17300 網頁設計 乙級 工作項目 04：資訊安全

1. (3)關於「入侵偵測系統(Intrusion Detection System)」具有何種功能？①防止電腦病毒感染電腦中的檔案 ②預防網路詐騙 ③偵測可能危害內部網路安全的威脅 ④防止使用者連上含有惡意軟體的網站。
2. (1)何項網路裝置的主要功能在保護內部網路，阻擋遠端非法使用者的入侵？①防火牆(Firewall)②垃圾郵件過濾系統(Spam Filtering System)③ 特洛伊木馬(Trojan)④防毒軟體(Antivirus)。
3. (1)何者對於防範惡意軟體的入侵最有幫助的作法？①安裝防毒軟體 ②提高瀏覽器的安全性 ③採用 SSL 技術 ④採用 SET 技術。
4. (1)關於防火牆之敘述何者正確？A.主要功能是過濾封包 B.可以防止 Hacker 從特定連接埠入侵電腦 C.可搜尋已感染病毒的電腦並掃除病毒 D.只能用硬體來完成防火牆的功能 ①AB ②CD ③BC ④ABD。
5. (1)何種網路設備或軟體可保護內部網路，以阻擋遠端使用者的非法使用？①防火牆(Firewall)②垃圾郵件過濾系統(Spam Filtering System)③特洛伊木馬(Trojan)④集線器(Hub)。
6. (2)一般大眾經常收到許多企業利用電子郵件濫發廣告文宣的電子郵件，此類郵件統稱為何？①行銷郵件 ②垃圾郵件 ③病毒郵件 ④惡意郵件。
7. (1)關於防火牆之敘述：A.主要功能是過濾封包、B.可以防止 Hacker 從特定連接埠入侵電腦、C.可搜尋已感染病毒的電腦並掃除病毒、D.只能用硬體來完成防火牆的功能；何者正確？①AB ②CD ③BC ④ABD。
8. (2)關於「妥善保管客戶資料，確保客戶相關資料及客戶隱私的保密性」是基於何項原則之表現？①守法原則 ②保密原則 ③能力原則 ④誠信原則。
9. (3)關於「系統在檢查使用者的密碼設定時，會作某些特性的限制或規定」之敘述何者錯誤？①密碼有效性 ②禁止更新密碼時延用舊密碼 ③禁止不同使用者的密碼相同 ④密碼必須有一定困難度。
10. (2)關於「資料外洩」是破壞了「資訊安全」中的那一面向？①可用性(Availability)②機密性(Confidentiality)③不可否認性(Non-repudiation)④完整性(Integrity)。
11. (4)關於電腦系統安全之敘述何者最不妥當？①設定密碼(Password)②設定存取權限(Access Right)③將資訊設備放置地點予以管制人員進出 ④將資料複製給他人保管。
12. (3)人工檢查資料輸入是否正確，是屬於何種安全管理？①行政安全 ②通訊安全 ③資料安全 ④程式安全。
13. (1)關於資訊安全中系統備援之描述何者正確？①重要系統設備(含軟、硬體)必須有備援措施 ②備援方法必須以 1：1 對應的方式才可以 ③遠端備援方式由於需佔空間且人力支援不易，故不必考慮 ④備援需花費更多費用，因此不必考慮備援。
14. (3)何者不屬於密碼學演算法？①DES ②IDEA ③ZIP ④RSA。
15. (1)關於「資料隱碼攻擊(SQL Injection)」之敘述何者最不妥當？①為使用者而非開發程式者造成 ②造成資料庫資料遭竄改或外洩 ③主要原因為程式缺乏輸入驗證 ④可跳過驗證並入侵系統。
16. (3)何者不是密碼學原理最主要的應用？①數位簽章(Digital Signature)② 數位浮水印(Digital Watermarking)③藍牙(Bluetooth)技術 ④公開金鑰基礎建設(Public Key Infrastructure，PKI)。
17. (2)何者不是資訊安全研究領域中，為維護資料安全的技術性防護方法？① 密碼轉換 ②類比簽章 ③通行碼 ④授權矩陣。
18. (2)何者不是數位簽章(Digital Signature)的功能？①可證明信件的來源 ② 做為信件分類之用 ③可檢測信件是否遭竄改 ④發信人無法否認曾發過信。
19. (3)何者不是「虛擬私人網路(VPN，Virtual Private Network)」採用的技術原理？①穿隧技術 ②加解密技術 ③備援技術 ④使用者與設備身份鑑別技術。
20. (1)何者可用來存放與管理通訊錄及信用卡資料，以確保交易時各項資料的隱密性與安全性？①電子錢包 ②商店伺服器 ③付款轉接站 ④認證中心。
21. (4)何者是良好的電子郵件使用習慣？①收到信件趕快打開或執行郵件中的附檔 ②利用電子郵件傳遞機密資料 ③使用電子郵件大量寄發廣告信 ④ 不輕易將自己的電子郵件位址公佈於網站中。
22. (2)數位浮水印(Digital Watermarking)的主要應用為何？①上網撥接 ②電子商務的安全查核 ③網域名稱的查詢 ④使用者管理。
23. (1)關於「資訊系統安全措施」之敘述何者最不妥當？①資訊系統操作者統一保管密碼 ②資料加密 ③密碼變更 ④公佈之電子文件設定成唯讀檔。
24. (3)何者與管制人員進入電腦系統之措施最不相關？①名牌 ②密碼 ③不斷電系統 ④門鎖。
25. (4)關於資訊安全之敘述何者最不妥當？①設定檔案存取權限，如只允許讀取、不准寫入 ②設定檔案密碼保護，僅擁有密碼之人才得以使用 ③隨時將檔案備份，以備檔案資料被破壞時可回存使用 ④設定檔案資料公開，任何人皆可以使用。
26. (1)資訊安全種類中，關於硬體環境控制是屬於何種工作項目？①實體安全 ②資料安全 ③程式安全 ④系統安全。
27. (3)關於安裝作業系統的安全，何者最不適當？①作業系統軟體的合法性 ②作業系統修補套件的安裝處理 ③作業系統軟體的破解版備份 ④預設環境設定中不安全因素的修改檢驗。
28. (2)可過濾、監視網路上的封包與通聯狀況，達到保護電腦的軟體為何？① 防毒軟體 ②防火牆 ③瀏覽器 ④即時通。
29. (4)任何資訊系統之運作都免不了會發生災變或差錯，如果發生不幸希望能馬上採取復原措施，使損失減至最小，因此在系統規劃時均有復原計畫，以備事故發生時之緊急救濟措施，何項敘述最不適當？①復原計畫必須時時加以演習，使參與作業人員熟練復原處理作業，以爭取時效 ② 對於備份的復原資料應妥為準備 ③應尋找後備支援之電腦中心，並與其訂立支援合約，以為應變支援之需 ④復原計畫必須評估其所花費之成本，如果企業能容忍風險，只要事前將復原計畫教育所有作業人員，使其心生警惕，就可不必做實地演練，以節省成本。
30. (4)在分散式開放系統中，何者不屬於安全管理之功能？①驗證(Authenticat ion)②授權(Authorization)③稽查(Auditing)④回答(Answering)。
31. (4)系統安全防護作業中，何種技術管理規劃最不妥當？①規劃安全稽核系統 ②採用防毒軟體 ③安排系統管理者接受訓練 ④規定密碼限定為有意義之名詞。
32. (3)關於遠端資料進行傳輸時，為避免資料被竊取，可以採用何種保護措施？①將資料壓縮 ②將資料解壓縮 ③將資料加密 ④將資料解密。
33. (2)在資料通訊系統中，資料傳輸時，為了避免資料被竊取而外洩，應做何種防範措施？①將資料做錯誤檢查 ②將資料加密 ③將資料解密 ④將資料解壓縮。
34. (2)何者是資訊安全系統為防止他人透過任何方式竊取資料，在伺服器端設定使用者權限？①監視性 ②資料存取控制 ③獨立性 ④識別。
35. (2)關於資訊安全系統的架構中，何者屬於偵測性質？①識別(Identification)②監視性(Surveillance)③獨立性(Isolation)④資料取得控制(Access C ontrol)。
36. (4)如何最有效建立員工資訊安全意識？①從工作中建立 ②懲罰 ③獎勵 ④ 定期提醒與教育訓練。
37. (2)關於「弱點法則」之敘述何者有誤？①舊的弱點攻擊重新發生的主要原因，多來自組織單位重新安裝佈署機器後未能立即修補 ②有心人士利用弱點的入侵攻擊行為，大約只有 20%的少部分比率是發生在重要弱點的頭二個半衰期 ③安全弱點半衰期指的是一個重要的弱點，每隔一般時間後，發現有此弱點的系統將會減半 ④常見的嚴重弱點一年內會被另一個新發現的弱點取代。
38. (3)關於備份資料儲存之位置何者最不適當？①存放於另外一棟堅固之建築物 ②存放於專業資料保管公司 ③存放於同一間辦公室內 ④存放於防火防震之堅固保險櫃內。
39. (1)關於資訊人員安全管理措施之敘述何者有誤？①單位中每一個人都可操作同一部電腦 ②對操作人員做好適當之教育訓練 ③製作識別卡以做為人員之進出管制 ④將已印出但無用之報表銷毀。
40. (3)關於資訊安全中公開鑰匙碼(Public Key)法之敘述何者有誤？①可減少因傳送 key 而發生洩密之情形 ②送方與受方各有一 key 用來編碼與解碼 ③接收方的 key 應讓送方瞭解以供轉換 ④接受方的 key 不必由傳送方傳送。
41. (1)關於資訊安全中系統設備備援之敘述何者正確？①重要系統設備(含軟、硬體)必須有備援措施 ②備援方法必須以 1:1 對應方式才可 ③遠端備援方式由於需佔空間且人力支援不易，故不必考慮 ④備援需花費更多費用，因此不必考慮備援。
42. (4)關於資訊安全中電子簽名保密技術之敘述何者正確？①電子簽名之技術不需解碼 ②若以設計問題的方法而論，電子簽名較公開鑰匙密碼法簡便③電子簽名乃是採用光筆、滑鼠等工具簽名，以供辨識 ④電子簽名乃是利用數字來代替票據必須由人親自簽名的方法。
43. (3)關於電腦安全防護的措施中，何者是同時針對實體及資料的防護措施？①保留日誌檔 ②管制上機次數與時間 ③不斷電系統 ④人員定期輪調。
44. (2)何者是不正確的「系統安全」措施？①加密保護機密資料 ②系統管理者統一保管使用者密碼 ③使用者不定期更改密碼 ④網路公用檔案設定成「唯讀」。
45. (2)完善的資訊安全系統，應在使用者、資料、作業系統和電腦來源中設立足夠的關卡，以防止使用者透過程式去存取不屬於自己的資料，這種是屬於何種概念？①獨立性(Isolation)②資料取得控制(Access Control)③ 監視性(Surveillance)④識別(Identification)。
46. (2)關於 IT 災害復原(Information Technology Disaster Recovery，ITDR)的首要工作為何？①軟體的重置 ②環境的重置 ③系統的重置 ④資料的重置。
47. (2)關於 IT 災害復原(Information Technology Disaster Recovery，ITDR)，那些人員參與較恰當？①程式設計人員 ②組織全員 ③系統操作人員 ④資料處理人員。
48. (2)系統安全漏洞發生的主要原因為何？①硬體速度過慢 ②系統程式開發之疏失 ③電腦儲存空間不足 ④電源供應不穩定。
49. (3)身分證字號的最後一碼是用來做為何種檢驗？①範圍 ②總數 ③檢查號碼的正確性 ④一致性。
50. (3)防火牆(Firewall)的主要作用為何？①防火 ②防搶 ③防止資料被竊取 ④ 硬體上的保護設施。
51. (1)定期性的資料備份，是防止資料意外毀壞的最佳方法，在整批處理系統下做異動處理時，常保留幾代的歷史資料？①3 代 ②4 代 ③1 代 ④2 代。
52. (2)政府機關公務內部網路系統資訊遭竊的最主要威脅來自何者？①社交工程與位址假造 ②社交工程與零時差攻擊結合 ③國際恐怖份子與國內政治狂熱者 ④實體安全防護不佳。
53. (3)為了防止資料庫遭破壞後無法回復，除了定期備份外，尚須進行那一項措施？①管制使用 ②人工記錄 ③隨時記錄變動日誌(Log)檔 ④程式修改。
54. (1)關於維護資料安全之敘述何者最不妥當？①為避免增加管理人員的困擾，系統密碼一旦設定便不宜任意變更 ②系統資料必須定時予以備份 ③備份資料應與系統設備及應用系統分開放置 ④應用系統必須設置專責人員，並設置使用日誌詳細記錄使用情形。
55. (4)為了讓郵件在傳送過程中不被駭客破壞，可以藉由電子郵件那一項功能來達成？①壓縮 ②反駭客 ③密件副本 ④加密。
56. (2)訂定災害防治標準作業程序及重要資料的備份，是屬何種時期所作的工作？①過渡時期 ②災變前 ③災害發生時 ④災變復原時期。
57. (4)資料庫中重要資料欄的更新作業，為保留其過程的相關資料，以供核驗防範不法行為，可以利用何種檔案？①密碼檔 ②關聯檔 ③組態檔 ④日誌檔。
58. (4)那一個不屬於資訊安全的威脅？①人為疏失 ②天災 ③機件故障 ④讀取資料。
59. (3)密碼術(Cryptography)中，替代(Substitution)是基本的加密(Encryption)技術之一，若明碼形式之本文為 MADAM，何者不是替代技術加密後所產生的密文？①1301040113 ②NBEBN ③AMADM ④NZWZN。
60. (1)從資訊安全的角度而言，何種作法最不適當？①轉寄信件時將前寄件人的收件名單引入信件中 ②不在網站中任意留下自己的私密資料 ③不使用電子郵件傳遞機密文件 ④使用防毒軟體保護自己的電腦。
61. (3)尋找第二儲存空間是資料備份的安全做法，這種做法不包括何者？①與專業儲存公司合作 ②使用防火保險櫃 ③儲存在同一辦公室內另一部電腦上 ④存放在另外一棟堅固之建築物上。
62. (3)關於資料安全之敘述何者正確？①純屬技術問題，無關管理問題 ②純屬管理問題，無關技術問題 ③不但是技術問題，且是管理問題 ④既不是技術問題，也不是管理問題。
63. (1)資料錯誤檢核方式中，何者最不常用？①存取權限檢查(Access Right V erification)②檢查號碼檢查(Check Digit)③型態檢查(Type Check)④範圍檢查(Range Check)。
64. (4)資訊安全中針對人為因素所做的事前預防措施，何項是不必要的？①門禁管制 ②技術性管制 ③內部管制 ④網路資料不開放。
65. (1)關於資訊系統的災害，何者最嚴重？①資料喪失 ②主管離職 ③硬體故障 ④軟體喪失。
66. (4)電子簽章法中，所稱「加密」通常是利用那一種方式來達成？①CA 憑證 ②宇宙放射法則 ③Unicode 法 ④數學演算法，將電子文件以亂碼方式處理。
67. (1)關於「零時差攻擊(Zero-Day Attack)」之敘述何者最妥當？①在軟體弱點被發現，但尚未有任何修補方法前所出現的對應攻擊行為 ②在午夜 12 點(零點)發動攻擊的一種病毒行為 ③弱點掃描與攻擊發生在同一天的一種攻擊行為 ④攻擊與修補發生在同一天的一種網路事件。
68. (2)關於安全的祕密金鑰密碼系統(Secret Key Cryptosystems)，何者不是該系統提供之功能？①保護資訊機密 ②鑑定發方之身分 ③自動修正資訊內容 ④確保資訊完整性。
69. (1)關於使用可攜式儲存媒體(如：隨身碟)之敘述何者最不妥當？①只要不開啟其中內容，就算已連接到電腦上，也是安全的 ②容易將電腦病毒、木馬程式傳回自己或其他的電腦 ③媒體容易遺失 ④儲存在其中的資料易遭竊取或竄改。
70. (34)關於網路安全之敘述何者錯誤？①近年來駭客攻擊的主要目的經常是謀取不法利益 ②惡意軟體通常藉由網際網路散播 ③阻斷服務是一種誘騙電腦使用者透過電子郵件或網站提供個人資訊的手段 ④入侵偵測系統可以防止使用者連上含有惡意軟體的網站。
71. (134)關於資訊安全之敘述何者正確？①經常備份檔案資料是做到資訊安全的一種方法 ②只要不收陌生人所寄送之電子郵件，即可避免感染病毒 ③ 入侵偵測系統可以偵測出來自外部危害電腦安全的威脅 ④設置連線網路之防火牆無法有效防止公司不肖員工對內部網路的侵害。
72. (24)關於防火牆之敘述何者錯誤？①會將不符合安全規則的資料封包丟棄 ②無法防止電腦病毒從特定連接埠入侵電腦 ③可用硬體或軟體來完成防火牆的功能 ④可搜尋已感染病毒的電腦並掃除病毒。
73. (123)何者是網路安全威脅？①個資外洩 ②駭客入侵 ③網路釣魚 ④網路團購。
74. (24)何者不是防毒軟體？①Avast! ②Twitter ③Kaspersky ④Partition Magic。
75. (1234)何者是選用軟體防火牆應考慮的重點？①主機作業系統 ②應用系統的可能衝突 ③穩定度 ④防火牆的效能 。