兆豐國際商業銀行 107 年第二次新進行員甄選試題

甄才類別【代碼】：網路技術專業人員【N2610】、微軟/Oracle 資料庫專業人員【N2611】

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、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 1.25 分，共 50 分；非選擇題二大題，每題 25 分，共 50 分】，共 100 分。
③選擇題限以 2B 鉛筆於答案卡上作答，請選出一個正確或最適當答案，答錯不倒扣；以複選作答或未作答者，該題不予計分。
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）

【4】1. AAA 是網路或資源存取控制的機制，它是三個以 A 開頭英文字的縮寫，請問下列何者不屬於 AAA 中？
① Authentication (驗證)　② Authorization (授權)
③ Accounting (計費、審計)　④ Audit (稽核)

【1】2.下列何種攻擊手法是利用人性弱點來騙取存取權限？
①社交工程 (Social Engineering)　②特權升級 (Privilege Escalation)
③密碼詐騙 (Password Fraud)　④暴力破解 (Brute-force Attack)

【2】3.下列何種惡意軟體會將受害者電腦的檔案加密，受害者要付出贖金才能還原檔案？
①木馬程式 (Trojan Horse)　②勒索軟體 (Ransonware)
③廣告軟體 (Adware)　④殭屍軟體 (Zombie)

【1】4.要讓未經授權者無法讀取檔案內容，可以使用下列何種技術？
①檔案加密　②檔案分段儲存
③檔案後面加入檢查碼　④檔案加入數位簽章

【3】5.相較於 HTTP 協定，HTTPS 通訊協定增加了資料傳輸的機密性，其主要原因為何？
① HTTPS 數據之傳輸速度比 HTTP 傳輸快很多
② HTTPS 連線不需要驗證(Authentication)
③ HTTPS 傳輸數據加密是採端點到端點(end-to-end)方式進行
④ HTTPS 用非對稱式加解密(Asymmetric Encryption)演算法對所有傳輸之數據資料加密

【2】6.駭客入侵的第一步是情報蒐集 (Reconnaissance)，請問這個動作的目的為何？
①讓其他使用者無法使用目標系統　②掃描目標系統，藉以獲取其網路及裝置資訊
③取得或修改目標系統的資料　④提升在目標系統的權限

【1】7.阻斷服務攻擊 (Deny of Service；DoS)主要欲達到的目標為何？
①讓目標伺服器無法處理新的連線請求　②掃描並取得目標系統中的資料
③干擾目標系統以利取得外部資料　④修改目標系統的設定資料讓其無法正常運作

【2】8.憑證可視為網站或是個人在網路上的身分證，請問憑證是下列哪種中心負責發放？
①文件中心(DA)　②憑證中心(CA)　③註冊中心(RA)　④安全中心(SA)

【4】9.在資訊安全管理的要求中，有關滲透測試(Penetration Testing)的目的是以駭客思維對企業進行下列何種工作？
①以金錢收買企業之員工以取得該企業的機敏資料
②以各種密碼排列組合嘗試登入企業的資訊系統(MIS)
③尾隨該單位的員工，看是否能成功進入需要刷卡才能進入的區域
④設法入侵企業的網站或資訊系統看看是否有漏洞

【3】10.虛擬私有網路(VPN)可以透過加密機制提供使用者與工作單位之間的安全傳輸管道，請問下列何者不是 VPN 的技術？
①網際網路安全協定(IPSec)　②第二層通道協定(L2TP)
③遠端桌面協定(RDP)　④點對點通道協定(PPTP)

【2】11.何種工具或軟體可以讓管理者取得與分析網路上的封包傳輸內容？
①日誌檔管理員(Log Manager)　②封包擷取軟體(Packet Capture Software)
③惡意軟體分析工具(Malware Analysis Tool)　④票據系統(Tickiting System)

【1】12.下列何者可以強化系統的安全性？
①使用者與管理員定期變更密碼
②開啟 USB 自動偵測與執行
③不論系統修補(Patch)何時發布，固定每年只做一次系統修補
④讓所有預設的服務程式保持啟動狀態

【1】13.關於防火牆的敘述，下列何者錯誤？
①防火牆需靠硬體來實作，無法利用軟體實作
②防火牆可用來隔離兩個安全信任度不同的網路
③防火牆可有效地控制對內與對外的流量
④防火牆無法有效地防範病毒威脅

【2】14.關於零時差攻擊(Zero Day Attack)的敘述，下列何者正確？
①是社交工程常用的一種攻擊方式
②通常是指攻擊者利用系統或應用程式中還沒有修補程式的安全漏洞進行攻擊
③只要定期更新防毒軟體以及作業系統、應用程式等至最新狀態，就不用擔心零時差攻擊的威脅
④攻擊者透過網路，從四面八方進行同步攻擊沒有時差，因而得名

【4】15.近年來勒索病毒的攻擊興起，並常要求受害者利用虛擬貨幣如比特幣(bitcoin)等進行贖金繳納以換取檔案的解密金鑰。請問攻擊者要求利用比特幣等虛擬貨幣進行匯款最主要的原因為何？
①投資價值高，未來可以更高價值轉賣　②成本低廉，透過網路即可進行匯款
③區塊鏈的新興技術，可展現自己的科技素養　④匿名性高，不易被追蹤

【2】16. X.800 和 RFC 2828 都將攻擊分成「主動式攻擊」和「被動式攻擊」，下列何者屬於「被動式攻擊」？
①重送攻擊　②監控資訊傳輸　③偽裝攻擊　④阻絕服務攻擊

【4】17. Digital signature（數位簽章，或稱電子簽章）是一種密碼學技術，主要用來保障資訊安全的哪一項特性？
①機密性　②可用性　③不可再生性　④不可否認性

【1】18. BS7799 對於資訊安全管理系統標準的定義，下列何者正確？
①對組織而言，資訊與其他實體營運資產一樣有價值
②資訊安全管理在於建置時的周全，而非不斷地修正
③資訊安全是一種實施成果，而非過程與程序
④資訊對組織而言，是一種交流方式，而非資產

【3】19.下列何者屬於有效的系統安全措施？
①限制使用者硬碟使用空間　②採用開放性系統(Open System)
③對使用者設定存取權限(Access Right)　④使用電腦網路

【3】20.關於密碼學上使用的安全雜湊函數(hash function)如 SHA2 及 SHA3，下列敘述何者錯誤？
①是單向函數，輸入任意檔案，即可透過雜湊函數算出此檔案的雜湊值(hash value)。但無法從雜湊值反推回原始檔案的訊息
②數位簽章(digital signature)通常需搭配雜湊函數一起使用
③只要在傳輸時，將訊息與雜湊函數一同送出，則傳輸過程中任何人為的惡意竄改或更動訊息，最後都能夠被訊息接收方檢驗出來
④現實中，目前無任何人或組織有能力找出兩個不同的檔案，其有相同的 SHA2 或 SHA3 的雜湊值

【2】21.下列何種密碼學機制，其演算法可以用在加解密，也可以用在數位簽章？
① AES　② RSA　③ RC4　④ One time pad

【1】22.發生於應用程式與資料庫層的安全漏洞。在輸入的字串之中夾帶惡意指令，在設計不良的程式當中如果忽略了輸入字元檢查，那麼這些夾帶進去的惡意指令就會被資料庫伺服器誤認為是正常的指令而執行，因此資料庫遭到破壞或是入侵。下列何者屬於此種攻擊？
① SQL Injection　② Cross-Site Scripting ,XSS
③ Security Misconfiguration　④ Broken Access Control

【4】23.有一種安全協定，它可以讓欲通訊的雙方在完全沒有對方任何預先資訊的條件下，透過不安全信道建立起一個秘密金鑰。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，此種安全協定稱為下列何者？
①進階密鑰交換標準(Advanced Key Exchange Standard；AKES)
②基於通行碼的密鑰交換協定(Password-based Key Exchange；PKE)
③可認證密鑰交換協定 (Authenticated Key Exchange Standar；AKES)
④密鑰交換協定(Diffie-Hellman Key Exchange；Diffie-Hellman)

【1】24.資訊倫理是與資訊利用和資訊科技相關的價值觀。Mason 定義資訊倫理的四大範疇或稱四大議題，亦即 PAPA。請問 PAPA 所指為何？
① Privacy, Accuracy, Property, Access　② Personality, Authentication, Policy, Accuracy
③ Privacy, Authentication, Property, Accuracy　④ Politics, Accuracy, Property, Access

【請接續背面】

【4】25.為保護 Wifi 無線網路資料傳輸安全，需要採用無線網路資料傳輸加密技術，請問以下技術何者不是無線網路加密技術？
① WEP ② WPA ③ WPA2 ④ WPS

【2】26.一個網站伺服器收到大量建立連線請求，但攻擊方卻藉由不讓連線請求完成來消耗伺服器的資源，這是屬於何種攻擊？
① Smurf Attack ② Syn Flood ③ Ping to Death ④ IP Spoofing

【3】27.一組程式碼可用來提升使用者的權限或是取得作業系統一般不允許存取的部分，並隱藏自己的蹤跡或是取得最高管理權限帳號的權限，這種軟體程式稱為下列何者？
①編譯器(Compiler) ②連結器(Linker)
③根套件工具(Rootkit) ④套件管理員(Packet Manager)

【4】28.殭屍網路(Botnet)中的殭屍(Zombies)在網路攻擊中扮演的角色為何？
①它們對準特定人員感染以取得企業或個人資料
②它們會掃描其他主機看看是否有開放的端口(Port)，來探知有哪些應用服務在運行中
③它們是惡意軟體片段，用來取代正常應用程式中的一部分
④它們在宿主被感染之後，通常會讓宿主被用來發動分散式阻斷服務(DDoS)攻擊

【3】29.下列何種協定提供了驗證(Authentication)、完整性(Integrety)及機密性(Confidentiality)的 VPN 協定？
① ESP ② MD5 ③ IPSec ④ AES

【2】30.請問駭客可以在下列何種協定上建構惡意的 iFrame？
① DHCP ② HTTP ③ IMAP ④ SMTP

【1】31.規則偵測法（Rule-based detection）是常用的入侵偵測手法。關於規則偵測法的說明，下列何者錯誤？
①這種偵測方法要定義檢測各種事件的發生頻率，也就是門檻值(Threshold)。以此檢視使用者是否出現不合法的行為
②這種方法定義了一組規則，然後比對規則與使用者的行為，藉以決定使用者是否符合入侵者條件
③規則偵測法有誤判的可能
④規則偵測法定義適當行為應有的規則，以此判斷目前行為是否有異常

【1】32.有一種 DoS 攻擊方法主要是廣播大量的 ICMP (Internet Control Message Protocol 的縮寫)封包到網路上，並且將來源 IP 位址假造為受害者電腦位址，如此一來所有的電腦收到 ICMP 封包後，全部都會回覆給受害者電腦，透過這個方式導致受害者電腦癱瘓。請問這是屬於哪一種 DoS 攻擊？
① Smurf 攻擊 ② TCP SYN Flood 攻擊
③緩衝區溢位攻擊(Buffer overflow) ④ Ping of Death 攻擊

【2】33. Message Authentication Code (MAC)訊息認證碼不具備下列哪一項安全性？
①可認證性。亦即確認作為訊息來源的身分驗證，確認訊息的來源
②不可否認性。亦即透過 MAC 驗證，可確保發送方無法否認曾經發送過此訊息
③訊息完整性驗證。檢查在訊息傳遞過程中，其內容是否被更改過
④即使訊息在傳輸過程中被人惡意竄改，也能透過 MAC 發現訊息曾經被更動過

【1】34.密碼學(Cyptography)中，替代(Substitution)與置換(Permutation)是兩個最基本的加密(Encryption)技術。假設未加密前的明文為 CIPHER，下列何者不是替代技術加密後所產生的密文？
① KCXICP ② REHPIC ③ 123456786625 ④ ABCDEF

【2】35.IPsec 是一種網路安全協定，可用來建構個人虛擬網路(VPN)。請問 IPsec 是工作在 OSI 網路模型中的哪一層？
①實體層(Physical Layer) ②網路層(Network Layer)
③傳輸層(Transport Layer) ④應用層(Application Layer)

【2】36.蜜罐(honeypot)是一個電腦術語，專指用來偵測或抵禦未經授權操作或是駭客攻擊的陷阱，因原理類似誘捕昆蟲的蜜罐因而得名。關於蜜罐的敘述，下列何者錯誤？
①是一種誘捕系統
②內部資料包含偽造資料與真實資料，因此並非所有存取蜜罐的行為都是可疑的
③可用來收集攻擊者的活動資訊
④是一種入侵偵測技術

【4】37.將乙太網路的網路卡置於何種工作模式下，就可以達到對網路訊息監聽捕獲的目的？
①廣播模式(Broad Cast Model) ②群播模式(MultiCast Model)
③直接模式(Direct Model) ④混雜模式(Promiscuous Model)

【2】38.網路型入侵偵測系統(IDS)主要藉著偵測器來蒐集資料。偵測器可擺放於四個不同的點，以監測不同的攻擊。請問將 IDS 偵測器配置於何處，可偵測所有來自網際網路的攻擊，有利於網管人員分析與掌握？
①防火牆內側 ②防火牆外側
③重要子網路節點 ④連結 DMZ(Demilitarized Zone)非軍事區的節點

【2】39.駭客用其筆記型電腦實作出一個惡意無線基地台(Rogue AP)，可以擷取連到此基地台上網之裝置所收發的數據封包，請問這是何種手法？
①端口重導(Port Redirection) ②中間人攻擊(Man-in-the-Middle)
③無線路由器劫持(Wireless Router Hijacking) ④網路位址轉譯(Network Address Translation)

【3】40.在網路通訊協定中，ICMP 訊息之目的為何？
①確保 IP 封包成功遞送 ②通知路由器有關路徑改變的訊息
③提供 IP 封包傳送過程的狀況 ④監控用網域名稱解析 IP 位址的過程

貳、非選擇題 2 大題（每題 25 分）

第一題：

資訊安全的三項要素是機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)，簡稱為 CIA，請回答下列問題：

（一）請說明何謂機密性。【5 分】

（二）請說明何謂完整性。【5 分】

（三）請說明何謂可用性。【5 分】

（四）請說明如何確保機密性。【5 分】

（五）請說明如何確保完整性。【5 分】

第二題：

現在的通訊以及電子商務都是以現代密碼機制來達成其安全性。現代密碼可區分為兩大部分：公開金鑰密碼(Public key cryptography)以及非公開金鑰密碼。非公開金鑰密碼又稱為對稱式密碼(Symmetric key cryptography)。對稱式密碼可再細分為兩種：區塊加密法(block cipher)以及串流加密法(stream cipher)。請回答以下問題：

（一）請說明何謂公開金鑰密碼？其與對稱式密碼最主要的差異為何？並請說明公開金鑰密碼的加解密演算法的運作模式（重點說明如何加密，以及如何解密）。【5 分】

（二）請分別說明何謂區塊加密與串流加密。這兩個模式的主要差別為何？【5 分】

（三）如果要對線上影音傳輸，例如視訊會議、網路電話及實況轉播等即時傳輸性要求很高的資訊進行加密並傳輸，請問你會使用公開金鑰密碼、區塊加密法，還是串流加密法？請說明原因？【5 分】

（四）假設某個加密演算法，其初始密鑰為(k1,k2,k3,k4,k5)=(1,0,1,1,0)，加密使用之密鑰可用初始密鑰代入以下函數生成 ki+5=(ki+ki+2+ki+4) mod 2，i>0。加密方法就是將加密使用之密鑰與明文進行 Exclusive-OR（互斥或運算）。現有一 2 進制明文 1010101010 需加密，請問加密使用之密鑰值為何？而加密後之密文為何？【5 分】

（五）假設利用 RSA 加密演算法加密訊息明文 m,m=7，加密鑰匙為(e,n)=(3,15)。請問密文值為何？【5 分】