

合作金庫商業銀行 109 年度新進人員甄試試題

甄才類別【代碼】：資安防護分析師【Q6533】

專業科目：(1)計算機概要；(2)作業系統管理(Windows /AIX/Linux)；(3)網路管理；
(4)資訊安全管理(資安事件管理與監控(SIEM & SOC)、資安事件鑑識分析、網站應用程式防火牆(WAF)、分散式阻斷服務攻擊防禦(DDOS)、滲透測試、防火牆(FW)、入侵偵測防禦系統(IPS)、個資外洩防護(DLP)、進階持續威脅(APT)、防毒)

*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，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：

請回答下列問題：

- (一) 使用 5 個位元二補數表示正負整數時，請問 10 進位數值-5 的表示字串為何？【5 分】
- (二) 使用 5 個位元二補數表示正負整數時，請問能夠表示的最小 10 進位整數值及其表示字串為何？【5 分】
- (三) 請說明何謂驅動程式(driver)。【5 分】
- (四) 請說明快取記憶體(cache)的作用。【5 分】
- (五) 請問何謂熱插拔(hot swapping)？【5 分】

第二題：

若您為公司的資安防護管理人員，在未獲得資產管理或派版解決方案下要確保公司 20 台伺服器作業系統的系統安全，其中資訊資產的盤點對判讀有無安裝修補程式極為重要，請說明此狀況下如何自動化定期盤點各系統的資訊資產清單與版本，說明中必須提出 Windows、AIX、Linux 的排程服務名稱，以及修補程式安裝狀況與軟體清單取得方式。

【25 分】

第三題：

簡單網路管理協定(Simple Network Management Protocol, SNMP)網路管理模型中 Manager 通常使用輪詢(Polling)監視 Agent 端之資訊，再使用控制機制變更網路設備之參數，請回答下列問題：

- (一) 請敘述 SNMP 網路管理模型中之“監視機制”及“控制機制”各如何運作？各使用哪些 PDU(Protocol Data Unit)？【10 分】
- (二) 請說明 GetNextRequest PDU 之使用目的為何。【5 分】
- (三) 請解釋何謂 RMON。【5 分】
- (四) 請解釋何謂 OID。【5 分】

第四題：

在遠距工作時，常需要進行遠端存取，因此需要對於遠端存取進行控制。在「資通安全責任等級分級辦法」中，附表十之資通系統防護基準，就有針對遠端存取，做出控制措施之要求。而在該項控制措施當中，分成普級與更高等級的要求。普級的要求是：對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化，使用者之權限檢查作業應於伺服器端完成。

請問，在資通系統防護基準當中，在更高等級的遠端存取安全控制措施有哪些額外需求？【25 分】