 Linux 已在核心作業系統有提供緩衝區溢位保護機制

18 使用軟體定義網路交換器進行封包過濾與傳統防火牆的規則模式（Rule-Based）最大的差異為何？
㈠可阻斷（drop）送往某個特定的 IP 位址的封包
㈡可阻斷含有特定應用程式封包內容（payload）的封包
㈢可依各埠的封包數量統計資料透過程式自動、動態新增過濾條件
㈣可阻斷某個使用者送出的封包

19 下列有關虛擬區域網路（Virtual LAN, VLAN）技術的敘述，何者正確？
㈠一個 VLAN 的成員可來自不同 switch 下的 hosts，而同一 switch 下的 hosts 可被切割成屬於不同 VLAN
㈡兩 VLAN 間互通封包只需透過 layer 2 switch
㈢不同的 VLAN 可共用一個 IP subnet，以節省 IP 的使用
㈣IEEE 802.1Q 是 VLAN 的標準，其所定義的 VLAN ID 有 16 bits

20 網路除錯工具，例如 ping, traceroute 等，是利用那一個協定來實作？
㈠SNMP ㈡HTTP ㈢ICMP ㈣ARP

21 某單位取得 200.100.100.0/22 的網路位址，下列敘述何者錯誤？
㈠其網路位址（network address）為 200.100.100.0 ㈡其廣播位址（broadcast address）為 200.100.100.255
㈢其可分配給單位內的電腦 IP 位址數有 1022 個 ㈣此網段為四個連續的 Class C 所組成

22 Internet Protocol 從 IPv4 演進到 IPv6 後，下列那一個欄位已不在 IPv6 的表頭（header）中？
㈠payload length ㈡traffic class ㈢version ㈣checksum

23 橢圓曲線密碼系統（ECC）與 RSA 加密演算法的比較何者正確？
㈠RSA 安全性比較高 ㈡ECC 適用於計算能力較差的設備，例如行動裝置
㈢ECC 是對稱式加密法 ㈣TLS 只採用 RSA

24 下列何者不是實現虛擬私人網路（Virtual Private Network）的必要機制？
㈠訊息加密/解密 ㈡身分驗證（Authentication）
㈢IPSEC 協定 ㈣金鑰交換

25 有關網路管理協定（SNMP），下列敘述何者錯誤？
㈠目前最新版本為 SNMPv3
㈡為了增加效能，SNMPv2 中加入了 GetBulkRequest 指令
㈢SNMPv3 增加了遠端組態設定（remote configuration）的機制
㈣SNMPv2c 是採 SNMPv1 的 community-based security 機制，可向後相容於 SNMPv1

測驗式試題標準答案

考試名稱：107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

類科名稱：外交行政人員資訊組

科目名稱：資訊安全與網路管理概要（試題代號：5202）

單選題數：25題　　單選每題配分：2.00分

複選題數：　　複選每題配分：

標準答案：

題號	第1題	第2題	第3題	第4題	第5題	第6題	第7題	第8題	第9題	第10題
答案	A	D	D	B	C	D	B	B	C	C

題號	第11題	第12題	第13題	第14題	第15題	第16題	第17題	第18題	第19題	第20題
答案	A	A	D	C	A	B	B	C	A	C

題號	第21題	第22題	第23題	第24題	第25題	第26題	第27題	第28題	第29題	第30題
答案	B	D	B	C	D					

題號	第31題	第32題	第33題	第34題	第35題	第36題	第37題	第38題	第39題	第40題
答案										

題號	第41題	第42題	第43題	第44題	第45題	第46題	第47題	第48題	第49題	第50題
答案										

題號	第51題	第52題	第53題	第54題	第55題	第56題	第57題	第58題	第59題	第60題
答案										

題號	第61題	第62題	第63題	第64題	第65題	第66題	第67題	第68題	第69題	第70題
答案										

題號	第71題	第72題	第73題	第74題	第75題	第76題	第77題	第78題	第79題	第80題
答案										

題號	第81題	第82題	第83題	第84題	第85題	第86題	第87題	第88題	第89題	第90題
答案										

題號	第91題	第92題	第93題	第94題	第95題	第96題	第97題	第98題	第99題	第100題
答案										

備　　註：