代號：41460
頁次：1－1

108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：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、請說明系統稽核紀錄應包含那些項目？稽核紀錄分析的目的為何？以及系統稽核紀錄的保護方式有那些。（30 分）

二、Bind Shell 與 Reverse Shell 是惡意攻擊者為了取得目標的作業系統權限寫出的惡意程式碼，會以多種方式植入目標的作業系統並執行。攻擊者會利用社交工程或是伺服器可提供檔案上傳的漏洞，將 Shell 上傳並執行。請說明何謂 Bind Shell 與 Reverse Shell，並說明如何防止 Bind Shell 與 Reverse Shell 的攻擊。（30 分）

三、何謂錯誤行為入侵偵測（Misuse Intrusion Detection）？其運作方式為何？（25 分）

四、假設您曾經註冊過一個網站的會員，但是忘了密碼，點選忘記密碼的功能後，該網站將您本來的密碼以明文方式寄出。請說明該網站可能存在那些安全問題？並提出可行的改善措施。（15 分）