兆豐國際商業銀行 106 年第二次新進行員甄選試題

甄才類別【代碼】：系統、網路管理人員【K7404】
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），測驗入場通知書號碼、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本試卷為一張雙面，測驗題型分為【四選一單選選擇題 40 題，每題 1.5 分，合計 60 分】與【非選擇題 2 題，每題 20 分，合計 40 分】，共 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、入場通知書號碼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、工程函數功能、儲存程式功能)，但不得發出聲響；若應考人於測驗時將不符規定之電子計算器放置於桌面或使用，經勸阻無效，仍執意使用者，該節扣 10 分；該電子計算器並由監試人員保管至該節測驗結束後歸還。
⑦**答案卡（卷）務必繳回，未繳回者該節以零分計算。**

壹、四選一單選選擇題 40 題（每題 1.5 分）

【2】1.管理人員希望在防火牆阻擋資料庫通訊埠(Port)，則應將哪個通訊埠(Port)放進阻止列表中？
① 445 ② 1433 ③ 1501 ④ 3389

【2】2.有關傳統安全及雲端自身安全解決方案之比較敘述，哪些是正確的？ A.雲端集中化部署使用者資料儲存與應用，除傳統部署防毒軟體及防火牆外，需要增強型資料安全解決方案；B.雲端及傳統安全方案的病毒樣本庫均是位於本地機器內；C.雲端安全機制部署不當，易於造成用戶遺失對自己資料的控制許可權；D.雲端方案具備網路安全型態感知功能，但傳統安全方案則不具備；E.傳統安全方案占用較少的本地計算資源
① ABC ② ACD
③ BCD ④ ADE

【2】3.企業組織在網路安全考量時，哪些是專為內網存取外網所採取的可能資安防護措施？ A.防止未經授權的存取；B.防止機敏資料未經授權外傳；C.防止內部電腦瀏覽高風險網站；D.網路連線集中監控
① ABC ② BCD ③ ACD ④ ABCD

【1】4.有關個人資料保護與資訊安全的描述哪些正確？ A.資訊安全偏重在資料之機密性、完整性與可用性等；B.個人資料保護偏重在個人資料之價值與可能因洩漏引起之傷害等；C.資訊安全使用之安全控制措施偏重技術監控與管理；D.個人資料保護偏重作業流程控管與資料處理人員保護觀念之培養；E.有好的資訊安全系統就一定能保證有好的個人資料保護機制
① ABCD ② ABDE
③ ABCE ④ ABCDE

【4】5.哪些網路服務所使用的 TCP 通訊埠(Port)預設為 22？ A. SSH；B. SCP；C. TELNET；D. SFTP；E. TLS
① ABC ② BDE ③ ADE ④ ABD

【3】6.下列何項敘述錯誤？
①數位簽章(Digital Signature)可確保交易的不可否認性
② RSA 加密是使用非對稱式加密技術
③對稱式加密技術較非對稱式加密技術安全性高
④訊息鑑別碼(Message authentication code)可用來驗證資料是否被篡改

【1】7.下列何項資訊安全特性是為了確保資料和交易的真實性？
①鑑別性(Authenticity) ②可歸責性(Accountability)
③不可否認性(Non-repudiation) ④可靠度(Reliability)

【3】8.下列何種隱私類型是指規範個人資料的蒐集及處理，如：信用卡資料、醫療紀錄及政府紀錄？
①身體隱私(Bodily privacy)
②通訊隱私(Privacy of communications)
③資訊隱私(Information Privacy)
④領土隱私(Territorial privacy)

【2】9.美國政府「網路非法行為工作小組(The President's Working Group on Unlawful Conduct on the Internet)」將電腦犯罪區分成三大類，不包括下列何者？
①以電腦為攻擊目標(Computers as Targets)
②以電腦為資產(Computers as Assets)
③以電腦為儲存設備(Computers as Storage Devices)
④以電腦為通訊工具(Computers as Communications Tools)

【1】10.下列何者為目前最常被使用的電子商務交易安全機制？
① TLS/SSL ② PLS/SSS
③ PPP/AAA ④ KMS/IMS

【2】11.小駭是一位惡意攻擊者，他故意在銀行接待區遺失一個 USB 隨身碟（上頭標記「熱門電影」)，並希望銀行員工會發現該 USB 隨身碟進而使用，而該隨身碟內含惡意程式，請問這是何種攻擊手法？
① Vishing ② Social engineering ③ Spim ④ Impersonation

【2】12.下列何項個人資料保護工作是分析機關的作業流程、資訊系統及相關活動是否包含個人資料的蒐集、處理與利用？
①制訂個人資料保護政策與工作規劃
②執行個人資料盤點
③建置安全控制技術
④落實內部稽核程序

【4】13.下列何者是用來識別敏感位置員工欺詐行為的較佳做法？
①合理的使用政策 ②權責區分
③誤報 ④強制性休假

【2】14.公司組織沒有給安全管理人員完全的網路管理權限，安全管理人員權限只能審查網路設備的安全相關日誌和系統更新，其他管理權限則交付給另一位網路管理人員。請問上述係為何種存取控制方式？
①強制性休假 ②最小權限 ③全權委託 ④職務輪調

【1】15.哪項協定提供網路管理人員經由設備的陷阱(Trap)設定，以便網路設備發生服務變更的特定狀態時可通知網路管理人員？
① SNMP ② TLS ③ ICMP ④ SSH

【2】16.下列何項不屬於「社交工程」的攻擊手法？
①郵件仿冒或偽裝
②針對帳號密碼採行字典攻擊法
③網路釣魚
④電話詐騙個人資訊

【4】17.下列何者合併使用較可作為個人識別資訊(PII)？ A.全名；B.婚姻狀況；C.寵物的名字；D.生日
① AB ② BC ③ CD ④ AD

【2】18.安全管理人員實施隱私屏幕、螢幕保護程式使用密碼保護及使用安全碎紙處理裝置等措施，其目的主要在於減輕哪兩種威脅？ A.網路捕鯨；B.垃圾搜尋；C.肩窺攻擊；D.尾隨跟入；E.偽冒身份
① AB ② BC ③ CD ④ DE

【1】19.在提供相同級別的安全性下，下列何種加密演算技術類型，在有限領域的對數計算方面可使用較小的金鑰長度和較少的計算資源？
① Elliptical curve ② Diffie-Hellman
③ Quantum ④ El Gamal

【3】20.近日爆發的 WannaCry 軟體可說是席捲全球，只要是 Windows 10 以下的作業系統且沒有更新相關修補軟體，則電腦檔案都有可能受到攻擊。請問 WannaCry 軟體是何種惡意程式軟體？
①惡作劇軟體 ②木馬程式
③勒索軟體 ④間諜軟體

【2】21. Diffie-Hellman 密鑰交換(Key Exchange)機制是一種安全協定，它可以讓雙方在完全沒有對方任何預先資訊的條件下通過不安全通信道建立起一個金鑰。這個金鑰可以在後續的通訊中作為對稱金鑰來加密通訊內容。假設小明與小華欲利用 Diffie-Hellman 密鑰交換方式建立共享密鑰，小明首先算出了 g=2, p=5 以及 $X=g^a \bmod p = 3$，小明送出了(g,p,X)三個值給小華，小華計算了 $Y=g^b \bmod p = 4$ 並回傳 Y 給小明，請問小明與小華所建立之共享密鑰 K 其值為何？
① 5 ② 4 ③ 11 ④ 13

【1】22. RSA 加密系統的安全性是基於何種假設性的問題？
①質因數分解問題
②離散對數問題
③ Diffie-Hellman 密鑰分配問題
④演算法不公開的假設

【4】23. PKI（公開金鑰基礎建設）中的 OCSP（Online Certificate Status Protocol；線上憑證狀態協定）的功能為何？
①提供用戶查詢憑證對應的公開金鑰值
②確認已失效憑證的更新狀況
③當憑證對應的密鑰遺失時，提供用戶申請復原密鑰時使用
④提供用戶查詢憑證是否已失效或被註銷的資訊

【4】24.區塊加密法(block cipher)是連續地將訊息區塊一個接一個加密成密文區塊，串流加密(stream cipher)則是先產生一長串的密鑰，再將訊息與產生的密鑰作互斥或(XOR)運算。區塊加密法提供了幾種操作模式，各有其優缺點。請問下列哪一種模式可將區塊加密法轉變成串流加密法使用？
①電子書編碼模式(Electronic Code Book；ECB)
②區塊鏈結模式(Cipher Block Chaining；CBC)
③密文反饋模式(Cipher Feedback；CFB)
④輸出反饋模式(Output Feedback；OFB)

【2】25. X.509 是由 ITU-T 所定義的國際標準，請問下列何者為 X.509 所規範之相關標準？
①數位簽章標準 ②公鑰憑證的標準
③網路協定的標準 ④認證協定的標準

【2】26.數位簽章可以用來確認使用者身分，下列何者不是數位簽章所具有的特性？
①確認簽章者身份 ②有資料加密的功能
③具有法律效力 ④可確認訊息的完整性

【請接續背面】

【3】27.當一個異常行為發生，入侵偵測系統卻將此異常行為誤判為正常，此種是屬於下列何種判定？
① True Positive　② True Negative
③ False Positive　④ False Negative
【4】28. IP 安全通訊協定(IPSec)所提供的功能，不包含下列哪一項？
①確認訊息內容的完整性
②防止重送攻擊
③利用 Diffie-Hellman 演算法協議通訊金鑰
④利用 Reed-Solomon 編碼進行錯誤更正(Error Correcting)
【4】29.網路攻擊可分為「主動式攻擊」與「被動式攻擊」，下列何者屬於被動式攻擊的範圍？
①竄改訊息內容　②重送攻擊
③偽裝攻擊　④流量分析攻擊
【1】30.當安全漏洞一旦被發現，短時間內便會有許多駭客利用此漏洞展開攻擊，這就是所謂的何種攻擊？
①零時差攻擊(zero day attack)
②無差別攻擊(no difference attack)
③無選擇攻擊(no choice attack)
④零距離攻擊(zero distance attack)
【3】31.選擇或決定一個安全的通行碼(password)，下列敘述何者錯誤？
①長度至少 8 個字元以上
②要確保自己能夠記得住此通行碼
③預設密碼如果夠長，就可以不需更換
④不要用個人的身分資料當通行碼
【2】32.美國國家標準與技術研究院(NIST)經公開甄選，於 2001 年 11 月 26 日發布於 FIPS PUB 197，並於 2002 年成為有效的標準。目前被公認為最安全的對稱式密碼系統，也是美國聯邦政府採用的區塊加密(block cipher)標準加密演算法為何？
① DES　② AES　③ RC4　④ IDEA
【1】33.針對特定組織所作的複雜且多方位的網路攻擊。此種攻擊可以從蒐集情報開始，這可能持續幾天，幾週或甚至更久的時間。攻擊者往往都會透過長時間且持續性的潛伏及監控，趁使用者稍有疏忽時撈取其所需要的資訊。此種攻擊方式稱為：
①進階持續性攻擊(Advanced Persistent Threat；APT)
②水坑式攻擊(Watering Hole)
③殭屍網路攻擊(Botnet)
④中間人攻擊(Man-in-the-Middle)
【1】34.下列何者不屬於公開金鑰密碼技術？
① 3-DES　② RSA
③ ElGamal　④ DSS（亦稱 DSA）
【3】35.下列何者係為偵測並預防電腦中毒的軟體？
①加解密軟體　②作業系統
③防毒軟體　④繪圖軟體
【1】36.在應用程式中若有下列何種狀況，則可能應用程式正暴露資料隱碼攻擊(SQL Injection)的高風險情況？
①太過於信任使用者所輸入的資料，未限制輸入的字元數，以及未對使用者輸入的資料做潛在指令的檢查
②未使用 Kerberous 身分鑑別系統
③未使用基於角色的存取控制模式(Role-based Access Control)
④太過相信 SSL 安全傳輸協定的安全性
【2】37.由於微軟的 Word 以及 Excel 等軟體允許使用者自行設計一些命令，以便某些指令或動作得以自動運行。此特性被有心人士利用來編寫病毒程式，造成對系統的傷害，或破壞使用者的資料。此類病毒名稱為何？
①開機病毒(Boot type virus)
②巨集病毒(Macro virus)
③電腦蠕蟲(Worm)
④邏輯炸彈(Logic bomb)
【1】38.當發現作業系統有安全漏洞時，下列何者為正確的處理方式？
①立即進行系統更新
②只要確認自己沒有不良的上網習慣，就不用擔心電腦會中毒或被入侵了
③雖有安全漏洞，但可等到工作告一段落，再進行系統更新
④確認有安裝防毒軟體的話，就不用擔心了
【3】39.為預防如地震、水災及火災等天然災害，而造成系統損壞無法使用，可以使用下列何種方式對資料與系統進行管理？
①資料加密　②機房入出境管制
③異地備援機制　④定期進行滲透測試
【1】40.攻擊者假裝是某合法使用者而獲得使用權限的攻擊稱之為：
①偽裝(masquerade)　②竊聽(eavesdropping)
③重送(replay)　④阻斷服務(DoS)

貳、非選擇題 2 大題（每題 20 分）

第一題：

開放 Web 軟體安全計畫(Open Web Application Security Project，OWASP)定期根據 Web 應用程式的威脅趨勢，編訂發布十大 Web 風險防護守則(OWASP Top 10)。請回答下列各項安全弱點之造成原因及攻擊結果？

（一） Injectioin。【4 分】

（二） Cross Site Scripting。【4 分】

（三） Broken Authentication and Session Management。【4 分】

（四） Insecure Direct Object References。【4 分】

（五） Cross Site Request Forgery。【4 分】

第二題：

RSA 是基本且被廣泛應用的公開金鑰（非對稱式）密碼系統之一。假設王小明的公鑰(public key)的值為(n,e)=(65, 29)，請回答下列問題：

（一）相較於對稱式密碼系統，公開金鑰密碼系統的優點為何？【5 分】

（二）相較於對稱式密碼系統，公開金鑰密碼系統的缺點為何？【5 分】

（三）請問王小明的私鑰(private key)值 d=?【5 分】

（四）若有個明文 p（加密前的訊息稱之為明文），其值為 3，請問加密後其密文值為何？【5 分】