105年公務人員特種考試司法人員、法務部調查局調查人員、國家安全局國家安全情報人員、海岸巡防人員及移民行政人員考試試題

代號：40960　　全一頁

考 試 別：調查人員
等　　別：三等考試
類 科 組：資訊科學組
科　　目：資訊安全實務
考試時間：2 小時　　座號：_____

※注意：㈠禁止使用電子計算器。
㈡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、企業為了解本身之網路設施安全程度，往往會進行滲透測試（Penetration Test）。何謂滲透測試？並詳述其測試程序內容。（20 分）

二、何謂數位鑑識？為能有效保全及使用數位證據，說明其方法與基本原則為何？（20 分）

三、所謂身分認證是要系統能辨認出使用者的真正身分，採用的認證資訊必須要有唯一性，不會與其他人重複。目前有那三種身分認證方式可達到此種要求？並舉例說明利用前述身分認證方式達到雙重因子認證（two-factor authentication）的目的。（20 分）

四、日前報章雜誌報導企業或公司行號遭受勒索病毒（Ransomware）的攻擊。何謂勒索病毒？並說明其可能感染途徑及防禦措施。（20 分）

五、若資安事故生命週期是以事前預防、事中監看與事後處理等三個階段做區分：
㈠說明資訊安全監控中心（Security Operation Center, SOC）大致可分為那五項主要功能以滿足資安事故生命週期之需求。（10 分）
㈡國內各級政府機關在國家資通安全會報的要求下，均已完成或正在進行資訊安全管理制度（Information Security Management System, ISMS）的導入，說明 SOC 與 ISMS 之間的關係。（10 分）