彰化銀行 107 年度新進人員甄試試題

甄試類別【代碼】：6 職等-資安工程師【L9115】

第二節／專業科目：(1)邏輯推理、(2)作業系統管理、(3)資料庫系統管理、(4)網路管理、(5)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、應試科目是否相符，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 6 大題，請參考各題配分，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)，且不得發出聲響。應考人如有下列情事扣該節成績 10 分，如再犯者該節不予計分。1.電子計算器發出聲響，經制止仍執意續犯者。2.將不符規定之電子計算器置於桌面或使用，經制止仍執意續犯者。
⑥**答案卷務必繳回，未繳回者該節以零分計算。**

第一題：

某企業年度最傑出行政人員的選拔已進入到最後階段，結果由甲、乙、丙三人脫穎而出，但必須由 100 位同仁進行最後的投票，每位同仁均須對甲、乙、丙三人分別投支持或不支持票。已知支持甲有 32 人，支持乙有 31 人，支持丙有 30 人，同時支持甲及乙有 10 人，同時支持乙及丙有 5 人，同時支持甲及丙有 11 人，同時支持甲、乙、丙三人有 3 人。請回答下列問題：

（一）請推論求算出只支持甲或乙或丙當中一人的人數總共有幾位？【10 分】

（二）請推論求算出在甲、乙、丙三人中，至少支持其中一人的人數總共有幾位？【10 分】

第二題：

有關作業系統中的死結 (Deadlock) ，請回答下列問題：

（一）何謂死結？【4 分】

（二）發生死結的四個必要條件為何？【16 分】

第三題：

有關關聯式資料模型 (Relational Data Model) 中對關聯(Relation)執行正規化(Normalization)的部分，請回答下列問題：

（一）何謂第一正規型式(First Normal Form, 1NF)？【5 分】

（二）何謂第二正規型式(Second Normal Form, 2NF)？【5 分】

（三）何謂第三正規型式(Third Normal Form, 3NF)？【5 分】

第四題：

當一台用戶裝置要透過網路傳送封包給另一台目標裝置時，若已知目標裝置的 IP 位址，但沒有它的實體(Media Access Control, MAC)位址就需要藉由位址解析協定(Address Resolution Protocol, ARP)來取得目標裝置的 MAC 位址，請回答下列問題：

（一）請簡述為何要取得封包接收裝置的 MAC 位址？【4 分】

（二）若目標裝置的 IP 位址和用戶裝置的 IP 位址不在同一個網段，需要使用哪一個裝置的 MAC 位址來傳送封包？如何得知該負責轉送封包之裝置的 IP 位址？【4 分】

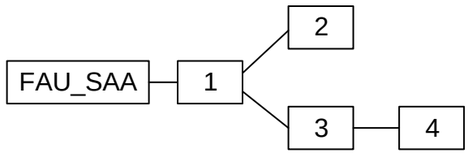
（三）如何判斷用戶裝置的 IP 位址和目標裝置的 IP 位址是否在同一個網段？【4 分】

（四）中間人攻擊(Man-in-the-middle attack, MITM)可以讓攻擊者側錄被攻擊者所傳送的封包，其中一種做法是利用 ARP 協定的弱點，藉由所謂的 ARP 欺騙(ARP Spoofing)來進行，請簡述此種攻擊的原理。【3 分】

【請接續背面】

第五題：

目前許多防火牆或是入侵偵測產品都會被要求通過共通準則 (Common Criteria) 或是 ISO/IEC 15408 的認證，而在 ISO/IEC 15408-2 當中，條列了許多安全功能要求。這些要求分成許多家族 (Family)，與防火牆或入侵偵測相關的一項是安全稽核家族 (Family of Security Audit)，就這安全功能要求家族中，有一個元件是安全稽核紀錄分析，而分成四個等級：



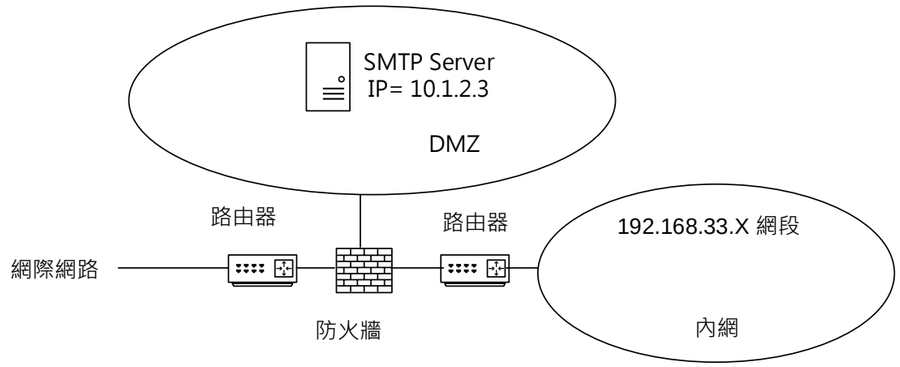
- FAU_SAA.1 潛在違反分析 (Potential violation analysis)
- FAU_SAA.2 異常偵測 (Profile based anomaly detection)
- FAU_SAA.3 簡單攻擊偵測 (Simple attack heuristics)
- FAU_SAA.4 複雜攻擊偵測 (Complex attack heuristics)

如果在原文中，FAU_SAA.1 是要求需要能夠針對超過基於固定規則集合所設定的門檻值進行偵測(basic threshold detection on the basis of a fixed rule set is required)；而 FAU_SAA.2 是要求維護個別系統的使用剖繪 (maintains individual profiles of system usage, where a profile represents the historical patterns of usage performed by members of the profile target group)，以便能夠據此偵測偏離過去使用剖繪的情況；FAU_SAA.3 是要能夠偵測可能會造成嚴重威脅事件的發生 (be able to detect the occurrence of signature events that represent a significant threat to associated enforcement)。請各舉一個例子，說明依照 FAU_SAA.2 和 FAU_SAA.3 的規則可以找到的資安事件。【15 分】

第六題：

請回答下列問題：

（一）請問在 2017 年 5 月所發生的 WannaCry 勒索病毒攻擊事件，該病毒主要是針對哪個 Windows 服務之協定？在不經由 NetBIOS 的情況下，其使用的埠號(Port)為何？【5 分】



（二）倘若某公司之網路架構如上圖，該公司將電子郵件伺服器放置在 10.1.2.3 的 IP 位址，請問可以如何對防火牆做設定，以避免員工由內網透過其他網際網路上的 SMTP 伺服器寄信 (暫不考慮使用 Web Mail 或 VPN 的方式)？倘若該防火牆是封包過濾式，其規則以 (Source, Source Port, Destination, Destination Port, Action) 方式呈現 (如果不知道 SMTP 服務的埠號，可以用 P 代替)。【10 分】