## D5-002 結果 12/8/2022

### 問題一

tb787631.CISSPPT3E.c05.036

當一個主體聲稱身份時，發生了什麼過程？

一、登錄

B. 身份證明

C、授權

D. 代幣展示

你回答正確！

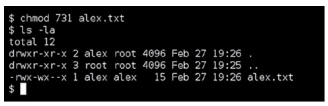
主體聲稱或表明身份的過程稱為身份識別。授權通過檢查密碼等因素來驗

證主體的身份。登錄通常包括身份驗證和授權，令牌表示是一種身份驗證 。

### 問題 2

tb787631.CISSPPT3E.c05.090

當亞歷克斯作為 Linux 服務器上的眾多用戶之一設置下圖中顯示的權限時，他利用的是哪種類型的訪問控制模型？




A. 基於角色的訪問控制

B. 基於規則的訪問控制

C.強制訪問控制（MAC）

D. 自主訪問控制 (DAC)

您回答錯誤。

Linux 文件系統允許對象的所有者決定主體對它們的訪問權限。這意味著

它是一種自主訪問控制。如果系統強制執行基於角色的訪問控制，亞歷克

斯就不會設置控制；它們將根據分配給每個主題的角色來設置。基於規則

的訪問控制系統將在整個系統中應用規則，而強制訪問控制系統使用分類

標籤。

## 問題三

tb787631.CISSPPT3E.c05.058

銀行的一位新客戶使用指紋掃描儀對其用戶進行身份驗證，當他掃描指紋並登錄到另一位客戶的帳戶時，他感到很驚訝。發生了什麼類型的生物識別因素錯誤？

A.註冊錯誤

B. 第一類錯誤

C. 類型 2 錯誤

D.使用時間、使用方法錯誤

您回答錯誤。

當無效主體被錯誤地認證為有效用戶時，生物識別系統中會發生類型 2

錯誤。在這種情況下，在掃描指紋時，除了實際客戶之外，沒有人應該被

驗證。類型 1 錯誤發生在有效主體未通過身份驗證時；如果現有客戶被

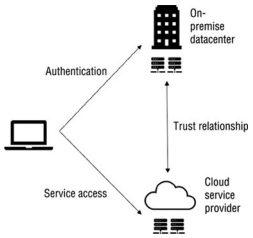
拒絕，則屬於 1 類錯誤。註冊是添加用戶的過程，但註冊錯誤和使用時

間、使用方法錯誤不是特定的生物認證術語。

## 問題四

tb787631.CISSPPT3E.c05.074

下圖顯示了哪種類型的身份驗證場景？




A. 混合聯邦

B. 內部聯合

C.雲聯邦

D. Kerberos 聯盟

你回答正確！

此圖顯示了混合聯合的示例，其中身份驗證在本地進行，服務通過雲中的

聯合身份服務提供。

## 問題 5

tb787631.CISSPPT3E.c05.086

Isabelle 想要防止通過其組織的服務帳戶進行的特權升級攻擊。以下哪項安全實踐最適合於此？

A. 刪除不必要的權限。

B. 禁用服務帳戶的交互式登錄。

C.限制賬號何時可以登錄。

D. 為服務帳戶使用無意義的或隨機的名稱。

你回答正確！

確保服務帳戶安全的最重要步驟是確保它們僅具有完成其設計任務所絕對

需要的權限。禁用交互式登錄也很重要，這將是下一個最佳答案。限制帳

戶可以登錄的時間以及使用隨機或無意義的帳戶名在某些情況下都可能有

所幫助，但遠沒有那麼重要。

## 問題 6

tb787631.CISSPPT3E.c05.059

防火牆通常使用什麼類型的訪問控制？

A. 自主訪問控制

B. 基於規則的訪問控制

C. 基於任務的訪問控制

D. 強制訪問控制

你回答正確！

防火牆在其訪問控制列表中使用基於規則的訪問控製或 Rule-BAC，並將管理員創建的規則應用於通過它們的所有流量。DAC，即自主訪問控制，允許所有者決定誰可以訪問他們控制的對象，而基於任務的訪問控制則為用戶列出任務。MAC 或強制訪問控制使用分類來確定訪問。

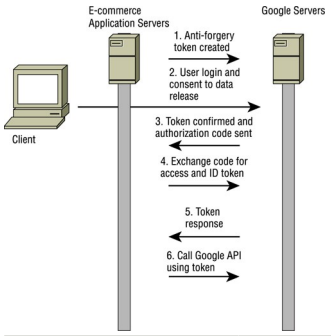
**問題 7**

tb787631.CISSPPT3E.c05.066

請參考以下場景和圖表：

- Chris 是一家不斷發展的電子商務網站的身份架構師，該網站希望利用社交身份。為此，他和他的團隊打算允許用戶在使用電子商務網站時使用他們現有的谷歌賬戶作為他們的主要賬戶。這意味著，當新用戶最初連接到電子商務平台時，他們可以選

擇是使用 OAuth 2.0 使用他們的 Google 帳戶，還是使用他們自己的電子郵件地址和他們選擇的密碼在平台上創建一個新帳戶。




以下哪項負責 Google 用戶的用戶身份驗證？

A.電子商務應用。

B. 電子商務應用程序和谷歌服務器。

C. 谷歌服務器。

D. 該圖沒有提供足夠的信息來確定這一點。

您回答錯誤。

當第三方站點通過 OAuth 2.0 集成時，身份驗證由服務提供商的服務器處理。在這種情況下，谷歌充當用戶身份驗證的服務提供商。創建自己帳戶的本地用戶的身份驗證將在電子商務應用程序（或相關服務器）中進行，但這不是這裡要問的問題。

**問題 8**

tb787631.CISSPPT3E.c05.068

諸如“你的寵物叫什麼名字？”之類的問題。什麼類型的身份證明的例子？

A. 基於知識的認證

B. 基於動態知識的認證

C. 帶外身份證明

D. 類型 3 認證因素

你回答正確！

基於知識的身份驗證依賴於預設問題，例如“您的寵物叫什麼名字？” 和

答案。由於社交媒體或其他網站上的答案的可用性，它可能容易受到攻擊 。

基於知識的動態身份驗證依賴於用戶已經知道的事實或數據，這些事實或

數據可用於創建他們可以根據需要回答的問題（例如，以前的地址或他們

就讀的學校）。帶外身份證明依賴於備用渠道，如電話或短信。最後，類

型 3 身份驗證因素是生物識別的，或者“你是什麼”，而不是基於知識的 。

**問題 9**

tb787631.CISSPPT3E.c05.087

允許 OpenID 依賴方控制與 OpenID 提供商的連接會產生什麼危險？

A. 這可能會導致錯誤選擇正確的 OpenID 提供商。

B. 它通過將數據發送到偽造的 OpenID 提供者來創建網絡釣魚攻擊的可能性。

C. 依賴方可能竊取客戶的用戶名和密碼。

D. 依賴方可能不會發送已簽名的斷言。

你回答正確！

允許依賴方提供到 OpenID 提供商的重定向可能會通過將客戶端定向到

可以捕獲有效憑據的虛假 OpenID 提供商來允許網絡釣魚攻擊。由於

OpenID 提供者 URL 由客戶端提供，因此依賴方無法選擇錯誤的提供者 。

依賴方永遠不會收到用戶的密碼，這意味著他們無法竊取密碼。最後，依

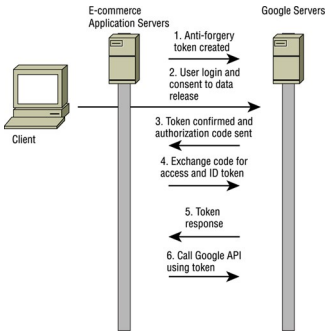
賴方收到簽名的斷言但不發送。

**問題 10**

tb787631.CISSPPT3E.c05.065

請參考以下場景和圖表：

- Chris 是一家不斷發展的電子商務網站的身份架構師，該網站希望利用社交身份。為此，他和他的團隊打算允許用戶在使用電子商務網站時使用他們現有的谷歌賬戶作為他們的主要賬戶。這意味著，當新用戶最初連接到電子商務平台時，他們可以選擇是使用 OAuth 2.0 使用他們的 Google 帳戶，還是使用他們自己的電子郵件地址和他們選擇的密碼在平台上創建一個新帳戶。




當電子商務應用程序為 Google 用戶創建帳戶時，該用戶的密碼應該存儲在哪裡？

A. 密碼存儲在電子商務應用程序的數據庫中。

B. 密碼存儲在電子商務應用服務器的內存中。

C. 密碼保存在谷歌的賬戶管理系統中。

D. 密碼永不存儲；相反，加鹽哈希存儲在谷歌的賬戶管理系統中。

您回答錯誤。

在設計良好的環境中，永遠不會為 Web 應用程序存儲密碼。取而代之的是，在對密碼進行加鹽和散列處理後，會存儲加鹽哈希值並將其與密碼進行比較。如果哈希匹配，則用戶通過身份驗證。

## 問題 11

tb787631.CISSPPT3E.c05.053

Selah 希望對通過其組織的主要業務線應用程序執行的操作負責。在這種情況下，最常使用哪些控制措施來提供問責制？（選擇所有符合條件的。）

A. 啟用審計日誌。

B. 為每個員工提供一個唯一的帳戶並啟用多因素身份驗證。

C. 啟用基於時間和位置的登錄要求。

D. 為每一位員工提供一個唯一的賬戶，並要求一個自選的密碼。

您回答錯誤。

由於使用多因素身份驗證，審計日誌與用戶帳戶結合使用時可以可靠地預

期只能由特定用戶訪問，這經常用於為通過系統和應用程序採取的操作提

供強有力的責任。密碼可以共享，從而降低其可靠性，時間和地點要求是

有用的安全控制措施，但不會影響問責制。

## 問題 12

tb787631.CISSPPT3E.c05.012

以下哪種 AAA 協議最常用？

A. TACACS

B. TACACS+

C.XTACACS

D. 超級 TACACS

你回答正確！

TACACS+ 是列表中唯一的現代協議。它提供了 TACACS 和 XTACACS 的優點以及一些優於 RADIUS 的優點，包括所有身份驗證信息的加密。

Super TACACS 並不是一個實際的協議。

**問題 13**

tb787631.CISSPPT3E.c05.078

Jim 想要實施一種訪問控制方案，以確保用戶不能委託訪問。他還想在操作系統級別實施訪問控制。什麼訪問控制機制最適合這些要求？

A. 基於角色的訪問控制
B. 自主訪問控制
C. 強制訪問控制
D. 基於屬性的訪問控制

你回答正確！

在強制訪問控制系統中，操作系統強制執行訪問控制，用戶不能委託權限。

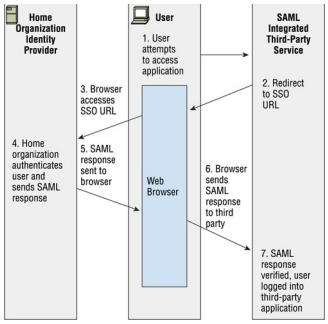
自主訪問控制允許用戶委託權限，而基於屬性和角色的訪問控制都不能滿足這些要求。

**問題 14**

tb787631.CISSPPT3E.c05.045

請利用您對 SAML 集成和安全架構設計的了解，並參考以下場景和圖表：

- Alex 負責 SAML 與主要第三方合作夥伴的集成，該合作夥伴為其組織提供各種業務生產力服務。




如圖中的步驟 2 所示，哪種解決方案最能幫助解決對控制 SSO 重定向的第三方的擔憂？

A. 關於可信第三方的宣傳活動

B、TLS

C. 在本地站點處理重定向

D. 實施 IPS 以捕獲 SSO 重定向攻擊

你回答正確！

雖然許多解決方案都是技術性的，但如果受信任的第三方重定向到意外的

身份驗證站點，意識通常是最好的防禦措施。使用 TLS 將使交易保密，

但不會阻止重定向。在本地處理重定向僅適用於本地託管站點，使用第三

方服務需要站外重定向。IPS 可能會檢測到攻擊者的重定向，但跟踪大

多數大型提供商使用的大量負載平衡服務器即使不是不可能，也是具有挑

戰性的。此外，IPS 依賴於對流量的可見性，SAML 集成應該加密以確

保安全，這需要配置中間人類型的 IPS。

**問題 15**

tb787631.CISSPPT3E.c05.004

語音模式識別是什麼類型的認證因素？

A. 你知道的事

B. 你有的東西

C. 你是什麼

D. 你所在的地方

您回答錯誤。

語音模式識別是“你是什麼”，一種生物特徵認證因素，因為它測量個人認

證的物理特徵。

**問題 16**

tb787631.CISSPPT3E.c05.094

Brian 想要向其組織的領導層解釋內部部署聯合身份驗證方法的好處。以下哪項不是聯合身份系統的共同優勢？

A. 易於賬戶管理

B、單點登錄

C. 防止暴力攻擊

D. 提高生產力

你回答正確！

單點登錄 (SSO) 是身份聯合的一部分。這也意味著帳戶管理更簡單，因為不必為需要跨聯合訪問系統和資源的用戶維護多個帳戶。工作效率可以提高，因為員工不必記住多次登錄並且可以使用 SSO 登錄一次而不是多次。然而，它並沒有採取任何措施來防止暴力攻擊，事實上，具有廣泛訪問權限的單個帳戶可以使攻擊者更容易獲得更廣泛的訪問權限，除非採用多因素身份驗證等解決方案。

**問題 17**

tb787631.CISSPPT3E.c05.046

蘇珊被要求推薦她的組織應該使用 MAC 方案還是 DAC 方案。如果靈活性和可擴展性是實施訪問控制的重要要求，她應該推薦哪種方案，為什麼？

A. MAC，因為它提供了更大的可擴展性和靈活性，因為您可以根據需要簡單地添加更多標籤

B. DAC，因為允許單個管理員選擇他們控制的對象提供了可擴展性和靈活性

C. MAC，因為劃分非常適合靈活性，並且添加隔間將使其能夠很好地擴展

D. DAC，因為中央決策過程允許快速響應，並將通過減少所需決策的數量來提供可擴展性，並通過將這些決策移交給中央機構來提供靈活性

你回答正確！

自主訪問控制 (DAC) 可以通過利用許多管理員來提供更大的可擴展性，

並且這些管理員可以通過決定訪問他們的對象來增加靈活性，而無需適應

不靈活的強制訪問控制系統 (MAC)。MAC 由於提供了一組強大的控件而

更加安全，但它的擴展性不如 DAC，相比之下也相對不靈活。

## 問題 18

tb787631.CISSPPT3E.c05.092

下圖顯示了哪種類型的授權機制？

| 團體 | 特權 |
| --- | --- |
| 系統管理員 | 桌面上的超級用戶，域管理員 |
| 應用管理員 | 應用程序服務器上的 Sudo 權限 |
| 數據庫管理員 | 數據庫服務器上的 Sudo 權限 |
| 用戶 | 桌面工作站的用戶權限 |

A、RBAC

B、ABAC

C.MAC

D、解碼器

你回答正確！

這是一個基於角色的訪問控制 (RBAC) 圖表，指出每個組都有特定的角色權限。基於屬性的訪問控制 (ABAC) 將使用其他屬性，包括位置、強制訪問控制 (MAC) 將由操作系統強制執行，而自主訪問控制 (DAC) 允許用戶等主體在他們控制的對像上設置權限。

**問題 19**

tb787631.CISSPPT3E.c05.010

回撥固定電話號碼是哪種因素的一個例子？

A. 你知道的事
B. 你所在的地方
C. 你有的東西
D. 你是什麼

您回答錯誤。

由於有線電話的固定物理位置，回撥固定電話號碼是“您所在的地方”因素的一個示例。回撥手機將是一個“你擁有的東西”因素。

## 問題 20

tb787631.CISSPPT3E.c05.088

Jim 正在為其組織實施雲身份解決方案。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. 基於雲的 RADIUS

D.OAuth

您回答錯誤。

IDaaS，即身份即服務，提供身份平台作為第三方服務。這可以帶來好

處，包括與雲服務的集成和消除傳統本地身份系統維護的開銷，但它也可

能由於身份服務的第三方控制和對異地身份基礎設施的依賴而產生風險。

## 問題 21

tb787631.CISSPPT3E.c05.033

Jim 的 Microsoft Exchange 環境包括位於全球多個業務辦公室的本地數據中心的服務器，以及為不在這些辦公室之一的員工部署的 Office 365。身份在兩種環境中創建和使用，並將在兩種環境中工作。Jim 正在運行什麼類型的聯合系統？

A. 一個主雲系統

B. 一個主要的本地系統

C. 混合系統

D. 多租戶系統

你回答正確！

混合系統同時使用本地和雲身份和服務在兩種環境中提供資源和工具。雖

然它們可能很複雜，但混合系統還提供了遷移到完全雲部署或容錯設計的

路徑，該設計可以在保持功能的同時處理本地或云中斷。

## 問題 22

tb787631.CISSPPT3E.c05.093

Susan 正在對 Kerberos 身份驗證問題進行故障排除，其症狀包括 TGT 不被接受為有效以及無法接收新票證。如果她正在排除故障的系統正確配置了 Kerberos 身份驗證，她的用戶名和密碼正確，並且她的網絡連接正常，那麼最有可能的問題是什麼？

A. Kerberos 服務器離線。

B. 協議不匹配。

C. 客戶的 TGT 已被標記為受損和取消授權。

D. Kerberos 服務器和本地客戶端的時鐘不同步。

你回答正確！

Kerberos 依賴於連接兩端正確同步的時間才能正常工作。如果本地系統

時間不同步超過五分鐘，有效的 TGT 將失效，系統將不會收到任何新工

單。

**問題 23**

tb787631.CISSPPT3E.c05.083

梅根的公司希望使用 Google 帳戶讓用戶快速採用他們的 Web 應用程序。Megan 需要實施哪些常見的雲聯合技術？（選擇所有符合條件的。）

A. Kerberos

B、OpenID

C、OAuth

D. 半徑

您回答錯誤。

與許多雲身份提供商一樣，Google 帳戶也依賴 OpenID 和

OAuth。Kerberos 用於本地環境，RADIUS 經常用於網絡設備和服務

（如 VPN）的身份驗證和授權。

**問題 24**

tb787631.CISSPPT3E.c05.081

防火牆是哪種訪問控制機制的示例？

A. 強制訪問控制
B. 基於屬性的訪問控制
C. 自主訪問控制
D. 基於規則的訪問控制

你回答正確！

防火牆基於規則集運行，是基於規則的訪問控制方案的一個示例。

## 問題 25

tb787631.CISSPPT3E.c05.051

Amanda 開始了她的新工作，發現她可以訪問各種她不需要完成工作的系統。她遇到了什麼問題？

A. 特權蔓延
B. 權利衝突
C. 最小特權
D. 過度特權

您回答錯誤。

當用戶擁有的權利多於他們完成工作所需的權利時，他們就擁有過多的特權。這違反了最小特權的概念。與爬行權限不同，這是一個配置或權限管

理問題，而不是保留用戶需要但不再需要的權限的問題。權利衝突是一個

虛構的術語，因此在這裡不是問題。

## 問題 26

tb787631.CISSPPT3E.c05.079

Susan 所在公司的安全管理員已將她使用的工作站配置為僅允許她在工作時間登錄。什麼類型的訪問控制最能描述這種限制？

A. 約束接口
B. 上下文相關的控制
C. 內容相關控制
D. 最小特權

您回答錯誤。

基於時間的控件是上下文相關控件的一個示例。受約束的界面會限制

Susan 在應用程序或系統界面中能夠執行的操作，而內容相關的控制會

根據她的角色或權限限制她對內容的訪問。最小特權用於確保主體僅獲得

執行其角色所需的權限。

## 問題 27

tb787631.CISSPPT3E.c05.048

Jessica 需要將有關她正在供應的服務的信息發送給第三方組織。她應該選擇哪種基於標準的標記語言來構建界面？

A.SAML

B、香皂

C、SPML

D.XACML

您回答錯誤。

服務供應標記語言或 SPML 是一種基於 XML 的語言，旨在允許平台生成和響應供應請求。SAML 用於製作授權和認證數據，而 XACML 用於描述訪問控制。SOAP 或簡單對象訪問協議是一種消息傳遞協議，可用於任何 XML 消息傳遞，但它本身不是標記語言。

**問題 28**

tb787631.CISSPPT3E.c05.089

Kristen 希望根據工作人員的職位、每組職位對應用程序所需的權限以及一天中的時間和位置的組合來控制對其組織中應用程序的訪問。她應該選擇什麼類型的控制方案？

A.ABAC

B、解碼器

C.MAC

D. 角色 BAC

你回答正確！

用於 ABAC 的屬性通常屬於以下四類之一：主題屬性，如部門或職位；

操作屬性，例如查看、編輯或刪除的能力；描述可能受到影響的對象的對

象屬性；和上下文屬性，如位置、時間或元素。自主訪問控制會將這些決

定交到受信任的主體手中，MAC 將在操作系統級別強制執行，角色

BAC 將僅使用角色而不是 Kristen 想要應用的全套標準。

**問題 29**

tb787631.CISSPPT3E.c05.050

Google 與跨域的各種組織和應用程序的身份集成是以下哪項的示例？

A.公鑰基礎設施

B. 聯邦

C、單點登錄

D.供應

你回答正確！

Google 與其他應用程序和組織的聯合允許單點登錄以及管理其電子身份

及其相關屬性。雖然這是 SSO 的示例，但它不僅僅是簡單的單點登錄 。

Provisioning 提供帳戶和權限，公鑰基礎設施用於證書管理。

**問題 30**

tb787631.CISSPPT3E.c05.025

Biba 是什麼類型的訪問控制模型？

A.MAC

B、解碼器

C. 角色 BAC

D、ABAC

你回答正確！

Biba 使用網格來控制訪問，是強制訪問控制 (MAC) 模型的一種形式。

它不使用規則、角色或屬性，也不允許用戶自行決定。用戶可以在他們的

級別或更低級別創建內容，但不能決定誰獲得訪問權限，級別不是角色，

並且屬性不用於決定訪問控制。

## 問題 31

tb787631.CISSPPT3E.c05.076

像 Yubikey 或 Titan Security Key 這樣的設備是什麼類型的 Type 2 身份驗證因素？

A、令牌

B. 生物特徵標識符

C、智能卡

D、PIV

你回答正確！

Yubikeys、Titan 安全密鑰和類似設備都是令牌的示例。PIV 代表個人身份驗證，是一個完整的多因素身份驗證解決方案，而不是一個設備。生物識別符是你的身份，智能卡是帶有嵌入式芯片的卡。

## 第 32 題

tb787631.CISSPPT3E.c05.009

分散的訪問控制通常會導致什麼主要問題？

A. 可能會發生訪問中斷。

B. 控制不一致。

C. 控製過於細化。

D、培訓成本高。

你回答正確！

分散的訪問控制可能會導致一致性降低，因為負責控制的個人可能會以不

同的方式解釋策略和要求，並可能以不同的方式履行其職責。訪問中斷、

過於細化的控制和培訓成本可能會發生，具體取決於具體的實施，但它們

通常不是分散式訪問控制的問題。

## 問題 33

tb787631.CISSPPT3E.c05.001

以下哪項最適合描述為關注主體並標識每個主體可以訪問的對象的訪問控制模型？

A. 訪問控制列表
B. 隱含的拒絕名單
C. 能力表
D. 權限管理矩陣

你回答正確！

能力表列出了分配給主體的權限，並標識了主體可以訪問的對象。訪問控

制列表以對象為中心，而不是以主題為中心。隱式拒絕是一種原則，它聲

明任何未明確允許的內容都會被拒絕，並且權限管理矩陣不是訪問控制模

型。

## 第 34 題

tb787631.CISSPPT3E.c05.032

Geoff 希望在他的組織中防止特權升級攻擊。以下哪種做法最有可能防止橫向特權升級？

A. 多因素認證
B. 限制組和帳戶的權限
C. 禁用未使用的端口和服務
D. 淨化用戶對應用程序的輸入

你回答正確！

Multifactor authentication is most likely to limit horizontal privilege

escalation by making it difficult to access user accounts and to

authenticate to a compromised account. Limiting permissions for groups

and accounts can also help, but disabling unused ports and services and

sanitizing user inputs both address threats that are most frequently

associated with vertical privilege escalation attacks.

## Question 35

tb787631.CISSPPT3E.c05.026

Which of the following is a client/server protocol designed to allow network access servers to authenticate remote users by sending access request messages to a central server?

A. Kerberos
B. EAP
C. RADIUS
D. OAuth

You Answered Correctly!

RADIUS 是一種 AAA 協議，用於提供身份驗證和授權；它通常用於調製

解調器、無線網絡和網絡設備。它使用網絡訪問服務器向中央 RADIUS

服務器發送訪問請求。Kerberos 是一種基於票據的身份驗證協議；

OAuth 是一種開放的身份驗證標準，允許在第三方站點上使用來自一個

站點的憑據；EAP 是 Extensible Authentication Protocol，一種常用於無線網絡的認證框架。

## 問題 36

tb787631.CISSPPT3E.c05.015

什麼類型的訪問控制允許文件的所有者使用訪問控制列表授予其他用戶訪問權限？

A. 基於角色
B. 非自由裁量權
C. 基於規則
D. 酌情決定

你回答正確！

當文件的所有者決定誰擁有文件的權限或訪問權限時，他們使用的是自主訪問控制。基於角色的訪問控制將根據主體的角色授予訪問權限，而基於規則的控制將根據一組規則或要求做出決定。非隨意訪問控制將一組固定的規則應用於環境以管理訪問。非自主訪問控制包括基於規則、角色和格的訪問控制。

## 問題 37

tb787631.CISSPPT3E.c05.062

Theresa 希望她的員工能夠安全地存儲和管理系統密碼，包括服務帳戶和其他很少使用的管理憑據。她應該實施什麼類型的工具來實現這一點？

A、單點登錄

B. 聯合身份系統

C. 密碼管理器

D. 多因素認證系統

你回答正確！

企業密碼管理工具允許安全地生成、存儲和管理密碼。他們可以提供有關

誰使用密碼、何時更新密碼以及密碼是否滿足複雜性和其他要求的日誌。

當然，這意味著您環境的密鑰都在一個地方，因此保護和管理企業密碼管

理器非常重要！

## 問題 38

tb787631.CISSPPT3E.c05.096

Windows 默認為 Active Directory 系統使用什麼身份驗證協議？

A. 半徑

B. Kerberos

C、OAuth

D.戰術戰術攻擊+

你回答正確！

Windows 使用 Kerberos 進行身份驗證。RADIUS 通常用於無線網絡、

調製解調器和網絡設備，而 OAuth 主要用於 Web 應用程序。TACACS+

用於網絡設備。

## 第 39 題

tb787631.CISSPPT3E.c05.035

米歇爾的公司正在創建一個新部門，將營銷和傳播部門分成兩個獨立的組。她想創建角色來提供對每個組使用的資源的訪問權。她應該怎麼做才能為每個群體維護適當的安全和權利？

A. 將營銷和傳播團隊都放入現有組中，因為他們會有類似的訪問要求。

B. 將營銷團隊保留在現有組中，並根據他們的特定需求創建一個新的通信組。

C. 將傳播團隊保留在現有組中，並根據他們的特定需求創建新的營銷組。

D. 創建兩個新組，評估他們需要哪些權限來執行其角色，然後在需要時添加其他權限。

你回答正確！

將現有權利複製給具有不同需求的新群體通常會導致特權過於寬泛。

Michelle 應該創建新組，將所有員工移動到適當的組中，然後確保他們擁有所需的訪問權限。

**問題 40**

tb787631.CISSPPT3E.c05.024

過去幾年，Jim 在他的公司從事人事關係、薪資和客戶服務等工作。他的公司應該執行什麼類型的流程來確保他擁有適當的權利？

A. 重新配置
B. 賬戶審核
C. 特權蔓延
D. 賬戶撤銷

您回答錯誤。

隨著員工角色的變化，他們經常會經歷特權蔓延，這是舊權利和角色的積累。帳戶審查是審查帳戶並確保其權利與其所有者的角色和工作要求相匹配的過程。帳戶撤銷會刪除帳戶，而如果員工被解僱並返回或請假並返回，則可能會發生重新配置。

## 問題 41

tb787631.CISSPPT3E.c05.056

Elle 負責建立一個銀行網站。她需要網站註冊用戶的身份證明。她應該如何驗證用戶身份？

A. 要求用戶創建只有他們自己知道的獨特問題。

B. 要求新用戶本人攜帶駕照或護照到銀行辦理。

C. 使用銀行和用戶都有的信息，例如從他們的信用報告中提取的問題。

D. 撥打用戶註冊的電話號碼以驗證他們是否是他們聲稱的人。

你回答正確！

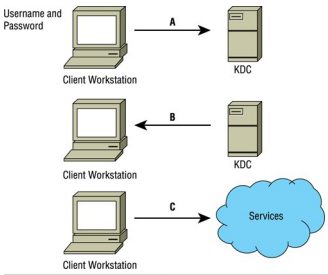
可以通過比較組織已有的用戶信息（如帳號或個人信息）來進行身份證明。

要求用戶創建獨特的問題可以為他們提供一種重置密碼的方法，從而有助於未來的支持。使用電話只能驗證創建該帳戶的個人是否擁有他們註冊的電話，而不會證明他們的身份。面對面驗證不適合大多數網站的業務需求。

## 問題 42

tb787631.CISSPPT3E.c05.018

請利用您對 Kerberos 登錄過程的了解並參考下圖：




在圖中的 B 點，KDC 在驗證用戶名有效後向客戶端發送哪兩個重要元素？

A. 加密的 TGT 和公鑰

B. 訪問票和公鑰

C. 一個加密的、帶時間戳的 TGT 和一個用用戶密碼的散列加密的對稱密鑰

D. 加密的、帶時間戳的 TGT 和訪問令牌

您回答錯誤。

KDC 使用用戶的密碼生成散列，然後使用該散列來加密對稱密鑰。它向客戶端傳輸加密的對稱密鑰和加密的時間戳 TGT。

## 問題 43

tb787631.CISSPPT3E.c05.047

以下哪個工具通常不用於驗證是否以確保遵循組織的安全策略的方式遵循供應過程？

A. 日誌審查

B. 人工審核權限

C. 基於簽名的檢測

D. 審查審計線索

你回答正確！

雖然基於簽名的檢測用於檢測攻擊，但供應過程的審查通常涉及檢查日誌 、

審查審計跟踪或對供應過程中授予的權限執行手動審查。

**問題 44**

tb787631.CISSPPT3E.c05.080

Ben 使用基於軟件的令牌，每分鐘都會更改其代碼。他使用什麼類型的令牌？

A、異步

B、智能卡

C、同步

D、靜態

你回答正確！

同步軟令牌，例如 Google Authenticator，使用基於時間的算法生成一系

列不斷變化的代碼。異步令牌通常需要在令牌上輸入質詢以允許它計算響

應，服務器將響應與它期望的響應進行比較。智能卡通常提供證書，但可

能具有其他內置令牌功能。靜態令牌是可以包含憑據並包括智能卡和存儲

卡的物理設備。

## 問題 45

tb787631.CISSPPT3E.c05.064

哪些客體和主體在 MAC 模型中有標籤？

A. 分類為機密、機密或最高機密的對象和主題都有標籤。

B. 所有的對像都有一個標籤，所有的主題都有一個隔間。

C. 所有的客體和主體都有一個標籤。

D. 所有主題都有一個標籤，所有對像都有一個隔間。

你回答正確！

在強制訪問控制系統中，所有主體和客體都有一個標籤。可以使用也可以

不使用隔間，但是對於要分隔的主題或對像沒有特定要求 。

Confidential、Secret 和 Top Secret 的特定標籤不是 MAC 所要求的。

## 問題 46

tb787631.CISSPPT3E.c05.061

Kathleen 在數據中心託管設施工作，該設施為個人和組織提供物理數據中心空間。直到最近，每個客戶都獲得了一張基於磁條的鑰匙卡，用於訪問他們服務器所在的設施部分，他們還獲得了一把鑰匙，可以進入他們服務器所在的籠子或機架。在過去的一個月裡，許多服務器被盜，但密碼卡片的日誌只顯示有效的 ID。凱瑟琳要確保密碼卡片的用戶是他們應該成為的人，最好的選擇是什麼？

A. 為密碼卡用戶添加需要 PIN 的讀卡器。

B. 在設施中添加攝像頭系統以觀察誰在訪問服務器。

C. 添加生物識別因素。

D. 用智能卡替換磁條鑰匙卡。

你回答正確！

凱瑟琳應該實施生物識別因素。卡片和鑰匙是類型 2 因素或“您擁有的東西”的示例。使用智能卡可以用另一個類型 2 因素代替它，但這些卡仍然可以被借出或被盜。添加 PIN 會遇到同樣的問題：PIN 可能會被盜。添加攝像頭不會阻止對設施的訪問，因此不會解決眼前的問題（但這是個好主意！）。

**問題 47**

tb787631.CISSPPT3E.c05.070

在審查支持票時，Ben 的組織發現密碼更改佔其服務台案例的四分之一以上。以下哪個選項最有可能顯著減少該數字？

A.雙因素認證

B. 生物認證

C.自助密碼重置

D. 密碼

你回答正確！

自助式密碼重置工具通常會對幫助台擁有的密碼重置聯繫人數量產生重大影響。雙因素和生物識別身份驗證都增加了複雜性，實際上可能會增加聯繫人的數量。密碼短語比傳統的複雜密碼更容易記住，並且可能會減少呼叫，但它們的影響不如自助服務系統。

**問題 48**

tb787631.CISSPPT3E.c05.073

Ben 的組織遇到了一個問題，即在員工不在辦公桌前的午餐時間未經授權訪問應用程序和工作站。Ben 推薦哪些最好的會話管理解決方案來幫助防止此類訪問？

A. 使用會話 ID 進行所有訪問並驗證所有工作站的系統 IP 地址。

B. 為應用程序設置會話超時，並在工作站上使用具有不活動超時的密碼保護屏幕保護程序。

C. 對所有應用程序使用會話 ID，並在工作站上使用具有不活動超時的密碼保護屏幕保護

程序。

D. 為應用程序設置會話超時並驗證所有工作站的系統 IP 地址。

您回答錯誤。

由於對工作站的物理訪問是問題的一部分，設置應用程序超時和具有相對較短的不活動超時的密碼保護屏幕保護程序可以幫助防止未經授權的訪問。對所有應用程序使用會話 ID 並驗證系統 IP 地址將有助於針對應用程序的在線攻擊。

**問題 49**

tb787631.CISSPPT3E.c05.037

狗、守衛和柵欄都是什麼類型的控制的常見例子？

A.偵探

B. 恢復

C. 行政

D. 物理的

你回答正確！

狗、警衛和柵欄都是物理控制的例子。雖然狗和警衛可能會發現問題，但

柵欄不能，所以它們並不都是偵探控制的例子。這些控制都不會在問題發

生後幫助修復或恢復功能，因此它們不是恢復控制，也不是涉及政策或程

序的管理控制，儘管警衛在履行職責時可能會參考它們。

**第 50 題**

tb787631.CISSPPT3E.c05.020

Jacob 正在規劃他的組織的生物認證系統，並正在考慮視網膜掃描。他的組織中的其他人可能會對視網膜掃描提出什麼擔憂？

A. 視網膜掃描可以揭示有關醫療狀況的信息。

B. 視網膜掃描很痛苦，因為它們需要在用戶眼中吹入一股空氣。

C. 視網膜掃描儀是最昂貴的生物識別設備。

D. 視網膜掃描儀的誤報率很高，會導致支持問題。

你回答正確！

視網膜掃描可以揭示更多信息，包括高血壓和懷孕，從而引起隱私問題。

較新的視網膜掃描不需要吹氣，視網膜掃描儀也不是最昂貴的生物識別因

素。他們的誤報率通常可以在軟件中進行調整，允許管理員根據需要調整

他們的接受率以平衡可用性和安全性。

**問題 51**

tb787631.CISSPPT3E.c05.060

當您輸入用戶 ID 和密碼時，您正在執行什麼重要的身份和訪問管理活動？

一、授權

B. 驗證

C. 認證

D. 登錄

您回答錯誤。

當您輸入用戶名和密碼時，您通過提供唯一標識符和驗證您是應該擁有該

標識符（密碼）的人來驗證自己。授權是確定允許用戶做什麼的過程。驗

證和登錄都描述了過程中發生的事情的元素；但是，它們並不是最重要的

身份和訪問管理活動。

**問題 52**

tb787631.CISSPPT3E.c05.013

以下哪項不是單點登錄實現？

A. Kerberos

B、ADFS

C、中科院

D. 半徑

您回答錯誤。

Kerberos、Active Directory Federation Services (ADFS) 和中央身份驗證服務 (CAS) 都是 SSO 實現。RADIUS 不是單點登錄實現，儘管一些供應商在幕後使用它來為專有 SSO 提供身份驗證。

## 問題 53

tb787631.CISSPPT3E.c05.095

Aaron 工作的銀行希望允許客戶使用與他們合作的第三方合作夥伴提供的新附加應用程序。由於並非每個客戶都想要或需要一個帳戶，Aaron 建議銀行使用基於 SAML 的工作流程，在用戶下載應用程序並嘗試登錄時創建一個帳戶。他建議使用哪種類型的供應系統？

A.JIT

B、OpenID

C、OAuth

D. Kerberos

你回答正確！

JIT 或即時供應機制在需要時創建帳戶，而不是提前創建它們。這是一種

限制所維護帳戶數量的有效方法，如果用戶帳號是許可協議的一部分，它

會很有用。問題中沒有提到 OAuth、OpenID 和 Kerberos。

## 問題 54

tb787631.CISSPPT3E.c05.021

強制訪問控制是基於什麼類型的模型？

A. 酌情決定
B. 集團化
C. 基於格的
D. 基於規則

你回答正確！

強制訪問控制系統基於基於格的模型。基於格的模型使用分類標籤矩陣來

劃分數據。自主訪問模型允許對象所有者確定對他們控制的對象的訪問，

基於角色的訪問控制通常是基於組的，而基於規則的訪問控制（如防火牆

ACL）將規則應用於他們適用的所有主題。

## 問題 55

tb787631.CISSPPT3E.c05.011

Kathleen 需要設置 Active Directory 信任以允許使用現有 Kerberos K5 域進行身份驗證。她需要建立什麼樣的信任？

A. 捷徑信託
B. 森林信託
C. 外部信託
D. 領域信任

您回答錯誤。

Kerberos 使用領域，為需要連接到 K5 域的 Active Directory 環境設置的正確信任類型是領域信任。捷徑信任是域樹或林部分之間的可傳遞信任，它縮短了信任路徑，林信任是兩個林根域之間的可傳遞信任，外部信任是單獨林中 AD 域之間的不可傳遞信任。

## 問題 56

tb787631.CISSPPT3E.c05.022

Greg 希望控制對整個組織用作銷售點終端的 iPad 的訪問。他應該使用以下哪種方法來允許對共享環境中的設備進行邏輯訪問控制？

A. 為所有銷售點終端使用共享 PIN 以使其更易於使用。

B. 使用 OAuth 允許每個用戶進行雲登錄。

C. 為每個用戶發放一個唯一的 PIN 碼，用於他們獲得的 iPad。

D. 使用 AD 用戶 ID 和密碼使用 Active Directory 和用戶帳戶登錄 iPad。

你回答正確！

使用需要個人使用其憑據登錄的 Active Directory 之類的企業身份驗證系統，可以在出現問題時確定誰登錄了，還允許 Greg 快速輕鬆地刪除已終止或轉換角色的用戶。使用共享 PIN 不提供問責制，而在專門發行的 iPad 上每個用戶的唯一 PIN 意味著其他人將無法登錄。OAuth 本身不提供 Greg 需要的服務和功能——它是一種授權服務，而不是身份驗證服務.

**問題 57**

tb787631.CISSPPT3E.c05.007

布賴恩是一所主要大學的研究員。作為研究的一部分，他使用自己大學的憑證登錄到另一個機構託管的計算集群。登錄後，他可以根據他在研究項目中的角色訪問集群和使用資源，也可以使用他所在組織的資源和服務。Brian 的家鄉大學採取了什麼措施來實現這一目標？

A. 域堆疊

B. 聯合身份管理

C. 域嵌套

D、混合登錄

你回答正確！

Brian 的組織正在使用聯合身份管理方法，其中多個組織允許跨組織使用身份。每個組織都需要證明自己員工的身份，並為他們提供權利和角色信息，以允許他們在聯合身份環境中使用資源。

**問題 58**

tb787631.CISSPPT3E.c05.039

Alaina 正在對服務帳戶執行定期計劃審查。她最應該關注下列哪項事件？

A. 服務帳戶的交互式登錄

B. 服務帳戶的密碼更改

C. 對服務帳戶權利的限制

D. 本地使用服務賬號

您回答錯誤。

服務帳戶的交互式登錄是一個嚴重的警告信號，無論是妥協還是不良的管理做法。無論哪種情況，Alaina 都應立即著手確定帳戶登錄的原因、發

生了什麼，以及交互式登錄是遠程還是本地完成的。在任何專業維護的環

境中，服務帳戶的遠程交互式登錄幾乎是妥協的標誌。服務帳戶的密碼更

改可以作為正在進行的密碼過期過程的一部分來完成，應始終對服務帳戶

權限進行限制以確保它們只是那些需要的，並且作為服務的一部分在本地

使用服務帳戶是正常的事件。

**問題 59**

tb787631.CISSPPT3E.c05.003

以下哪項不是 Kerberos 的弱點？

A. KDC 是單點故障。

B. KDC 的妥協將允許攻擊者冒充任何用戶。

C. 認證信息不加密。

D.容易被密碼猜測。

你回答正確！

Kerberos 使用密鑰加密消息，為身份驗證流量提供保護。KDC 都是單

點故障，如果遭到破壞可能會導致問題，因為密鑰存儲在 KDC 上，允許

攻擊者冒充任何用戶。與許多身份驗證方法一樣，Kerberos 容易受到密

碼猜測的影響。

**問題 60**

tb787631.CISSPPT3E.c05.084

會話 ID 長度和會話 ID 熵對於防止哪種類型的攻擊都很重要？

A. 拒絕服務

B. Cookie 盜竊

C.會話猜測

D. 中間人攻擊

你回答正確！

會話管理的最佳實踐涉及長會話 ID（通常為 128 位或更長）和足夠的隨

機性或熵，以使其難以猜測會話 ID。這使得暴力或算法猜測攻擊不太可

能，除非實施中存在缺陷。這些並不能防止拒絕服務或中間人攻擊 ，

cookie 攻擊在大多數情況下都集中在獲取和讀取或重用 cookie。

**問題 61**

tb787631.CISSPPT3E.c05.041

最近有報告稱在下班後對工作站進行了不受歡迎的訪問，Derek 被要求找到一種方法來確保維護人員無法登錄業務辦公室的工作站。維護人員在他們的休息室和他們的組織辦公室中確實有系統，他們仍然需要訪問這些系統。Derek 應該做什麼來滿足這個需求？

A. 要求多因素身份驗證，只允許辦公室工作人員擁有多因素令牌。

B. 使用基於規則的訪問控制來防止在業務區域下班後登錄。

C. 通過設置一個包含所有維護人員的組來使用基於角色的訪問控制，然後賦予該組僅登錄指定工作站的權限。

D. 使用地理圍欄只允許在維護區域登錄。

您回答錯誤。

最有效地利用 Derek 時間的方法是創建一個由所有維護人員組成的組，然後僅向該組授予指定 PC 的登錄權限。雖然基於時間的限制可能會有所幫助，但在這種情況下，它將繼續允許維護人員登錄到他們不打算在工作時間使用的 PC，從而在控制中留下漏洞。所描述的多因素身份驗證不符合場景的要求，但總體上可能是一個好主意，可以提高整個組織身份驗證的安全性。地理圍欄通常不夠準確，無法依賴特定 PC 的建築物內部。

## 第 62 題

tb787631.CISSPPT3E.c05.071

Brian 的大型組織多年來一直將 RADIUS 用於其網絡設備的 AAA 服務，並且最近意識到身份驗證期間傳輸的未加密信息存在安全問題。Brian 應該如何為 RADIUS 實施加密？

A. 使用 RADIUS 中的內置加密。

B. 使用 TLS 保護在其本機 UDP 上實施 RADIUS。

C. 使用 TLS 保護通過 TCP 實施 RADIUS。

D. 在設備之間使用 AES256 預共享密碼。

您回答錯誤。

RADIUS 支持基於 TCP 的 TLS。RADIUS 不支持基於 UDP 的 TLS 模式。AES 預共享對稱密碼不是受支持的解決方案，並且難以在大型環境中實施和維護，並且 RADIUS 中的內置加密僅保護密碼。

## 問題 63

tb787631.CISSPPT3E.c05.008

按照 Kerberos 身份驗證過程中發生的順序執行以下步驟。

1. 生成的客戶端/服務器票證
2. TGT 生成
3. 生成客戶端/TGS 密鑰
4. 用戶接入服務

5. 用戶提供身份驗證憑據

A. 5, 3, 2, 1, 4

B. 5, 4, 2, 1, 3

C.3、5、2、1、4

D.5、3、1、2、4

您回答錯誤。

在 Kerberos 身份驗證過程中，步驟按以下順序進行：用戶提供身份驗證憑證；生成客戶端/TGS 密鑰；TGT 生成；生成的客戶端/服務器票證；和用戶訪問服務。

## 第 64 題

tb787631.CISSPPT3E.c05.082

米歇爾在一家金融服務公司工作，她想為她的 Web 應用程序註冊客戶。如果她想快速自動驗證此人是否是他們聲稱的人，而無需與他們之前有任何關係，她可以使用哪種類型的身份驗證機制進行初始登錄？

A. 索取他們的社會安全號碼。

B. 使用基於知識的認證。

C. 執行手動身份驗證。

D. 使用生物識別因素。

你回答正確！

一些金融機構使用基於知識的身份驗證來驗證新用戶的身份。它使用其他

人不太可能獲得的來自稅收和財務記錄的信息，允許新用戶提供詳細信息，

如他們最近一次信用卡付款、抵押貸款付款或其他信息來驗證他們的身份。

通過付費服務或其他方式獲取社會安全號碼有些微不足道，而且手動驗證

身份既不快速也不自動。生物識別因素需要事先註冊，因此不適合新客戶。

**問題 65**

tb787631.CISSPPT3E.c05.030

當應用程序或系統允許登錄用戶執行特定操作時，它是什麼的示例？

A. 角色

B、集團管理

C. 登錄

D、授權

你回答正確！

授權為用戶提供能力或權利。角色和組管理都是可以用來匹配用戶和權限

的方法。登錄用於驗證用戶。

## 第 66 題

tb787631.CISSPPT3E.c05.097

Valerie 需要控制對部署到 BYOD 環境中的移動設備的應用程序的訪問。哪種類型的解決方案最能讓她控制應用程序，同時確保它們不會在最終用戶使用的設備上留下殘餘數據？

A. 將應用程序部署到 BYOD 設備，並要求每台設備都有唯一的 PIN。

B. 將應用程序部署到桌面系統，並要求用戶使用遠程桌面使用企業身份驗證訪問它們。

C. 使用應用程序容器將應用程序部署到 BYOD 設備，並要求每台設備都有唯一的 PIN。

D. 使用需要使用企業憑據進行身份驗證的虛擬託管應用程序環境。

你回答正確！

當需要非常高級別的控製或無法信任端點設備時，使用具有遠程連接和企業身份驗證的集中式環境可以提供適當的安全性。

## 問題 67

tb787631.CISSPPT3E.c05.027

Henry 正在與 Web 應用程序開發團隊合作，為其公司的新應用程序進行身份驗證和授權流程。該團隊希望使會話 ID 盡可能安全。以下哪項不是 Henry 應該推薦的最佳實踐？

A. 會話 ID 令牌應該是可預測的。

B. 會話 ID 應該至少有 64 位的熵。

C. 會話長度應至少為 128 位。

D. session ID 應該是無意義的。

你回答正確！

Web 應用程序開發最佳實踐目前建議使用具有足夠熵（隨機性）的長會話 ID（128 位或更長）以確保它們不會被輕易複製或暴力破解。確保會話 ID 本身無意義以防止信息洩露攻擊也是最佳做法。然而，會話 ID 應該過期，因為即使滿足所有這些建議，永不過期的會話最終也可能被強制執行。

## 第 68 題

tb787631.CISSPPT3E.c05.006

Charles 想要部署憑證管理系統 (CMS)。他想盡可能保證密鑰的安全。以下哪項是他的 CMS 實施的最佳設計選項？

A. 使用 AES-256 而不是 3DES。
B. 使用長鍵。
C. 使用 HSM。
D. 定期更改密碼。

您回答錯誤。

硬件安全模塊或 HSM 是存儲與 CMS 關聯的密鑰的最安全方式。它們提

供增強的密鑰管理功能，並且通常需要通過 FIPS 認證。除了這些優勢

之外，HSM 還可以提高組織的加密性能，因為專為該目的而設計的專用

硬件。長密鑰和使用 AES-256 是很好的做法，但 HSM 提供更高的安全

性，並且已經需要適當的加密控制。在整個組織中更改密碼可能具有挑戰

性；相反，保護密碼短語和密鑰對大多數組織來說更為重要和合理。

## 第 69 題

tb787631.CISSPPT3E.c05.049

在滲透測試期間，Chris 恢復了一個文件，其中包含他試圖訪問的系統的散列密碼。哪種類型的攻擊最有可能成功破解散列密碼？

A. 暴力攻擊
B. 哈希傳遞攻擊
C. 彩虹桌攻擊
D. 鹽回收攻擊

您回答錯誤。

彩虹表是預散列密碼與高速查找功能配對的數據庫。由於他們可以快速將

已知哈希值與文件中的哈希值進行比較，因此使用彩虹表是根據哈希值快

速確定密碼的最快方法。蠻力攻擊可能最終會成功，但對大多數哈希來說

速度會很慢。傳遞哈希攻擊依賴於將嗅探或以其他方式獲取的 NTLM 或

LanMan 哈希發送到系統以避免需要知道用戶密碼。鹽是添加到散列中

的數據，以避免使用彩虹表等工具。添加到密碼中的鹽意味著哈希不會匹

配沒有相同鹽生成的彩虹表。

## 第 70 題

tb787631.CISSPPT3E.c05.002

Jim 在組織範圍內實施的 IDaaS 為基於雲的應用程序提供了廣泛的支持。Jim 的公司沒有內部身份管理人員，也不使用集中式身份服務。相反，他們依靠 Active Directory 提供 AAA 服務。Jim 應該推薦以下哪個選項來最好地處理公司的現場身份需求？

A. 使用 OAuth 集成現場系統。

B. 使用本地第三方身份服務。

C. 使用 SAML 集成現場系統。

D. 設計一個內部解決方案來處理組織的獨特需求。

你回答正確！

由於 Jim 的組織正在使用基於雲的身份即服務解決方案，第三方本地身份服務可以提供與 IDaaS 解決方案集成的能力，並且公司對 Active Directory 的使用得到了第三方的廣泛支持供應商。OAuth 用於使用現有憑據登錄第三方網站，無法滿足所述需求。SAML 是一種標記語言，不能滿足全套 AAA 需求。由於組織正在使用 Active Directory，自定義的內部解決方案不太可能像現有的第三方解決方案那樣有效，並且可能需要更多的時間和費用來實施。

## 第 71 題

tb787631.CISSPPT3E.c05.023

為身份使用提供問責制的最佳方式是什麼？

A. 日誌記錄

B、授權

C. 數字簽名

D. 類型 1 認證

您回答錯誤。

日誌系統可以通過跟踪用戶或帳戶執行的操作、更改和其他活動來為身份

系統提供責任。

## 第 72 題

tb787631.CISSPPT3E.c05.028

Angela 使用嗅探器監控來自配置了默認設置的 RADIUS 服務器的流量。她應該監控什麼協議，她能夠讀取什麼流量？

答：UDP，沒有。所有 RADIUS 流量都經過加密。

B. TCP，除密碼外的所有流量均已加密。

C. UDP，除密碼外的所有流量均已加密。

D. TCP，無。所有 RADIUS 流量都經過加密。

您回答錯誤。

默認情況下，RADIUS 使用 UDP 並且只加密密碼。RADIUS 支持 TCP

和 TLS，但這不是默認設置。

## 第 73 題

tb787631.CISSPPT3E.c05.057

Susan 的組織是聯合的一部分，該聯合允許來自多個組織的用戶訪問其他聯合站點的資源和服務。當 Susan 想要在合作夥伴站點使用服務時，使用哪個身份提供者？

A. Susan 所在組織的身份提供者

B. 服務提供者的身份提供者

C.他們的身份提供者和服務提供者的身份提供者

D. 服務提供者創建新身份

你回答正確！

聯盟使用用戶的家庭組織的身份提供者 (IDP)。當用戶嘗試對服務進行身份驗證時，服務提供者會查詢這些身份提供者，如果請求得到驗證，則根據 IDP 提供的可能相關的屬性，根據為服務設置的規則和策略允許訪問。

**第 74 題**

tb787631.CISSPPT3E.c05.054

Charles 希望提供授權服務作為他的 Web 應用程序的一部分。如果他想輕鬆地與其他網絡身份提供商集成，他應該使用什麼標準？

A. OpenID

B. TACACS+

C. 半徑

D.OAuth

你回答正確！

OAuth 是使用最廣泛的雲服務授權和授權開放標準。OpenID 用於認證 ，

TACAC+和 RADIUS 主要用於現場對網絡設備的認證授權。

## 第 75 題

tb787631.CISSPPT3E.c05.016

Alex 的工作要求他查看受保護的健康信息 (PHI)，以確保對患者進行適當的治療。他訪問他們的醫療記錄並不能訪問患者地址或賬單信息。什麼訪問控制概念最能描述這種控制？

A. 職責分離

B. 受限接口

C. 上下文相關的控制

D、需要知道

你回答正確！

當像亞歷克斯這樣的主體只能訪問他們完成工作所需的數據時，需要知道 。

職責分離用於通過讓多名員工執行部分任務來限制欺詐和濫用行為。受限

接口限制用戶可以看到或做的事情，如果需要知道在這種情況下沒有更完

整地描述他的訪問權限，這將是一個合理的答案。上下文相關的控制依賴

於正在執行的活動來應用控制，並且這個問題沒有指定工作流或過程。

**第 76 題**

tb787631.CISSPPT3E.c05.052

當 Chris 驗證個人身份並將用戶 ID 等唯一標識符添加到身份系統時，發生了什麼過程？

A. 身份證明
B. 註冊
C.目錄管理
D、會話管理

你回答正確！

註冊是將用戶添加到身份管理系統的過程。這包括創建他們的唯一標識符

並添加與其身份相關聯的任何屬性信息。驗證發生在用戶提供信息以證明

他們是誰時。管理目錄以維護用戶、服務和其他項目的列表。會話管理跟

踪應用程序和用戶會話。

**第 77 題**

tb787631.CISSPPT3E.c05.042

Nick 想為他的 Web 應用程序進行會話管理。以下哪些是常見的 Web 應用程序會話管理技術或方法？（選擇所有符合條件的。）

A. IP 跟踪
B. 餅乾
C. URL 重寫
D. TLS 令牌

您回答錯誤。

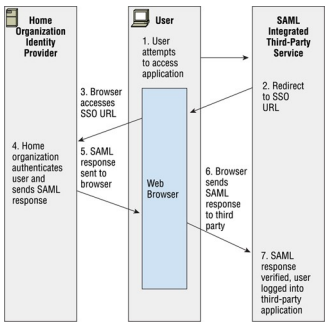
常見的會話管理技術包括使用 cookie、隱藏表單字段、URL 重寫和內置框架（如 Java 的 HTTPSession）。IP 跟踪可能包含在會話信息中但本身並不是一個完整的會話標識符，TLS 令牌綁定用於使 TLS 會話更安全，而不是提供會話標識。

## 第 78 題

tb787631.CISSPPT3E.c05.044

請利用您對 SAML 集成和安全架構設計的了解，並參考以下場景和圖表：

- Alex 負責 SAML 與主要第三方合作夥伴的集成，該合作夥伴為其組織提供各種業務生產力服務。




如果 Alex 的組織主要由異地旅行用戶組成，那麼將關鍵業務應用程序集成到現場身份驗證會產生哪些可用性風險，他將如何解決？

A. 第三方集成可能不可信；使用 SSL 和數字簽名。

B. 如果本國組織不在線，出差用戶將無法訪問第三方應用；實施混合雲/本地身份驗證系統。

C. 本地用戶可能無法正確重定向至第三方服務；實現本地網關。

D. 瀏覽器可能無法正確重定向；使用主機文件來確保重定向問題得到解決。

你回答正確！

如果本地組織的 Internet 連接或服務器離線，則與依賴本地身份驗證的基於雲的第三方集成可能會失敗。採用混合雲和本地身份驗證系統可以確保處理互聯網或服務器中斷，無論用戶身在何處或其家庭組織是否在線，都可以進行身份驗證。使用加密和簽名的通信無法解決可用性問題，重定向是第三方的配置問題，本地網關無法處理遠程用戶。此外，主機文件無助於解決 DNS 以外服務的可用性問題。

## 第 79 題

tb787631.CISSPPT3E.c05.034

下表顯示了哪種類型的訪問控制方案？

| 高度敏感 | 紅色的 | 藍色的 | 綠色的 |
| --- | --- | --- | --- |
| 機密的 | 紫色的 | 橙子 | 黃色的 |
| 內部使用 | 黑色的 | 灰色的 | 白色的 |
| 民眾 | 清除 | 清除 | 清除 |

A、RBAC

B、解碼器

C.MAC

D. 待定

你回答正確！

強制訪問控制使用格或矩陣來描述分類標籤如何相互關聯。在此圖像中，

為顯示的每個標籤設置了分類級別。自主訪問控制 (DAC) 系統將顯示對

象的所有者如何允許訪問。RBAC 可以是基於規則或基於角色的訪問控

制，並且可以使用系統範圍的規則或角色。基於任務的訪問控制 (TBAC)

將列出用戶的任務。

## 問題 80

tb787631.CISSPPT3E.c05.031

亞歷克斯在他的公司工作了十多年，並在公司擔任過多個職位。在審計過程中，發現由於他以前的角色，他可以訪問共享文件夾和應用程序。亞歷克斯的公司遇到了什麼問題？

A. 過度供應
B. 未經授權的訪問
C. 特權蔓延
D. 賬戶審查

你回答正確！

當用戶從他們以前擁有的角色中保留他們不需要完成當前工作的權利時，就會發生特權蔓延。當未經授權的用戶訪問文件時，就會發生未經授權的訪問。過度配置不是用於描述權限問題的術語，帳戶審查將有助於發現此類問題。

**問題 81**

tb787631.CISSPPT3E.c05.040

使用生物識別技術的組織何時可以選擇允許更高的 FRR 而不是更高的 FAR？

A. 當安全性比可用性更重要時
B. 當由於數據質量而導致錯誤拒絕不是問題時
C. 當系統的 CER 未知時
D. 當系統的 CER 很高時

您回答錯誤。

具有非常嚴格的安全要求且不能容忍錯誤接受的組織希望將錯誤接受率或

FAR 降低到盡可能接近於零。這通常意味著錯誤拒絕率或 FRR 增加。

不同的生物識別技術或更好的註冊方法可以幫助提高生物識別性能，但由

於數據質量導致的錯誤拒絕通常不是現代生物識別系統的問題。在這種情

況下，了解交叉錯誤率或 CER，或者擁有非常高的 CER 都無助於做出

決定。

**問題 82**

tb787631.CISSPPT3E.c05.072

Jim 希望允許基於雲的應用程序代表他訪問來自其他站點的信息。以下哪個工具可以做到這一點？

A. Kerberos
B、OAuth
C、OpenID
D、LDAP

您回答錯誤。

OAuth 提供了從其他服務訪問資源的能力，可以滿足 Jim 的需求 。

OpenID 將允許他在他的應用程序中使用來自其他服務的帳戶，而

Kerberos 和 LDAP 更頻繁地用於內部服務。

**問題 83**

tb787631.CISSPPT3E.c05.005

如果 Susan 的組織要求她使用用戶名、PIN、密碼和視網膜掃描進行登錄，她使用了多少種不同的身份驗證因素類型？

A、一個
B、兩個
C、三
D、四

你回答正確！

蘇珊使用了兩種不同類型的因素：PIN 和密碼都是類型 1 因素，視網膜

掃描是類型 3 因素。她的用戶名不是一個因素。

**問題 84**

tb787631.CISSPPT3E.c05.075

Chris 希望在識別個人身份的同時控制對其設施的訪問。他還想確保這些人是在沒有大量持續費用的情況下被錄取的人。以下選項中的哪些解決方案可以滿足所有這些要求？（選擇所有符合條件的。）

A. 保安人員和帶照片的身份證

B. RFID 徽章和帶密碼鍵盤的閱讀器

C. 磁條胸卡和帶密碼鍵盤的閱讀器

D. 保安人員和磁條閱讀器

您回答錯誤。

在 Chris 面臨的場景中，最好的答案是 RFID 或磁條閱讀器和密碼鍵盤。

警衛會產生持續的費用，任何沒有 PIN 的解決方案都將允許使用被盜或克隆的徽章，而無需驗證訪問建築物的人是否為合法用戶。雖然警衛可以防止徽章和 PIN 組合被盜，但這僅用於成本合理的環境。

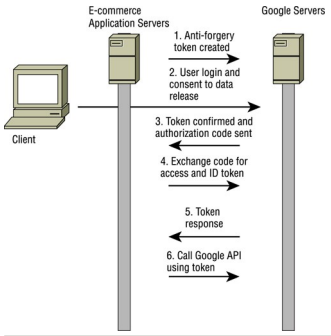
**問題 85**

tb787631.CISSPPT3E.c05.067

請參考以下場景和圖表：

- Chris 是一家不斷發展的電子商務網站的身份架構師，該網站希望利用社交身份。為此，他和他的團隊打算允許用戶在使用電子商務網站時使用他們現有的谷歌賬戶作為他們的主要賬戶。這意味著，當新用戶最初連接到電子商務平台時，他們可以選

擇是使用 OAuth 2.0 使用他們的 Google 帳戶，還是使用他們自己的電子郵件地址和他們選擇的密碼在平台上創建一個新帳戶。




創建和交換狀態令牌旨在防止哪種類型的攻擊？

A、XSS

B、CSRF

C、SQL 注入

D.XACML

你回答正確！

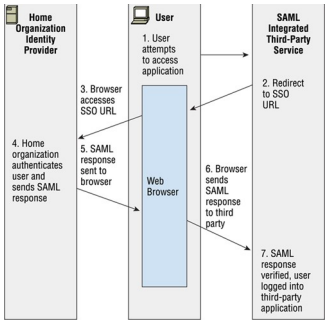
在 OAuth 會話期間交換的防偽狀態令牌旨在防止跨站點請求偽造。這確保了具有來自 Google 的 OAuth 服務的身份驗證響應的唯一會話令牌可用於驗證發出請求的是用戶，而不是攻擊者。XSS 攻擊側重於腳本，會涉及腳本標籤，SQL 注入會包含 SQL 代碼，XACML 是可擴展訪問控制標記語言，不是一種攻擊類型。

**問題 86**

tb787631.CISSPPT3E.c05.043

請利用您對 SAML 集成和安全架構設計的了解，並參考以下場景和圖表：

- Alex 負責 SAML 與主要第三方合作夥伴的集成，該合作夥伴為其組織提供各種業務生產力服務。




亞歷克斯擔心 SAML 流量被竊聽，還想確保偽造斷言不會成功。他應該怎麼做才能防止這些潛在的攻擊？

A. 使用 SAML 的安全模式提供安全認證。

B. 使用強大的密碼套件實施 TLS，這將防止兩種類型的攻擊。

C. 使用強大的密碼套件實施 TLS 並使用數字簽名。

D. 使用強大的密碼套件和消息哈希實現 TLS。

您回答錯誤。

TLS 提供消息的機密性和完整性，可以防止竊聽。當與提供完整性和身份驗證的數字簽名配對時，偽造的斷言也可以被擊敗。SAML 沒有安全模式，並且在需要時依靠 TLS 和數字簽名來確保安全。沒有簽名的消息散列將有助於防止修改消息，但不一定提供身份驗證。

## 問題 87

tb787631.CISSPPT3E.c05.091

Joanna 領導她所在組織的身份管理團隊，希望確保在工作人員更換新職位時正確更新角色。她應該為這些員工關注什麼問題，以避免未來出現角色定義問題？

一、報名

B. 特權蔓延

C. 取消配置

D. 問責制

您回答錯誤。

當員工隨著時間的推移改變角色時，權限蔓延是一個持續的問題。在過渡期間，以前角色的特權可能很容易忘記或保留，因為員工可能會繼續幫助完成個人以前執行的任務或流程。隨著時間的推移，這些被遺忘的權利和特權會疊加，使員工擁有他們當前角色不應該擁有的權利。註冊是新員工關心的問題，而取消配置是離職員工關心的問題。問責制通常由 IAM 系統通過驗證和記錄訪問和特權使用來提供。

## 問題 88

tb787631.CISSPPT3E.c05.038

Susan 的組織正在更新其密碼策略，並希望使用盡可能強的密碼。什麼密碼要求對防止暴力攻擊的影響最大？

A. Change maximum age from 1 year to 180 days.

B. Increase the minimum password length from 8 characters to 16 characters.

C. Increase the password complexity so that at least three character classes (such as uppercase, lowercase, numbers, and symbols) are required.

D. Retain a password history of at least four passwords to prevent reuse.

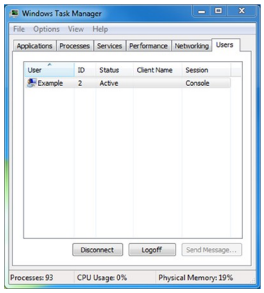
You Answered Correctly!

Password complexity is driven by length, and a longer password will be more effective against brute-force attacks than a shorter password. Each character of additional length increases the difficulty by the size of the potential character set (for example, a single lowercase character makes the passwords 26 times more difficult to crack). While each of the other settings is useful for a strong password policy, they won't have the same impact on brute-force attacks.

**Question 89**

tb787631.CISSPPT3E.c05.014

如下圖所示，Windows 系統上的用戶無法使用發送消息功能。哪種訪問控制模型最能描述這種類型的限制？




A. 最小權限

B、需要知道

C. 約束接口

D. 職責分離

您回答錯誤。

基於用戶權限的接口限制是受限接口的一個示例。最小特權描述了這樣一種想法，即只為用戶提供他們完成工作所需的權限，同時需要知道根據主體是否需要知道信息來完成分配的任務來限制訪問權限。職責分離的重點是通過在多個主體之間拆分任務來防止欺詐或錯誤。

## 問題 90

tb787631.CISSPPT3E.c05.029

哪種類型的訪問控制最能描述 NAC 的態勢評估能力？

A. 強制訪問控制

B. 基於風險的訪問控制

C. 自主訪問控制

D. 基於角色的訪問控制

您回答錯誤。

NAC 的偽裝能力決定了系統是否足夠安全和合規以連接到網絡。這是一種基於風險的訪問控制形式，因為不合規的系統被認為具有更高的風險，並且要么被放置在隔離和補救網絡或區域中，要么被禁止連接到網絡，直到它們合規為止。

**問題 91**

tb787631.CISSPPT3E.c05.063

Olivia 希望限制用戶可以通過 `sudo` 運行的命令，以限制權限升級攻擊的可能性。她應該修改哪個 Linux 文件以允許這樣做？

A. bash `.bin` 配置文件

B. `sudoers` 文件

C. bash `.allowed` 配置文件

D.sudont 文件_

你回答正確！

sudoers 文件可以列出可以使用 sudo 的特定用戶以及允許他們使用的

命令或目錄。

## 問題 92

tb787631.CISSPPT3E.c05.069

Madhuri 創建了一個表，其中包括分配的權限、對象和主體，以管理她負責的系統的訪問控制。每次主體嘗試訪問客體時，系統都會檢查該表以確保主體對客體具有適當的權限。Madhuri 使用什麼類型的訪問控制系統？

A.能力表

B. 訪問控制列表

C. 訪問控制矩陣

D. 主體/客體權限管理系統

您回答錯誤。

訪問控制矩陣是一個列出對象、主體及其權限的表。訪問控制列表側重於

對像以及哪些主體可以訪問它們。能力表列出了主題和他們可以訪問的對

象。主體/客體權限管理系統不基於訪問控制模型。

## 問題 93

tb787631.CISSPPT3E.c05.085

Naomi 組織的訪問控制系統會檢查她的計算機是否已完全打補丁，是否成功進行了乾淨的反惡意軟件掃描，以及防火牆是否已打開以及其他安全驗證，然後才允許她連接到網絡。如果存在潛在問題，則不允許她連接並且必須聯繫支持人員。什麼類型的訪問控制方案最能描述這種類型的過程？

A.MAC

B. 基於規則的訪問控制

C. 基於角色的訪問控制

D. 基於風險的訪問控制

你回答正確！

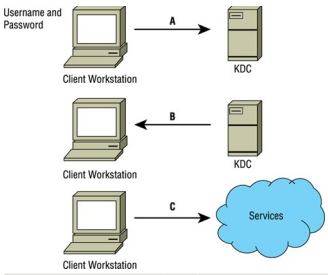
基於風險的訪問控制模型風險使用創建訪問請求時可用的信息。有關請求及其可能產生的風險的信息是根據風險值計算出來的，並與訪問策略進行比較。如果風險值可接受，則授予訪問權限。組織中最常見的例子之一是 NAC，即網絡訪問控制，其中對系統進行分析以確定安全風險和合規性，然後再進入網絡。這可以看作是基於規則的訪問控制的一個更具體的例子。

基於角色的訪問控制根據個人的角色做出決定，而強制訪問控制則由操作系統強制執行。

問題 94

tb787631.CISSPPT3E.c05.017

請利用您對 Kerberos 登錄過程的了解並參考下圖：




在圖中的 A 點，客戶端將用戶名和密碼發送到 KDC。如何保護用戶名和密碼？

A. 3DES 加密

B、TLS 加密

C、SSL 加密

D、AES 加密

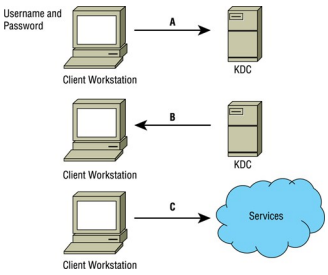
您回答錯誤。

Kerberos 登錄中的客戶端在將用戶名和密碼發送到 KDC 之前使用 AES 對其進行加密。

## 問題 95

tb787631.CISSPPT3E.c05.019

請利用您對 Kerberos 登錄過程的了解並參考下圖：



客戶端在使用 TGT 之前必須執行哪些任務？

A. 它必須生成 TGT 的散列並解密對稱密鑰。

B. 它必須接受 TGT 並解密對稱密鑰。

C. 它必須解密 TGT 和對稱密鑰。

D. 它必須使用對稱密鑰向 KDC 發送有效響應並且必須安裝 TGT。

您回答錯誤。

客戶端需要接受 TGT 以供使用，直到它過期並且還必須使用用戶密碼的

散列來解密對稱密鑰。

**問題 96**

tb787631.CISSPPT3E.c05.077

什麼認證技術可以與 OAuth 結合使用 RESTful API 進行身份驗證和獲取用戶資料信息？

A.SAML

B. 陳詞濫調

C. OpenID 連接

D.希金斯

你回答正確！

OpenID Connect 是一種基於 JSON 的 RESTful 身份驗證協議，與

OAuth 配合使用時，可以提供身份驗證和基本配置文件信息。SAML 是

安全斷言標記語言，Shibboleth 是一種聯合身份解決方案，旨在允許基

於 Web 的 SSO，而 Higgins 是一個開源項目，旨在為用戶提供對其身

份信息發布的控制權。

## 問題 97

tb787631.CISSPPT3E.c05.055

Cameron 工作的公司使用的系統允許用戶在必要時請求對系統的特權訪問。Cameron 請求訪問權限，並且由於他的角色，該請求已獲得預先批准。然後他能夠訪問系統以執行任務。一旦完成，權利將被刪除。他使用什麼類型的系統？

A. 零信任

B. 聯合身份管理

C、單點登錄

D. 即時訪問

你回答正確！

Cameron 正在使用準時制 (JIT) 系統，該系統可在需要時提供所需的訪問權限。零信任系統在執行操作時需要身份驗證和授權，但不一定需要在需要時授予和刪除特權。