

合作金庫商業銀行 107 年新進人員甄試試題

甄才類別【代碼】：資安防護系統管理人員【L9318】

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(Firewall、IPS、MDM、SIEM、WAF、DLP、防毒、
網路弱掃、原碼檢測)

*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本試卷為一張單面，非選擇題共 4 大題，每題各 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。
⑥答案卷務必繳回，未繳回者該節以零分計算。

第一題：

物聯網(Internet of Things, IoT)是網際網路中，可以讓所有能行使獨立功能的個別物體實現互相聯通的網路技術。在物聯網中，個別物體可以透過電子標籤將其與網際網路聯結，以實現全面數位化，透過資訊溝通與交換，廣泛地應用於各種領域。請說明物聯網的運作架構、其構成要件以及各要件可採用的技術。【25 分】

第二題：

請詳細說明以下指令所代表意義為何？

- (一) useradd -f 30 newuser 【5 分】
- (二) chmod 740 backup.sh 【5 分】
- (三) rm -rf test 【5 分】
- (四) find / -mtime 0 【5 分】
- (五) tar -N '2017/12/31' -zcvf home.tar.gz /home 【5 分】

第三題：

近年來網路威脅層出不窮，主要是因為軟體系統或網路服務的漏洞可以讓攻擊者有機可趁，因此弱點掃描就成為現在資安防護的重要技術之一。試說明弱點掃描的原理、其作業的三個階段、其掃描的範圍，並舉出三種以上常見的弱點掃描工具。【25 分】

第四題：

請回答下列問題：

- (一) 安全資訊與事件管理(Security Information and Event Management, SIEM)涵括「安全資訊管理」(SIM)以及「安全事件管理」(SEM)，請問 SIM 所側重的作業要點為何？【5 分】
- (二) 為防範內部網路遭受駭客入侵或惡意攻擊等情事，企業機構常架設「封包過濾型防火牆」(Packet-Filtering Firewall)，藉以篩選可進出網路層之封包，請問此類防火牆篩選封包之檢查規則以何為據？【10 分】
- (三) 面對駭客網路攻擊威脅下，企業為避免網頁應用系統(web application)存在安全漏洞，常見的防範措施包含執行「滲透測試」(Penetration Test)與「弱點掃描」(Vulnerability Scanning)，請問「滲透測試」之主要做法與特點分別為何？【10 分】