臺灣土地銀行106年度一般金融人員及專業人員甄試試題

甄試類組【代碼】：七職等-資訊安全人員（二）【L4525】

科目二：資訊安全【含作業系統管理、資料庫系統管理、網路管理、防火牆及IPS管理】

＊入場通知書編號：＿＿＿＿＿＿＿＿

注意：①作答前先檢查答案卷，測驗入場通知書編號、座位標籤號碼、甄試類別、需才地區等是否相符，如有不同應立即請監試人員處理。使用非本人答案卷作答者，不予計分。
②本試卷為一張單面，非選擇題共5大題，每題各20分，共100分。
③非選擇題限以藍、黑色鋼筆或原子筆於答案卷上採**橫式**作答，並請**依標題指示之題號於各題指定作答區內作答**。
④**請勿於答案卷上書寫姓名、入場通知書編號或與答案無關之任何文字或符號。**
⑤本項測驗僅得使用簡易型電子計算器(不具任何財務函數、工程函數、儲存程式、文數字編輯、內建程式、外接插卡、攝(錄)影音、資料傳輸、通訊或類似功能)，但不得發出聲響；若應考人於測驗時將不符規定之電子計算器放置於桌面或使用，經勸阻無效，仍執意使用者，該節扣10分；該電子計算器並由監試人員保管至該節測驗結束後歸還。
⑥**答案卷務必繳回，未繳回者該節以零分計算。**

第一題：

請回答下列問題：

（一）SIEM之運作架構可概分成三部分：事件收集器(connector)、日誌管理系統(logger)、事件關連分析平台(correlation)等，請問SIEM之英文（或中文）全名為何？【4分】

（二）駭客(Hacker)發動網路攻擊(Attack)常常危及遠端主機之資訊安全，請問由駭客啟動的DoS (Denial of Service)攻擊方式為何？遭受DoS攻擊之系統有何影響？【6分】

（三）非對稱密碼系統(Asymmetric Cryptosystem)可用於文件加解密或數位簽章，以維護資訊傳遞之安全性，請圖示“雙金鑰(Two-key)加密”系統於處理文件加密(Encryption)至解密(Decryption)之運作流程？並說明“公開金鑰” (Public key)係由何者提供？【10分】

第二題：

假設某支援SQL2的DBMS有U1, U2, U3, U4等資料庫帳號，且U1用CREATE TABLE指令建立了EMPLOYEE(Ssn, Name, Addr, Bdate)資料表。在U2, U3, U4對EMPLOYEE資料表都還沒有任何存取權限的情況下，請依序回答下列問題：

（一）若U1下了

GRANT INSERT, DELETE ON EMPLOYEE TO U2;

指令，此時U2, U3, U4對EMPLOYEE各有何權限？【5分】

（二）在完成（一）所述動作後，接著U1又下了

GRANT SELECT ON EMPLOYEE TO U3 WITH GRANT OPTION;

指令，此時U2, U3, U4對EMPLOYEE各有何權限？【5分】

（三）在完成（二）所述動作後，之後U3下了

GRANT SELECT ON EMPLOYEE TO U4;

指令，此時U2, U3, U4對EMPLOYEE各有何權限？【5分】

（四）在完成（三）所述動作後，然後U1下了

REVOKE SELECT ON EMPLOYEE FROM U3;

指令，此時U2, U3, U4對EMPLOYEE各有何權限？【5分】

第三題：

今年中秋節假日前後某銀行發生電腦病毒入侵事件，經該行初步檢視發現疑似駭客入侵SWIFT系統產生虛偽交易之情形，案件詳細情形該行及相關單位正調查中，該案件發生後即緊接國慶連續假期；在資訊安全維護，除應依「金融機構辦理電子銀行業務安全控管作業基準」等規定辦理外，請列舉說明四項國內銀行就此他行資安事件，尤其連續假期期間該有的注意事項與作為。【20分】

第四題：

請回答下列問題：

（一）何謂防火牆？【9分】

（二）何謂封包過濾防火牆？其優缺點為何？【8分】

（三）請說明封包過濾防火牆為何無法防止「IP位址偽裝」的攻擊？【3分】

第五題：

請回答下列問題：

（一）何謂入侵偵測與防禦系統？【10分】

（二）請說明入侵偵測(IDS)在蒐集資料後的分析方法有哪些？【10分】