代號：41460
頁次：1－1

115年公務人員特種考試司法人員、法務部調查局調查人員及海岸巡防人員考試試題

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。
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、傳統整合式安全郵件閘道器（Secure Email Gateway, SEG）防護方式為依賴靜態特徵碼與黑名單，過濾含有惡意附件或惡意連結的郵件。然而，「行動條碼釣魚（Quishing）」與「商業電子郵件詐騙（Business Email Compromise, BEC）」類型電子郵件攻擊手法越來越盛行，這類郵件攻擊可以順利穿透 SEG。請說明這兩類攻擊如何規避傳統防護？若你是電子郵件安全的專責人員，會採取什麼因應對策？（30分）

二、請分別說明動態分析在「網路通訊」、「檔案系統」與「登錄檔（Registry）」等三個層面上，通常會監控到那些典型的惡意活動？又請說明進階惡意程式如何利用「邏輯炸彈（Logic Bomb）」規避沙盒偵測？（提示：動態分析為將惡意程式放於受控環境（如沙盒Sandbox）中執行以觀察其行為）（30分）

三、行動通訊以身分驗證與金鑰協議（Authentication and Key Agreement, AKA）來確保通話與上網數據不被竊聽。請說明 5G-AKA 協定的完整技術流程。另外，請特別說明：當用戶在「漫遊（Roaming）」狀態下，外地網路（Visited Network/Visited Public Land Mobile Network, VPLMN）與本地核心網路（Home Network/Home Public Land Mobile Network, HPLMN）如何協同完成對用戶設備（User Equipment, UE）的「雙向身分驗證（Mutual Authentication）」？（25分）

四、請說明數位鑑識中「證據保全與映像檔製作」、「記憶體鑑識」及「網路與日誌鑑識」等三個工項之目的或工作要領，並分別提列說明可使用之工具及其功能。（15分）