

104年公務人員特種考試警察人員、一般警察人員考試及104年特種考試交通事業鐵路人員、退除役軍人轉任公務人員考試試題

代號：20160 全一頁

等 別：二等一般警察人員考試

類 科 別：刑事警察人員數位鑑識組

科 目：網路與資訊安全（包括資訊安全技術與應用、資安事件處理）

考試時間：2小時

座號：_____

※注意：(一)禁止使用電子計算器。

(二)不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。

一、請解釋下列名詞：（每小題5分，共20分）

(一)資料庫近似查詢法中的合成法（Combining results）

(二)數位簽章

(三)UNIX 作業系統存取控制

(四)隱藏式浮水印

二、(一)如何以單向雜湊函數（One-way hash function）驗證一個經過網路傳送之文件訊息（Message）的完整性？（10分）

(二)如何透過單向雜湊函數與對稱式金鑰驗證該文件訊息傳送者之身分？（10分）

三、(一)請描述以 TCP（Transmission control protocol）協定之三向交握（Three-way handshake）為基礎的阻絕式攻擊（Denial of service, DoS）。（10分）

(二)請問 SCTP（Stream control transmission protocol）協定用什麼機制改良了 TCP 協定，而讓該阻絕式攻擊無法形成？（10分）

四、(一)請說明網路位址轉譯（Network address translation, NAT）之功能，其對網路安全有何貢獻？（10分）

(二)何謂誤用偵測（Misuse detection）？（5分）

(三)何謂異常偵測（Anomaly detection）？（5分）

五、(一)稽核之目的為何？（5分）

(二)稽核的目標為何（至少包括政策、授權與資料本身）？請分別描述之。（15分）