105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、國際經濟商務人員及原住民族考試試題　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、請說明下列名詞的意涵：（每小題 5 分，共 20 分）

㈠魚叉式釣魚攻擊（Spear phishing attack）

㈡內容傳遞網路（Content Delivery Network, CDN）

㈢服務層級協議（Service Level Agreement, SLA）

㈣公眾交換資料網路（Public Switched Data Network, PSDN）

二、防火牆（Firewall）是一般組織最常見的安全防護工具，而現代防火牆多採用 Stateful Packet Inspection（SPI）技術，請詳細回答下列問題：

㈠何謂 SPI？為何要使用此技術？（10 分）

㈡ Packet-filtering Firewall 和 Web Application Firewall（WAF）有何不同？（10 分）

三、無線區域網路（Wireless LAN）已是目前非常普遍的網路技術，請問：

㈠為何無線區域網路在實體層要使用展頻（Spread spectrum）技術？（5 分）

㈡ Evil Twins Access Point 攻擊會對 WLAN 造成何種安全危害？請說明之。（5 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 ECDSA（Elliptic Curve Digital Signature Algorithm）技術無法提供的安全功能為何？
Ⓐ鑑別性（authentication）　Ⓑ機密性（confidentiality）
Ⓒ完整性（integrity）　Ⓓ不可否認性（non-repudiation）

2 有關 spam 之敘述何者錯誤？
Ⓐ不請自來的大量廣告行銷電子郵件為 spam 之一種
Ⓑ公務用的個人電子郵件信箱僅用於公務，私人網購或是訂閱免費電子報使用免費電子郵件服務如 gmail 之措施可以有效降低公務用的個人電子郵件信箱收到 spam
Ⓒ使用過濾識別黑名單機制無法改善 spam 的干擾
Ⓓ永遠不要回覆 spam，有機會降低 spam 的量

3 下列技術何者最適合通訊雙方用來建立會議密鑰（session key）？
Ⓐ AES　Ⓑ DES　Ⓒ DSA　Ⓓ RSA

4 下列區塊加解密模式何者在兼顧安全之前提下，有最適合網路高速傳輸之條件？
Ⓐ CTR mode　Ⓑ CFB mode　Ⓒ CBC mode　Ⓓ ECB mode

5 保護資料私密性目前大部分都不採取單一 DES 的最主要原因為何？
Ⓐ核心功能已被破解而不安全　Ⓑ受專利保護應用成本相對偏高
Ⓒ核心技術不夠公開透明有疑慮　Ⓓ密鑰長度太短容易受暴力攻擊

6 Diffie-Hellman Key Exchange 技術潛存何種攻擊之威脅？
Ⓐ DDOS attack　Ⓑ Phishing attack　Ⓒ Man-in-the-middle attack　Ⓓ Meet-in-the-middle attack

（請接背面）

105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、國際經濟商務人員及原住民族考試試題　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

7 數位憑證之應用與下列資訊安全技術之關聯性何者最直接？
㈠AES ㈡Triple DES ㈢RC6 ㈣RSA

8 數位憑證的最主要功能為何？
㈠提供公鑰與驗證其正確之資訊 ㈡儲存並提供私鑰之資訊
㈢證明數位簽章的正確性 ㈣保護資料的隱私性

9 有一數位影像傳送前須經下列三處理程序以確保資訊安全與傳輸效率，處理程序在傳送端之先後順序，何者最理想？
①壓縮　②加密　③數位簽章
㈠③①② ㈡②①③ ㈢③②① ㈣②③①

10 下列技術，何者包含鑑別鏈結伺服器身分之功能？
㈠RC6 ㈡SHA512 ㈢TLS ㈣DES

11 攻擊者寄出假冒官方來源之電子郵件，使收信者誤認信件來源正常，並進而回應個人隱私資料或連結信件提供的超連結網站之攻擊方式與下列攻擊模式何者最接近？
㈠XSS attack ㈡DDoS attack ㈢Phishing attack ㈣Trojans attack

12 下列何種技術可用在電子商務系統的交易中，作為確認交易存在及後續有交易糾紛時釐清權責之根據？
㈠AES ㈡DES ㈢DSA ㈣SHA512

13 UDP 封包表頭的檢查碼（Checksum）如果設定為 0，下列敘述何者正確？
㈠檢查碼是 0 ㈡檢查碼功能不使用 ㈢封包有錯 ㈣封包太大

14 關於網頁代理伺服器（HTTP Proxy）的運作，下列敘述何者錯誤？
㈠使用 TCP 協定 ㈡可提供快取（Cache）功能，加速瀏覽網頁效能
㈢可提供資料加密功能，提昇瀏覽網頁安全 ㈣可解析網址（DNS name resolution），便利瀏覽網頁

15 IPv4 封包（IP datagram）最多可被路由器（Router）轉送（Forward）幾次？
㈠15 ㈡31 ㈢127 ㈣254

16 如果電腦開機後，網路介面的 IP 是 169.254.0.181，是下列何者網路協定出問題？
㈠DNS ㈡DHCP ㈢SMTP ㈣SNMP

17 如果將一台家裏個人使用的電腦的 IP 設定為 74.200.13.235，子網路遮罩（netmask）設定為 255.0.0.0，則當此電腦要連線至 www.google.com（IP：74.125.23.106）時，會出現下列何者結果？
㈠正常連線，可以看見網頁 ㈡正常連線，連線速度很慢
㈢無法正常連線，憑證錯誤 ㈣無法連線

18 如果一台電腦要使用 RIP 路由協定與相鄰網路設備交換路由表，有關這台電腦的防火牆設定，下列敘述何者正確？
㈠允許 UDP Port 520 ㈡允許 TCP Port 520 ㈢允許 IP 224.0.0.5 ㈣允許 TCP Port 179

19 關於 HTTP（Hyper Text Transfer Protocol）網路協定的運作，下列敘述何者正確？
㈠封包有加密功能 ㈡基本認證（Basic Authentication）有加密功能
㈢是無狀態協定（Stateless） ㈣預設通訊埠（Port）是 8080

20 關於網頁第三方 Cookies（Third-Party Cookies）的敘述，下列何者正確？
㈠可以增加網頁瀏覽的速度 ㈡可以提昇網頁瀏覽的安全
㈢會洩漏網頁瀏覽的隱私 ㈣會無法瀏覽 HTTPS 的網站

21 關於 SSH（Secure Shell）網路協定的運作，下列何者錯誤？
㈠封包有加密功能
㈡有主機驗證（host-based authentication）功能
㈢有金鑰的安全驗證（public key-based authentication）功能
㈣有憑證的安全驗證（X.509 certificate-based authentication）功能

22 電腦網路探測工具 traceroute 是利用下列何者網路協定的功能來探測封包路徑？
㈠ICMP Echo Reply ㈡ICMP Echo Request ㈢ICMP Time Exceeded ㈣ICMP Redirection

23 一個 IPv4 的封包在轉送途中如果被分段（Fragmentation），會在那裏被還原組合（Reassembly）？
㈠下個路由器（Router） ㈡目的主機（Host） ㈢目的交換器（Switch） ㈣不用還原組合

24 一台手機的 IP 位址是 10.67.99.18，可以正常連線至 Internet，主要是靠下列何者網路協定？
㈠NAT ㈡ICMP ㈢SNMP ㈣IGMP

25 下列何者網路攻擊不是中間人攻擊（Man-In-The-Middle Attack）？
㈠ARP poisoning ㈡ICMP redirect ㈢DNS spoofing ㈣IP address spoofing