

考試別：國家安全情報人員考試

等別：三等考試

類科組別：資訊組（選試英文）

科目：網路應用與安全

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。

(三)本科目除專門名詞或數理公式外，應使用本國文字作答。

- 一、什麼是進階持續性攻擊（Advanced Persistent Threat, APT）？請說明 APT 攻擊常見的攻擊流程，並針對「管理者端的防護策略」及「使用者端的防護準則」提出適當的建議。（20 分）
- 二、保護企業資訊安全的方式有很多種，但為了防範企業資訊系統的資料損壞且難以回復的災難，最直接有效的辦法就是做好「定期備份」，請說明以下三種資料備份策略及其優缺點。（20 分）
 - (一)完整備份（Completely backup）
 - (二)差異備份（Different backup）
 - (三)增量備份（Incremental backup）
- 三、請說明下列防火牆的三種運作模式。（20 分）
 - (一)透通模式（Transparent mode）
 - (二)路由模式（Routed mode）
 - (三)位址轉譯模式（NAT mode）
- 四、為了維護資訊安全的目的，根據 ISO 27001 資訊安全管理系統（Information Security Management System）的規範，系統必須對其機密性（Confidentiality）、完整性（Integrity）及可用性（Availability）做適當的風險管理。何謂機密性、完整性及可用性？請舉例說明。（20 分）
- 五、目前網路詐騙已經成為嚴重的治安問題，請舉例說明三種常見的網路詐騙手法，並提出因應防制策略。（20 分）