D3-002 結果 2022 年 11 月 23 日

問題一

tb787631.CISSPPT3E.c03.085

在傳輸層安全中，什麼類型的密鑰用於加密 Web 服務器和客戶端之間通信的實際內容？

A. 臨時會話密鑰
B. 客戶端的公鑰
C. 服務器的公鑰
D. 服務器的私鑰

你回答正確！

在 TLS 中，服務器和客戶端都使用臨時對稱會話密鑰進行通信。他們使用非對稱加密交換此密鑰，但所有加密內容都使用對稱加密進行保護。

問題 2

tb787631.CISSPPT3E.c03.009

Helen 是一名軟件工程師，她正在開發代碼，出於安全目的，她希望將這些代碼限制在隔離的沙箱中運行。Helen 使用的是什麼軟件開發技術？

A. 邊界
B. 輸入驗證
C. 坐月子
D、TCB

您回答錯誤。

使用沙箱是限制的一個例子，其中系統限制特定進程的訪問以限制其影響

在同一系統上運行的其他進程的能力。

問題三

tb787631.CISSPPT3E.c03.039

Eimear 的軟件開發團隊使用一種方法創建許多離散的軟件對象，然後使用 API 將它們綁定在一起。哪個術語最能描述這種架構？

A、微服務

B. 功能即服務

C. 容器化

D、虛擬化

您回答錯誤。

這是一個微服務架構的例子。每個組件微服務執行一個獨立的任務，然後

使用 API 與其他微服務通信。這可以使用 FaaS 雲計算、容器化和/或虛

擬化來實現，但沒有跡象表明這些服務是否正在該場景中使用。

問題四

tb787631.CISSPPT3E.c03.078

霍華德正在為他的組織選擇一種密碼算法，他想選擇一種支持創建數字簽名的算法。以下哪一種算法能滿足他的要求？

A.RSA

B、3DES

C、AES

D、河豚

你回答正確！

數字簽名只有在使用非對稱加密算法時才有可能。在列出的算法中，只有

RSA 是非對稱的並且支持數字簽名功能。

問題 5

tb787631.CISSPPT3E.c03.062

一名黑客最近通過使用精確定時攻擊修改文件，破壞了 James 公司的數據完整性。攻擊者一直等到 James 使用哈希值驗證文件內容的完整性，然後在 James 驗證完整性和讀取文件內容之間修改文件。發生了什麼類型的攻擊？

A. 社會工程學

B.托圖

C. 數據欺騙

D. 參數檢查

你回答正確！

在時間檢查到使用時間 (TOCTOU) 攻擊中，攻擊者利用驗證安全控件與

實際使用該控件保護的數據之間的時間差。

問題 6

tb787631.CISSPPT3E.c03.081

在第三方漏洞掃描和安全測試中，Danielle 的雇主最近發現為管理她公司的新建築而安裝的嵌入式系統存在嚴重的遠程訪問漏洞。製造商已經倒閉，並且沒有針對設備的補丁或更新。Danielle 應該建議她的雇主如何處理數百台易受攻擊的設備？

A. 確定更換設備型號並更換每台設備。

B. 關閉所有設備。

C. 將設備移動到安全且隔離的網段..

D. 對設備進行逆向工程並構建內部補丁。

你回答正確！

提出的最合理的選擇是將設備移動到安全且隔離的網段。這將使設備能夠

繼續發揮其預期功能，同時防止它們受到損害。所有其他情況要么產生重

大的新成本，要么剝奪她的組織購買設備所提供的功能。

問題 7

tb787631.CISSPPT3E.c03.083

Mike 的任務是防止 Mirai 等惡意軟件的爆發，Mirai 是一種針對基於 IP 的攝像頭和路由器的殭屍網絡。他的組織應該保護什麼類型的系統？

A. 服務器

B、SCADA

C. 移動設備

D. 物聯網 (IoT) 設備

你回答正確！

Mirai 的目標是“物聯網”設備，包括路由器、相機和 DVR。隨著組織將越來越多的此類設備引入其企業網絡，保護內部和外部目標免受不安全、更新不頻繁且經常易受攻擊的物聯網設備的侵害變得越來越重要。

問題 8

tb787631.CISSPPT3E.c03.095

Todd 認為他的組織使用的數字證書已被洩露，他想將其添加到證書撤銷列表 (CRL) 中。CRL 中包含證書的哪些元素？

A、序列號

B、公鑰

C. 數字簽名

D、私鑰

你回答正確！

證書撤銷列表包含證書頒發機構頒發的後來被撤銷的數字證書的序列號。

問題 9

tb787631.CISSPPT3E.c03.030

Colin 是一家非營利組織的首席隱私官，正在協助該團隊過渡到通過設計保護隱私的方法。在這種方法下，哪一項不是團隊應該接受的設計隱私原則？

A. 主動，而不是被動
B. 隱私作為默認設置
C. 端到端安全
D、縱深防禦

您回答錯誤。

雖然深度防禦是一項強大的安全原則，但它不是設計隱私的組成部分。以下是 Privacy by Design 模型的七項原則：

1.主動，而不是被動；預防性的，而不是補救性的

2.隱私作為默認設置

3.隱私嵌入設計

4.完整功能——正和，而非零和

5.端到端安全——全生命週期保護

6.可見性和透明度——保持開放

7.尊重用戶隱私——以用戶為中心

問題 10

tb787631.CISSPPT3E.c03.016

請參考以下場景：

- Alice 和 Bob 想使用非對稱密碼系統相互通信。它們位於該國的不同地區，但通過使用由相互信任的證書頒發機構簽署的數字證書來交換加密密鑰。

如果 Alice 想向 Bob 發送一條為保密而加密的消息，她使用什麼密鑰來加密該消息？

A. 愛麗絲的公鑰

B.愛麗絲的私鑰

C. Bob 的公鑰

D. Bob 的私鑰

您回答錯誤。

在非對稱密碼系統中，消息的發送者使用接收者的公鑰加密消息。然後收

件人可以使用他們自己的私鑰解密該消息，只有他們應該擁有該私鑰。

問題 11

tb787631.CISSPPT3E.c03.046

Philip 正在開發一種新的安全工具，供其組織的許多不同子公司的個人使用。他選擇使用 Docker 部署工具來簡化配置。哪個術語最能描述這種方法？

A. 虛擬化
B、抽象
C. 簡化
D. 容器化

你回答正確！

所有這些術語都準確地描述了這種技術的使用。但是，Docker 的使用最

好被描述為一種容器化技術，因此這是最佳的答案選擇。

問題 12

tb787631.CISSPPT3E.c03.011

當開發人員為了測試目的方便他們自己訪問他們開發的軟件時，他們最有可能在代碼中引入什麼類型的安全漏洞？

A、維護掛鉤

B. 跨站腳本

C、SQL 注入

D、緩衝區溢出

你回答正確！

維護掛鉤，也稱為後門，使開發人員可以輕鬆訪問系統，繞過正常的安全控制。如果在最終確定代碼之前未將其刪除，則當攻擊者發現維護掛鉤時，它們會造成嚴重的安全漏洞。

問題 13

tb787631.CISSPPT3E.c03.043

James 正在與國防部系統合作，該系統被授權同時處理機密和絕密級別的信息。他使用什麼類型的系統？

A. 單一狀態

B. 未分類

C. 分隔的

D. 多狀態

您回答錯誤。

通過實施適當隔離數據的保護機制，多狀態系統經認證可以同時處理來自

不同安全分類的數據。

問題 14

tb787631.CISSPPT3E.c03.060

羅伯特正在調查一個安全漏洞，並發現他環境中的一個系統上安裝了 Mimikatz 工具。可能發生了哪種類型的攻擊？

A、密碼破解

B.傳遞哈希

C. MAC 欺騙

D、ARP 中毒

你回答正確！

使用 Mimikatz 工具表明試圖捕獲用戶密碼哈希值以用於對 Microsoft

Active Directory 帳戶的哈希傳遞攻擊。

問題 15

tb787631.CISSPPT3E.c03.073

Grace 想在她的組織中實施應用程序控制技術。用戶經常需要安裝新的應用程序用於研究和測試目的，她不想干擾這個過程。同時，她想阻止使用已知的惡意軟件。哪種類型的應用程序控制適合這種情況？

A. 黑名單
B. 灰名單
C. 白名單
D. 藍名單

您回答錯誤。

應用程序控制的黑名單方法允許用戶安裝他們希望安裝的任何軟件，但管理員特別指定為禁止的軟件包除外。在用戶應該能夠安裝他們希望使用的任何非惡意軟件的情況下，這將是一種合適的方法。

問題 16

tb787631.CISSPPT3E.c03.015

Chris 想要驗證他下載的軟件包是否與原始版本匹配。如果他認為技術嫻熟的攻擊者可能已將軟件包替換為包含後門的版本，他應該使用什麼散列工具？

A、MD5
B、3DES
C、SHA1
D. SHA 256

你回答正確！

MD5 已經產生了故意衝突，並且在 2017 年初宣布了針對 SHA 1 的真實

世界衝突攻擊。3DES 不是散列工具，因此 Chris 在這個過程中唯一真

正的選擇是 SHA 256（有時稱為 SHA 2）列表。

問題 17

tb787631.CISSPPT3E.c03.094

作為其團隊取證調查流程的一部分，Matt 在處理驅動器和證據存儲設施中的其他證據之前簽署了這些證據。他正在創建什麼類型的文檔？

一名罪犯

B. 監管鏈

C. 民事

丁

你回答正確！

Matt 正在幫助維護電子證據的監管鏈文件。如果他的組織需要證明他們

處理的數字證據沒有被篡改，這可能很重要。一個更好的過程將涉及不止

一個人，以確保不可能被篡改。

問題 18

tb787631.CISSPPT3E.c03.037

艾倫正在審查一個系統，該系統已根據通用標準指定了 EAL1 評估保證級別。他對系統的確信程度如何？

A. 它已經過功能測試。

B. 它已經過結構測試。

C. 已經過正式驗證、設計和測試。

D. 它經過了系統的設計、測試和審查。

你回答正確！

當相關係統已經過功能測試時，EAL1 保證適用。這是通用標準下的最低保證級別。

問題 19

tb787631.CISSPPT3E.c03.038

Jake 為一家研究機構工作，該機構正在尋求部署一個網格計算系統，該系統將在用戶工作站上執行循環清理，以執行需要高性能計算的研究任務。與此操作相關的最重大風險是什麼？

A. 數據保密

B.隔離突破

C. 數據完整性

D. 數據可用性

您回答錯誤。

系統的設計方式可以保護數據的機密性、完整性和可用性。網格中包含的

研究工作站來自內部用戶，最大限度地降低了分發數據的風險。然而，分

佈式計算客戶端中的隔離漏洞可能是災難性的，允許破壞控制器的人控制

組織中的每個設備。

問題 20

tb787631.CISSPPT3E.c03.065

Johnson Widgets 嚴格限制對總銷量信息的訪問，並將其歸類為競爭機密。但是，發貨員可以不受限制地訪問訂單記錄以促進交易完成。一位發貨員最近從數據庫中提取了一個季度的所有個人銷售記錄，並將它們加總以確定總銷量。發生了什麼類型的攻擊？

A. 社會工程學

B. 推理

C、聚合

D. 數據欺騙

你回答正確！

在聚合攻擊中，個人使用他們對特定信息片段的訪問來拼湊出他們無權訪

問的更大圖景。

問題 21

tb787631.CISSPPT3E.c03.008

Michael 負責法醫調查，正在調查一起涉及公司網站遭到破壞的中等嚴重性安全事件。有問題的 Web 服務器在虛擬化平台上運行，營銷團隊希望盡快啟動並運行該網站。Michael 採取的最合理的下一步是什麼？

A. 在調查完成之前保持網站離線。

B、以虛擬化平台下線為證。

C. 拍攝受感染系統的快照並將其用於調查。

D. 忽略事件並專注於快速恢復網站。

你回答正確！

Michael 應該進行調查，但迫切需要使網站恢復在線。最合理的做法是

拍攝受感染系統的快照並使用快照進行調查，盡快恢復網站運行，同時使

用調查結果提高網站的安全性。

問題 22

tb787631.CISSPPT3E.c03.035

Lana 最近在她的組織中實施了一個新流程，其中不允許負責向用戶授予系統訪問權限的經理參與訪問審查。她在執行什麼原則？

A.兩人控制

B. 最小權限

C. 特權蔓延

D. 職責分離

你回答正確！

職責分離原則規定，任何員工都不應獲得執行兩項任務的許可，這兩項任務結合起來會帶來安全風險。在這種情況下，員工審核自己的工作會產生利益衝突，因此 Lana 實施了職責分離。兩人控制密切相關，但它需要兩個不同的員工批准一個動作。如果她要求兩名經理批准新賬戶，那就是兩人控制的一個例子。

問題 23

tb787631.CISSPPT3E.c03.026

在這裡顯示的圖中，Harry 寫入數據文件的請求被阻止。Harry 擁有機密安全許可，數據文件屬於機密級別。Bell-LaPadula 模型的什麼原理阻止了這個請求？

A. 簡單安全屬性

B. 簡單完整性屬性

C. *-安全財產

D. 全權擔保財產

你回答正確！

*-Security 屬性聲明個人不得寫入比個人級別更低的文件。這也稱為限制

屬性。

問題 24

tb787631.CISSPPT3E.c03.023

Susan 想以一種為數據包內容提供機密性的方式配置 IPsec。IPsec 的哪個組件提供此功能？

A.啊

B、ESP

C、權力

ISAKMP 先生

你回答正確！

封裝安全負載 (ESP) 協議為數據包內容提供機密性和完整性。它加密數

據包有效負載並提供有限的身份驗證和防止重放攻擊。

問題 25

tb787631.CISSPPT3E.c03.014

由於硬件故障，Sonia 最近從筆記本電腦上卸下了一個加密硬盤驅動器，並將其移至新設備上。儘管她知道用戶的密碼，但她仍難以訪問驅動器上的加密內容。什麼硬件安全功能可能導致此問題？

A. TCB

B.TPM

C. NIACAP

D、RSA

你回答正確！

可信平台模塊 (TPM) 是一種硬件安全技術，它將加密密鑰存儲在主板上的芯片上，並防止有人通過將其安裝在另一台計算機上來訪問加密驅動器。

問題 26

tb787631.CISSPPT3E.c03.051

Darcy 的組織正在部署無服務器計算技術，以更好地滿足開發人員和用戶的需求。在無服務器模型中，通常誰負責配置操作系統安全控制？

A. 軟件開發人員

B. 網絡安全專業人員

C、雲架構師

D. 賣方

您回答錯誤。

在無服務器計算模型中，供應商不會向其客戶公開操作系統的詳細信息。

因此，供應商保留在雲計算的責任共擔模型下安全配置它的全部責任。

問題 27

tb787631.CISSPPT3E.c03.084

下列關於 Biba 訪問控制模型的陳述，哪一項是正確的？

A. 它涉及機密性和完整性。

B. 它解決了完整性和可用性問題。

C. 防止隱蔽通道攻擊。

D. 它側重於保護對象免受完整性威脅。

你回答正確！

Biba 模型只關注保護完整性，不提供針對機密性或可用性威脅的保護。

它也不提供針對隱蔽通道攻擊的保護。Biba 模型側重於外部威脅並假設

內部威脅以編程方式解決。

問題 28

tb787631.CISSPPT3E.c03.069

作為事件響應流程的一部分，Charles 安全地擦除受感染機器的驅動器並從原始介質重新安裝操作系統 (OS)。完成後，他會對機器進行全面修補，並在將系統重新連接到網絡之前應用其組織的安全模板。幾乎在系統恢復服務後，他立即發現它已重新連接到它之前所屬的同一殭屍網絡。Charles 應該在哪裡尋找導致這種行為的惡意軟件？

A.操作系統分區

B.系統 BIOS 或固件

C.系統內存

D、安裝介質

你回答正確！

Charles 正在修復的系統可能感染了固件或 BIOS，系統板上駐留了惡意軟件。這種類型的惡意軟件雖然不常見，但很難找到和刪除。由於他使用的是原始媒體，因此惡意軟件不太可能來自軟件供應商。查爾斯擦除系統分區，系統在重建之前會重新啟動，從而清除系統內存。

問題 29

tb787631.CISSPPT3E.c03.072

雙 DES (2DES) 加密算法從未用作原始 DES 算法的可行替代方案。DES 或 3DES 方法不存在的 2DES 易受哪些實施攻擊？

A.選擇密文

B、蠻力

C. 中間人

D. 中間相遇

你回答正確！

中間相遇攻擊使用已知的明文消息，並以暴力方式同時使用明文加密和密文解密，以大約兩倍於暴力攻擊的時間來識別加密密鑰基本的 DES 算法。

問題 30

tb787631.CISSPPT3E.c03.048

在供應商為客戶提供存儲服務訪問權限的基礎架構即服務 (IaaS) 環境中，通常誰負責從停止服務的驅動器中刪除敏感數據？

A. 客戶的安全團隊

B、客戶倉儲團隊

C. 客戶的供應商管理團隊

D. 賣方

您回答錯誤。

在基礎架構即服務環境中，安全職責遵循責任共擔模型。由於供應商負責管理存儲硬件，因此供應商將保留在驅動器停止服務時銷毀或擦除驅動器

的責任。但是，在使用供應商的存儲服務之前，客戶仍有責任驗證供應商

的消毒程序是否滿足他們的要求。

問題 31

tb787631.CISSPPT3E.c03.024

以下哪一項加密目標可以防止設備丟失或被盜時帶來的風險？

A. 不可否認性

B. 認證

C. 誠信

D. 保密

你回答正確！

設備丟失或被盜時的最大風險是設備中包含的敏感數據會落入壞人之手。

保密性可以防止這種風險。不可否認性是指消息的接收者可以向第三方證

明發起者的身份。身份驗證是證明一個人身份的一種手段。完整性表明信

息自傳輸以來未被修改。

第 32 題

tb787631.CISSPPT3E.c03.066

什麼物理安全控制不斷廣播虛假輻射以掩蓋來自計算設備的真實電磁輻射的存在？

A. 法拉第籠

B. 鍍銅窗

C. 屏蔽佈線

D、白噪音

你回答正確！

雖然提到的所有控件都可以防止不需要的電磁輻射，但只有白噪聲是主動控件。白噪聲會產生虛假輻射，有效地“干擾”來自電子設備的真實輻射。

問題 33

tb787631.CISSPPT3E.c03.098

以下哪一項是使用自簽名數字證書的合理應用？

A. 電子商務網站

B. 銀行申請

C. 內部調度應用

D. 客戶門戶

您回答錯誤。

自簽名數字證書應僅用於面向內部的應用程序，其中用戶群信任內部生成的數字證書。

第 34 題

tb787631.CISSPPT3E.c03.090

Tommy 計劃為其數據中心的服務器機架實施電源調節 UPS。以下哪一項情況如果長期持續存在，UPS 將無法防範？

A、故障
B. 停電
C.案例
D.噪音

你回答正確！

UPS 設計用於防止短期斷電，例如電源故障。當他們進行功率調節時，他們還能夠防止下垂和噪音。UPS 的電池壽命有限，無法在持續停電期間保持連續運行。

問題 35

tb787631.CISSPPT3E.c03.067

在軟件即服務雲計算環境中，通常誰負責確保適當的防火牆控製到位以保護應用程序？

A. 客戶的安全團隊

B. 供應商

C. 客戶的網絡團隊

D. 客戶的基礎設施管理團隊

你回答正確！

在軟件即服務環境中，客戶無法訪問任何底層基礎設施，因此在雲計算共享責任模型下，防火牆管理是供應商的責任。

問題 36

tb787631.CISSPPT3E.c03.099

羅恩正在調查一起發生在高度安全的政府機構的安全事件。他認為加密密鑰在攻擊過程中被盜，並找到了攻擊者使用乾冰凍結加密組件的證據。可能嘗試了哪種類型的攻擊？

A.側信道攻擊

B. 暴力破解

C、定時攻擊

D.故障注入攻擊

你回答正確！

在故障注入攻擊中，攻擊者試圖通過引起某種類型的外部故障來破壞加密設備的完整性。例如，他們可能會利用高壓電、高溫或低溫等因素導致故障，從而破壞設備的安全性。側信道攻擊尋求使用有關係統活動的信息並檢索正在主動加密的信息。暴力攻擊會嘗試密鑰或密碼的所有可能的有效組合。在定時攻擊中，攻擊者精確測量加密操作完成所需的時間，獲取有關可能用於破壞其安全性的加密過程的信息。

問題 37

tb787631.CISSPPT3E.c03.074

Warren 正在設計一種用於敏感媒體存儲設施的物理入侵檢測系統，並希望包括在警報系統的通信線路意外中斷時發出警報的技術。什麼技術可以滿足這個要求？

A. 心跳傳感器
B. 發射安全
C. 運動檢測器
D. 法拉第籠

你回答正確！

心跳傳感器將報警系統的周期性狀態消息發送到監控中心。監控中心如果長時間沒有收到狀態信息，就會觸發告警，表明通信中斷。

問題 38

tb787631.CISSPPT3E.c03.031

加密算法應該對公眾檢查開放這一想法背後的加密原理是什麼？

A. 默默無聞的安全

B. Kerckhoffs 原則

C、縱深防禦

D. 海森堡原則

你回答正確！

Kerckhoffs 的原則表明，即使系統的所有內容（密鑰除外）都是公共知識，加密系統也應該是安全的。

第 39 題

tb787631.CISSPPT3E.c03.019

Alice 還想對她發送給 Bob 的消息進行數字簽名。她應該使用什麼密鑰來創建數字簽名？

A. 愛麗絲的公鑰

B.愛麗絲的私鑰

C. Bob 的公鑰

D. Bob 的私鑰

你回答正確！

Alice 使用她自己的私鑰創建數字簽名。然後 Bob 或任何其他用戶可以

使用 Alice 的公鑰驗證數字簽名。

問題 40

tb787631.CISSPPT3E.c03.077

Tonya 認為攻擊者能夠通過 DNS 中毒攻擊竊聽她的用戶與遠程 Web 服務器之間的合法 HTTPS 通信。在進行 DNS 中毒之後，攻擊者可能會使用什麼技術來進行這種竊聽？

A. 中間人

B、蠻力

C. 時機

D. 中間相遇

你回答正確！

在中間人攻擊中，攻擊者誘使用戶與攻擊者建立連接。然後，攻擊者與合

法服務器建立連接，並在兩者之間中繼通信，竊聽內容。中間相遇攻擊是

針對使用多輪加密的密碼算法的攻擊。場景中沒有跡象表明攻擊者使用窮舉暴力攻擊或專門的定時攻擊來實現他們的目標。

問題 41

tb787631.CISSPPT3E.c03.063

Carl 正在部署一組視頻傳感器，這些傳感器將作為研究項目的一部分放置在偏遠地區。由於連接限制，他希望在將結果發送回雲端進行進一步分析之前，盡可能多地在設備上執行圖像處理和計算。哪種計算模型最能滿足他的需求？

A. 無服務器計算
B. 邊緣計算
C.IaaS 計算
D.SaaS 計算

你回答正確！

在這種情況下，大多數雲服務模型（包括 IaaS、SaaS 和無服務器/FaaS）都需要將大部分信息傳輸回雲端。邊緣計算服務模型會更合適，因為它將計算能力放在傳感器上，最大限度地減少必須通過有限的連接網絡鏈接發送回雲的數據。

問題 42

tb787631.CISSPPT3E.c03.070

Lauren 實施 ASLR 以幫助防止系統受損。她使用了什麼技術來保護她的系統？

A. 加密

B. 強制訪問控制

C.內存地址隨機化

D. 自主訪問控制

您回答錯誤。

Lauren 實現了地址空間佈局隨機化，這是一種隨機化內存位置的內存保

護方法，可防止攻擊者使用已知地址空間和連續內存區域通過溢出或堆棧

粉碎攻擊來執行代碼。

問題 43

tb787631.CISSPPT3E.c03.097

以下哪一項是用於從組織中洩露信息的隱蔽定時通道的示例？

A. 發送電子郵件消息

B. 在點對點文件共享服務上發布文件

C. 以摩爾斯電碼的節奏打字

D. 將數據寫入共享內存空間

你回答正確！

隱蔽通道使用秘密通信路徑。隱蔽的時間通道以可測量的方式改變資源的

使用以洩露信息。如果用戶使用特定節奏的摩爾斯電碼打字，這就是隱蔽

定時通道的示例。觀看或收聽擊鍵的人可能會收到一條秘密消息，而不會

在日誌中留下任何消息痕跡。

問題 44

tb787631.CISSPPT3E.c03.033

以下哪一項沒有描述配線間的標準物理安全要求？

A. 僅放置在有保安人員監控的區域。

B、衣櫃內不要存放易燃物品。

C. 使用門上的傳感器記錄條目。

D. 定期檢查壁櫥。

你回答正確！

雖然在安全人員監控的位置安裝配線櫃是理想的選擇，但這在大多數環境

中是不可行的。配線櫃必須在地理上分佈在組織使用的每棟建築物的多個

位置。

問題 45

tb787631.CISSPPT3E.c03.001

Matthew 是一家諮詢公司的安全管理員，他必須實施訪問控制，根據用戶以前的活動限制他們的訪問。例如，一旦顧問訪問了屬於諮詢客戶 Acme Cola 的數據，他們就不能再訪問屬於 Acme 任何競爭對手的數據。哪種安全模型最適合 Matthew 的需求？

A. 克拉克-威爾遜
B. 比巴
C. Bell-LaPadula
D.布魯爾-納什

你回答正確！

Brewer-Nash 模型允許訪問控制根據用戶的操作動態變化。它通常用於

像 Matthew 的環境中，以在屬於不同客戶端的數據之間實現“中國牆”。

問題 46

tb787631.CISSPPT3E.c03.091

以下哪個濕度值在數據中心運行的可接受範圍內？

A. 0%
B. 10%
C. 25%
D、40%

你回答正確！

數據中心濕度應保持在 40% 到 60% 之間。低於此範圍的值會增加靜電

風險，而高於此範圍的值可能會產生損壞設備的水分。

問題 47

tb787631.CISSPPT3E.c03.034

在這裡顯示的圖中，Sally 被 Biba 完整性模型阻止寫入數據文件。

Sally 擁有機密安全許可，該文件屬於最高機密。什麼原則阻止她寫入

文件？

A. 簡單安全屬性

B. 簡單完整性屬性

C. *-安全財產

D. *-完整性屬性

您回答錯誤。

*-Integrity 屬性聲明主體不能修改比主體擁有的更高完整性級別的對象。

問題 48

tb787631.CISSPPT3E.c03.049

在系統審核期間，Casey 注意到她所在組織的 Web 服務器的私鑰已在公共 Amazon S3 存儲桶中存儲了一年多。她應該首先採取以下哪一項行動？

A. 從桶中取出鑰匙。

B. 通知所有客戶他們的數據可能已被洩露。

C. 使用新密鑰申請新證書。

D. 沒有，因為私鑰應該可以訪問以進行驗證。

您回答錯誤。

Casey 應該做的第一件事是通知她的管理人員，但在那之後，更換證書並使用新證書的密鑰使用適當的密鑰管理實踐應該是她的首要任務。

問題 49

tb787631.CISSPPT3E.c03.071

艾倫攔截了一條加密消息，並想確定創建該消息所使用的算法類型。他首先進行了頻率分析，並註意到消息中字母的頻率與英語中字母的分佈非常匹配。最有可能使用哪種類型的密碼來創建此消息？

A. 代換密碼

B、AES

C. 換位密碼

D、3DES

你回答正確！

這條消息很可能是用換位密碼加密的。使用替代密碼（包括 AES 和

3DES 的類別）會改變頻率分佈，因此它不會反映英語的頻率分佈。這

種攻擊者只能訪問加密消息的攻擊類型也稱為純密文攻擊。

第 50 題

tb787631.CISSPPT3E.c03.004

Harry 想從使用 m of n 控制的數據庫中檢索丟失的加密密鑰，其中 m = 4 和 n = 8。檢索密鑰所需的最少託管代理數量是多少？

A2

B.4

C.8

D.12

你回答正確！

在 m of n 控制系統中，n 個可能的託管代理中至少有 m 個必須協作從託

管數據庫中檢索加密密鑰。

問題 51

tb787631.CISSPPT3E.c03.088

Rick 是一名主要使用 Python 的應用程序開發人員。他最近決定評估一項新服務，在該服務中，他將自己的 Python 代碼提供給供應商，然後供應商在他們的服務器環境中執行它。這項服務是什麼類型的雲計算環境？

A、SaaS

B、PaaS

C、基礎設施即服務

D、CaaS

您回答錯誤。

客戶僅提供應用程序代碼以在供應商提供的計算平台上執行的雲計算系統

是平台即服務 (PaaS) 計算的示例。

問題 52

tb787631.CISSPPT3E.c03.082

什麼類型的運動檢測器可以感應監控區域中電磁場的變化？

A、紅外線

B. 波型

C、電容

D、光電

你回答正確！

電容式運動檢測器監控受監控區域中的電磁場，感應與運動相對應的干擾 。

問題 53

tb787631.CISSPPT3E.c03.068

Alice 對某個對象具有讀取權限，並且她希望 Bob 擁有這些相同的權限。Take-Grant 保護模型中的哪一條規則允許她完成此操作？

A. 創建規則
B. 刪除規則
C. 授予規則
D、採取規則

你回答正確！

授予規則允許一個主體將其對某個對象擁有的權利授予另一個主體。

問題 54

tb787631.CISSPPT3E.c03.040

Adam 最近在 NTFS 文件系統上配置了權限，通過單獨列出每個用戶來描述不同用戶對文件的訪問權限。亞當創造了什麼？

A. 訪問控制列表
B. 一個訪問控制入口
C. 基於角色的訪問控制
D. 強制訪問控制

您回答錯誤。

Adam 創建了一個可以訪問該文件的個人用戶列表。這是一個訪問控制

列表，由多個訪問控制條目組成。它包括用戶名，所以它不是基於角色的

，

而且 Adam 能夠修改列表，所以它不是強制訪問控制。

問題 55

tb787631.CISSPPT3E.c03.010

什麼概念描述了組織對其控制滿足安全要求的信心程度？

A. 信任
B. 資格認證
C. 驗證
D. 保險

您回答錯誤。

保證是組織對其安全控制得到正確實施的信心程度。必須對其進行持續監

控和重新驗證。

問題 56

tb787631.CISSPPT3E.c03.053

Chris 正在設計一個在他的公司內使用的加密系統。公司有 1000 名員工，他們計劃使用非對稱加密系統。他們希望建立系統，以便任何一對任意用戶都可以私下通信。他們總共需要多少把鑰匙？

答：500

B. 1,000

約 2,000

D. 4,950

你回答正確！

非對稱密碼系統為每個用戶使用一對密鑰。在這種情況下，如果有 1,000 個用戶，系統將需要 2,000 個密鑰。

問題 57

tb787631.CISSPPT3E.c03.079

Laura 負責保護其公司基於 Web 的應用程序，並希望為開發人員開展有關常見 Web 應用程序安全漏洞的教育計劃。她在哪裡可以找到最常見的 Web 應用程序問題的簡明列表？

A. CVE

B、美國國家安全局

C.OWASP

D、CSA

你回答正確！

開放 Web 應用程序安全項目 (OWASP) 每年都會列出十大 Web 應用程

序安全問題，全世界的開發人員和安全專業人員都依賴這些問題進行教育

和培訓。OWASP 漏洞構成了許多 Web 應用程序安全測試產品的基礎。

問題 58

tb787631.CISSPPT3E.c03.086

Beth 想在她的數據中心的安全區域中加入技術，以防止不需要的電磁輻射。什麼技術可以幫助她實現這個目標？

A. 心跳傳感器

B. 法拉第籠

C. 搭載

D、WPA2

你回答正確！

法拉第籠是一種金屬外殼，可防止電磁輻射散出。這是一種很少使用的技

術，因為它笨重且昂貴，但它在阻擋不需要的輻射方面非常有效。

問題 59

tb787631.CISSPPT3E.c03.013

Tom 負責維護用於控制發電廠內工業流程的系統的安全性。用什麼術語來描述這些系統？

A. 權力

B、SCADA

C.哈弗

D. COBOL

你回答正確！

監控和數據採集 (SCADA) 系統用於控制和收集來自工業過程的數據。它們常見於發電廠和其他工業環境中。

問題 60

tb787631.CISSPPT3E.c03.080

Bell-LaPadula 和 Biba 模型以使用什麼特定狀態機模型的方式實現狀態機？

A. 信息流

B. 不干涉

C、級聯

D. 反饋

你回答正確！

信息流模型將狀態機應用於信息流。Bell-LaPadula 模型將信息流模型應

用於機密性，而 Biba 模型將其應用於完整性。

問題 61

tb787631.CISSPPT3E.c03.036

下列關於系統開發的說法正確的是？（選擇所有符合條件的。）

A. 如果用戶不執行其他配置，系統應設計為以安全方式運行。

B. 系統應該被設計成在遇到錯誤時回退到安全狀態。

C. 系統的設計應該將安全作為一個設計特徵。

D. 系統的設計方式應使其功能盡可能簡單。

你回答正確！

所有這些陳述都是正確的。如果用戶不執行其他配置，系統應設計為以安

全方式運行的想法是安全默認原則。系統應該設計為在遇到錯誤時回退到

安全狀態的想法是故障安全原則。系統的設計應將安全性作為設計特徵納

入這一想法是設計原則中的安全性。系統設計應盡可能保持其功能簡單的

想法是保持簡單原則。

第 62 題

tb787631.CISSPPT3E.c03.052

Harold 正在評估他的環境對硬件故障的敏感性，並想確定硬件的預期壽命。為此，他應該採取什麼措施？

A、MTTR

B、MTTF

C. 反收購行動

D、甲基丙烯酸甲酯

你回答正確！

平均無故障時間 (MTTF) 提供了特定規格的設備發生故障之前的平均時間量。

問題 63

tb787631.CISSPPT3E.c03.017

請參考以下場景：

- Alice 和 Bob 想使用非對稱密碼系統相互通信。它們位於該國的不同地區，但通過使用由相互信任的證書頒發機構簽署的數字證書來交換加密密鑰。

當 Bob 收到來自 Alice 的加密消息時，他使用什麼密鑰來解密消息的明文內容？

A. 愛麗絲的公鑰

B.愛麗絲的私鑰

C. Bob 的公鑰

D. Bob 的私鑰

您回答錯誤。

當 Bob 收到消息時，他使用自己的私鑰對其進行解密。由於他是唯一擁

有私鑰的人，因此他是唯一能夠解密私鑰的人，從而保護了機密性。

第 64 題

tb787631.CISSPPT3E.c03.027

Florian 和 Tobias 想開始使用對稱密碼系統進行通信，但他們沒有預先安排好的秘密，也無法親自見面以交換密鑰。他們可以使用什麼算法來安全地交換密鑰？

A. 想法

B. 迪菲赫爾曼

C、RSA

D、MD5

你回答正確！

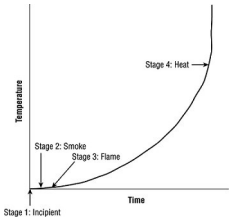
Diffie-Hellman 算法允許在公共網絡上安全地交換對稱加密密鑰。IDEA

和 RSA 是加密算法。MD5 是一種哈希函數。

問題 65

tb787631.CISSPPT3E.c03.002

參考這裡顯示的圖，可以使用檢測技術識別的最早火災階段是什麼？



A.初期

B、煙

C、火焰

D.熱

你回答正確！

早在初期階段就可以檢測到火災。在此階段，空氣發生電離，專門的初期

火災探測系統可以識別這些變化，從而提供火災預警。

第 66 題

tb787631.CISSPPT3E.c03.041

Betty 擔心針對為她的組織使用而開發的自定義應用程序使用緩衝區溢出攻擊。什麼安全控制可以提供最強大的防禦來抵禦這些攻擊？

A. 防火牆

B. 入侵檢測系統

C. 參數檢查

D.漏洞掃描

你回答正確！

參數檢查或輸入驗證用於確保用戶提供給應用程序的輸入與應用程序的預

期參數匹配。開發人員可以使用參數檢查來確保輸入不超過預期長度，從

而防止緩衝區溢出攻擊。

問題 67

tb787631.CISSPPT3E.c03.021

以下哪一項不是哈希算法的屬性？

A. 他們需要加密密鑰。

B. 它們是不可逆的。

C、很難找到哈希值相同的兩條消息。

D. 他們接受可變長度的輸入。

你回答正確！

哈希函數不包含任何保密元素，因此不需要加密密鑰。

第 68 題

tb787631.CISSPPT3E.c03.022

什麼類型的滅火系統在檢測到火災的初始階段後閥門打開後充滿水，然後在分配水之前需要噴頭熱激活？

A、濕管

B、幹管

C. 洪水

D. 預作用

你回答正確！

預作用滅火系統分兩步激活。一旦檢測到火災的早期跡象，管道就會充滿水。在噴頭上的熱傳感器觸發第二階段之前，系統不會分配水。

第 69 題

tb787631.CISSPPT3E.c03.093

亞歷克斯的雇主將他們的大部分工作輸出創建為 PDF 文件。亞歷克斯擔心將 PDF 文件的受眾限制為已付費的個人。他可以使用什麼技術來最有效地控制對這些文件的訪問和分發？

A、電火花加工

B、加密

C. 數字簽名

D、數字版權管理

你回答正確！

Alex 可以使用數字版權管理技術將 PDF 的使用限制為付費客戶。雖然

DRM 很少是完美的解決方案，但在這種情況下，它可能符合他的組織的

需要。EDM 是電子舞曲，他的客戶可能會喜歡，但解決不了問題。加密

和數字簽名有助於確保文件安全並證明文件的來源，但無法解決 Alex 正

在處理的權限管理問題。

第 70 題

tb787631.CISSPPT3E.c03.092

Kristen 的組織遭受了勒索軟件感染，並且無法訪問關鍵業務數據。她正在考慮支付贖金以重新獲得對她數據的訪問權。關於這筆付款，下列哪些說法是正確的？（選擇所有符合條件的。）

A. 支付贖金可能是非法的。

B. 支付贖金可能會導致進一步的付款要求。

C. 支付贖金保證獲得解密密鑰。

D. 支付贖金可能導致數據洩露。

你回答正確！

支付贖金通常會導致解密密鑰的釋放，但不能以任何方式保證這一點。支付贖金與未來的數據洩露之間也沒有聯繫，因為無論是否支付贖金，攻擊者都可能選擇發布機密信息。根據適用的司法管轄區，根據反腐敗法或針對恐怖組織的禁運，支付贖金可能是非法的。例如，美國外國資產控制辦公室 (OFAC) 在 2020 年發布了一份諮詢報告，指出支付贖金可能違反制裁規定。支付贖金還可能導致攻擊者將受害者視為“標記”，並要求未來支付贖金以換取繼續訪問其數據。

第 71 題

tb787631.CISSPPT3E.c03.042

以下哪一種控制組合最能體現縱深防禦原則？

A. 電子郵件加密和網絡入侵檢測
B. 雲訪問安全代理 (CASB) 和安全意識培訓
C. 數據丟失防護和多因素身份驗證
D. 網絡防火牆和主機防火牆

您回答錯誤。

縱深防禦原則建議使用多個重疊的安全控制來實現相同的控制目標。網絡和主機防火牆都旨在限製網絡流量，因此是縱深防禦的一個例子。電子郵件的加密和網絡入侵檢測是不相關的控制，不滿足相同的目標。CASB與安全意識培訓相結合，DLP 與多因素認證相結合也是如此。

第 72 題

tb787631.CISSPPT3E.c03.005

Fran 的公司正在考慮從供應商處購買基於 Web 的電子郵件服務，並取消其自己的電子郵件服務器環境，作為一種節省成本的措施。Fran 的公司正在考慮哪種類型的雲計算環境？

A、SaaS
B、基礎設施即服務
C、CaaS
D、PaaS

你回答正確！

這是供應商提供功能齊全的應用程序作為基於 Web 的服務的示例。因此，它符合軟件即服務 (SaaS) 的定義。在基礎架構即服務 (IaaS)、計算即服

務 (CaaS) 和平台即服務 (PaaS) 方法中，客戶提供自己的軟件。在此示

例中，供應商提供電子郵件軟件，因此這些選擇都不合適。

第 73 題

tb787631.CISSPPT3E.c03.087

在虛擬化計算環境中，哪個組件負責強制執行客戶機之間的分離？

A. 來賓操作系統

B、管理程序

C、內核

D.保護管理器

你回答正確！

管理程序負責協調對物理硬件的訪問，並在同一物理平台上運行的不同虛

擬機之間實施隔離。

第 74 題

tb787631.CISSPPT3E.c03.058

Jorge 認為攻擊者已經從其組織的 Active Directory 服務器之一獲取了 Kerberos 服務帳戶的哈希值。這將啟用什麼類型的攻擊？

A、金票

B. Kerberoasting

C. 傳票

D、蠻力

你回答正確！

黃金票證攻擊使用 Kerberos 服務帳戶的哈希值在 Active Directory 環境

中創建票證。Kerberoasting 攻擊依賴於收集的 TGS 票證。通過票據攻

擊依賴於從 lsass 進程中獲取的票據。暴力攻擊依賴於沒有任何附加信

息的隨機猜測。

第 75 題

tb787631.CISSPPT3E.c03.012

在這裡顯示的圖中，由於 Biba 完整性模型，Sally 無法讀取文件。

Sally 擁有機密安全許可，並且該文件屬於機密級別。正在執行 Biba

模型的什麼原則？

A. 簡單安全屬性

B. 簡單完整性屬性

C. *-安全財產

D. *-完整性屬性

你回答正確！

簡單完整性屬性規定，個人不得閱讀分類為低於個人安全許可的安全級別的文件。

第 76 題

tb787631.CISSPPT3E.c03.096

艾莉森正在檢查她的銀行網站提供給她的數字證書。以下哪一項不是她信任數字證書的必要條件？

A. 她知道服務器屬於銀行。
B. 她信任證書頒發機構。
C. 她確認證書沒有列在 CRL 上。
D. 她驗證了證書上的數字簽名。

你回答正確！

數字證書的意義在於向艾莉森證明服務器是屬於銀行的，所以她不需要事先有這個信任。要信任證書，她必須驗證 CA 在證書上的數字簽名，信任 CA，驗證證書未列在 CRL 上，並驗證證書包含銀行名稱。

第 77 題

tb787631.CISSPPT3E.c03.003

Ralph 正在為一個基本上無人值守的新計算設施設計物理安全基礎設施。他計劃在設施中安裝運動檢測器，但也希望包括針對物理存在的二次驗證控制。以下哪一項最能滿足他的需要？

A、中央電視台

B、IPS

C. 十字轉門

D. 法拉第籠

你回答正確！

閉路電視 (CCTV) 系統可作為實體存在的輔助驗證機制，因為它們允許

安全官員在移動警報響起時查看設施內部，以確定當前居住者及其活動。

第 78 題

tb787631.CISSPPT3E.c03.045

加里截獲了兩個人之間的通信，並懷疑他們正在交換秘密信息。通訊內容似乎就是這裡顯示的圖像。這些人可能使用什麼類型的技術來隱藏此圖像中的消息？

A. 視覺密碼學

B.隱寫術

C. 加密散列

D. 傳輸層安全

你回答正確！

隱寫術是使用加密技術將秘密消息嵌入其他內容的藝術。一些隱寫術算法

通過改變構成圖像文件的許多位中的最低有效位來工作。

第 79 題

tb787631.CISSPPT3E.c03.007

Harry 想要訪問 Sally 擁有並存儲在文件服務器上的文檔。將主體/客體模型應用到這個場景中，資源請求的主體是誰或什麼？

A.哈利

B.莎莉

C、服務器

D. 文件

你回答正確！

在訪問控制的主體/客體模型中，請求資源的用戶或進程是該請求的主體 。

在此示例中，Harry 正在請求資源訪問，因此是主題。

問題 80

tb787631.CISSPPT3E.c03.056

Rhonda 正在考慮在她的組織中使用新的身份證進行物理訪問控制。她遇到了一個使用此處顯示的卡片的軍事系統。這是什麼類型的卡？

A. 智能卡

B. 感應卡

C、磁條卡

D.階段三卡

你回答正確！

圖中顯示的卡片在美國國旗下方有一個智能芯片。因此，它是智能卡的一個例子。這是最安全的身份識別卡技術。

問題 81

tb787631.CISSPPT3E.c03.076

在掃描了他的無線網絡上的所有系統後，Mike 注意到一個系統被識別為 iOS 設備，運行著一個非常過時的 Apple 移動操作系統版本。當他進一步調查時，他發現該設備是原始 iPad，並且無法更新到操作系統的當前安全版本。處理此設備的最佳選擇是什麼？

A. 報廢或更換設備。

B. 將設備隔離在專用無線網絡上。

C. 在平板電腦上安裝防火牆。

D. 重新安裝操作系統。

你回答正確！

當操作系統補丁不再適用於移動設備時，最好的選擇通常是淘汰或更換設備。構建隔離網絡不會阻止設備用於瀏覽或其他目的，這意味著它很可能會繼續暴露在威脅之下。安裝防火牆不會修復操作系統中的安全漏洞，儘管它可能會有所幫助。最後，重新安裝操作系統將不允許新的更新或修復根本問題。

問題 82

tb787631.CISSPPT3E.c03.061

Tom 是一名密碼分析師，致力於破解密碼算法的密鑰。他有一份被截獲的加密消息的副本，還有一份該消息的解密版本的副本。他想使用加密的消息及其解密的明文來檢索用於解密其他消息的密鑰。Tom 正在進行什麼類型的攻擊？

A.選擇密文
B. 選擇明文
C. 已知明文
D、蠻力

你回答正確！

在已知的明文攻擊中，攻擊者擁有加密消息的副本以及用於生成該密文的明文消息。在選擇明文攻擊中，攻擊者可以選擇要加密的明文。在選擇密文攻擊中，攻擊者可以選擇密文輸出。在暴力攻擊中，攻擊者只是嘗試所有可能的組合鍵。

問題 83

tb787631.CISSPPT3E.c03.025

Joanna 想查看她的組織用於樓宇控制的工業控制系統的狀態。她應該查詢訪問哪種類型的系統？

A、SCADA

B、決策支持系統

C.DOWN

D.ICS-CSS

你回答正確！

監控和數據採集系統，或 SCADA 系統，提供了一個圖形界面來監控工業控制系統 (ICS)。Joanna 應該詢問有關她所在組織的 SCADA 系統的訪問權限。

問題 84

tb787631.CISSPPT3E.c03.018

請參考以下場景：

- Alice 和 Bob 想使用非對稱密碼系統相互通信。它們位於該國的不同地區，但通過使用由相互信任的證書頒發機構簽署的數字證書來交換加密密鑰。

在這種情況下，Bob 不會擁有以下哪一個密鑰？

A. 愛麗絲的公鑰

B.愛麗絲的私鑰

C. Bob 的公鑰

D. Bob 的私鑰

你回答正確！

每個用戶都保留他們的私鑰作為秘密信息。在這種情況下，Bob 只能訪

問他自己的私鑰，而不能訪問 Alice 或任何其他用戶的私鑰。

問題 85

tb787631.CISSPPT3E.c03.020

為了抵禦彩虹表攻擊而添加到密碼中的隨機值的名稱是什麼？

A.哈希

B、鹽

C. 擴展器

D、鋼筋

你回答正確！

salt 是在操作系統對密碼進行哈希處理之前添加到密碼中的隨機值。然

後將鹽與散列密碼一起存儲在密碼文件中。通過否定使用預先計算的哈希

值（例如彩虹表）的攻擊的有用性，這增加了密碼分析攻擊的複雜性。

問題 86

tb787631.CISSPPT3E.c03.055

愛麗絲給鮑勃發了一條消息。Bob 想向 Charlie 證明他收到的消息肯定來自 Alice。Bob 試圖實現什麼密碼學目標？

A. 認證
B. 保密
C. 不可否認性
D. 誠信

你回答正確！

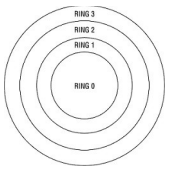
當消息的接收者能夠向第三方證明該消息來自聲稱的發送者時，就會發生

不可否認性。

問題 87

tb787631.CISSPPT3E.c03.047

在這裡所示的環保護模型中，哪個環包含操作系統的內核？



A.環 0

B. 環 1

C. 環 2

D. 環 3

你回答正確！

內核位於中央環 Ring 0 內。從概念上講，Ring 1 包含其他操作系統組件 。

Ring 2 用於驅動程序和協議。用戶級程序和應用程序在 Ring 3 上運行 。

Ring 0 到 2 在特權模式下運行，而 Ring 3 在用戶模式下運行。值得注意的是，許多現代操作系統並未完全實現此模型。

問題 88

tb787631.CISSPPT3E.c03.050

以下哪一項系統保證流程提供了對系統控制的獨立第三方評估，可能會受到許多不同組織的信任？

一、認證

B. 定義

C. 驗證

D. 認證

您回答錯誤。

驗證過程類似於認證過程，因為它驗證安全控制。通過涉及第三方測試服

務和編譯可能被許多不同組織信任的結果，驗證可能會更進一步。認可是

管理層正式接受評估系統的行為，而不是評估系統本身。

問題 89

tb787631.CISSPPT3E.c03.064

在重新使用驅動器之前，您可以採取什麼措施來防止由於 SSD 設備上的磨損均衡而導致的意外數據洩露？

A. 重新格式化

B、磁盤加密

C、消磁

D. 物理破壞

你回答正確！

加密 SSD 驅動器上的數據確實可以防止磨損均衡。磁盤格式化不會有效地從任何設備中刪除數據。消磁只對磁性介質有效。物理銷毀驅動器將不允許重新使用。

問題 90

tb787631.CISSPPT3E.c03.054

Gary 擔心將一致的安全設置應用於整個組織中使用的許多移動設備。什麼技術最能幫助應對這一挑戰？

A、MDM
B、IPS
C、入侵檢測系統
D、SIEM

您回答錯誤。

移動設備管理 (MDM) 產品提供一致的集中式界面，用於將安全配置設置應用到移動設備。

問題 91

tb787631.CISSPPT3E.c03.028

Carl 的組織最近接受了用戶訪問審查。在審查結束時，審計員注意到幾個特權蔓延的案例。違反了什麼安全原則？

A. 安全失敗

B、保持簡單

C. 信任但驗證

D. 最小特權

你回答正確！

最小特權原則表明，員工應該只擁有執行其工作所需的最低必要特權。特權蔓延表示員工積累了他們不再需要的權限，這表明違反了最小特權原則。

信任但驗證原則指出，組織應該使用審計來確保達到控制目標。故障安全原則指出，在控制失敗的情況下，安全控制應該默認為安全狀態。保持簡單原則表明，安全控制和其他技術在完成其目標的同時應盡可能保持簡單。

問題 92

tb787631.CISSPPT3E.c03.057

Gordon 擔心黑客可能會利用 Van Eck 輻射現象遠程讀取其設施內受限工作區域內計算機顯示器的內容。什麼技術可以防止這種類型的攻擊？

A.TCSEC

B、SCSI

C.幽靈

D. 暴風雨

你回答正確！

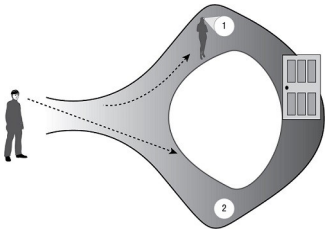
TEMPEST 程序創建了不易受到 Van Eck phreaking 攻擊的技術，因為

它減少或抑制了自然電磁輻射。

問題 93

tb787631.CISSPPT3E.c03.075

John 和 Gary 正在協商一項業務交易，John 必須向 Gary 證明他有權訪問系統。他參與了這裡顯示的“魔法門”場景的電子版本。約翰使用什麼技術？



A. 分裂知識證明

B. 零知識證明

C. 邏輯證明

D. 數學證明

你回答正確！

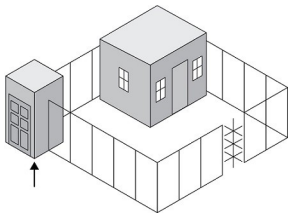
在零知識證明中，一個人向另一個人證明他們可以在不實際披露敏感信息

的情況下實現需要敏感信息的結果。

問題 94

tb787631.CISSPPT3E.c03.032

Ryan 正在為其組織的數據中心製定物理訪問計劃，並希望實施此圖中箭頭指示的安全控制。這個控件的名稱是什麼？



A. 咒語

B、閘機

C. 入侵防禦系統

D.網關

你回答正確！

陷阱使用兩組門來控制對設施的訪問。這可用於通過監視對誘捕器的使用

以一次只允許一個人進入設施來防止搭載。它們還可用於允許對個人進行

手動檢查或執行其他安全檢查。Mantraps 通常也稱為訪問控制前庭。

問題 95

tb787631.CISSPPT3E.c03.029

Matt 的組織最近採用了零信任網絡架構。在這種方法下，在授予對象資源訪問權限時，以下哪一項標準最不適合使用？

一、密碼

B. 雙因素認證

C、IP 地址

D. 生物識別掃描

你回答正確！

在零信任網絡架構中，永遠不應根據系統在網絡上的位置做出訪問控制決策。因此，永遠不要使用 IP 地址，它是這些選項中最不合適的。雖然其他選項具有不同級別的安全性（雙因素身份驗證顯然比單獨使用密碼或生物識別技術更強），但它們並不違反零信任網絡架構的原則。

問題 96

tb787631.CISSPPT3E.c03.059

Sherry 對其組織內使用的加密技術進行了清點，發現了以下算法和協議在使用中。由於不再被認為是安全的，她應該更換其中的哪一項技術？

A、MD5

B、AES

C、PGP

D.WPA3

您回答錯誤。

MD5 散列算法存在已知的衝突，並且自 2005 年起，不再被認為在現代

環境中使用是安全的。AES、PGP 和 WPA3 算法仍然被認為是安全的 。

問題 97

tb787631.CISSPPT3E.c03.044

Kyle 被授予訪問使用系統高級模式的軍用計算機系統的權限。Kyle 的安全審查要求有什麼不正確的地方？

答：Kyle 必須獲得系統處理的最高級別機密的許可，無論他的訪問權限如何。

B. Kyle 必須獲得系統處理的所有信息的訪問權限。

C. Kyle 必須有有效的了解系統處理的所有信息的需要。

D. Kyle 必須擁有有效的安全許可。

您回答錯誤。

對於以系統高級模式運行的系統，用戶必須對系統處理的所有信息具有有

效的安全許可，對系統處理的所有信息具有訪問權限，並且對某些（但不

一定是所有）處理的信息具有有效的知情權由系統。

問題 98

tb787631.CISSPPT3E.c03.006

Bob 是美國聯邦政府的一名安全管理員，他想選擇一種數字簽名方法，該方法是 FIPS 186-4 下聯邦數字簽名標準的批准部分。以下哪一種加密算法不是用於數字簽名的可接受選擇？

A、DSA

B、哈弗

C、RSA

D.ECDSA

你回答正確！

數字簽名標準批准了三種用於數字簽名的加密算法：數字簽名算法 (DSA)；Rivest、Shamir、Adleman (RSA) 算法；和橢圓曲線 DSA (ECDSA) 算法。HAVAL 是哈希函數，不是加密算法。雖然散列函數用作數字簽名過程的一部分，但它們不提供加密。

問題 99

tb787631.CISSPPT3E.c03.089

主 HVAC 系統中的組件故障導致 Kim 管理的數據中心出現高溫警報。解決問題後，Kim 應該考慮什麼以防止將來出現此類問題？

A. 閉環冷水機

B. 冗餘冷卻系統

C. 沼澤冷卻器

D. 將數據中心遷移到氣候較冷的地方

您回答錯誤。

一個設計良好的數據中心應該為其基礎設施的每個關鍵部分提供冗餘系統和功能。這意味著電源、冷卻和網絡連接都應該是冗餘的。Kim 應該確定如何確保單個系統故障不會使她的數據中心離線。