代號：20830
頁次：1－1

115年公務人員特種考試警察人員、一般警察人員、國家安全局國家安全情報人員及移民行政人員考試試題

考 試 別：警察人員考試
等　　別：三等考試
類科組別：警察資訊管理人員
科　　目：電腦犯罪偵查
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、犯罪集團利用被植入木馬的物聯網設備，組成殭屍網路，對某機構之資訊系統發動分散式阻斷服務攻擊。從網路流量分析角度，列舉三種偵測分散式阻斷服務攻擊之流量特性。對受駭物聯網設備進行數位取證時，揮發性證據應採取那些現場蒐證策略，以便保存易揮發性證據？（25 分）

二、為落實零信任，某政府機關將資訊系統遷移至雲端，採用條件式存取（conditional access / attribute-based access control）的 IAM 機制，存取雲端服務。請列舉三種可用於 IAM 決策的環境因素（contextual factors）。某日該機構發生資安事件需要還原現場時，若嫌犯宣稱其帳密遭盜用，警察如何從 IAM 存取日誌中提取數位證據，以便判斷該行為是人為操作或異常自動化行為？（25 分）

三、某詐騙集團利用虛擬帳號做為收取被害人匯款之管道。被害人匯款新臺幣 200 萬元至該集團提供之虛擬帳號後，該款項隨即被轉出至多個人頭帳戶。請說明虛擬帳號與實體銀行帳戶的差異。若執法之偵查人員發現贓款流入第三方支付平台，應如何執行數位足跡追蹤，查找出背後真正的特約商店身分及實體資金流向？（25 分）

四、某機關線上申辦系統遭 SQL 注入攻擊，導致大量個資外洩。經查駭客可能利用網頁中輸入欄位框的漏洞，下達惡意指令，竊取資料庫內容。請說明 SQL 注入之基本原理，並列舉兩項網頁開發者應採取之防範作為。警察在受理報案後，如何篩選網頁伺服器之存取紀錄，找出駭客攻擊來源 IP 與惡意請求？（25 分）