中華郵政股份有限公司 111 年職階人員專業職(一)資訊類科甄試試題

職階／甄試類科【代碼】：專業職（一）／資安與網路管理(1)【T3504】、資安與網路管理(2)【T3505】

第一節／專業科目（1）：資訊系統安全管理概要

＊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、應試科目等是否相符，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，該節不予計分。
②本試卷為一張單面，非選擇題共 4 大題，每題 25 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應考人姓名、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：

請說明資訊系統中營運持續管理(Business Continuity Management)的：

（一）風險評鑑(Risk Assessment)【5 分】

（二）營運衝擊分析(Business Impact Analysis)【5 分】

（三）營運持續計畫(Business Continuity Plan)【5 分】

（四）營運復原計畫(Business Recovery Plan)【5 分】

（五）災害復原計畫(Disaster Recovery Plan)【5 分】

第二題：

請回答下列問題：

（一）請說明何謂 FIDO Authentication。【5 分】

（二）請說明 FIDO Authentication 所使用的鑑別機制與流程。【15 分】

（三）請說明使用 FIDO Authentication 的優點。【5 分】

第三題：

請回答下列問題：

（一）請簡單解釋 TCP 協定之三向交握(three way hand shaking)機制的用途及其步驟。【9 分】

（二）請說明駭客如何利用 TCP 協定之三向交握機制進行阻絕服務(denial of service, DoS)攻擊。【5 分】

（三）請列舉一種防制第（二）小題之阻絕服務(DoS)攻擊的方法。【5 分】

（四）請問 IPSec 與 SSL 安全協定，各運作於網路之哪一層？【6 分】

第四題：

入侵偵測系統(intrusion detection system, IDS)依其偵測方式，通常分為異常偵測式(abnormal detection)與特徵偵測式(signature detection)兩種。請回答下列問題：

（一）請說明異常偵測式 IDS 之運作原理，以及特徵偵測式 IDS 之運作原理。【4 分】

（二）請就實作效率、比對效率、指示出特定攻擊、偵測出未知攻擊、誤判率等 5 方面，比較異常偵測式 IDS 與特徵偵測式 IDS。【10 分】

（三）以黑名單(black list)與白名單(white list)機制之概念，討論異常偵測式 IDS 與特徵偵測式 IDS 各屬何者。【4 分】

（四）有關異常偵測式 IDS，假設張三對 4 個檔案 *F0*、*F1*、*F2*、*F3* 之長期檔案存取比率分別為：*H0=0.15, H1=0.40, H2=0.25, H3=0.20*，*而最近檔案存取比率分別為：A0=0.15, A1 =0.35, A2 =0.30, A3 = 0.20*。就張三而言，請判斷此是否正常？（假設判斷式為 $S = \sum_{i=0}^{3}(Hi - Ai)^2$ 是否<= 0.01）【4 分】

（五）假設第（四）小題中最近檔案存取比率為正常，通常以 *Hi = 0.2Ai + 0.8Hi*，更新 *Hi* 之值。請說明攻擊者如何利用更新機制達成攻擊目的。【3 分】