代號：50860
頁次：1－1

112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考試及112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

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、請解釋何謂 MITRE ATT&CK 資安框架，並且說明此框架對偵辦電腦犯罪之幫助。（25 分）

二、請說明駭客發起分散式阻斷服務攻擊（DDoS）之流程；（10 分）DNS 放大攻擊為 DDoS 攻擊手法之一，請說明其攻擊特點以及原理。（15 分）

三、虛擬貨幣為目前常被犯罪者使用之貨幣之一，請舉例說明三種虛擬貨幣犯罪態樣並且說明虛擬貨幣查扣之流程。（25 分）

四、調查惡意程式相關案件時，可能會使用靜態分析以及動態分析的技術，請說明何謂靜態分析及動態分析？並說明這兩種分析方式的優缺點。（25 分）