P1-002 結果 2022 年 12 月 19 日

問題一

tb787631.CISSPPT3E.pt1.045

海倫最近構建了一個新系統，作為其組織欺騙活動的一部分。系統的配置方式使其容易受到攻擊，並表明它可能包含高度敏感的信息。哪個術語最能描述這個系統？

A.蜜網

B. 暗網

C、蜜罐

D. 偽法律

你回答正確！

蜜罐是一種誘餌計算機系統，用於誘使入侵者進行攻擊。蜜網是由多個蜜罐組成的網絡，它為入侵者創造了一個更複雜的探索環境。偽缺陷是系統中可能吸引攻擊者的虛假漏洞。暗網是一段未使用的網絡地址空間，應該沒有網絡活動，因此可以很容易地用於監視非法活動。

問題 2

tb787631.CISSPPT3E.pt1.025

戈登正在為他的組織進行風險評估，並確定洪水預計每年對其設施造成的破壞程度。戈登確定了什麼指標？

A. 但是

B、ARO

C、系統性紅斑狼瘡

D.英孚

您回答錯誤。

年化損失預期 (ALE) 是組織預計每年因給定風險而發生的損失量。

問題三

tb787631.CISSPPT3E.pt1.003

Fran 正在構建取證分析工作站，並正在選擇要包含在設置中的取證磁盤控制器。以下哪些是取證磁盤控制器的功能？（選擇所有符合條件的。）

A. 防止存儲設備上的數據被修改

B. 返回設備請求的數據

C. 報告設備發送給取證主機的錯誤

D. 阻塞發送到設備的讀取命令

您回答錯誤。

取證磁盤控制器執行四個功能。其中之一，寫阻塞，攔截發送到設備的寫

命令並阻止它們修改設備上的數據。其他三個功能包括返回讀取操作請求

的數據、從設備返回訪問重要信息以及從設備向取證主機報告錯誤。控制

器不應阻止將讀取命令發送到設備，因為這些命令可能會返回關鍵信息。

問題四

tb787631.CISSPPT3E.pt1.077

Seth 正在為他的組織正在建造的新設施設計物理安全控制。他想盡可能地阻止攻擊。以下哪些控制措施起到了威懾作用？ (選擇所有符合條件的。)

A. 運動探測器

B、護衛犬

C. 陷阱

D、燈光

你回答正確！

威懾控制旨在首先防止入侵者嘗試攻擊。看門狗具有令人生畏的存在，可

以很好地滿足這個目的。根據他們的訓練，它們還可以用於拒絕、檢測和

延遲入侵。照明還可以通過使潛在入侵更加明顯來阻止攻擊，從而降低入

侵者進入光線充足區域的可能性。Mantraps 旨在拒絕入侵者訪問，而不

是阻止嘗試。運動檢測器旨在檢測入侵者而不是阻止他們。

問題 5

tb787631.CISSPPT3E.pt1.048

Roger 擔心受僱為內部應用程序開發代碼的第三方公司會在代碼中嵌入後門。開發商保留對知識產權的權利，並且只會以最終形式交付軟件。以下哪一種語言最不容易受到這種類型的攻擊，因為它會為 Roger 提供最終形式的人類可讀代碼？

A. JavaScript

公元前

C、C++

D.Java

你回答正確！

JavaScript 是一種解釋型語言，因此代碼在執行前不會被編譯，從而允許羅傑檢查代碼的內容。C、C++ 和 Java 都是編譯語言——編譯器生成人類不可讀的可執行文件。

問題 6

tb787631.CISSPPT3E.pt1.078

Thomas 最近簽署了一項無服務器計算環境協議，他的組織的開發人員將能夠在其中使用 Python 編寫函數並將它們部署在雲提供商的服務器上以供執行。雲提供商將管理服務器。哪個術語最能描述這個模型？

A、SaaS

B、PaaS

C、基礎設施即服務

D. 容器化

你回答正確！

這是功能即服務 (FaaS) 計算的示例。但是，FaaS 並未列為答案選項，

因此您還必須知道 FaaS 是平台即服務 (PaaS) 計算的子類別才能正確回

答此問題。該模型不一定利用容器化。雲提供商正在管理基礎架構，並且

只向客戶提供平台，因此它不是基礎架構即服務 (IaaS)。客戶正在運行

他們自己的代碼，因此它不是軟件即服務 (SaaS)。

問題 7

tb787631.CISSPPT3E.pt1.054

約翰正在為他的組織開發有形資產清單。以下哪些項目最有可能包含在該清單中？（選擇所有符合條件的。）

一、知識產權

B、服務器硬件

C. 存儲在服務器上的文件

D. 移動設備

你回答正確！

有形資產庫存包括組織擁有的物理項目。這將包括服務器硬件和移動設備。

存儲在服務器上的知識產權和文件不是有形財產，而是包含在無形資產清單中。

問題 8

tb787631.CISSPPT3E.pt1.046

Nandi 正在評估一組候選系統，以取代她組織中的生物特徵認證機制。什麼指標是比較不同系統有效性的最佳方式？

A.遠
B、FRR
C. CER
D、羅斯福

您回答錯誤。

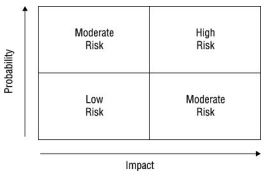
The false acceptance rate (FAR) is the rate at which the system inadvertently admits an unauthorized user, while the false rejection rate (FRR) is the rate at which the system inadvertently rejects an authorized

user. Both the FAR and FRR may be modified by adjusting the sensitivity of the system. The crossover error rate (CER) is the point where both the false acceptance rate and the false rejection rate cross. The CER is less subject to manipulation and is, therefore, the best metric to use for evaluating systems. The FDR is not a metric used to evaluate authentication systems.

Question 9

tb787631.CISSPPT3E.pt1.091

What type of risk assessment uses tools such as the one shown here?



A. Quantitative

B. Loss expectancy

C. Financial

D. Qualitative

You Answered Incorrectly.

使用概率/影響矩陣是定性風險評估的標誌。它使用概率和影響的主觀度

量，例如“高”和“低”，而不是定量度量。

問題 10

tb787631.CISSPPT3E.pt1.115

請參考以下場景：

- 在 Web 應用程序漏洞掃描測試期間，史蒂夫對他認為可能容易受到攻擊的 Web 服務器運行 Nikto。使用此處顯示的 Nikto 輸出，回答以下問題。

為什麼 Nikto 認為目錄索引是一個問題？

A. 它列出目錄中的文件。

B. 它可能允許 XDRF。

C. 目錄索引可能導致拒絕服務攻擊。

D. 默認情況下目錄索引是關閉的，可能表示妥協。

你回答正確！

在滲透測試期間，目錄索引最初可能看起來不是問題，但僅僅知道文件的

名稱和位置就可以為攻擊者提供大量關於組織的信息，以及潛在可訪問文

件的列表。XDRF 不是一種攻擊類型，索引也不是拒絕服務攻擊向量。

目錄索引被打開通常是由於錯誤配置或設計，或者是因為服務器在設置時

未正確配置，而不是攻擊的跡象。

問題 11

tb787631.CISSPPT3E.pt1.088

會話層從傳輸層發送的數據中刪除標頭時發生的過程是什麼？

A. 封裝
B. 數據包解包
C. 解封裝
D. 有效載荷

你回答正確！

從 OSI 模型的前一層接收到的數據中刪除標頭（可能還有腳註）的過程

稱為解封裝。添加頁眉和/或頁腳時會發生封裝。有效載荷是傳送到目標

的病毒或惡意軟件包的一部分，而數據包解包是一個虛構的術語。

問題 12

tb787631.CISSPPT3E.pt1.120

以下哪項技術旨在防止 Web 服務器離線成為 Web 應用程序架構中的單點故障？

A、負載均衡

B、雙電源

C、IPS

D、RAID

你回答正確！

負載平衡有助於確保發生故障的服務器不會使網站或服務脫機。雙電源僅

用於防止電源或電源發生故障。IPS 可以幫助防止攻擊，RAID 可以幫助

防止磁盤故障導致系統脫機。

問題 13

tb787631.CISSPPT3E.pt1.020

Barb 正在審查她的組織面臨的合規義務以及每個人可能承擔的責任類型。違反下列哪些法律法規可能會受到刑事處罰？（選擇所有符合條件的。）

A. FERPA

B. HIPAA

C、SOX

D. PCI DSS

您回答錯誤。

The Health Insurance Portability and Accountability Act (HIPAA) is a U.S. law governing the healthcare sector that does provide for criminal penalties. The Sarbanes–Oxley (SOX) Act governs publicly traded corporations and also provides for criminal penalties. The Family Educational Rights and Privacy Act (FERPA) is a U.S. law governing educational records, but it does not provide for criminal penalties. PCI DSS, the Payment Card Industry Data Security Standard, is an industry standard for credit card operations and handling. Because it is not a law, PCI DSS violations cannot incur criminal sanctions.

Question 14

tb787631.CISSPPT3E.pt1.009

Please refer to the following scenario:

- Ben owns a coffeehouse and wants to provide wireless internet service for his customers. Ben's network is simple and

uses a single consumer-grade wireless router and a cable modem connected via a commercial cable data contract.

How can Ben provide access control for his customers without having to provision user IDs before they connect while also gathering useful contact information for his business purposes?

A. WPA2 PSK

B. A captive portal

C. Require customers to use a publicly posted password like “BensCoffee”

D. WPA3 SAE

You Answered Incorrectly.

強制門戶可能需要那些想要連接和使用 WiFi 的人提供電子郵件地址才能連接。這使 Ben 能夠在滿足其業務目的的同時提供易於使用的無線網絡。

WPA2 PSK 是 WPA 的預共享密鑰模式，不會提供有關獲得密鑰的用戶的信息。WPA3 的 SAE 模式比 WPA2 PSK 更可取，但它仍然不允許收集 Ben 想要的數據。共享密碼也不允許收集數據。

問題 15

tb787631.CISSPPT3E.pt1.067

Lisa 想要與使用 OAuth 2.0 的雲身份提供商集成，她想要選擇合適的身份驗證框架。以下哪一項最符合她的需要？

A. OpenID 連接

B、SAML

C. 半徑

D. Kerberos

你回答正確！

OpenID Connect 是一個身份驗證層，它使用 OAuth 2.0 作為其底層授權框架。它已被雲服務提供商廣泛採用並得到廣泛支持 。

SAML、RADIUS 和 Kerberos 是替代身份驗證技術，但與 OAuth 的無縫集成級別不同。

問題 16

tb787631.CISSPPT3E.pt1.113

Kara 正在記錄漏洞掃描的結果。在查看一項調查結果後，她確定該漏洞確實存在。該團隊隨後實施了配置更改以糾正該問題。Kara 應該如何在她的報告中對這個漏洞進行分類？

A. 真陽性

B、真陰性

C. 誤報

D、假陰性

你回答正確！

這是一個真正的肯定報告，因為掃描檢測到漏洞並且漏洞確實存在。該團隊後來修復了該漏洞的事實可能會在報告中註明，但這不會改變掃描結果或其分類。當掃描正確地註意到不存在漏洞時，就會出現真陰性。當掃描報告存在實際上並不存在的漏洞時，就會出現誤報。當掃描報告不存在漏洞而實際上存在漏洞時，就會出現漏報。

問題 17

tb787631.CISSPPT3E.pt1.021

Quentin 正在分析他使用 Wireshark 在 TCP/IP 網絡上收集的網絡流量。他想識別在他的流量收集期間建立的所有新連接。如果他正在尋找構成用於建立新連接的 TCP 三次握手的三個數據包，那麼前三個數據包應該設置什麼標誌？

A. SYN、ACK、SYN/ACK
B、PSH、RST、ACK
C. SYN、SYN/ACK、ACK
D. SYN、RST、FIN

你回答正確！

TCP 三向握手包括通過 SYN 或同步標記數據包的初始聯繫；它接收帶

有 SYN/ACK 的響應，或同步和確認標記的數據包；由原始發件人使用

ACK 或確認數據包確認。RST 在 TCP 中用於重置連接，PSH 用於立即

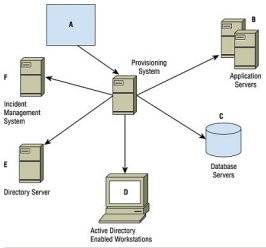
發送數據，FIN 用於結束連接。

問題 18

tb787631.CISSPPT3E.pt1.080

請參考以下場景：

- Alex 已經在他工作的大學工作了 10 多年。在那段時間裡，他擔任過系統管理員和數據庫管理員，還曾在大學的服務台工作。他現在是運行大學 Web 應用程序的團隊的經理。使用此處顯示的配置圖，回答以下問題。



如果亞歷克斯僱用了一名新員工，並且在人力資源部根據亞歷克斯通過一系列表格提供的數據將信息手動輸入到供應系統之後供應了該員工的帳戶，那麼發生了哪種類型的供應？

A. 全權委託賬戶撥備

B. 基於工作流的賬戶配置

C. 自動賬戶配置

D. 自助賬戶開通

你回答正確！

通過已建立的工作流程（例如通過 HR 流程）進行的供應是基於工作流程的帳戶供應。如果亞歷克斯在他管理的系統上為他的新員工設置了賬戶，他就會使用自主賬戶配置。如果供應系統允許新員工自行註冊賬戶，他們就會使用自助服務賬戶供應，如果有一個中央的、軟件驅動的流程，而不是人力資源表格，它就會自動化帳戶配置。

問題 19

tb787631.CISSPPT3E.pt1.090

哪種標記語言使用請求機構、供應服務點和供應服務目標的概念來處理其核心功能？

A.SAML

B. 樣品

C、SPML

D.XACML

你回答正確！

服務供應標記語言 (SPML) 使用請求機構向供應服務點發出 SPML 請求。

供應服務目標通常是用戶帳戶，並且需要在其實施中允許數據的唯一標識。

SAML 用於安全斷言，SAMPL 是一種代數建模語言，XACML 是一種訪問控制標記語言，用於以 XML 格式描述和處理訪問控制策略。

問題 20

tb787631.CISSPPT3E.pt1.018

Ben 正在設計一個數據庫驅動的應用程序，他希望通過將中間結果存儲在數據庫中來確保兩個正在執行的事務不會相互影響。他要強制執行什麼財產？

A. 原子性
B. 隔離
C. 一致性
D. 耐用性

你回答正確！

隔離要求事務彼此分開操作。原子性確保如果數據庫事務的任何部分失敗，則必須回滾整個事務，就好像它從未發生過一樣。一致性確保所有事務都

符合數據庫的邏輯規則，例如具有主鍵。持久性要求一旦事務提交到數據

庫就必須保留它。這些屬性共同構成了 ACID 模型。

問題 21

tb787631.CISSPPT3E.pt1.108

在這裡顯示的圖中，Harry 讀取數據文件的請求被阻止。哈利擁有機密安全許可，數據文件屬於絕密級別。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！

簡單安全屬性可防止個人閱讀比他或她的許可所允許的更高安全級別的信

息。這也稱為“不讀”規則。簡單完整性屬性表示用戶不能將數據寫入比他

們自己更高的完整性級別。*-Security 屬性表示用戶不能將數據寫入比他

們自己更低的安全級別。自主安全屬性允許使用矩陣來確定訪問權限。

問題 22

tb787631.CISSPPT3E.pt1.012

Kevin 正在審查和更新他的組織使用的安全文檔。他想記錄他的團隊在過去一年中開發的一些保護物聯網設備的最佳實踐。這些做法本質上是概括性的，不涵蓋特定設備。什麼類型的文件最適合這個目的？

一項政策

B、標準

C. 指南

D. 程序

你回答正確！

Kevin 可能會使用這些文件中的任何一份。我們應該將問題中表明這些是最佳實踐的部分歸零。這意味著建議不是強制性的，因此不會成為政策或標準。該建議本質上是一般性的，這意味著它可能不太適合程序的逐步性質。指南是記錄這些最佳實踐的最佳場所。

問題 23

tb787631.CISSPPT3E.pt1.039

Greg 正在評估一家將為其組織提供網絡設備的新供應商。由於其組織的工作性質，Greg 擔心攻擊者可能會嘗試利用供應鏈。假設 Greg 的組織和供應商都在合理的安全程序下運作，以下哪一項活動可能對設備造成最大的供應鏈風險？

A. 未經授權的第三方在供應商網站上進行篡改

B. 攔截傳輸中的設備

C. 安裝後管理員配置錯誤

D. 未經授權的第三方在 Greg 的網站上進行篡改

您回答錯誤。

如果供應商採用合理的安全程序進行操作，則設備不太可能在供應商的站點上被篡改。同樣，如果 Greg 的組織有合理的安全程序，那麼在他的站點上進行篡改也是不太可能的。管理員的錯誤配置始終是可能的，但這是安裝後風險而不是供應鏈風險。在從供應商到 Greg 的組織的運輸過程中，設備可能會被攔截和篡改。

問題 24

tb787631.CISSPPT3E.pt1.004

Mike 正在構建一個容錯服務器並希望實施 RAID 1。構建此解決方案需要多少物理磁盤？

A. 1

B.2

C.3

D.5

你回答正確！

RAID 1，磁盤鏡像，需要兩個包含相同數據副本的物理磁盤。

問題 25

tb787631.CISSPPT3E.pt1.110

Kolin 正在尋找一種網絡安全解決方案，使他能夠幫助減少零日攻擊，同時在系統連接到網絡之前使用身份在系統上實施安全策略。Kolin 應該實施什麼類型的解決方案？

A、防火牆

B. NAC 系統

C. 入侵檢測系統

D. 港口安全

您回答錯誤。

網絡訪問控制 (NAC) 系統可用於對用戶進行身份驗證，然後在允許用戶

連接到網絡之前驗證其係統是否符合安全標準。實施安全配置文件有助於

減少零日攻擊，使 NAC 成為一個有用的解決方案。防火牆無法強制執行

系統安全策略，而 IDS 只能在攻擊發生時進行監控和警報。因此，無論是防火牆還是 IDS 都不能滿足 Kolin 的需求。最後，端口安全是一種基於 MAC 地址的安全功能，只能限制哪些系統或設備可以連接到給定端口。

問題 26

tb787631.CISSPPT3E.pt1.057

當 Ben 記錄數據然後在他的測試網站上重播以驗證它如何根據實際生產工作負載執行時，他正在進行哪種類型的性能監控？

A、被動
B. 主動
C.反應性
D.重放

您回答錯誤。

主動監控，也稱為綜合監控，使用記錄或生成的流量來測試系統和軟件。

被動監控使用網絡跨度、分路器或其他設備來捕獲要分析的流量。反應式和重播不是監視類型的行業術語。

問題 27

tb787631.CISSPPT3E.pt1.114

請參考以下場景：

- 在 Web 應用程序漏洞掃描測試期間，史蒂夫對他認為可能容易受到攻擊的 Web 服務器運行 Nikto。使用此處顯示的 Nikto 輸出，回答以下問題。

為什麼 Nikto 標記`/test`目錄？

A. `/test` 目錄允許對 PHP 進行管理訪問。

B. 用於存儲敏感數據。

C. 測試目錄通常包含可能被濫用的腳本。

D. It indicates a potential compromise.

You Answered Incorrectly.

Test directories often include scripts that may have poor protections or may have other data that can be misused. There is not a default test directory that allows administrative access to PHP. Test directories are

not commonly used to store sensitive data, nor is the existence of a test directory a common indicator of compromise.

Question 28

tb787631.CISSPPT3E.pt1.101

Gavin is an internal auditor working to assess his organization's cybersecurity posture. Which of the following would be appropriate recipients of the reports he generates from his work? (Select all that apply.)

A. Managers
B. Individual contributors
C. Suppliers
D. Board members

You Answered Correctly!

將內部審計報告分發給組織中有正當需要知道的任何人是完全合適的。這可能包括負責解決問題的管理層和個人貢獻者，以及負責監督的董事會成員。將內部審計報告分發給供應商和客戶等外部實體通常是不合適的。

問題 29

tb787631.CISSPPT3E.pt1.118

Ursula 認為，她組織中的許多人都以不安全且可能違反組織安全策略的方式將敏感信息存儲在他們的筆記本電腦上。她可以使用什麼控件來識別這些文件的存在？

A. 網絡 DLP

B、網絡 IPS

C. 端點 DLP

D. 端點 IPS

你回答正確！

數據丟失防護 (DLP) 系統專門用於識別敏感信息。在這種情況下，Ursula 想要確定端點設備上是否存在此信息，因此她應該選擇端點 DLP 控件。基於網絡的 DLP 不會檢測存儲的信息，除非用戶通過網絡傳輸它。入侵防禦系統 (IPS) 旨在檢測和阻止正在進行的攻擊，不一定是敏感信息的存在。

問題 30

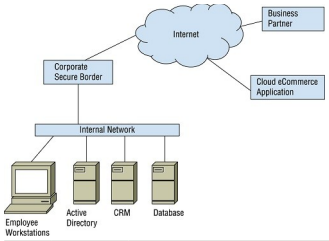
tb787631.CISSPPT3E.pt1.043

請參考以下場景：

- Ben 工作的組織有一個傳統的現場 Active Directory 環境，該環境使用手動配置過程來為其 350 名員工的公司添加每個新成員。

隨著公司採用新技術，他們越來越多地使用軟件即服務應用程序來取代他們內部開發的軟件堆棧。

- Ben 的任務是設計一個身份管理實現，使他的公司能夠在支持其現有系統的同時使用雲服務。使用此處顯示的邏輯圖，回答以下有關 Ben 應該提出的身份建議的問題。



當 Ben 的組織需要為其云電子商務應用程序提供身份驗證和授權斷言時，可能會涉及到哪些技術？

A. 活動目錄

B、SAML

C. 半徑

D.SPML

你回答正確！

安全斷言標記語言 (SAML) 經常用於集成雲服務，並提供進行身份驗證

和授權斷言的能力。Active Directory 集成是可能的，但對於雲服務提供

商來說不太常見，並且 RADIUS 通常不用於此類集成。服務供應標記語

言 (SPML) 用於供應用戶、資源和服務，而不是用於身份驗證和授權。

問題 31

tb787631.CISSPPT3E.pt1.008

Susan 設置了一個防火牆，跟踪兩個系統之間的通信狀態，並允許遠程系統只有在本地系統開始通信後才能響應本地系統。Susan 使用什麼類型的防火牆？

A.靜態包過濾防火牆

B. 應用級網關防火牆

C. A stateful packet inspection firewall

D. A circuit-level gateway firewall

You Answered Correctly!

Stateful packet inspection firewalls, also known as dynamic packet filtering firewalls, track the state of a conversation and can allow a response from a remote system based on an internal system being allowed to start the communication. Static packet filtering and circuit-level gateways only filter based on source, destination, and ports, whereas application-level gateway firewalls proxy traffic for specific applications.

Question 32

tb787631.CISSPPT3E.pt1.027

Frank 是 Web 服務器的安全管理員，該服務器向世界各地的人們提供新聞和信息。他的服務器收到異常高的流量，無法處理並被迫拒絕請求。Frank 將流量的來源追溯到殭屍網絡。發生了什麼類型的攻擊？

A. 拒絕服務

B、偵察

C、妥協

D. 惡意內幕

你回答正確！

這是拒絕服務攻擊的一個明顯例子——通過使用大量流量來拒絕合法用戶對系統的授權訪問。它超越了偵察攻擊，因為攻擊者正在影響系統，但它不是妥協，因為攻擊者沒有嘗試訪問系統。沒有理由相信其中涉及惡意的內部人員。

問題 33

tb787631.CISSPPT3E.pt1.013

Tom 正在調整他的安全監控工具，試圖在不遺漏重要安全事件的情況下減少管理員收到的警報數量。他決定將系統配置為僅在一小時內有五次嘗試訪問同一帳戶失敗時才報告失敗的登錄嘗試。哪個術語最能描述 Tom 使用的技術？

A. 閾值

B、抽樣

C. 賬戶鎖定

D、裁剪

你回答正確！

裁剪是一種分析技術，僅在超過設定閾值後才報告警報。它是一種特定形式的抽樣，是一個更通用的術語，描述了任何試圖摘錄記錄以供審查的嘗試。閾值不是一個常用的術語。管理員可以選擇在登錄嘗試失敗後配置自動或手動帳戶鎖定，但這在場景中沒有描述。

第 34 題

tb787631.CISSPPT3E.pt1.031

Brian 正在考慮增加他的組織使用的加密密鑰的長度。如果他在加密密鑰中增加 8 位，那麼該算法的密鑰空間中還會增加多少個可能的密鑰？

A. 鍵空間的大小會加倍。

B. 鍵空間的大小將增加 8 倍。

C. 鍵空間的大小將增加 64 倍。

D. 鍵空間的大小將增加 256 倍。

您回答錯誤。

二進制密鑰空間包含許多密鑰，這些密鑰的數量等於 2 的位數次方。2

的 8 次方是 256，因此鍵空間將增加 256 倍。

問題 35

tb787631.CISSPPT3E.pt1.038

一名攻擊者最近致電某組織的服務台，並說服他們為另一個用戶的帳戶重置密碼。哪個術語最能描述這種攻擊？

A. 人類特洛伊木馬
B. 社會工程
C. 網絡釣魚
D. 捕鯨

你回答正確！

社會工程學利用人類來讓攻擊得逞。由於服務台員工的具體任務是提供幫

助，因此他們可能會成為冒充合法員工的攻擊者的目標。特洛伊木馬是一

種惡意軟件，而網絡釣魚是通過旨在捕獲密碼或其他敏感數據的電子通信

方法進行的有針對性的攻擊。捕鯨是一種針對高知名度或重要目標的網絡

釣魚。

問題 36

tb787631.CISSPPT3E.pt1.015

Christopher's Cheesecakes 的會計文員無法訪問個別員工的工資信息，但想知道新員工的工資。在僱用新人之前，他提取了支付期間的總工資支出，然後提取了下一個支付期間的相同費用。他計算這兩個數額之間的差額以確定個人的薪水。發生了什麼類型的攻擊？

A. 意大利臘腸切片

B. 數據欺騙

C、推論

D. 社會工程

你回答正確！

在推理攻擊中，攻擊者使用幾條通用的非敏感信息來確定特定的敏感值。

在香腸切片攻擊中，攻擊者多次竊取少量資金以積累大量資金。在數據欺

騙攻擊中，攻擊者更改數據庫的內容。社會工程攻擊利用人類心理來實現

其目標。

問題 37

tb787631.CISSPPT3E.pt1.010

請參考以下場景：

- 本擁有一家咖啡館，他想為他的顧客提供無線互聯網服務。Ben 的網絡很簡單，使用一個消費級無線路由器和一個通過商業電纜數據合同連接的電纜調製解調器。

Ben 打算運行一個開放（未加密）的無線網絡。他應該如何連接他的業務設備？

A. 在同一個 SSID 上運行 WPA3。

B. 使用 WPA3 設置一個單獨的 SSID。

C. 以企業模式運行開放網絡。

D. 使用 WEP 設置單獨的無線網絡。

您回答錯誤。

許多現代無線路由器可以提供多個 SSID。Ben 可以為他的業務運營創建一個私有的安全網絡，但他需要確保客戶和業務網絡有防火牆或以其他方式在邏輯上相互隔離。如果不創建另一個無線網絡，就不可能在同一個 SSID 上運行 WPA3，並且會導致客戶混淆（SSID 不需要是唯一的）。在企業模式下運行網絡不適用於開放網絡，WEP 已過時且極易受到攻擊。

問題 38

tb787631.CISSPPT3E.pt1.034

Viola 正在進行用戶帳戶審核，以確定帳戶是否具有適當級別的權限，以及所有權限是否已通過正式流程獲得批准。該組織擁有大約 50,000 個用戶帳戶，年員工流動率為 24%。在選擇記錄進行人工審查時，以下哪一種抽樣方法最有效地利用了她的時間？

A. 選擇上個月修改過的所有記錄。

B. 要求訪問管理員確定最有可能出現問題的帳戶並對其進行審計。

C. 從整個總體或審計期間發生變化的記錄總體中隨機選擇記錄樣本。

D. 抽樣在這種情況下是無效的，所有的賬目都應該被審計。

您回答錯誤。

抽樣應隨機進行，以避免人為偏差。如果對足夠大的真正隨機樣本進行抽樣以提供對用戶群的有效覆蓋，則抽樣是一個有效的過程。一個人不可能查看每一條記錄。在一個擁有 50,000 名用戶且年營業額為 24% 的組織中，很可能其中至少有 1,000 條記錄在上個月發生了更改。這仍然是太多的記錄來審查。要求賬戶管理員選擇要審查的記錄是一種利益衝突，因為他們是被審計的群體。

第 39 題

Harry 想要訪問存儲在文件服務器上的 Sally 擁有的文檔。將主體/客體模型應用到這個場景中，資源請求的對像是誰或者是什麼？

A.哈利

B.莎莉

C、文件服務器

D. 文件

您回答錯誤。

在主體/客體模型中，客體是主體請求的資源。在此示例中，Harry 想要訪問文檔，使文檔成為請求的對象。

問題 40

tb787631.CISSPPT3E.pt1.056

Bert 正在考慮使用基礎架構即服務的雲計算合作夥伴來提供虛擬服務器。在這種情況下，以下哪一項是供應商的責任？

A.維護管理程序

B. 管理操作系統安全設置

C.維護主機防火牆

D. 配置服務器訪問控制

你回答正確！

在 IaaS 服務器環境中，客戶在責任共擔模型下保留對大多數服務器安全操作的責任。這包括管理操作系統安全設置、維護主機防火牆和配置服務器訪問控制。供應商將負責管理程序層及以下的所有安全機制。

問題 41

tb787631.CISSPPT3E.pt1.096

羅伯特是一家小型企業的網絡管理員，最近安裝了新的防火牆。在看到異常繁忙的網絡流量跡像後，他檢查了他的入侵檢測系統，該系統報告說正在進行 smurf 攻擊。Robert 可以更改哪些防火牆配置以最有效地防止此攻擊？

A. 阻斷攻擊的源 IP 地址。
B. 阻止入站 UDP 流量。
C. 封鎖攻擊的目的 IP 地址。
D. 阻止入站 ICMP 流量。

您回答錯誤。

Smurf 攻擊使用分佈式攻擊方法從許多不同的源地址向目標系統發送 ICMP 回應回复。阻止此攻擊的最有效方法是阻止入站 ICMP 流量。阻止源地址是不可行的，因為攻擊者可能會簡單地更改源地址。阻止目標地

址可能會破壞正常活動。smurf 攻擊不使用 UDP，因此阻止該流量不會

有任何效果。

問題 42

tb787631.CISSPPT3E.pt1.011

請參考以下場景：

- 本擁有一家咖啡館，他想為他的顧客提供無線互聯網服務。Ben 的網絡很簡單，使用一個消費級無線路由器和一個通過商業電纜數據合同連接的電纜調製解調器。

實施第一個問題的解決方案後，Ben 收到投訴稱其咖啡館的用戶劫持其他客戶的網絡流量，包括使用他們的用戶名和密碼。這怎麼可能？

A. 密碼由所有用戶共享，使流量容易受到攻擊。

B. 惡意用戶在路由器上安裝了木馬。

C. 用戶使用 ARP 欺騙路由器，將所有流量廣播給所有用戶。

D. 開放網絡未加密，使流量很容易被嗅探。

你回答正確！

未加密的開放網絡以明文方式廣播流量。這意味著可以使用數據包嗅探器

輕鬆捕獲網站的未加密會話。FireSheep 等一些工具專門設計用於從流

行網站捕獲會話。幸運的是，許多網站現在默認使用 TLS，但其他網站

仍以明文形式發送用戶會話信息。共享密碼不是漏洞的原因，ARP 欺騙

不是無線網絡的問題，木馬的設計看起來像是安全軟件，而不是破壞路由

器。

問題 43

tb787631.CISSPPT3E.pt1.069

丹妮絲正在準備就她的公司與軟件供應商之間的合同糾紛進行審判。供應商聲稱 Denise 達成了口頭協議，修改了他們的書面合同。丹妮絲在為她辯護時應該提出什麼樣的證據規則？

A. 真實證據規則
B. 最佳證據規則
C. 口頭證據規則
D. 證明證據規則

你回答正確！

口頭證據規則規定，當雙方之間的協議以書面形式出現時，除非以書面形

式進行修改，否則假定為整個協議。最佳證據規則規定，如果原始文件可

用，則文件副本不予受理。真實證據和證明證據是證據類型，而不是證據規則。

問題 44

tb787631.CISSPPT3E.pt1.022

Daniel 正在為他的組織選擇一個新的移動設備管理 (MDM) 解決方案，並且正在編寫 RFP。在使組織的安全需求與 MDM 平台的功能保持一致後，他正在嘗試決定應將哪些功能作為要求包括在內。以下哪些是 MDM 解決方案的典型功能？（選擇所有符合條件的。）

A. 遠程擦除移動設備的內容
B. 假設控制未註冊的 BYOD 移動設備
C. 強制使用設備加密
D. 管理設備備份

你回答正確！

MDM 產品不具備控制當前不受組織管理的設備的能力。這相當於侵入他人擁有的設備，可能構成犯罪。它們通常提供管理設備備份、強制使用加密和遠程擦除移動設備內容的能力。

問題 45

tb787631.CISSPPT3E.pt1.073

Greg 正在為他的組織製定災難恢復計劃，他想確定在中斷後恢復特定 IT 服務所需的時間。Greg 在計算什麼變量？

A、MTD

B. 反收購行動

C、RPO

D、服務水平協議

你回答正確！

恢復時間目標 (RTO) 是指 IT 服務或組件在發生故障後恢復運行所需的時間。最長可容忍停機時間 (MTD) 是 IT 服務或組件可能不可用而不會對組織造成嚴重損害的最長時間。恢復點目標 (RPO) 確定在恢復工作期間可能丟失的最大數據量（按時間衡量）。服務級別協議 (SLA) 是記錄服務期望的書面合同。

問題 46

tb787631.CISSPPT3E.pt1.049

Jesse 正在查看配置為使用隱藏密碼的系統上的`/etc/passwd`文件。她希望在此文件的密碼字段中看到什麼？

A.明文密碼

B. 加密密碼

C. 散列密碼

D.x

您回答錯誤。

當系統配置為使用隱藏密碼時，`/etc/passwd` 文件僅包含字符 **x** 來代替密碼。它不會包含任何明文、加密或散列形式的密碼。

問題 47

tb787631.CISSPPT3E.pt1.094

Sally 正在為千兆以太網佈線。她應該做出什麼樣的佈線選擇以確保她能夠以她想要提供給用戶的全部 1000 Mbps 的速度使用她的網絡？

A. Cat 5 和 Cat 6

B. Cat 5e 和 Cat 6

C. Cat 4e 和 Cat 5e

D. Cat 6 和 Cat 7

你回答正確！

5e 類和 6 類 UTP 電纜的額定速率均為 1000 Mbps。Cat 5（不是 Cat 5e）的額定速率僅為 100 Mbps，而 Cat 7 的額定速率為 10 Gbps。沒有 Cat 4e。

問題 48

tb787631.CISSPPT3E.pt1.086

Dana 正在為她的組織選擇一個哈希函數，並希望在對加密強哈希的關注與算法的速度和效率之間取得平衡。以下哪一個哈希函數最能滿足她的需求？

A、MD5
B. RIPEMD
C.SHA-2
D、SHA-3

您回答錯誤。

原始版本的 RIPEMD 和 MD5 哈希算法存在已知漏洞，不應再使用。

SHA-2 和 SHA-3 現在都被認為是安全的，並且提供相同級別的安全性。

然而，SHA-3 的效率低於 SHA-2，這使得 SHA-2 成為滿足 Dana 需求的更好選擇。

問題 49

tb787631.CISSPPT3E.pt1.026

Greg 希望在他的組織中實施應用程序控制技術。他想限制用戶在他們的系統上只安裝批准的軟件。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。

應用程序控制的白名單方法允許用戶只安裝那些管理員特別批准的軟件包。

在需要嚴格控制應用程序安裝的情況下，這將是一種合適的方法。

第 50 題

tb787631.CISSPPT3E.pt1.085

在電子發現參考模型的哪個階段，組織確保潛在的可發現信息受到保護以防止更改或刪除？

A. 識別
B. 保存
C. 收藏
D、加工

您回答錯誤。

在保存階段，組織確保與手頭事項相關的信息受到保護，免遭有意或無意的更改或刪除。識別階段定位相關信息但不保存它。收集階段發生在保存之後並收集響應信息。處理階段對收集到的相關信息進行粗略切割。

問題 51

tb787631.CISSPPT3E.pt1.119

客戶在自己的數據中心搭建雲計算環境，還是在其他數據中心搭建客戶獨享的環境，屬於哪種雲計算模式？

A.公共雲
B、私有云
C、混合雲
D、共享雲

你回答正確！

In the private cloud computing model, the cloud computing environment is dedicated to a single organization and does not follow the shared tenancy model. The environment may be built by the company in its own data center or built by a vendor at a co-location site.

Question 52

tb787631.CISSPPT3E.pt1.047

Sean suspects that an individual in his company is smuggling out secret information despite his company's careful use of data loss prevention systems. He discovers that the suspect is posting photos, including the one shown here, to public internet message boards. What type of technique may the individuals be using to hide messages inside this image?

A. Watermarking

B. VPN

C. Steganography

D. Covert timing channel

You Answered Correctly!

隱寫術是使用加密技術將秘密消息嵌入其他內容的藝術。隱寫術算法通過

對文件進行不可見的更改來工作，例如修改構成圖像文件的許多位中的最

低有效位。VPN 可用於隱藏秘密通信，但它們在傳輸過程中提供保護並

且不能用於將信息嵌入圖像中。水印確實會在圖像中嵌入信息，但目的是

保護知識產權。靜止圖像不會用於隱蔽定時通道，因為它是固定文件。

問題 53

tb787631.CISSPPT3E.pt1.075

Jen 正在為其組織的數據中心選擇滅火系統，並希望縮小候選名單的範圍。以下哪一個抑制系統最不適合使用？

A、乾式管道

B、濕管

C. 行動前

D、FM-200

你回答正確！

濕管抑制系統的管道中始終存在水，這對包含電子設備的數據中心構成了

不可接受的風險水平，如果管道洩漏，這些電子設備可能會損壞。乾式管

道和預作用系統僅在可能發生火災時觸發時才含水。FM-200 是一種化

學抑製劑，常用於代替數據中心的水。

問題 54

tb787631.CISSPPT3E.pt1.102

Kim 正在對她的組織開發的 Web 應用程序進行測試，並希望確保它可以從所有常用的 Web 瀏覽器訪問。她應該進行什麼類型的測試？

A. 回歸測試

B、接口測試

C. 模糊測試

D. 白盒測試

你回答正確！

Web 應用程序通過接口與 Web 瀏覽器通信，使得接口測試成為此處的最佳答案。回歸測試可用作接口測試的一部分，但過於具體，不是最佳答案。同樣，測試可能是白盒測試或全知識測試，但接口測試更好地描述了這個特定示例。模糊測試不太可能作為瀏覽器兼容性測試的一部分，因為它測試的是意外輸入，而不是功能。

問題 55

tb787631.CISSPPT3E.pt1.123

Monica 正在開發一種軟件應用程序，用於計算個人的體重指數以用於醫療計劃。她想在醫生輸入個人體重的字段中包含一個控件，以確保體重在預期範圍內。Monica 應該使用什麼類型的控件？

A. 失敗打開

B. 故障保護

C、極限檢查

D. 緩衝區邊界

你回答正確！

輸入驗證確保作為輸入提供給程序的數據與預期參數匹配。限制檢查是一

種特殊形式的輸入驗證，可確保值保持在預期範圍內，如本場景中所述。

在規劃可能的系統故障時，故障開放和故障安全是選項。緩衝區邊界不是

一種軟件控制。

問題 56

tb787631.CISSPPT3E.pt1.014

Sally 的任務是在她的組織中為無線網絡服務部署身份驗證、授權和記帳服務器，並且需要避免使用專有技術。她應該選擇什麼技術？

A.OAuth

B. 半徑

C.XTACACS

D.戰術戰術攻擊+

你回答正確！

RADIUS 是一種常見的 AAA 技術，用於為撥號、無線網絡、網絡設備和

一系列其他系統提供服務。OAuth 是一種身份驗證協議，用於允許應用

程序在不共享密碼的情況下代表用戶執行操作，並用於許多 Web 應用程

序。雖然 XTACACS 和 TACACS+ 都提供了 Sally 正在尋找的功能，但

它們都是 Cisco 專有協議。

問題 57

tb787631.CISSPPT3E.pt1.044

Dave 負責其組織中的密碼安全，並希望加強密碼文件的安全性。他想捍衛他的組織免受彩虹表的使用。以下哪一項技術是專門設計來阻止彩虹表的使用的？

A. 密碼過期政策
B. 鹽醃
C. 用戶教育
D. 密碼複雜性政策

你回答正確！

Rainbow tables 使用預先計算的密碼哈希對密碼文件進行破解攻擊。他

們可能會對使用加鹽感到沮喪，加鹽會在散列之前將指定值添加到密碼中，

這使得執行預計算變得更加困難。密碼過期策略、密碼複雜性策略和用戶

教育都可能有助於密碼安全，但它們並不是針對彩虹表使用的直接防禦措

施。

問題 58

tb787631.CISSPPT3E.pt1.006

Evelyn 認為她所在組織的供應商之一違反了保護敏感數據的合同義務，並希望對相關情況進行調查。根據調查結果，Evelyn 的組織很可能會起訴供應商違約。哪個術語最能描述 Evelyn 正在進行的調查類型？

A. 行政調查
B. 刑事偵查
C. 民事偵查
D. 監管調查

您回答錯誤。

This is an example of a civil investigation because it relates to a contract

dispute and will likely wind up being litigated in civil court. Administrative

investigations are for internal purposes and are not applicable when a

third party is being investigated. Criminal and regulatory investigations may only be initiated by those with regulatory authority, typically government agencies.

Question 59

tb787631.CISSPPT3E.pt1.060

Mark is planning a disaster recovery test for his organization. He would like to perform a live test of the disaster recovery facility but does not want to disrupt operations at the primary facility. What type of test should Mark choose?

A. Full interruption test

B. Checklist review

C. Parallel test

D. Tabletop exercise

You Answered Correctly!

During a parallel test, the team actually activates the disaster recovery site for testing, but the primary site remains operational. During a full interruption test, the team takes down the primary site and confirms that

the disaster recovery site is capable of handling regular operations. The full interruption test is the most thorough test but also the most disruptive. The checklist review is the least disruptive type of disaster recovery test. During a checklist review, team members each review the contents of their disaster recovery checklists on their own and suggest any necessary changes. During a tabletop exercise, team members come together and walk through a scenario without making any changes to information systems.

Question 60

tb787631.CISSPPT3E.pt1.035

Lila 正在審查她的組織的不利終止流程。在此過程中，什麼時候撤銷用戶對數字系統的訪問權限最合適？

A. 通知用戶終止時
B. 在僱傭的最後一天結束時
C. 作出決定時
D. 最後一天工作後的幾天

您回答錯誤。

在不利情況下非自願終止的情況下，用戶將被解僱，並可能產生負面和潛

在的敵意反應。因此，重要的是在用戶被告知終止後立即終止訪問。在通

知之前終止訪問可能會提示用戶提前終止。在終止後保留訪問權限會帶來

惡意內部活動的風險。

問題 61

tb787631.CISSPPT3E.pt1.100

Matthew 在其組織的網絡上遇到網絡服務質量問題。主要症狀是數據包偶爾會花費太長時間從其來源傳輸到目的地。此延遲的長度因單個數據包而異。哪個詞描述了馬修面臨的問題？

A. 延遲

B、抖動

C.丟包

D、干擾

您回答錯誤。

延遲是數據包從源到目的地的傳輸延遲。抖動是不同數據包延遲的變化。

數據包丟失是指數據包在傳輸過程中丟失，需要重新傳輸。干擾是破壞數

據包內容的電噪聲或其他干擾。

第 62 題

tb787631.CISSPPT3E.pt1.052

Tony 正在為他的組織開發一個數據分類系統。在確定每類信息的分類級別時，他應該使用什麼因素作為主要驅動因素？

A、靈敏度

B. 來源

C. 盜竊的可能性

D. 數據丟失的可能性

你回答正確！

Information should be classified based upon its sensitivity. This may be

due to the value of the information to the organization, the damage

caused if lost or compromised, or other factors. The source of the

information is one possible contributing factor to the sensitivity level. The

likelihood of loss or theft is a component of risk, but does not contribute to the classification level.

Question 63

tb787631.CISSPPT3E.pt1.089

Rob is reviewing his organization's campus for physical security using the Crime Prevention Through Environmental Design (CPTED) framework. Which one of the following is NOT a strategy in this framework?

A. Natural intrusion detection
B. Natural access control
C. Natural surveillance
D. Natural territorial reinforcement

You Answered Incorrectly.

CPTED 實施三種策略：自然訪問控制、自然監視和自然領土加固。自然訪問控制使用路障和其他物理元素在安全和不安全空間之間創建分隔。自然監視設計的環境使潛在入侵者暴露於合法居住者的自然審查之下。自然

領土加固使用柵欄、標誌和其他元素來明確定義安全空間。自然入侵檢測

不是 CPTED 的組成部分。

第 64 題

tb787631.CISSPPT3E.pt1.024

Gina 最近參加了 CISSP 認證考試，然後寫了一篇博客文章，其中包含她遇到的許多考試問題的文本。在這種情況下，最直接違反 (ISC) 2 道德規範的 哪一方面？

A. 促進和保護職業。

B. 以正直、誠實、公正、負責任和合法的方式行事。

C. 保護社會、共同利益、必要的公眾信任和信心以及基礎設施。

D. 為校長提供勤奮和稱職的服務。

你回答正確！

吉娜的行為破壞了考試過程的完整性，從而損害了 CISSP 認證和信息安

全社區。雖然 Gina 的行為也不誠實，但對職業的危害更多的是直接違反

(ISC) 2 道德規範。

問題 65

tb787631.CISSPPT3E.pt1.062

在安全審計期間，Susan 發現該組織正在使用手部幾何掃描儀作為其安全數據中心的訪問控制機制。關於手部幾何掃描儀的使用，蘇珊應該提出什麼建議？

A. 它們的 FRR 很高，應該更換。

B. 應該添加第二個因素，因為它們不是可靠區分個體的好方法。

C. 手部幾何掃描儀為數據中心提供適當的安全保護，應考慮用於其他高安全性區域。

D. 它們可能會引起可訪問性問題，應考慮使用替代生物識別系統。

你回答正確！

手部幾何掃描儀評估個人手部的物理尺寸，但不驗證有關個人的其他獨特因素，甚至不驗證他們是否還活著。這意味著不應將手部幾何掃描儀作為安全環境的唯一身份驗證因素。手部幾何掃描儀沒有異常高的 FRR，與其他生物識別系統相比，從可訪問性的角度來看，它也不是一個突出的問題。

第 66 題

tb787631.CISSPPT3E.pt1.083

羅伯特正在審查一個系統，該系統已根據通用標準指定了 EAL2 評估保證級別。他對系統的最高保證是什麼？

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. 經過半形式化設計和測試。

您回答錯誤。

當系統已經過結構測試時，EAL2 保證適用。這是通用標準下倒數第二的保證級別。

問題 67

tb787631.CISSPPT3E.pt1.002

Ed 的任務是確定一項服務，該服務將提供一種低延遲、高性能和高可用性的方式來為其雇主託管內容。他應該尋找什麼類型的解決方案來確保他雇主在世界各地的客戶能夠快速、輕鬆、可靠地訪問他們的內容？

A、熱點站點

B、CDN

C. 冗餘服務器

D. P2P CDN

你回答正確！

內容分發網絡 (CDN) 旨在提供可靠、低延遲、地理分佈的內容分發。在這種情況下，CDN 是一個理想的解決方案。像 BitTorrent 這樣的 P2P

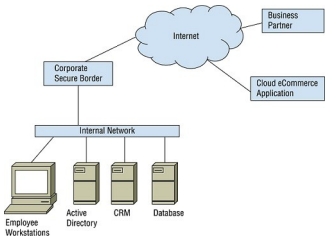
CDN 不是商業實體的典型選擇，而冗餘服務器或熱點站點可以提供高可用性，但不會滿足其餘要求。

第 68 題

tb787631.CISSPPT3E.pt1.041

請參考以下場景：

- Ben 工作的組織有一個傳統的現場 Active Directory 環境，該環境使用手動配置過程來為其 350 名員工的公司添加每個新成員。隨著公司採用新技術，他們越來越多地使用軟件即服務應用程序來取代他們內部開發的軟件堆棧。
- Ben 的任務是設計一個身份管理實現，使他的公司能夠在支持其現有系統的同時使用雲服務。使用此處顯示的邏輯圖，回答以下有關 Ben 應該提出的身份建議的問題。



如果身份驗證服務的可用性是組織的重中之重，Ben 應該推薦什麼類型的身份平台？

A、現場

B. 基於雲

C、混合型

D、外包

你回答正確！

混合身份驗證服務可以在雲端和本地提供身份驗證服務，確保最大限度地

減少因鏈路中斷導致的服務中斷。現場服務將在互聯網中斷期間繼續工作，

但不允許電子商務網站進行身份驗證。雲服務將使公司位置脫機。外包身

份驗證並不表明解決方案是在內部還是外部，因此不是一個有用的答案。

第 69 題

tb787631.CISSPPT3E.pt1.007

Ivan 正在安裝一個運動探測器來保護一個敏感的工作區域，該區域使用高頻微波信號傳輸來識別潛在的入侵者。他安裝的是什麼類型的檢測器？

A、紅外線

B. 熱基

C. 波形

D、電容

您回答錯誤。

波形運動檢測器將超聲波或微波信號傳輸到監控區域，觀察從物體反射回

來的信號的變化。基於頭部的紅外探測器會觀察異常的熱模式。電容檢測

器基於電磁場工作。

第 70 題

TB787631.CISSPPT3E.PT1.074

在對系統進行修改之前，什麼業務流程通常需要經理的簽字？

一、SDN

B. 發布管理

C. 變革管理

D. 版本控制

你回答正確！

變更管理通常需要在進行變更之前獲得經理或主管的簽字同意。這有助於

確保適當的意識和溝通。SDN 代表軟件定義網絡，發布管理是新軟件發

布被接受的過程，版本控制用於區分軟件、代碼或其他對象的版本。

第 71 題

tb787631.CISSPPT3E.pt1.033

GAD Systems is concerned about the risk of hackers stealing sensitive information stored on a file server. They choose to pursue a risk mitigation strategy. Which one of the following actions would support that strategy?

A. Encrypting the files
B. Deleting the files
C. Purchasing cyber-liability insurance
D. Taking no action

You Answered Correctly!

Encrypting the files reduces the probability that the data will be successfully stolen, so it is an example of risk mitigation. Deleting the files would be risk avoidance. Purchasing insurance would be risk transference. Taking no action would be risk acceptance.

Question 72

tb787631.CISSPPT3E.pt1.079

攻擊者攔截了大量使用相同算法和加密密鑰加密的數據。在沒有更多信息的情況下，以下哪些密碼分析攻擊是可能的？（選擇所有符合條件的。）

A. 已知明文
B.選擇密文
C.頻率分析
D、蠻力

您回答錯誤。

攻擊者可能會嘗試對大量加密密文進行頻率分析或暴力破解。由於攻擊者無法訪問明文信息，因此不可能進行已知明文攻擊。攻擊者也沒有加密信息的能力，因此他們不能使用選擇密文攻擊。

第 73 題

tb787631.CISSPPT3E.pt1.059

艾倫正在考慮在他的組織中使用新的身份證，以用於物理訪問控制。他偶然發現了一張樣本卡，但不確定該技術。他打開它，看到了下面的內部結構。這是什麼類型的卡？

A. 智能卡

B. 感應卡

C、磁條

D. 二期卡

你回答正確！

使用卡內的電磁線圈表明這是一張感應卡。

第 74 題

tb787631.CISSPPT3E.pt1.107

Ron 的組織沒有資源來執行使用時間密集型手動技術的滲透測試，但他希望獲得滲透測試的一些好處。他可以從事以下哪一項技術需要最少的體力勞動？

A. 白盒測試
B. 黑盒測試
C. 灰盒測試
D. 破壞和攻擊模擬

您回答錯誤。

破壞和攻擊模擬 (BAS) 平台旨在自動化滲透測試的某些方面。這些系統旨在將威脅指標註入系統和網絡，以觸發其他安全控制措施。白盒、灰盒和黑盒測試都涉及更多的手動工作。

第 75 題

tb787631.CISSPPT3E.pt1.066

Jerry 正在調查一次攻擊，攻擊者從用戶的 Web 會話中竊取身份驗證令牌並使用它在站點上冒充用戶。哪個術語最能描述這種攻擊？

A. 偽裝
B.重播
C. 欺騙
D. 修改

您回答錯誤。

偽裝（或冒充）攻擊使用竊取或偽造的憑據來繞過身份驗證機制。該術語

確實描述了這種攻擊，但即使在找到可能的正確答案後，您也應該繼續閱

讀答案選擇。在這種情況下，重播攻擊是一種更具體的偽裝攻擊類型，它

依賴於捕獲的身份驗證令牌，因此這是一個更好的答案。欺騙攻擊依賴於

在沒有憑據的情況下偽造身份，例如 IP 地址或主機名。當捕獲的數據包

被修改並重播到系統以嘗試執行操作時，就會發生修改攻擊。

第 76 題

tb787631.CISSPPT3E.pt1.070

當 Lauren 監控網絡連接兩端的流量時，她看到進入公共 IP 地址的流量出現在生產網絡內部。它前往具有 RFC 1918 保留目標地址的內部主機。她應該期望在網絡邊界使用什麼技術？

a.nat

B. VLAN

C.S/NAT

D、BGP

你回答正確！

網絡地址轉換 (NAT) 將內部地址轉換為外部地址。VLAN 是用來在邏輯

上劃分網絡的，BGP 是一種路由協議，S/NAT 是一個虛構的名詞。

第 77 題

tb787631.CISSPPT3E.pt1.084

Adam 正在處理最終用戶的訪問請求。在授予訪問權限之前，他應該驗證哪兩項？

A. 分離和需要知道
B. 清關和背書
C. 許可和需要知道的
D. 第二因素和間隙

你回答正確！

Before granting any user access to information, Adam should verify that

the user has an appropriate security clearance as well as a business

need to know the information in question.

Question 78

tb787631.CISSPPT3E.pt1.098

Frances is concerned that equipment failures within her organization's servers will lead to a loss of power to those servers. Which one of the following controls would best address this risk?

A. Redundant power sources
B. Backup generators
C. Dual power supplies
D. Uninterruptible power supplies

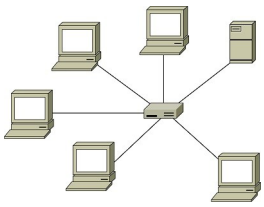
You Answered Incorrectly.

所有這些控制都用於提高服務器電源的可靠性。但是，只有雙電源可以解決服務器內部出現的硬件問題，從而允許服務器在其中一個電源出現故障時繼續運行。冗餘電源、備用發電機和不間斷電源 (UPS) 旨在提高流向服務器的電力的可靠性。

第 79 題

tb787631.CISSPPT3E.pt1.122

此處顯示的是什麼網絡拓撲？



A、戒指

B、公交車

C、一顆星星

D、網格

你回答正確！

星形拓撲使用中央連接設備。以太網網絡可能看起來像星形，但它們實際

上是一種邏輯總線拓撲結構，有時會部署在物理星形中。

問題 80

tb787631.CISSPPT3E.pt1.029

Gwen 是一家維護客戶記錄的金融服務公司的網絡安全專家。這些記錄包括每個客戶的個人信息，包括客戶姓名、社會安全號碼、出生日期和出生地點以及母親的娘家姓。哪個類別最能描述這些記錄？

A. 圖

B. 專有數據

C.二

D、EDI

你回答正確！

個人身份信息 (PII) 包括可用於區分或追踪個人身份的數據，還包括其醫

療、教育、財務和就業信息等信息。PHI 是個人健康信息，EDI 是電子

數據交換，專有數據用於保持組織的競爭優勢。

問題 81

tb787631.CISSPPT3E.pt1.064

Bailey is concerned that users around her organization are using sensitive information in a variety of cloud services and would like to enforce security policies consistently across those services. What security control would be best suited for her needs?

A. DRM
B. IPS
C. CASB
D. DLP

You Answered Incorrectly.

Cloud access security brokers (CASB) are designed to enforce security

policies consistently across cloud services and would best meet Bailey's

needs. Data loss prevention (DLP) and digital rights management (DRM)

solutions may be able to detect, block, and control some use of information in the cloud, but they would not provide a way to consistently enforce security policies across cloud platforms. Intrusion prevention systems (IPS) are designed to detect and block malicious activity and would not be relevant in this scenario.

Question 82

tb787631.CISSPPT3E.pt1.097

以下哪一種防火牆不具備跟踪不同數據包之間連接狀態的能力？

A. 狀態檢查
B. 申請代理
C. 數據包過濾器
D、下一代

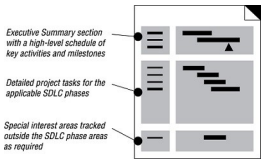
您回答錯誤。

靜態包過濾防火牆被稱為第一代防火牆，不跟踪連接狀態。狀態檢查、應用程序代理和下一代防火牆都增加了連接狀態跟踪功能。

問題 83

tb787631.CISSPPT3E.pt1.109

Norm 正在與一家使用 SDLC 方法進行開發的供應商開始一個新的軟件項目。當他到達工作崗位時，他會收到一份包含此處所示部分的文檔。這是什麼類型的規劃文件？



一、功能需求

B. 工作分解結構

C. 測試分析報告

D、項目計劃

你回答正確！

工作分解結構 (WBS) 是一種重要的項目管理工具，它將為大型項目完成的工作分成較小的部分。它不是項目計劃，因為它沒有描述時間或資源。在開發工作的後期階段使用測試分析來報告測試結果。功能需求可能包含在工作分解結構中，但它們不是完整的 WBS。

問題 84

tb787631.CISSPPT3E.pt1.019

Kim 是一個遇到安全問題的小型企業網絡的系統管理員。她晚上在辦公室處理這個問題，沒有其他人在那裡。在她注視的過程中，她可以看到辦公室另一側以前運行正常的系統現在一個接一個地出現感染跡象。Kim 可能處理什麼類型的惡意軟件？

A、病毒

B、蠕蟲

C、特洛伊木馬

D、邏輯炸彈

您回答錯誤。

蠕蟲具有不需要用戶交互的內置傳播機制，例如掃描包含已知漏洞的系統，然後利用這些漏洞獲取訪問權限。病毒和特洛伊木馬通常需要用戶交互才能傳播。邏輯炸彈不會從一個系統傳播到另一個系統，而是一直等待，直到滿足特定條件，觸發其有效載荷的交付。

問題 85

tb787631.CISSPPT3E.pt1.023

Jim 正在為其組織實施 IDaaS 解決方案。他採用了什麼類型的技術？

A. 身份即服務

B. 員工 ID 即服務

C. 入侵檢測即服務

D.OAuth

你回答正确！

Identity as a service (IDaaS) provides an identity platform as a third-party service. This can provide benefits, including integration with cloud services and removing overhead for maintenance of traditional on-premises identity systems, but can also create risk due to third-party control of identity services and reliance on an offisite identity infrastructure.

Question 86

tb787631.CISSPPT3E.pt1.030

Bob is configuring egress filtering on his network, examining traffic destined for the internet. His organization uses the public address range 12.8.195.0/24. Packets with which one of the following destination addresses should Bob permit to leave the network?

A. 12.8.195.15
B. 10.8.15.9
C. 192.168.109.55
D. 129.53.44.124

You Answered Correctly!

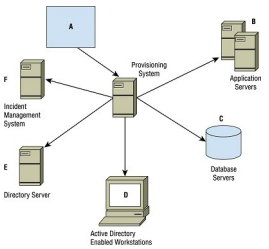
129.53.44.124 是一個有效的公共 IP 地址，也是離開 Bob 網絡的流量的合法目的地。12.8.195.15 是 Bob 網絡上的公共地址，不應是離開網絡的數據包的目標地址。10.8.15.9 和 192.168.109.55 都是私有 IP 地址，不應路由到 Internet。

問題 87

tb787631.CISSPPT3E.pt1.082

請參考以下場景：

- Alex 已經在他工作的大學工作了 10 多年。在那段時間裡，他擔任過系統管理員和數據庫管理員，還曾在大學的服務台工作。他現在是運行大學 Web 應用程序的團隊的經理。使用此處顯示的配置圖，回答以下問題。



當亞歷克斯改變角色時，應該發生什麼？

A. 他應該被取消配置，並且應該創建一個新帳戶。

B. 他應該將他的新權利添加到他現有的帳戶中。

C. 應該只為他提供與其角色相匹配的權利。

D. 他的權利應該與他所取代的人的權利相匹配。

你回答正確！

當用戶的角色發生變化時，應根據他們的角色和其他訪問權限對他們進行配置。取消配置和重新配置非常耗時，並且可能導致更改 ID 和現有憑據的工作方式出現問題。簡單地添加新權限會導致權限蔓延，而匹配另一個用戶的權限可能會由於其他用戶的權限蔓延而導致過多的權限。

問題 88

tb787631.CISSPPT3E.pt1.055

Maria is analyzing a security incident where she believes that an attacker gained access to a fiber-optic cable and installed a tap on that cable. What layer of the OSI model did this attack occur at?

A. Transport
B. Network
C. Data Link
D. Physical

You Answered Correctly!

The Physical layer deals with the electrical impulses or optical pulses that are sent as bits to convey data. This is the layer where cable tapping would occur. Attacks at the Data Link, Network, or Transport layers would involve higher levels of activity in the OSI model, such as compromising a device and using a protocol analyzer to sniff network traffic.

Question 89

tb787631.CISSPPT3E.pt1.104

Alan is installing a fire suppression system that will activate after a fire breaks out and protect the equipment in the data center from extensive damage. What metric is Alan attempting to lower?

A. Likelihood
B. 反收購行動
C、RPO
D. 影響

你回答正確！

滅火系統不會阻止火災發生，但會減少火災造成的損害。這是通過降低事件的影響來降低風險的示例。

問題 90

tb787631.CISSPPT3E.pt1.058

Kailey 正在審查她的組織保存的一組舊記錄，並希望安全地處理它們。她不確定該組織應將記錄保留多長時間，因為它們涉及稅務數據。Kailey 如何確定記錄是否可以處置？

A. 查閱組織的記錄保留政策。

B. 諮詢 IRS 要求。

C. 保留記錄至少七年。

D. 永久保留記錄。

你回答正確！

Kailey 應該查閱她所在組織的記錄保留政策，以確定保存記錄的適當時間長度。組織可能需要遵守這方面的稅務要求，許多會計師建議將記錄保存至少七年，但組織自身的要求可能比這些要求更嚴格。

問題 91

tb787631.CISSPPT3E.pt1.063

Colleen 正在為她的組織進行業務影響評估。什麼指標提供了有關組織在造成無法彌補的損害之前可能沒有服務的時間量的重要信息？

A、MTD

B. 但是

C、RPO

D. 反收購行動

你回答正確！

最大可容忍停機時間 (MTD) 是指在發生無法彌補的損害之前，企業可能沒有服務的時間量。此度量有時也稱為最大可容忍中斷 (MTO) 或最大允許停機時間 (MAD)。

問題 92

tb787631.CISSPPT3E.pt1.112

Ed 正在為其組織的信息安全計劃開發一組關鍵績效和風險指標。以下哪些是常用的指標？（選擇所有符合條件的。）

A. 預定審核次數

B. 解決漏洞的時間

C. 惡意站點訪問嘗試次數

D. 帳戶洩露次數

您回答錯誤。

組織通常使用解決漏洞的時間、帳戶洩露的次數以及用戶嘗試訪問惡意站點的次數作為指標。計劃審計的數量通常不是衡量信息安全團隊績效的指標。這方面更合適的指標是重複審計結果的數量。

問題 93

tb787631.CISSPPT3E.pt1.050

Rob 最近收到供應商的通知，稱其組織中使用的防火牆平台的 EOL 日期臨近。Rob 應該採取什麼行動？

A. 準備盡快停止使用該平台。

B. 立即停止使用該設備。

C. 準備停止使用設備作為組織正常計劃週期的一部分。

D. 無需採取任何行動。

你回答正確！

產品的生命週期結束 (EOL) 日期通常是供應商停止銷售產品的日期。只要支持仍然可用，就可以繼續使用該產品。在宣布終止支持 (EOS) 日期之前，Rob 應該開始製定停止使用該產品的計劃。

問題 94

tb787631.CISSPPT3E.pt1.099

Peter 正在審查他的組織使用的遠程訪問技術，並希望消除對不包括內置加密的任何技術的使用。他應該保留以下哪種方法？（選擇所有符合條件的。）

A. RDP

B、遠程登錄

C、SSH

D、撥號

你回答正確！

遠程桌面協議 (RDP) 和安全外殼 (SSH) 是包含加密功能的現代遠程訪問方法。Telnet 和撥號是過時的方法，不提供加密，不應依賴於安全訪問。

問題 95

tb787631.CISSPPT3E.pt1.071

以下哪些關於 SSAE-18 的陳述是正確的？（選擇所有符合條件的。）

A. 它要求一個特定的控制集。

B. 是認證標準。

C. 用於外部審計。

D. 它使用一個框架，包括 SOC 1、SOC 2 和 SOC 3 報告。

你回答正確！

SSAE-18 不聲明特定控制。相反，它審查了受審計組織中控制的使用和

應用。它是一種證明標準，用於外部審計，並構成 SOC 1、2 和 3 報告

基礎框架的一部分。

問題 96

tb787631.CISSPPT3E.pt1.072

Elliott is using an asymmetric cryptosystem and would like to add a digital signature to a message. What key should he use to encrypt the message digest?

A. Elliott’s private key
B. Elliott’s public key
C. Recipient’s private key
D. Recipient’s public key

You Answered Correctly!

When creating a digital signature, the sender of a message always

encrypts the message digest with their own private key. The recipient (or

any third party) may then verify the digital signature by decrypting it with

the sender’s public key and then comparing that decrypted signature with

a message digest that the recipient computes themselves.

Question 97

tb787631.CISSPPT3E.pt1.028

In the database table shown here, which column would be the best candidate for a primary key?

Company ID	Company Name	Address	City	State	ZIP Code	Telephone	Sales Rep
1	Acme Widgets	234 Main Street	Columbia	MD	21040	(301) 555-1212	14
2	艾布拉姆斯諮詢	樣品街 1024 號	邁阿密	佛羅里達州	33131	(305) 555-1995	14
3	圓頂小部件	索林街 913 號	南本德	在	46556	(574) 555-5863	26

A. 公司編號

B. 公司名稱

C. 郵政編碼

D. 銷售代表

你回答正確！

公司 ID 列對於表中的每一行可能是唯一的，這使其成為主鍵的最佳選擇。

可能有多家公司共享相同的名稱或郵政編碼。同樣，一名銷售代表可能服

務於多家公司，這使得這些字段不適合用作唯一標識符。

問題 98

tb787631.CISSPPT3E.pt1.005

Darren 正在為他的組織使用的 Kerberized 應用程序解決身份驗證問題。他認為問題在於會話密鑰的生成。他應該首先調查什麼 Kerberos 服務？

A、KDC

B、TGT

C.AS

D、TGS

您回答錯誤。

TGS 或票證授予服務（通常與 KDC 在同一台服務器上）從客戶端接收

TGT。它驗證 TGT 和用戶訪問他們請求使用的服務的權利。然後 TGS

向客戶端發出票據和會話密鑰。AS 作為認證服務器，將用戶名轉發給

KDC。值得注意的是，客戶端不直接與 KDC 通信。相反，它將與 TGT

和 AS 通信，這意味著 KDC 在這裡不是一個合適的答案。

問題 99

tb787631.CISSPPT3E.pt1.065

Matt 正在為他的組織設計一組信息處理要求，並希望藉鑑通用的行業慣例。

Matt 應該實施以下哪些實踐？（選擇所有符合條件的。）

A. Labeling both paper and electronic documents with their classification level

B. Automatically granting senior executives full access to all classified information

C. Automatically granting visitors access to information classified at the lowest level of sensitivity

D. Encrypting sensitive information in storage and at rest

You Answered Correctly!

Organizations should always label classified information in whatever form, paper or electronic, that it appears. This allows employees to apply proper handling procedures. It is also a common practice to encrypt sensitive information both at rest and in transit. Organizations should grant access to classified information on a need-to-know basis.

Automatically granting access to information, whether it is to a visitor or a senior executive, should not occur.

Question 100

Perry is establishing information handling requirements for his organization. He discovers that the organization often needs to send sensitive information over the internet to a supplier and is concerned about it being intercepted. What handling requirement would best protect against this risk?

A. Require the use of transport encryption.
B. Require proper classification and labeling.
C. Require the use of data loss prevention technology.
D. Require the use of storage encryption.

You Answered Correctly!

All of these controls are good practices for protecting sensitive information. However, Perry is most concerned about the risk of interception while in transit over the internet. Transport encryption would, therefore, be the most appropriate control, as anyone intercepting the information would be unable to read its contents. Storage encryption would protect against the theft of information at rest, rather than in transit over a network. Classification and labeling would not protect against interception. Data loss prevention technology may block the transfer

entirely and would not meet the business requirement if it blocked the transmission and would not meet the security requirement if it did not detect the data transfer.

Question 101

tb787631.CISSPPT3E.pt1.105

Alan's Wrenches 最近為其產品開發了一種新的製造工藝。他們計劃在內部使用這項技術，不與他人分享。他們希望它能盡可能長時間地受到保護。哪種類型的知識產權保護最適合這種情況？

一、專利

B.版權

C、商標

D、商業秘密

你回答正確！

專利和商業秘密都可以以過程的形式保護知識產權。專利需要公開披露並有有效期，而商業秘密只要保密就一直有效。因此，商業秘密保護最符合公司的目標。

問題 102

tb787631.CISSPPT3E.pt1.111

Gwen 遇到了一個在 Web 服務器上的服務帳戶下運行的應用程序。服務帳戶對服務器具有完全的管理權限。這違反了什麼信息安全原則？

A、需要知道

B. 職責分離

C. 最小特權

D. 工作輪換

你回答正確！

這種情況違反了最小權限原則，因為應用程序永遠不需要完全管理權限才能運行。Gwen 應將服務帳戶更新為僅具有支持該應用程序所需的權限。

問題 103

tb787631.CISSPPT3E.pt1.093

Mandy 是一個由六人組成的項目團隊的組長。她想為這些人提供私下交流的能力，這樣任何一對人都可以交換不受任何其他人（團隊成員或非團隊成員）攔截的通信。她使用的是非對稱加密算法。實現這些要求需要多少個密鑰？

A.6

B.12

C.15

D. 36

你回答正確！

非對稱加密算法要求每個用戶有兩個密鑰，而不管參與者的數量。因此，

這個六人小隊需要十二把鑰匙。如果這個團隊要使用對稱加密，他們將需

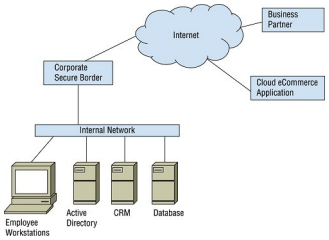
要 (n*(n-1))/2，或 (6*(6-1))/2 = 15 個密鑰。

問題 104

tb787631.CISSPPT3E.pt1.042

請參考以下場景：

- Ben 工作的組織有一個傳統的現場 Active Directory 環境，該環境使用手動配置過程來為其 350 名員工的公司添加每個新成員。隨著公司採用新技術，他們越來越多地使用軟件即服務應用程序來取代他們內部開發的軟件堆棧。
- Ben 的任務是設計一個身份管理實現，使他的公司能夠在支持其現有系統的同時使用雲服務。使用此處顯示的邏輯圖，回答以下有關 Ben 應該提出的身份建議的問題。



如果 Ben 需要與顯示的業務合作夥伴共享身份信息，他應該調查什麼？

A、單點登錄

B. 多因素認證

C.聯合會

D.IDaaS

你回答正確！

聯合會鏈接多個組織之間的身份信息。與業務合作夥伴聯合可以允許在他

們之間進行身份驗證和授權，從而使集成更加容易。單點登錄會減少用戶

必須登錄的次數，但不會促進身份信息的共享。Multifactor 可以幫助保

護身份驗證，但同樣無助於與第三方集成。最後，作為服務提供者的身份

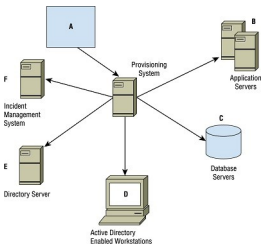
可能提供聯合，但不保證它。

問題 105

tb787631.CISSPPT3E.pt1.081

請參考以下場景：

- Alex 已經在他工作的大學工作了 10 多年。在那段時間裡，他擔任過系統管理員和數據庫管理員，還曾在大學的服務台工作。他現在是運行大學 Web 應用程序的團隊的經理。使用此處顯示的配置圖，回答以下問題。



Alex 可以訪問圖中的 B、C 和 D。他應該向大學的身份管理團隊提出什麼問題？

A. 配置過程沒有給他所需的權利。

B. 他有過多的特權。

C. 可能正在發生特權蔓延。

D. 沒有正確啟用日誌記錄。

您回答錯誤。

由於 Alex 改變了角色，他保留了對他不再管理的系統的訪問權。供應系統已向他管理的工作站和應用程序服務器提供權限，但他不應訪問他不再管理的數據庫。沒有指定權限級別，因此我們無法確定他是否擁有過多的權限。可能會或可能不會啟用日誌記錄，但無法從圖表或問題中分辨出來。

問題 106

tb787631.CISSPPT3E.pt1.116

請參考以下場景：

- 在 Web 應用程序漏洞掃描測試期間，史蒂夫對他認為可能容易受到攻擊的 Web 服務器運行 Nikto。使用此處顯示的 Nikto 輸出，回答以下問題。

Nikto 列出了 OSVDB-877，指出該系統可能容易受到 XST 攻擊。這種類型的攻擊允許攻擊者做什麼？

A. 使用跨站點定位。

B. 竊取用戶的 cookie。

C. 計數器 SQL 跟踪。

D.修改用戶的 TRACE 信息。

您回答錯誤。

跨站點跟踪 (XST) 利用 HTTP TRACE 或 TRACK 方法，可用於通過跨站點腳本 (XSS) 竊取用戶的 cookie。其他選項不是 Web 應用程序或 Web 服務器攻擊或漏洞的行業術語。

問題 107

tb787631.CISSPPT3E.pt1.095

Ursula 正在尋求擴大其組織網站的覆蓋範圍和可擴展性。她想將她在世界各地的數據副本放置在靠近網站訪問者的位置，以減少加載時間和服務器的負擔。哪種類型的雲服務最能滿足她的需求？

A. 基礎設施即服務

B. 容器化

C、CDN

D、軟件即服務

你回答正確！

雖然 Ursula 可能會使用各種不同的選項來滿足她的需求，但最好的方法是使用內容分發網絡 (CDN)。CDN 是專門為這個角色設計的，將內容分發到許多遠程端點，本地用戶可以在這些端點快速加載內容。

問題 108

tb787631.CISSPPT3E.pt1.103

Kathleen 正在為她的組織實施訪問控制系統並構建以下數組：

- 審稿人：更新文件，刪除文件
- 提交者：上傳文件
- 編輯器：上傳文件，更新文件
- 檔案管理員：刪除文件

凱瑟琳實施了哪種類型的訪問控制系統？

A. 基於角色的訪問控制

B. 基於任務的訪問控制

C. 基於規則的訪問控制

D. 自主訪問控制

你回答正確！

Role-based access control gives each user an array of permissions based on their position in the organization, such as the scheme shown here. Task-based access control is not a standard approach. Rule-based access controls use rules that apply to all subjects, which isn’t something we see in the list. Discretionary access control gives object owners rights to choose how the objects they own are accessed, which is not what this list shows.

Question 109

tb787631.CISSPPT3E.pt1.017

During a log review, Danielle discovers a series of logs that show login failures:

```
Jan 31 11:39:12 ip-10-0-0-2 sshd[29092]: Invalid user admin from remotehost passwd=aaaaaaaa
```

```
Jan 31 11:39:20 ip-10-0-0-2 sshd[29098]: Invalid user admin from remotehost passwd=aaaaaaab
```

```
Jan 31 11:39:23 ip-10-0-0-2 sshd[29100]: Invalid user admin from remotehost passwd=aaaaaaac
```

`1 月 31 日 11:39:31 ip-10-0-0-2 sshd [29106]`：來自 `remotehost passwd=aaaaaaad` 的無效用戶管理員

`1 月 31 日 20:40:53 ip-10-0-0-254 sshd [30520]`：遠程主機密碼無效的用戶管理員 `= aaaaaaae`

丹妮爾發現了什麼類型的攻擊？

A. 哈希傳遞攻擊

B. 暴力攻擊

C. 中間人攻擊

D. 字典攻擊

您回答錯誤。

暴力攻擊會嘗試所有可能的密碼。在這次攻擊中，每次嘗試密碼都會改變

一個字母，這表明這是一次暴力攻擊。字典攻擊將使用字典單詞進行攻擊 ，

而中間人攻擊或哈希傳遞攻擊很可能在身份驗證日誌中不可見，除非是成功登錄。

問題 110

tb787631.CISSPPT3E.pt1.121

Alice 希望向 Bob 發送一條消息，並確信 Bob 會知道消息在傳輸過程中沒有被更改。Alice 試圖實現什麼安全目標？

A. 保密
B. 不可否認性
C. 認證
D. 誠信

您回答錯誤。

完整性確保在存儲或傳輸過程中不會對數據進行未經授權的更改。

問題 111

tb787631.CISSPPT3E.pt1.117

誰是組織首席審計執行官 (CAE) 最合適的主管？

A.首席信息官
B.首席信息安全官
C、首席執行官
D、首席財務官

您回答錯誤。

首席審計執行官 (CAE) 應向最高級別的領導匯報，以避免利益衝突。在提供的選擇中，首席執行官（CEO）是最高級別的職位，也是最佳選擇。還可以通過讓 CAE 向董事會報告（作為主要報告線或虛線關係）來提供更高程度的獨立性。

問題 112

tb787631.CISSPPT3E.pt1.001

Lisa 正試圖防止她的網絡成為 IP 欺騙攻擊的目標，並防止她的網絡成為這些攻擊的來源。以下哪些規則是 Lisa 應該在她的網絡邊界配置的最佳實踐？（選擇所有符合條件的。）

A. 阻止具有內部源地址的數據包進入網絡。
B. 阻止具有外部源地址的數據包離開網絡。
C. 阻止具有公共 IP 地址的數據包進入網絡。
D. 阻止具有私有 IP 地址的數據包退出網絡。

您回答錯誤。

具有公共 IP 地址的數據包通常會被允許進入網絡，因此您不應創建規則

來阻止它們，這是正確的答案。具有內部源地址的數據包不應來自網絡外

部，因此應阻止它們進入網絡。具有外部源地址的數據包永遠不會在內部

網絡中被發現，因此應該阻止它們離開網絡。最後，永遠不要在 Internet

上使用私有 IP 地址，因此應阻止包含私有 IP 地址的數據包離開網絡。

問題 113

tb787631.CISSPPT3E.pt1.040

Kevin is operating in a single-level security environment and is seeking to classify information systems according to the type of information that they process. What procedure would be the best way for him to assign asset classifications?

A. Assign systems the classification of information that they most commonly process.

B. Assign systems the classification of the highest level of information that they are expected to process regularly.

C. Assign systems the classification of the highest level of information that they are ever expected to process.

D. Assign all systems the same classification level.

You Answered Incorrectly.

在單級安全環境中，應為系統分配它們預期處理的最高級別信息的級別。

如果不向上重新分類系統，系統可能無法處理高於其分類級別的信息。

問題 114

tb787631.CISSPPT3E.pt1.037

Roger 正在查看其組織中的安全漏洞列表，並根據它們的嚴重程度對其進行評級。以下哪一個模型對他的工作最有用？

A、CVSS

B. 跨步

C.粘貼

D. ATT&CK

您回答錯誤。

Common Vulnerability Scoring System (CVSS) 是一種對漏洞嚴重性進行評級的標準化方法，將是對 Roger 的工作最有幫助的工具。STRIDE 和 ATT&CK 模型用於對威脅的性質而非嚴重性進行分類。PASTA 模型旨在幫助選擇對策。

問題 115

tb787631.CISSPPT3E.pt1.106

Ben 想要使用標準化協議與國家漏洞數據庫進行交互。他應該使用什麼選項來確保他構建的工具與 NVD 中包含的數據一起工作？

A.XACML

B.SCML

C、VSML

D. SCAP

你回答正確！

安全內容自動化協議 (SCAP) 是一套用於處理漏洞和安全配置信息的規範。NIST 提供的國家漏洞數據庫使用 SCAP。XACML 是可擴展訪問控制標記語言，一種用於訪問控制決策的 OASIS 標準，VSML 和 SCML 都不是行業術語。

問題 116

tb787631.CISSPPT3E.pt1.036

William 正在審查存儲在系統中的日誌文件，該系統疑似遭到破壞。他找到了此處顯示的日誌文件。這是什麼類型的日誌文件？

A. 防火牆日誌

B、變更日誌

C. 申請日誌

D、系統日誌

您回答錯誤。

該文件清楚地顯示了 HTTP 請求，正如許多 GET 命令所證明的那樣。

因此，這是來自 HTTP 服務器的應用程序日誌示例。

問題 117

tb787631.CISSPPT3E.pt1.092

以下哪項不是強制訪問控制設計？

A. 等級制

B. 括號內

C. 分區化

D. 混合型

您回答錯誤。

強制訪問控制系統可以是分層的，其中每個域都是有序的，並且與它之上

和之下的其他域相關；分隔的，每個域之間沒有關係；或混合，其中同時

使用層次結構和隔間。強制訪問控制設計中沒有括號的概念。

問題 118

tb787631.CISSPPT3E.pt1.016

Alice 想擁有一個對象的讀取權限，並且知道 Bob 已經擁有這些權限並想將這些權限授予自己。如果 Alice 和 Bob 之間存在關係，那麼 Take-Grant 保護模型中的哪一條規則允許她完成此操作？

A. 採取規則
B. 授予規則
C. 創建規則
D.遠程規則

您回答錯誤。

take 規則允許主體取得屬於另一個客體的權利。如果 Alice 擁有 Bob 的

權限，她可以授予自己 Bob 已經擁有的相同權限。

問題 119

tb787631.CISSPPT3E.pt1.032

使用粉碎可以安全有效地處理以下哪些數據資產？（選擇所有符合條件的。）

A. 紙質記錄

B、信用卡

C. 可移動媒體

D、SSD 硬盤

你回答正確！

傳統的辦公室碎紙機可用於處理紙質記錄，並且根據其等級，還可以切碎

信用卡。工業碎紙機能夠銷毀較大的設備，包括可移動媒體和硬盤驅動器 。

問題 120

tb787631.CISSPPT3E.pt1.068

Owen 最近設計了一種安全訪問控制結構，可以防止單個用戶同時擁有創建新供應商所需的角色和簽發支票所需的角色。歐文執行什麼原則？

A.兩人控制

B. 最小權限

C. 職責分離

D. 工作輪換

你回答正確！

這個場景描述了職責分離——不允許同一個人擔任兩個角色，這兩個角色

在組合時是敏感的。雖然雙人控制是一個類似的概念，但它不適用於這種

情況，因為該場景並未說明任何一個操作都需要兩個用戶的同意。最小特

權表示個人應具有執行其工作所需的最低權限集。工作輪換使人們定期輪

換工作以防止欺詐。

問題 121

tb787631.CISSPPT3E.pt1.051

什麼原則規定個人應盡一切努力準確及時地完成其職責？

A. 最小權限

B. 職責分離

C. 應有的注意

D、盡職調查

你回答正確！

應有的注意原則規定，個人應對情況做出反應時應使用與任何合理的人所

期望的相同程度的注意。這是一個非常廣泛的標準。盡職調查原則是應有

註意的一個更具體的組成部分，它規定被分配責任的個人應該盡到應有的

注意，準確及時地完成它。最小特權表示個人應具有執行其工作所需的最

低權限集。職責分離說，任何一個人都不應該有權執行兩項不同的任務，

當這兩項任務結合在一起時，就構成了高度特權的行為。

問題 122

tb787631.CISSPPT3E.pt1.061

以下哪一項不是敏捷軟件開發方法的原則？

A. 最好的架構、需求和設計來自自組織團隊。

B. 不經常交付工作軟件，重點是在更長的時間內創建準確的代碼。

C. 歡迎不斷變化的需求，即使是在開發過程的後期。

D. 簡單是必不可少的。

你回答正確！

軟件開發的敏捷方法包含敏捷宣言中的 12 條核心原則。這些原則之一是

最好的架構、需求和設計來自自組織團隊。另一個是團隊應該歡迎在過程

中的任何步驟更改需求。第三，簡單是必不可少的。敏捷方法強調頻繁而

不是不頻繁地交付軟件。

問題 123

tb787631.CISSPPT3E.pt1.076

Chris 工作的公司在每個門上都張貼了通知，提醒員工在有人進入時要小心，不要讓他們進入。這是哪種類型的控件？

A.偵探

B. 物理的

C. 預防

D. 指令

你回答正確！

通知和程序（例如 Chris 工作的公司張貼的標誌）是指令訪問控制的示

例。偵探控制旨在事後操作。門和門上的鎖是物理控制的例子。預防性控

制旨在阻止事件發生，還可能包括門上的鎖。