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】：八職等-資訊安全人員（一）【L4524】

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本試卷為一張雙面，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：事件收集器(connector)、日誌管理系統(logger)、事件關連分析平台(correlation)等三部分，請問“事件收集器”之主要功用為何？【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 DDoS (Distributed Denial-of-Service)攻擊方式為何？遭受 DDoS 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“數位簽章(Digital Signature)”系統針對訊息(Message)建立簽章至驗證簽章之運作程序？並說明“公開金鑰” (Public key)係由何者提供？【10 分】

第二題：

當資料庫存取控制策略採用強制存取控制(Mandatory Access Control)時，每個 Subject(如使用者、帳號、應用程式)及 Object(如資料表、資料列、資料欄…)都被強制歸類為某個安全級別，且這些安全級別間有順序關係，例如 TS(Top Secret), S(Secret), C(Confidential), N(Normal)等級別的關係是 TS ≧ S ≧ C ≧ N，如果我們用 class(S)代表一個 Subject S 的安全級別，用 class(O)代表一個 Object O 的安全級別，則下列兩個存取控制規則必須被遵循，請分別說明其原因。

（一）Subject S 不能讀取安全級別比他高的 Object O，也就是只有在 class(S) ≧ class(O)時，S 對 O 才有讀取權限。【10 分】

（二）Subject S 不能產製(write)安全級別比他低的 Object O，也就是 S 只允許產製 class(O) ≧ class(S)的 O。【10 分】

第三題：

請自下列密碼技術元件中選取部分（或全部）用以設計出一適合手機對手機安全交換資料的機制（請用圖形區塊表示但須標示每一區塊所代表的之安全元件；又請以 A 為發送者而 B 為接收者為例說明），此機制須提供下列安全功能：【20 分】

（一）傳送資料私密性；

（二）傳送資料完整性；

（三）發送者傳送資料不可否認性；

（四）發送者身分鑑別性。

請以下列參數說明您所設計的機制，又這些參數已安全地存在於適當的持有者

PRA、PRB：分別代表 A 和 B 之非對稱式密碼技術之私鑰

PUA、PUB：分別代表 A 和 B 之非對稱式密碼技術之公鑰

K：A 和 B 已共同擁有之對稱式密碼技術之密鑰

M：A 欲傳送給 B 之明文資料

C：A 傳送給 B 之封包資料

密碼技術元件：RSA、ECC、AES、3DES、DES、SHA2、MD5、SHA1、Diffe-Hellman Key Exchange

【請接續背面】

第四題：

某小型企業為了佈建 DMZ，將公司內部分為兩個子網路 10.10.10.0/24（local zone）和 10.10.11.0/24 (DMZ)，並用一台架設了防火牆的閘道器同時連接兩者以及外部的網際網路。請回答下列相關問題：

（一）這個閘道器至少需要安裝幾個網路卡？各自連接到哪一個網路或子網路？【4 分】

（二）若將 local zone 簡稱為 LZ，網際網路簡稱為 IN，該企業禁止員工從 LZ 上網，則理論上以下六種不同流向的網路封包會流經防火牆：LZ 到 DMZ、LZ 到 IN、DMZ 到 LZ、DMZ 到 IN、IN 到 LZ、IN 到 DMZ，然而實際上會發生的流向是哪幾種？【6 分】

（三）承上，這台機器在哪些流向的封包需要做 IP 掩蔽(IP masquerading)？為什麼一定要做 IP 掩蔽？【6 分】

（四）承上，如果這個企業為了增進資訊安全防護，決定引進第二個防火牆，則就資訊安全的角度來看，這兩台安裝防火牆的機器應都屬於 DMZ 的一部分？還是一台屬於 LZ，一台屬於 DMZ？【4 分】

第五題：

請回答下列有關入侵防禦系統(IPS, Intrusion Prevention System)和入侵偵測系統(IDS, Intrusion Detection System)的問題：

（一）有人說防火牆的過濾規則(filtering rules)無法抵擋針對網頁伺服器的緩衝區溢位攻擊(buffer overflow attack)，必須安裝 IPS 才行。請問這種說法是基於何種基礎？並請在 30 字以內說明同意或不同意的理由為何？【8 分】

（二）IPS 或 IDS 在運行中可能產生判斷錯誤的情形。請說明 IPS 和 IDS 的偽陰性(false negative)和偽陽性(false positive)這兩類錯誤的意涵？【6 分】

（三）IPS 和 IDS 偵測攻擊的技術可大致分為利用特徵判斷(signature-based detection)與異常行為偵測(anomaly-based detection)兩種，而採用異常行為偵測時設定的門檻值(threshold)的放寬緊縮對於偽陰性和偽陽性有什麼影響？【6 分】