兆豐國際商業銀行 107 年新進行員甄選試題

甄才類別【代碼】：資訊安全專責人員【L8106】、系統/網路管理人員【L8107】

科目二：資訊安全

＊入場通知書編號：＿＿＿＿＿＿＿＿

注意：①作答前先檢查答案卡（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。使用非本人答案卡（卷）作答者，不予計分。
②本試卷一張雙面，四選一單選選擇題 40 題，每題 1.25 分，共 50 分；非選擇題二大題，每題 25 分，共 50 分；合計 100 分。
③選擇題限以 2B 鉛筆於答案卡上作答，請選出最適當答案，答錯不倒扣；未作答者，不予計分。
④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**。
⑤**請勿於答案卡（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。**
⑥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。
⑦**答案卡（卷）務必一併繳回，未繳回者該節以零分計算。**

壹、四選一單選選擇題 40 題（每題 1.25 分）

【1】1. HTTPS 通訊協定使用了 TLS (Transport Layer Security)來確保資訊安全，以下何者不是 TLS 的工作？
①驗證客戶端使用者的帳號密碼是否正確
②建立伺服端和客戶端之間的會議金鑰(session key)
③驗證伺服端的憑證是有效的
④在傳送的資料中加入訊息認證碼，讓接收方用以鑑別訊息是否被修改或是偽造

【4】2.電腦作業系統為防止使用者密碼被系統管理員或駭客偷取，均使用雜湊函數(hash function)來轉換密碼成為類似隨機的字串，也就是雜湊值，而在此過程中加鹽(salt)可以讓攻擊者更難破解密碼。以下何者是加鹽的正確做法之一？
①把密碼重複一次變成雙倍長度後，作為雜湊函數的輸入
②把每個密碼的雜湊值後面都加上如同亂數的固定字串
③把每個密碼的雜湊值後面都加上如同亂數的隨機字串
④在每個密碼前面加上如同亂數的固定字串，再計算雜湊值

【4】3.關於設定密碼的要領，以下何者錯誤？
①密碼應該選好記又不容易被猜中的字串
②密碼應該避免使用自己的電話號碼或生日，原因是容易被猜中
③密碼應該避免使用家人的電話號碼或生日，原因是容易被猜中
④各式各樣的網站會員、電郵帳號、系統帳戶都需要密碼，我們應該盡可能全部用同一組密碼才好記

【4】4.以下何種情境非使用雙重認證(two factor authentication, 2FA)？
①去郵局提款，插入晶片卡並輸入密碼
②去商店用信用卡消費，刷卡後簽名
③登入網站會員頁面，輸入使用者名稱和密碼，再輸入網站透過手機傳來的驗證碼
④用登記過的指紋或密碼開啟 iPhone 手機主畫面

【3】5.雲平台供應商均會對其服務承諾每年可上線時間的比率下限以及斷線後直到恢復的最長時間，也就是服務水準協議(service level agreement, SLA)。然而，為何客戶需要在意服務水準？
①透過理解服務水準，客戶才能評估租賃的價格是否划算
②透過理解服務水準，客戶才能知道作業系統被駭的風險有多高
③客戶可以根據服務水準來評估雲服務的穩定度，再進一步估算服務中斷的風險損失
④其實 SLA 只是聊備一格，沒有價值

【3】6.關於系統常用服務與伺服端埠號的組合，下列何者錯誤？
① DNS: 53 埠　② SSH: 22 埠
③ HTTPS: 334 埠　④ HTTP: 80 埠

【4】7.關於公開金鑰演算法和秘密金鑰演算法的比較，下列何者正確？
①前者是每個人有一把金鑰，與他人溝通時再交換金鑰
②後者是每個人有一把金鑰，與他人溝通時再交換金鑰
③前者是每兩個人有兩把金鑰，要溝通時再決定誰用哪一把金鑰
④後者是兩者以上要溝通前，事先決定一把共同金鑰

【1】8.關於數位簽章(digital signature)的敘述，下列何者正確？
①可以用來確保被簽章資料的不可否認性(Non-repudiation)
②必須加密傳送或保存，以免被複製
③就是利用觸控筆在螢幕上簽名後儲存的電子檔案
④可以用公開金鑰演算法或秘密金鑰演算法來製作

【4】9.下列何者是資訊安全的三個基本性質之一？
①可驗證性(confirmability)　②強固性(robustness)
③一致性(consistency)　④可用性(availability)

【1】10.現今大多數系統要求使用者登入時輸入帳號（或使用者名稱）及密碼（或通行碼），部分系統還要求輸入驗證碼。請問哪些資訊不能讓系統認證(authenticate)是合法登入？
①帳號名或使用者名稱
②帳號名和密碼組合
③帳號名和密碼和驗證碼的組合
④帳號名和透過手機遞送的驗證碼組合

【4】11.生物特徵辨識是一個常見的識別手段，但是以下哪個生物特徵並不適合用來識別使用者？
①臉　②眼睛的虹膜　③手掌形狀和指紋　④體重和體脂肪率

【3】12.某些登入畫面上常出現變形的英數字要求我們辨識後輸入，此類驗證碼(CAPTCHA)其作用為何？
①讓登入的過程變長，據說可以降低輸入密碼時打錯字的機率
②利用人類的辨識結果來訓練並增強電腦的辨識能力
③防止駭客等利用電腦程式登入
④只是近年流行的花樣，讓登入過程不會太死板

【2】13.以下何者不是釣魚網站攻擊的目的之一？
①偷取或詐騙個資　②打廣告
③在使用者電腦植入惡意程式　④偷取帳號密碼

【3】14.資安稽核中有所謂第一方、第二方和第三方稽核，請問哪些是外部稽核？
①第一方　②第二方　③第三方　④第二方和第三方都是

【2】15.風險評估時常用的公式是Ｒ＝Ｖ×Ｌ×Ｉ，等號右邊三者的意義分別為何？
① Ｖ是資產價值、Ｌ是風險影響程度、Ｉ是與其他風險的連帶程度
② Ｖ是資產價值、Ｌ是風險發生機率、Ｉ是影響程度
③ Ｖ是弱點、Ｌ是風險影響程度、Ｉ是與其他風險的連帶程度
④ Ｖ是弱點、Ｌ是風險發生機率、Ｉ是影響程度

【1】16.現今的惡意軟體常有多種變種(variant)，導致傳統用特徵碼比對(signature based)的偵測方式往往緩不濟急。另一個常見的有效手段是下列何者？
①軟體行為模式偵測　②軟體源碼分析　③系統日誌分析　④定期快速掃瞄

【2】17.近幾年流行的勒索軟體(ransomware)，是用何種方法綁架被害者電腦內的資料？
①將硬碟的檔案配置表改成只有攻擊者能讀取的格式
②加密硬碟中的內容，而解密金鑰只有攻擊者知道
③將硬碟中的內容回傳給攻擊者後刪除
④利用被害者的電腦執行挖礦程式，讓電腦處理器永遠處於過載狀態而無法進行操作

【1】18.關於社交工程(social engineering)這種攻擊方式的描述，下列何者正確？
①釣魚網站就是社交工程的一種形式
②只使用話術來欺騙人，不會透過電腦
③可以利用電腦溝通，但重點是攻擊者與被攻擊者之間有對話
④前一陣子流行的勒索軟體會強迫受害者與攻擊者聯繫，因此也是社交工程的一種形式

【2】19.個人電腦作業系統上執行的防火牆軟體屬於以下何者的範疇？
①作業系統安全　②網路安全
③實體安全(physical security)　④人身安全

【1】20.檔案系統的存取控制(access control)屬於以下何者的範疇？
①作業系統安全　②網路安全
③實體安全(physical security)　④人身安全

【2】21. ISO 27001：2013 新版本為了更符合資訊安全的現況及需求，由原先 ISO 27001:2005 的 A.5 至 A.15 變成 A.5 至 A.18。其中，2013 年版本新增了兩個領域分別是 A.10 密碼(Cryptography)領域與下列何者？
①人力資源安全(Human Resource Security)　②供應商關係(Supplier Relationships)
③存取控制(Access Control)　④安全政策(Security Policies)

【1】22. APT 攻擊過程有下列幾個階段：a.情報收集 b.資料竊取 c.命令與控制 d.資料發掘 e.橫向發展 f.找到進入點，其正確順序為何？
① afcedb　② abcdef　③ afcbed　④ acfdeb

【請接續背面】

【1】23.關於在 Chrome 瀏覽器中使用無痕瀏覽模式，下列敘述何者正確？
①在無痕模式中開啟的網頁與下載的檔案，都不會出現在瀏覽紀錄與下載紀錄中
②您所瀏覽的網站也不會保有您的瀏覽紀錄
③無痕模式中無法下載檔案，這是為了避免被記錄與追蹤
④無痕模式就不用擔心會連到釣魚網站了

【3】24. A 公司於建立 ISO 27001 管理機制的過程中，已經開始執行內部稽核及風險再評估等作業，請問 A 公司目前處於 PDCA 的哪個階段？
① P　② D　③ C　④ A

【2】25.下列何者最終目的就是搜集情資、等待時機執行破壞任務、當作跳板進行滲透？
①病毒　②木馬　③蠕蟲　④中間人攻擊

【2】26.入侵偵測系統簡單來說就是根據使用者的行為，來判斷目前所做的行為是否異常。當一個異常行為發生，而入侵偵測系統正確的判定其為異常行為，則屬於下列四種情況的哪一種？
① True Positive　② True Negative　③ False Positive　④ False Negative

【2】27.磁碟陣列(Redundant Array of Inexpensive Disks; RAID），其基本思想就是把多個相對便宜的硬碟組合起來，成為一個硬碟陣列組。請問下列何者的可靠性最高？其原理為在主硬碟上存放資料的同時也在鏡像硬碟上寫入一樣的資料，資料安全性在所有的 RAID 級別上來說是最好的。
① RAID 0　② RAID 1　③ RAID 2　④ RAID 3

【1】28.下列何者屬於傳輸層中的非連結導向傳輸協定？只要確認接收端存在就可以不斷地傳送資料。因此速度快，但缺點是缺乏相關的偵錯及確認機制。
① UDP　② TCP　③ ARP　④ ICMP

【1】29.請問下列何者不是一般駭客入侵會進行的動作？
①干擾無線網路訊號　②提升自我帳號權限
③掃描並利用主機弱點　④取得系統控制權

【4】30.關於密碼猜測中的字典攻擊法(Dictionary Attack)，下列敘述何者正確？
①使用各種語言當作密碼來進行測試
②使用各種亂數加以組合來進行測試
③使用英文字典上有的單字來測試密碼
④將常見的密碼當作字典資料庫來測試密碼

【3】31.下列各項關於資安事件回應敘述，何者錯誤？
①留存記錄及落實稽核為事前防控
②資安事件判讀及處理為事中應變
③資安事件回應與處理常利用經驗法則，目前並無相關標準作業流程(SOP)
④數位鑑識及訴訟為事後取證

【4】32.下列何者不是電腦犯罪的特色？
①具隱匿性　②具廣泛性
③擴散迅速　④受害對象通常具有針對性

【2】33.收到往來銀行寄來的電子郵件，內容是要求立即透過電子郵件的連結來進行個人資料的更新。這時應該如何處理？
①電子郵件是可以相信的，可立即更新個人資料以免有所耽誤
②可能是網路釣魚郵件，不要點選郵件中的網址，如要進入相關連結，應自行輸入正確網址或事前打電話向銀行確認
③只要確認與該銀行有往來，即表示這封電子郵件沒問題
④點選連結郵件中的網址，再檢視網頁是否顯示為該銀行，如正確再進行個人資料更新

【1】34.下列何者是做資料備份較適合的時機？
①重要的資料檔案有變更的時候　②感染病毒之後
③每分每秒都備份　④臨時想到的時侯

【3】35.面對外部資安威脅，公司或個人應採取何種措施？
①購買最新最昂貴的資安設備，即可杜絕所有外部攻擊
②建置完美防護措施並安排大量資安人員進行防控及應變
③沒有百分之百安全，所以應識別風險、管理風險及做好風險應變計畫
④只要不上網、不存取任何主機介面，就不會發生資訊安全事件

【4】36.請問下列何者不屬於 ISO 27001 所提的資訊安全的三要素(CIA)?
①機密性(Confidentiality)　②完整性(Integrity)
③可用性(Availability)　④可認證性(Authenticity)

【2】37.下列何種攻擊手法由於不需高深的攻擊技巧，而是利用人性的弱點進行攻擊。因此近年來造成個人或企業極大的危害？
① DoS 及 DDoS 攻擊　②社交工程
③ Buffer Overflow 攻擊　④ Zero Day 零時差攻擊

【1】38.使用者身份認證(Authentication)是指當使用者輸入使用者名稱(User Name)後，必須再提供密碼(Password)，以確認其是否為合法的使用者。若通過認證才能登錄系統。有關密碼的設定及使用，下列敘述何者不恰當？
①系統預設的密碼通常較為安全，因此可以不進行變更
②不可用使用者的個人相關資料（如出生日期、姓名等）來設定密碼
③密碼必須定期更換
④如有多個帳號，則多個帳號應設定不同的密碼

【3】39.有關密碼技術(Cryptography)的敘述，下列何者正確？
①文件經過加密後，可以確保文件在透過網路傳輸時，不會誤傳到其他目的地
②文件經過加密後，可以確保文件在透過網路傳輸時，不會被惡意複製多份再發送給不相關的人
③文件經過加密後，可以確保未經授權的使用者無法得知文件的確實內容，可保障機密性
④文件經過加密後，檔案會變小，因此可以使文件在網路傳輸時的速度變快

【1】40.請問進行風險評鑑前應先完成下列哪項作業？
①資產盤點　②管理或處理風險　③內部稽核　④異地備援

貳、非選擇題二大題（每大題 25 分）

第一題：

2016 年 10 月駭客利用網路監控攝影機、家用影音播放器等物聯網(IoT)設備發起史上最大規模的分散式網路服務阻斷攻擊(DDoS attack)，專家也都認為萬物聯網時代，具備連網能力的各式嵌入式系統將是這類型攻擊最大的溫床。試從入侵的難易度、入侵被偵測的機率、頻寬使用以及數量等面向，列舉至少三個原因說明為何萬物聯網比傳統由電腦組成的網際網路更適合發動 DDoS 攻擊？【25 分】

第二題：

會議金鑰(session key) 是指一次性用於對談中，交談雙方用於加密用的對稱式金鑰。若會議金鑰安全性不夠，則機密性將不能確保，請問：

（一）假設某人利用 26 個英文字母中隨機選出 10 個英文字母（假設不考慮大小寫）當作會議金鑰，且此 10 個英文字母皆不重複。則請問此會議金鑰的可能情形有多少種？【3 分】

（二）承（一），假設利用此會議金鑰加密英文訊息。請問此會議金鑰的安全性夠不夠？請說明之。【3 分】

（三）假設利用密碼學中替代(substitution)的技巧，將 26 個英文字母替換成 26 個符號。26 個字母和 26 個符號是一對一的對應關係，所以要送出英文字母，就改送出對應的符號。此時字母和符號的對應關係就是會議金鑰。請問此時此會議金鑰的可能情形有多少種？【4 分】

（四）承（三），假設利用此會議金鑰加密英文訊息。請問此會議金鑰的安全性夠不夠？請說明之。【4 分】

（五）Diffie 與 Hellman 兩人於 1976 年提出了著名的 Diffie-Hellman 金鑰交換協議，解決了會議金鑰交換問題。他們的方法是基於離散對數問題，也就是給定三個數字(g, p, y)，找出 x 滿足 y= gx mod p 的問題。

1.假設 g=3, x=5, p=11，請計算 y 值，其中，y≤11。【5 分】

2.假設 Alice 與 Bob 要透過此金鑰交換機制建立金鑰，Alice 取 g=2, p=11，並計算出 y=5。Alice 送出(g, p,y)=(2,11,5)給 Bob，另外，Bob 回了 y’=8，請問兩方建立的密鑰值為何？【6 分】