代號：50860
頁次：1－1

113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、為評估系統遭受攻擊所受到的影響，多採用 CIA triad（資安鐵三角）方式評估受攻擊所遭受的衝擊程度。請說明何謂 CIA？若網站伺服器遭受 SQL 注入（SQL injection）攻擊，試以 CIA 說明其遭受到的影響，並說明 SQL 注入攻擊之原理，以及如何防範此類之攻擊。（25 分）

二、許多組織與企業遭受勒索軟體攻擊，被要求支付大量贖金。請說明勒索軟體攻擊原理，並說明其加密檔案之原理與技術、和如何偵查與分析此類攻擊事件。（25 分）

三、警察機關執行資訊數位化行之有年，因此累積大量犯罪資料；另一方面，在電腦犯罪案件蒐證中也收集到大量的數位證據。警調單位為追查與蒐集電腦犯罪相關資訊，可能會利用公開情資 OSINT（Open Source Intelligence），協助偵查。請說明何謂公開情資，並舉 2 項公開情資應用案例，說明公開情資如何協助偵查電腦犯罪。（25 分）

四、惡意軟體分析乃偵查電腦犯罪案件之重要步驟之一，請說明惡意軟體之類型與傳播方式，並舉例說明之。（25 分）