代號：20250
頁次：4－1

106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、稅務人員及原住民族考試試題

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。
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、請試述下列名詞之意涵：（每小題 7 分，共 28 分）
㈠存取控制（Access Control）
㈡被信任的第三方（Trusted Third Party）
㈢組態管理（Configuration Management）
㈣服務品質（Quality of Service, QoS）

二、國際規範對資訊安全的定義如下：維護資產的隱密性（Confidentiality）、完整性（Integrity）、可用性（Availability）；請說明此三個安全需求與相關的解決方案。（22 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　依網路傳輸與系統處理需求，設定各類通訊協定的優先權與頻寬百分比限制，這是 ISO 7498.4 網路管理的那一項功能？

㈠組態管理（Configuration Management）　　㈡效能管理（Performance Management）

㈢障礙管理（Fault Management）　　㈣帳務管理（Accounting Management）

2　下列那一項通訊協定可以達到網管組態管理所需的網路拓樸資訊、自動搜尋網路設備、路由資訊及設定資訊等管理功能？

㈠ SNMPv2　　㈡HTTP　　㈢DHCP　　㈣ICMP

3　關於 TCP 與 UDP，下列那一個是相同的？

㈠錯誤控制的機制　　㈡建立連線的機制

㈢都是傳輸層的協定　　㈣協定的主要標頭（Header）

4 有關集線器（Hub）與交換器（Switch）的不同，下列敘述何者正確？

㈠集線器主要是廣播，任何一部連到集線器的電腦，所傳送出來的資料，集線器會將其廣播給所有連到該集線器的電腦。交換器則會依所傳資料的目的地，經過濾（Filter）後傳給適當區段的電腦

㈡集線器就是 IP 分享器，交換器也就是路由器（Router）

㈢交換器會有資料競爭與碰撞（Contention & Collision）問題，集線器則不會

㈣集線器與交換器沒什麼不同

5 下列那一項不是虛擬區域網路（Virtual LAN）的特性？

㈠是一種邏輯性（Logical）分群的概念，透過交換器（Switch）與軟體的設定達成

㈡可有效管理頻寬，避免資料流量過多壅塞的問題

㈢就是俗稱的網路翻牆的技術

㈣也有保障資訊安全的效益

6 伴隨 IP 協定，提供網路錯誤偵測與回報機制的網路層協定（如 ping, traceroute）的是：

㈠ ICMP ㈡HTTP ㈢TCP ㈣FTP

7 IPv4 的主要標頭（Header）的欄位中，那一個欄位是封包在傳送過程中，每經過一個路由器（Router）一定會改變的？

㈠ Total Length ㈡Fragmentation Offset ㈢Protocol ㈣Time-to-live

8 某 IP 位址為 200.107.16.17/18，則其所屬的網路位址區塊的起、迄位址為何？

㈠ 200.107.16.0/18～200.107.16.255/18 ㈡200.107.0.0/18～200.107.63.255/18

㈢200.107.16.17/18～200.107.16.18/18 ㈣200.107.0.0/18～200.107.255.255/18

9 有關動態主機設置協定（DHCP, Dynamic Host Configuration Protocol），以及網路位址轉換（NAT, Network Address Translation）的敘述，下列何者錯誤？

㈠兩者皆可解決在組織內 IP 不夠用的問題

㈡DHCP 是當主機有需要上 Internet 時，動態指派一個 IP 給它，NAT 則是指派內部私有 IP 給主機來上網

㈢主機要上 Internet 一定要有 DHCP 或 NAT 才行

㈣如果某主機是在 NAT 裡面的機器，如沒特別的設定，在 NAT 外部的電腦無法從外部直接連到該主機

10 下列那種網路攻擊的方式，不是屬於誠信（Integrity）威脅這一類的樣態？

㈠阻斷服務（Denial of Service） ㈡修改（Modification）

㈢重放（Replaying） ㈣否認（Repudiation）

11 有關數位簽章（Digital Signature）的敘述，下列何者錯誤？

㈠可以提供私密（Confidential）服務 ㈡可以提供忠誠、完整（Message Integrity）服務

㈢可以提供認證（Message Authentication）服務 ㈣可以提供不可否認（Nonrepudiation）服務

12 封包過濾（Packet-filter）防火牆，無法過濾／阻擋下列何種封包？

㈠從某個特定 IP 送來的封包

㈡內部封包要連至任何機器上的某個特定 port 服務的封包

㈢要連至某個特定 IP 機器上的某個特定 port 服務的封包

㈣阻斷某個特定使用者送來的封包

13 虛擬私人網路（VPN, Virtual Private Network）是藉由那些機制，來保有它的私密性（Privacy）？

㈠點對點隧道協定（PPTP, Point-to-Point Tunneling Protocol），以及安全連線，如 IPSec 協定

㈡加密以及網路位址轉換（NAT）

㈢點對點隧道協定（PPTP）以及網路位址轉換（NAT）

㈣使用帳號以及密碼控制權限

14 勒索病毒使得被勒索者難以在有效時間內解開，卻又可以在收到錢後將資料還原，下列那一項技術不會用於此攻擊？

㈠非對稱式金鑰技術，以勒索者所擁有的公開金鑰（Public Key）加密使用者資料，再於取款之後，以勒索者所擁有的私密金鑰（Private Key）來解密

㈡對稱式金鑰技術，被勒索者不擁有解密金鑰，只有勒索者才能解密

㈢採用加強式 RSA+AES 來進行加密，而難以在有效時間內破解

㈣採用分散式阻斷式攻擊（DDoS, Distributed Denial of Service），讓使用者系統處於忙碌中，無法正常開啟資料檔案

15 解決勒索病毒最根本的作法，不包括下列何者？

㈠資料離線備份　　㈡加強防火牆

㈢重新組態軟體設定和更新補強軟體漏洞　　㈣建構大量計算設備，以縮短解密和解病毒時間

16 對於虛擬私人網路（VPN, Virtual Private Network）達成「在家上班」的目的，下列敘述何者錯誤？

㈠必須事先申裝專屬實體線路直接連結家中電腦和目的地的網路（如總公司網路）

㈡即使存取公司外的網際網路資料，所有傳送封包都會先送至連結目的地的網路（如總公司網路）

㈢運用諸如網際網路安全協定（IPSec）來執行加密和認證功能，以保護傳送封包避免遭到攻擊

㈣提供使用者在家直接通過防火牆認證，以存取企業內部網路的資源

17 認證中心（CA, Certificate Authority）功能不包括下列何者？

㈠憑證核發和註銷　　㈡時戳服務

㈢數位簽章公開和私密金鑰產製及認證　　㈣保護核發的個人私密金鑰不被盜取

18 某銀行遭國外分行入侵，進而遠端遙控臺灣自動提款機自動吐出錢鈔，下列何者不是達成這次盜領的技術？

㈠利用遠端植入可控制開啟吐鈔開關 cnginfo.exe 和吐鈔 cngdisp.exe 程式

㈡運用刪除程式 delete.exe 和指令檔 cleanup.bat，清除 cnginfo.exe 和 cngdisp.exe 程式，以避開稽核

㈢利用電話錄音伺服器，提供作案者直接以手機語音服務，在自動提款機前控制機器吐鈔

㈣仿冒派送軟體並開啟控制服務執行 cnginfo.exe 和 cngdisp.exe 程式，以達到吐鈔功能

19 為避免火災、水災及地震等自然災害影響資訊安全，應採取下列那一個方法為宜？

㈠資料加密　　㈡異地備援

㈢離線資料處理　　㈣設置於大樓地下室獨立空間

20 指紋、人臉、瞳孔等辨識是用來達到何種資訊安全功能？

㈠認證（Authentication）　　㈡完整性（Integrity）

㈢可用性（Availability）　　㈣機密性（Confidentiality）

21 利用電腦漏洞於區域網路中快速散播病毒的方式為下列那一個網路攻擊？

㈠阻斷式服務（DoS, Denial of Service）　　㈡蠕蟲（Worm）

㈢連線截奪（Session Hijacking）　　㈣邏輯炸彈（Logic Bomb）

22 下列那一類型的指令可以確認遠端的電腦或是伺服器主機是否為開啟狀態？

㈠ syn-sent　　㈡traceroute（or tracert）

㈢netstat（or netstat - r）　　㈣ipconfig（or ipconfig / all）

23 下列何者不隸屬於社交工程（Social Engineering）的攻擊手法？

㈠網路釣魚　　㈡電子郵件隱藏電腦病毒

㈢偽裝修補程式　　㈣利用程式破解作業系統漏洞

24 下列那項技術無法達到不可否認性（Non-repudiation）功能？

㈠區塊鏈（Block Chain）　　㈡RSA 加密技術

㈢AES 加密技術　　㈣數位簽章（Digital Signature）

25 下列那一項是區塊鏈技術的關鍵特點，可讓大家建構信任於去中心化之後的電腦網路？

㈠共識演算法（Consensus Algorithm），以多數電腦共同認證來增強信任

㈡加強金鑰長度，難以解密之下以建立信任機制

㈢採用大型主機以平行處理（Parallel Process）加快資料加解密速度

㈣運用開放原始碼（Open Source）來達到信任效果