臺灣銀行 108 年新進人員甄試試題

甄試類別【代碼】：資訊安全人員(一)【O8610】

科目三：綜合科目【含(1)資安事件分析(2)資訊安全管理制度實務(3)網路安全管理實務 (4)資通安全設備管理(含 Firewall、IPS、WAF、AD 與 Exchange Server、SIEM)等實務】

＊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 4 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，**請參照答案卷所載注意事項，於各題指定作答區內作答，並標明題號及小題號**。
④**請勿於答案卷上書寫姓名、入場通知書號碼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：

請回答下列問題：

（一）請依行政院公告之「資通安全事件通報及應變辦法」，條列說明公務機關或特定非公務機關發生各種資通安全事件時，四級資通安全事件中各級所涵蓋之情形。【20 分】

（二）請依行政院公告之「資通安全事件通報及應變辦法」，條列說明資通安全事件之通報內容應包括之項目。【10 分】

第二題：

在推動 ISMS（Information Security Management System，資訊安全管理系統）時，宜以 ISO27001 為標準並以 ISO17799 作為建置控制措施的參考。請條列並說明 ISO27001:2013 所規範控制面向中，通訊安全(communication security)控制面向所規範的兩項控制目標，以及此兩項控制目標各自的控制措施。【20 分】

第三題：

網路管理面臨愈來愈嚴酷的安全挑戰，安全防護須整合網路、系統與軟體的防護，通盤瞭解各種威脅，才能維運一個安全的網路環境。請回答下列問題：

（一）惡意軟體的威脅持續不斷，威脅比較大的有病毒(Virus)、蠕蟲(Worm)及木馬(Trojan Horse)，請簡要說明三者的定義與傳播方式。【6 分】

（二）在新版 Linux 中，其防火牆是以 firewall-cmd 命令來設定與控制，請說明下列兩個指令可以達成何種效果？【3 分】
#firewall-cmd --permanent --add-service={http, https}
#firewall-cmd --reload

（三）網路層防火牆分為無狀態感知(Stateless)及狀態感知(Stateful)兩類，請簡要說明兩者之運作方式。【6 分】

（四）請簡要說明何謂「滲透測試」及其實施方式。【5 分】

第四題：

為提升網路與資訊系統安全，企業在網路的入口處或是伺服器群之前會安裝各種資訊安全設備，例如防火牆、入侵偵測或入侵防禦系統、網站應用程式防火牆(Web Application Firewall, WAF)與防 DDoS 等設備，請回答下列問題：

（一）請簡要說明傳統的封包過濾(Packet Filtering)防火牆與網站應用程式防火牆所防護內涵之差異。這兩類防火牆分別是運作在網路七層模型(OSI 7-Layer Model)中的第幾層？【8 分】

（二）請簡要說明入侵偵測系統(Intrusion Detection System, IDS)與入侵防禦系統(Intrusion Prevention System, IPS)兩者之差異。【8 分】

（三）若網站運用 https 協定以加密方式傳送資料，請問網站應用程式防火牆(WAF)要做何種設定才可以將欲保護之網站傳輸的內容解密。【4 分】

（四）請簡單說明弱點掃描(Vulnerability Scanning)的目的與作法。【4 分】

（五）安全資訊事件管理系統(Security Information and Event Management, SIEM)是一個可以匯集各種裝置的日誌資料(Log)進行資安事件分析與告警的系統，聚合(Aggregation)、關聯(Correlation)及長期累積(Retention)是 SIEM 主要功能中的其中三項，請簡要說明這三項功能的用途。【6 分】