代號：11060
頁次：1－1

107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

考 試 別：司法人員
等　　別：三等考試
類 科 組：檢察事務官電子資訊組
科　　目：資通安全
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、為使執行資安事件調查時能有效保全及運用數位證據，執行人員應確保數位證據在識別、蒐集、擷取、封緘及運送作業過程中的完整性與一致性，避免數位證據遭受竄改等不當行為之發生。請說明數位證據在識別、蒐集、擷取、封緘及運送等作業中應有那些程序或措施以滿足數位證據完整性及一致性的要求。（25 分）

二、因應日益嚴重的駭客與惡意程式的危害，蜜罐（Honeypot）的設置是許多資安防禦方法的一種，請回答下列問題：
㈠請敘述何謂蜜罐（Honeypot）？（5 分）
㈡蜜罐（Honeypot）的佈署對於阻擋駭客攻擊威脅有何效果？（10 分）
㈢蜜罐（Honeypot）依其與入侵者的互動程度可分為低度互動與高度互動，請比較這兩者間的差異。（10 分）

三、注入攻擊（Injection Attack）是駭客常用的攻擊手法之一，請舉出三種注入攻擊的方法並說明如何做出有效防禦的措施。（25 分）

四、在許多網路安全通訊協定中常會使用 Diffie-Hellman 演算法來協議出共同的加密金鑰，其好處是加密金鑰只有在有需要的時候才產生，因此可以免去許多金鑰保管或金鑰遺失所引發的問題，減輕金鑰保存上的負擔。
㈠請說明通訊雙方利用 Diffie-Hellman 演算法共同協議加密金鑰的作法。（10 分）
㈡ Diffie-Hellman 金鑰協議演算法可能遭受「藏鏡人」（Man in the Middle Attack）攻擊，請說明 Man in the Middle Attack 的攻擊方式並說明如何預防。（15 分）