D6-002 結果 2022 年 12 月 15 日

問題一

tb787631.CISSPPT3E.c06.096

Elaine 在她的組織使用的產品中發現了一個以前未知的嚴重漏洞。她所在的組織對道德披露有著堅定的承諾，而 Elaine 希望遵循常見的道德披露慣例。她應該先做什麼？

A. 建立內部修復或控制，然後公開披露漏洞以促使供應商快速修補它。

B. 建立內部補救或控制，然後將問題通知供應商。

C. 通知供應商並給他們合理的時間來解決問題。

D. 公開披露漏洞，以便供應商在適當的時間內對其進行修補。

你回答正確！

道德（或負責任的）披露規範包括通知供應商並為他們提供合理的時間來補救問題。在大多數情況下，在通知供應商之前或在短時間內公開披露信息被認為是不道德的。雖然這個時間範圍有所不同，但由於軟件和其他技術的複雜性，90 到 120 天在整個行業並不罕見。

問題 2

tb787631.CISSPPT3E.c06.074

Ryan 的組織希望確保進行適當的帳戶管理，但沒有中央身份和訪問管理工具。Ryan 進行驗證過程的時間有限。作為內部審計的一部分，他測試賬戶管理流程的最佳選擇是什麼？

A. 驗證過去 90 天內更改的所有帳戶。

B. 選擇高價值的管理帳戶進行驗證。

C. 驗證過去 180 天內的所有帳戶更改。

D. 驗證一個隨機的賬戶樣本。

您回答錯誤。

如果無法驗證所有帳戶，則建議對帳戶進行隨機抽樣。僅選擇最近更改的

帳戶不會識別長期問題或歷史問題，並且僅檢查高價值帳戶不會顯示其他

帳戶類型是否存在問題或不良做法。

問題三

tb787631.CISSPPT3E.c06.017

Mark 的公司已收到通知，他們的 Web 應用程序存在缺陷。匿名人士已通知他們，他們有兩週的時間來修復它，然後才能發布漏洞的詳細信息以及示例利用代碼。聯繫 Mark 公司的個人違反了哪些行業規範？

A. 零日報告

B. 道德披露

C. 道德黑客

D. (ISC) ^{2} 漏洞披露道德聲明

您回答錯誤。

合乎道德（或負責任）的披露做法將為公司和組織提供一段合理的時間來

修復缺陷並將修復程序交到客戶手中。兩週不太可能是合理的時間。不幸

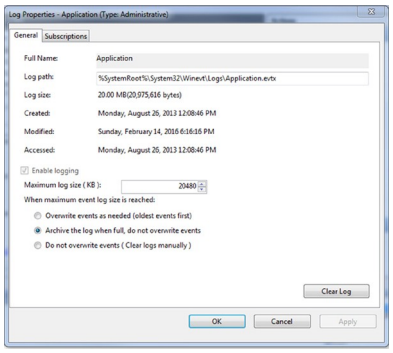
的是，Mark 可能無法說服個人做出不同的決定，而 Mark 的公司將需要

確定如何處理這個問題。

問題四

tb787631.CISSPPT3E.c06.051

在此圖中，日誌處理設置可能會出現什麼問題？



A. 日誌歸檔時，日誌數據可能會丟失。

B. 日誌數據可能被覆蓋。

C. 日誌數據可能不包含所需信息。

D. 日誌數據可能會填滿系統盤。

您回答錯誤。

當日誌達到允許的最大大小 (20 MB) 時，顯示的菜單將歸檔日誌。這些

檔案將被保留，這可能會填滿磁盤。日誌數據不會被覆蓋，數據歸檔時日

誌數據不應丟失。該問題未包含足夠的信息來確定是否可能未記錄所需的

信息。

問題 5

tb787631.CISSPPT3E.c06.050

在一次滲透測試中，Selah 打電話給她目標的服務台，自稱是公司某位官員的高級助理。由於該官員在旅行期間筆記本電腦出現問題，她要求幫助台重置該官員的密碼，並說服他們這樣做。她成功完成了哪種類型的攻擊？

A. 零知識
B. 服務台欺騙
C. 社會工程
D、黑匣子

你回答正確！

Selah 的社會工程攻擊成功地說服了服務台的一名工作人員為他們不僅

看不到而且無法驗證的人更改了密碼，實際上需要重設密碼。黑盒和零知

識都是描述滲透測試的術語，沒有關於組織或系統的信息，幫助台欺騙不

是行業術語。

問題 6

tb787631.CISSPPT3E.c06.049

以下哪項策略不是修復漏洞掃描程序識別的漏洞的合理方法？

A. 安裝補丁。

B. 使用解決方法修復。

C. 更新橫幅或版本號。

D. 使用應用層防火牆或 IPS 來防止針對已識別漏洞的攻擊。

你回答正確！

簡單地更新應用程序提供的版本可能會阻止漏洞掃描器標記它，但它不會

解決根本問題。打補丁、使用變通辦法或安裝應用層防火牆或 IPS 都可

以幫助修復或限制漏洞的影響。

問題 7

tb787631.CISSPPT3E.c06.083

Ken 正在為他的團隊開發的軟件設計一個測試流程。他正在設計一個測試，以驗證在測試期間是否執行了每一行代碼。Ken 正在進行什麼類型的分析？

A. 分支機構覆蓋

B. 條件覆蓋

C. 功能覆蓋

D. 語句覆蓋

您回答錯誤。

語句覆蓋測試驗證每一行代碼都在測試期間被執行。分支覆蓋驗證每個

`if` 語句是否在所有 `if` 和 `else` 條件下執行。條件覆蓋驗證代碼中的每

個邏輯測試都在所有輸入集下執行。函數覆蓋驗證代碼中的每個函數都被

調用並返回結果。

問題 8

tb787631.CISSPPT3E.c06.059

Nicole 想對她的組織進行一次基於標準的審計。以下哪項通常用於描述信息系統的共同要求？

A.國際電工委員會

B.COBIT

FISA

D. 數字千年版權法案

您回答錯誤。

COBIT，即信息和相關技術的控制目標，通常用作組織的審計框架 。

DMCA 是數字千年版權法，IEC 是國際電工聯盟，定義了電工技術標準 ，

而 FISA 是聯邦情報監視法，不是審計標準。

問題 9

tb787631.CISSPPT3E.c06.094

漏洞掃描器不會發現什麼類型的漏洞？

A. 本地漏洞

B. 服務漏洞

C. 零日漏洞

D. 需要認證的漏洞

你回答正確！

漏洞掃描器無法檢測到它們沒有測試、插件或簽名的漏洞。簽名通常包括

版本號、服務指紋或配置數據。如果向他們提供憑據，他們可以檢測本地

漏洞以及需要身份驗證的漏洞，當然，他們還可以檢測服務漏洞。

問題 10

tb787631.CISSPPT3E.c06.077

哪種類型的漏洞掃描會訪問其所針對的系統的配置信息以及可通過網絡可用服務訪問的信息？

A. 認證掃描

B. Web 應用程序掃描

C. 未經身份驗證的掃描

D、端口掃描

您回答錯誤。

經過身份驗證的掃描使用只讀帳戶訪問配置文件，從而可以更準確地測試漏洞。Web 應用程序掃描、未經身份驗證的掃描和端口掃描無法訪問配置文件，除非它們被無意中暴露。

問題 11

tb787631.CISSPPT3E.c06.031

今年早些時候，Jim 雇主的信息安全團隊在 Jim 負責維護的 Web 服務器中發現了一個漏洞。他立即應用了補丁並確定它安裝正確，但漏洞掃描器繼續錯誤地將系統標記為易受攻擊。以下哪個選項是吉姆處理問題的最佳選擇，這樣它就不會繼續被錯誤標記？

A. 卸載並重新安裝補丁。

B. 要求信息安全團隊將系統標記為已打補丁並且不易受到該特定缺陷的影響。

C. 更新網絡服務器配置中的版本信息。

D. 查看漏洞報告並使用替代修復選項。

您回答錯誤。

如果 Jim 確定已安裝補丁，他應該要求信息安全團隊將問題標記為已解決。許多漏洞掃描器依賴於版本信息或橫幅信息，如果軟件提供商不更新他們看到的信息，則可能會標記已打補丁的版本。卸載並重新安裝補丁不會改變這一點。更改版本信息可能不會更改掃描器標記的所有詳細信息，並可能在以後導致問題。查看漏洞信息以尋找解決方法可能是個好主意，但如果安裝了正確的補丁，則沒有必要；以後可能會造成維護問題。

問題 12

tb787631.CISSPPT3E.c06.047

Alan 的組織使用安全內容自動化協議 (SCAP) 來標準化其漏洞管理程序。Alan 可以使用 SCAP 的哪個組件來協調不同安全評估工具生成的漏洞的身份？

A. 橢圓形

B. XCCDF

C、CVE

D、SCE

您回答錯誤。

Common Vulnerabilities and Exposures (CVE) 數據庫為識別安全漏洞

提供了一致的參考。開放漏洞和評估語言 (OVAL) 用於描述系統的安全

狀況。可擴展配置清單描述格式 (XCCDF) 用於以標準化方式創建安全清

單。腳本檢查引擎 (SCE) 旨在使腳本可與安全策略定義互操作。

問題 13

tb787631.CISSPPT3E.c06.092

Joanna 是她所在組織的 CISO，在擔任安全運營監督職務時，她希望確保對與安全相關的變更進行管理監督。在大多數組織中，她應該關注哪個系統來跟踪此類數據？

A. SIEM 系統

B.IPS 系統

C. CMS 工具

D. ITSM 工具

你回答正確！

IT 服務管理或 ITSM 工具包括變更管理以及 Joanna 正在尋找的批准和

審查流程類型。SIEM 幫助處理安全日誌和事件，IPS 查找入侵和不需要

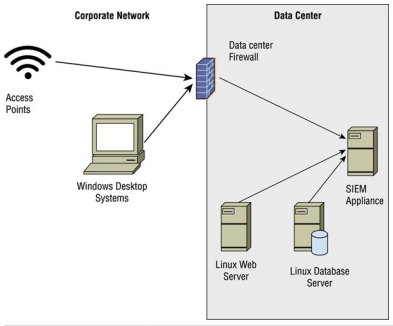
的流量，CMS 是一種內容管理工具。

問題 14

tb787631.CISSPPT3E.c06.018

請參考以下場景：

- Jennifer 工作的公司實施了中央日誌記錄基礎設施，如下圖所示。使用此圖和您對日誌系統的了解來回答以下問題。



Jennifer 需要確保所有 Windows 系統都向 SIEM 提供相同的日誌記錄信息。她如何才能最好地確保所有 Windows 桌面都具有相同的日誌設置？

A. 執行定期配置審核。

B. 使用組策略。

C. 使用本地策略。

D. 部署 Windows 系統日誌客戶端。

你回答正確！

Active Directory 實施的組策略可以確保一致的日誌記錄設置，並可以在

系統上定期實施策略。定期配置審核不會捕獲兩次審核之間所做的更改，

並且由於本地更改或部署差異，本地策略可能會發生變化。Windows 系

統日誌客戶端將使 Windows 系統能夠將系統日誌發送到 SIEM 設備，但

不能確保事件記錄的一致性。

問題 15

tb787631.CISSPPT3E.c06.039

合成監測和被動監測的主要區別是什麼？

A. 綜合監控僅在問題發生後才起作用。

B. 被動監控無法檢測功能問題。

C. 被動監控只有在問題發生後才起作用。

D. 綜合監控無法檢測功能問題。

你回答正確！

被動監控僅在問題發生後才起作用，因為它需要實際流量。綜合監控使用

模擬或記錄的流量，因此可用於主動識別問題。綜合監控和被動監控都可

用於檢測功能問題。

問題 16

tb787631.CISSPPT3E.c06.009

在響應提案請求時，Susan 收到了一份 SSAE 18 SOC 報告。如果她想要一份包含運營效率詳細信息的報告，蘇珊應該要求什麼作為後續行動，為什麼？

A. SOC 2 類型 II 報告，因為類型 I 不涵蓋運營有效性

B. SOC 1 類型 I 報告，因為 SOC 2 不涵蓋運營有效性

C. SOC 2 Type I 報告，因為 SOC 2 Type II 不涵蓋運營有效性

D. SOC 3 報告，因為 SOC 1 和 SOC 2 報告已過時

你回答正確！

正確回答這個問題的關鍵是理解 SOC 1 和 SOC 2 報告以及 I 類和 II 類

審計之間的區別。SOC 1 報告涵蓋財務報告，SOC 2 報告著眼於安全 。

I 類審計僅涵蓋一個時間點，並且基於管理對控制的描述。它們不包括對

運營效率的評估。II 類審計涵蓋一段時間，並且確實包括對運營有效性的評估。

問題 17

tb787631.CISSPPT3E.c06.093

Henry 想驗證他的備份是否正常工作。以下哪個選項是他確保備份在真正的災難恢復場景中有用的最佳方式？

A. 定期恢復隨機文件以確保備份有效。
B. 定期檢查配置和設置以驗證備份設置。
C. 查看備份日誌以確保沒有錯誤發生。
D. 定期從備份執行完全恢復以驗證其成功。

你回答正確！

所有這些都是備份策略的有用部分，但定期從備份執行完全恢復是列出的最佳選擇。如果常規恢復有效，那麼單個文件將是可恢復的，但單個文件可能不會顯示更大的備份問題。配置和設置審查很重要，但不會驗證備份本身，錯誤消息可以指示問題，但也不會顯示完整的日誌。

問題 18

tb787631.CISSPPT3E.c06.033

STRIDE，代表欺騙、篡改、否認、信息洩露、拒絕服務、特權提升，在應用程序威脅建模的哪個部分有用？

A. 脆弱性評估
B. 誤用案例測試
C. 威脅分類
D. 滲透測試計劃

您回答錯誤。

應用程序威脅建模的一個重要部分是威脅分類。它有助於評估影響應該實施的控制的攻擊者目標。其他答案都涉及不直接屬於應用程序威脅建模的主題。

問題 19

tb787631.CISSPPT3E.c06.095

Jacinda 希望將她的安全培訓的有效性作為她的安全指標之一來衡量。以下哪項措施最有助於評估安全意識培訓的有效性？（選擇所有符合條件的。）

A. 有多少人參加了培訓
B. 培訓前後的安全意識水平
C. 培訓時長
D. 今年每個人參加的培訓活動數量

您回答錯誤。

參加給定培訓的員工人數以及從培訓前到培訓後他們的意識的平均變化可

以讓您深入了解您有多少受過培訓的員工以及培訓的影響力。隨著時間的

推移，這將使您能夠確定您的培訓是否有幫助以及意識是否正在提高。培

訓的長度不評估其影響；此外，每個人參加的活動數量並不意味著工作人

員的意識越來越強。

問題 20

tb787631.CISSPPT3E.c06.022

在使用 nmap 進行端口掃描期間，Joseph 發現系統顯示兩個端口打開，這讓他立即擔心：

- 21/打開
- 23/打開

哪些服務可能在這些端口上運行？

A. SSH 和 FTP

B、FTP 和 Telnet

C. SMTP 和 Telnet

D. POP3 和 SMTP

你回答正確！

Joseph 可能會驚訝地發現在他的網絡上打開了 FTP（TCP 端口 21）和 Telnet（TCP 端口 23），因為這兩種服務都未加密，並且在很大程度上已被 SSH、SCP 或 SFTP 取代。SSH 使用端口 22，SMTP 使用端口 25，POP3 使用端口 110。

問題 21

tb787631.CISSPPT3E.c06.010

在無線網絡滲透測試期間，Susan 使用密碼文件對網絡運行 aircrack-ng。什麼可能導致她的密碼破解工作失敗？

A.使用 WPA2 加密
B. 在企業模式下運行 WPA2
C. 使用 WEP 加密
D. 在 PSK 模式下運行 WPA2

你回答正確！

WPA2 企業對用戶使用 RADIUS 身份驗證而不是預共享密鑰。這意味著密碼攻擊更有可能失敗，因為給定用戶的密碼嘗試可能會導致帳戶鎖定。

WPA2 加密不會阻止密碼攻擊，並且 WPA2 的預共享密鑰模式專門針對

試圖找到密鑰的密碼攻擊。WEP 加密不僅已經過時，而且還經常可以通

過 aircrack-ng 等工具快速破解。

問題 22

tb787631.CISSPPT3E.c06.082

Ryan 正在考慮在他的 Web 應用程序測試程序中使用模糊測試。Ryan 在做出決定時應該考慮以下關於模糊測試的哪一項陳述？

A. Fuzzer 只能發現複雜的故障。

B. 測試人員必須手動生成輸入。

C. Fuzzer 可能無法完全覆蓋代碼。

D. Fuzzer 無法重現錯誤。

你回答正確！

模糊測試器能夠自動生成輸入序列來測試應用程序。因此，測試人員不需

要手動生成輸入，儘管他們可以根據需要這樣做。模糊器可以重現錯誤

（因此，“模糊器無法重現錯誤”不是問題）但通常不會完全覆蓋代碼——

代碼覆蓋工具通常與模糊器配對以驗證可能的覆蓋範圍。模糊器通常僅限

於簡單的錯誤，因為它們不會處理需要應用程序用戶知識的業務邏輯或攻擊。

問題 23

tb787631.CISSPPT3E.c06.005

Alex 想使用自動化工具填寫 Web 應用程序表單以測試格式字符串漏洞。他應該使用什麼類型的工具？

A、黑匣子

B. 暴力破解工具

C. 一個模糊器

D. 靜態分析工具

你回答正確！

Fuzzer 是旨在向應用程序提供無效或意外輸入、測試格式字符串漏洞、緩衝區溢出問題和其他問題等漏洞的工具。靜態分析依賴於在不運行應用程序或代碼的情況下檢查代碼，因此不會將表單填寫為 Web 應用程序的一部分。蠻力工具試圖通過嘗試密碼或其他值的所有可能組合來繞過安全保護。黑匣子是一種滲透測試，測試人員對環境一無所知。

問題 24

tb787631.CISSPPT3E.c06.052

以下哪項不是與滲透測試相關的危害？

A. 應用程序崩潰
B. 拒絕服務
C. 停電
D. 數據損壞

你回答正確！

滲透測試通常不涉及停電。應用程序崩潰；由於系統、網絡或應用程序故障而導致的拒絕服務；甚至數據損壞都可能是滲透測試的危害。

問題 25

tb787631.CISSPPT3E.c06.016

Jim 已簽約進行灰盒滲透測試，他的客戶向他提供了有關其網絡的以下信息，以便他可以掃描它們：

- 數據中心：10.10.10.0/24
- 銷售：10.10.11.0/24
- 賬單：10.10.12.0/24
- 無線：192.168.0.0/16

如果吉姆受約在場外進行掃描，他會遇到什麼問題？

A. IP 範圍太大，無法有效掃描。

B. 無法掃描提供的 IP 地址。

C. IP 範圍重疊，會導致掃描問題。

D. 提供的 IP 地址是 RFC 1918 地址。

您回答錯誤。

他的客戶提供的 IP 地址是 RFC 1918 不可路由的 IP 地址，Jim 將無法從場外掃描它們。為了成功完成滲透測試，他必須首先滲透他們的網絡邊界，或者在他們的網絡中放置一台機器從內部進行掃描。IP 地址重疊並不是掃描的真正問題，當前掃描系統可以輕鬆處理這些範圍。

問題 26

tb787631.CISSPPT3E.c06.008

Jim 已簽約對一家銀行的主要分行進行滲透測試。為了使測試盡可能真實，除了銀行的名稱和地址之外，他沒有得到任何關於銀行的信息。Jim 同意執行哪種類型的滲透測試？

A. 水晶盒滲透測試

B. 灰盒滲透測試

C. 黑盒滲透測試

D. 白盒滲透測試

你回答正確！

Jim 已同意進行黑盒滲透測試，該測試不提供有關組織、其係統或防禦的信息。水晶或白盒滲透測試提供了攻擊者需要的所有信息，而灰盒滲透測試提供了部分但不是全部信息。

問題 27

tb787631.CISSPPT3E.c06.030

什麼被動監控技術記錄所有用戶與應用程序或網站的交互以確保質量和性能？

A. 客戶端/服務器測試

B.真實用戶監控

C.綜合用戶監控

D. 被動用戶記錄

您回答錯誤。

真實用戶監控 (RUM) 是一種被動監控技術，它記錄用戶與應用程序或系統的交互，以確保性能和正確的應用程序行為。RUM 通常用作使用實際用戶界面的預部署過程的一部分。其他的答案都是編出來的——綜合監控

使用的是模擬行為，但是綜合用戶監控不是一種測試方法。同樣，被動監

控監控實際流量，但被動用戶記錄不是行業術語或技術。客戶端/服務器

測試僅僅描述了一種可能的架構。

問題 28

tb787631.CISSPPT3E.c06.070

Frank 的團隊正在測試他公司的開發人員為他們的應用程序基礎架構構建的新 API。以下哪項不是您希望 Frank 的團隊發現的常見 API 問題？

A. 加密不當

B.對象級授權問題

C. 用戶認證問題

D. 缺乏速率限制

你回答正確！

API 通常通過 HTTPS 為 Web 應用程序傳輸數據，這意味著 API 本身不

負責加密。如果 Frank 的團隊發現 TLS 未啟用，他們將需要與基礎架構

或系統管理團隊合作以確保 TLS 已啟用並在使用中，而不是進行 API 更

改。對象訪問授權、身份驗證弱點和速率限制都是常見的 API 問題。如

果您不熟悉 API 中可能遇到的問題類型，可以在 OWASP API 安全性前

10 名中閱讀更多相關信息，網址為 github.com/OWASP/API-

Security/blob/master/2019/en/dist /owasp-api-security-

top-10.pdf。

問題 29

tb787631.CISSPPT3E.c06.035

Paul 正在審查滲透測試的批准流程，並希望確保它有適當的管理審查。他應該確保誰批准了對業務系統進行滲透測試的請求？

A. 變革諮詢委員會

B、高級管理人員

C. 系統管理員

D. 服務所有者

你回答正確！

在大多數組織中，由於組織面臨的風險和測試的潛在影響，高級管理層需

要批准滲透測試。在少數組織中，服務所有者可能能夠做出此決定，但滲

透測試通常比單一服務具有更廣泛的影響，這意味著高級管理人員是正確

的途徑。變更諮詢委員會批准變更，而不是滲透測試，系統管理員可能會

被告知測試，但在大多數組織中沒有權力簽署滲透測試。

問題 30

tb787631.CISSPPT3E.c06.004

網絡設備、Linux 和 Unix 系統以及許多其他企業設備通常使用什麼消息記錄標準？

A. 系統日誌
B. 網絡日誌
C. 事件日誌
D. 遠程日誌協議 (RLP)

你回答正確！

Syslog 是一種廣泛用於事件和消息記錄的協議。Eventlog、netlog 和

Remote Log Protocol 都是虛構的術語。

問題 31

tb787631.CISSPPT3E.c06.023

Aaron 想驗證他是否符合 PCI-DSS。他的公司是一家大型商業機構，每年的交易額達數百萬美元。對大型組織進行此類測試的最常用方法是什麼？

A. 自我評估

B. 使用 COBIT 進行三十方評估

C. 與另一家公司合作並在組織之間進行貿易評估

D. 使用合格的安全評估員進行第三方評估

你回答正確！

大型組織聘請 QSA 或合格的安全評估員來執行合規性檢查。PCI-DSS

要求大型組織進行第三方認證，但小型組織可以自行認證。

第 32 題

tb787631.CISSPPT3E.c06.002

以下哪項是用於自動設計新軟件測試並確保測試質量的方法？

A. 代碼審計

B. 靜態代碼分析

C. 回歸測試

D. 突變測試

你回答正確！

突變測試以小的方式修改程序，然後測試該突變以確定它的行為是否正常

或是否失敗。該技術用於通過變異來設計和測試軟件測試。靜態代碼分析

和回歸測試都是測試代碼的手段，而代碼審計是對源代碼的分析，而不是

設計和測試軟件測試的手段。

問題 33

tb787631.CISSPPT3E.c06.062

請參考以下場景：

- 蘇珊是她公司質量保證團隊的負責人。該團隊的任務是測試他們公司核心軟件產品的主要版本。

Susan 的軟件測試人員團隊需要測試每個代碼路徑，包括那些僅在出現錯誤情況時才會使用的代碼路徑。她的團隊需要什麼類型的測試環境來確保完整的代碼覆蓋率？

A、白框

B、灰盒

C、黑匣子

D、動態

你回答正確！

要全面測試代碼，需要進行白盒測試。如果沒有代碼的完全可見性，錯誤

條件或其他代碼可能會被遺漏，從而使灰盒或黑盒測試成為不合適的解決

方案。使用針對實時代碼運行的動態測試還可能導致某些情況被遺漏，因為代碼部分未暴露給典型用法。

第 34 題

tb787631.CISSPPT3E.c06.071

Jim 正在與一家滲透測試承包商合作，該承包商建議使用 Metasploit 作為她滲透測試工作的一部分。當使用 Metasploit 時，Jim 應該期望發生什麼？

A. 將對系統進行漏洞掃描。

B. 系統將有已知漏洞被利用。

C. 將探測服務是否存在緩衝區溢出和其他未知缺陷。

D. 系統將針對零日攻擊進行測試。

你回答正確！

Metasploit 是一個開發包，旨在幫助滲透測試人員。使用 Metasploit 的測試人員可以利用已創建漏洞利用的已知漏洞，也可以使用該工具創建自己的漏洞利用。雖然 Metasploit 提供對某些漏洞掃描功能的內置訪問，但應該期望使用 Metasploit 的測試人員主要執行可利用漏洞的實際測試。

同樣，Metasploit 支持創建緩衝區溢出攻擊，但它不是專門構建的緩衝

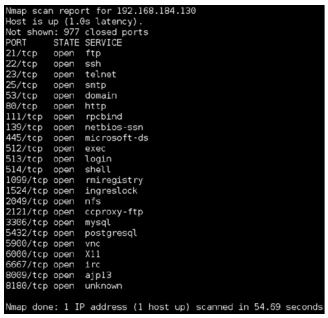
區溢出測試工具，當然，除非已發布，否則測試零日漏洞利用的系統將不

起作用。

問題 35

tb787631.CISSPPT3E.c06.085

請參考以下場景。在端口掃描期間，Ben 使用 nmap 的默認設置並看到以下結果。



根據掃描結果，被掃描的系統最有可能運行的是什麼操作系統 (OS)？

A. Windows 桌面

B、Linux

C、網絡設備

D、視窗服務器

你回答正確！

該系統很可能是 Linux 系統。系統顯示 X11，以及登錄、shell 和 nfs 端口，所有這些在 Linux 系統上比在 Windows 系統或網絡設備上更常見。該系統的安全性也很差；在其上運行的許多服務不應暴露在現代安全網絡中。

問題 36

tb787631.CISSPPT3E.c06.021

在滲透測試期間，Michelle 需要識別系統，但她沒有獲得對她用來生成原始數據包的系統的足夠訪問權限。她應該運行哪種類型的掃描來驗證最開放的服務？

A. TCP 連接掃描
B. TCP SYN 掃描
C. UDP 掃描
D. ICMP 掃描

您回答錯誤。

當測試人員沒有原始數據包創建權限時，例如當他們沒有在受感染主機上升級權限時，可以使用 TCP 連接掃描。由於需要寫入原始數據包，TCP SYN 掃描需要在大多數 Linux 系統上提升權限。UDP 掃描將錯過大多數

通過 TCP 提供的服務，而 ICMP 只是對響應 ping 的系統進行 ping 掃描 ，

根本不會識別服務。

問題 37

tb787631.CISSPPT3E.c06.038

Susan 需要為她的組織預測高風險區域，並希望在風險趨勢發生時使用指標來評估它們。她該怎麼辦？

A. 進行年度風險評估。

B. 聘請滲透測試公司定期測試組織安全。

C. 識別和跟踪關鍵風險指標。

D. 使用 SIEM 設備監控日誌和事件。

您回答錯誤。

關鍵風險指標用於告訴負責風險管理的人員一項活動的風險有多大，以及

變化對該風險狀況的影響有多大。識別關鍵風險指標並對其進行監控有助

於在其生命週期的早期識別高風險區域。年度風險評估可能是個好主意，

但只能提供時間點視圖，而滲透測試可能會錯過與安全不直接相關的風險 。

使用 SIEM 設備監控日誌和事件有助於檢測問題的發生，但不一定會顯

示風險趨勢。

問題 38

tb787631.CISSPPT3E.c06.061

以下哪種類型的代碼審查通常不是由人工執行的？

A. 軟件檢查

B.結對編程

C. 靜態程序分析

D. 軟件演練

你回答正確！

靜態程序審查通常由自動化工具執行。程序理解、程序理解、結對編程、

軟件檢查和軟件演練都是以人為中心的代碼審查方法。

第 39 題

tb787631.CISSPPT3E.c06.063

請參考以下場景：

- 蘇珊是她公司質量保證團隊的負責人。該團隊的任務是測試他們公司核心軟件產品的主要版本。

作為新應用程序持續測試的一部分，Susan 的質量保證團隊為一系列黑盒測試設計了一組測試用例。然後運行這些功能測試，並準備一份報告來解釋發生了什麼。在此測試期間通常會生成哪種類型的報告來指示測試指標？

A. 測試覆蓋率報告

B. 滲透測試報告

C. 代碼覆蓋率報告

D. 線路覆蓋報告

你回答正確！

測試覆蓋率報告衡量已經完成了多少測試用例，並用作在使用測試用例時提供測試指標的一種方式。進行滲透測試時會提供滲透測試報告——這不是滲透測試。代碼覆蓋率報告涵蓋了多少代碼已經過測試，行覆蓋率報告是一種代碼覆蓋率報告。

問題 40

tb787631.CISSPPT3E.c06.024

通常使用什麼方法來評估軟件測試覆蓋應用程序潛在用途的程度？

A. 測試覆蓋率分析

B. 源代碼審查

C.模糊分析

D. 代碼審查報告

您回答錯誤。

測試覆蓋率分析通常用於深入了解測試覆蓋應用程序正在測試的用例集的

程度。源代碼審查著眼於程序代碼中的錯誤，不一定是用例分析，而模糊

測試則測試無效輸入。代碼審查報告可能會作為源代碼審查的一部分生成 。

問題 41

tb787631.CISSPPT3E.c06.027

Derek 希望確保他的組織在帳戶的整個生命週期中跟踪帳戶的所有更改。他應該為他的組織投資什麼類型的工具？

A. 像 LDAP 這樣的目錄服務

B. IAM 系統

C. SIEM

D. EDR 系統

您回答錯誤。

身份和訪問管理 (IAM) 系統結合了生命週期管理和監控工具，以確保在

整個組織中正確處理身份和授權。Derek 應該投資一個功能強大的 IAM

系統，並確保將其配置為使用適當的工作流並生成他需要的日誌和報告 。

EDR 系統是端點檢測和響應工具，用於防止高級攻擊者的破壞。

問題 42

tb787631.CISSPPT3E.c06.026

什麼類型的監控使用網站的模擬流量來監控性能？

A、日誌分析

B. 綜合監測

C. 被動監測

D. 模擬交易分析

您回答錯誤。

綜合監控使用模擬或記錄的事務來監控響應時間、功能或其他性能監視器

的性能變化。被動監控使用跨端口或其他方法複製流量並實時監控。日誌

分析通常針對實際日誌數據執行，但也可以針對模擬流量執行以識別問題 。

模擬交易分析不是行業術語。

問題 43

tb787631.CISSPPT3E.c06.065

Robin 最近進行了一次漏洞掃描，並在處理敏感信息的服務器上發現了一個嚴重漏洞。羅賓接下來應該做什麼？

A. 打補丁
B. 報告
C. 整治
D. 驗證

您回答錯誤。

一旦漏洞掃描程序識別出潛在問題，就需要進行驗證以驗證該問題是否存

在。一旦漏洞得到確認，就可以進行報告、修補或其他補救措施。

問題 44

tb787631.CISSPPT3E.c06.015

莫妮卡想要收集有關其組織中安全意識的信息。什麼技術最常用於評估安全意識？

A. 網絡釣魚模擬器
B. 遊戲化應用
C. 評估測試
D. 調查

您回答錯誤。

大多數組織使用調查來評估安全意識。網絡釣魚模擬器也經常使用，但只測試對網絡釣魚問題和技術的認識，而不是一般的安全意識。遊戲化應用程序越來越受歡迎，但調查的易用性和可用性使其成為最受歡迎的應用程序。最後，當需要合規知識評估以滿足特定標準時，可以使用評估測試，但測試不像調查那樣普遍。

問題 45

tb787631.CISSPPT3E.c06.080

請參考以下場景：

- Ben 的組織已開始使用 STRIDE 來評估其軟件，並確定了威脅代理和這些威脅可能產生的業務影響。現在他們正在努力為他們發現的問題確定適當的控制措施。

由於拒絕服務攻擊期間的流量，Ben 希望使用第三方服務來幫助評估拒絕服務攻擊漏洞。他應該向他的組織建議什麼類型的參與？

A. 社會工程參與

B. 滲透測試

C. 負載或壓力測試

D. 使用模糊器進行測試

你回答正確！

Ben 應該聘請一家可以執行負載或壓力測試的公司來驗證應用程序在預

期負載和極端負載下的性能，以便他了解基於負載的拒絕服務攻擊會是什

麼樣子。社會工程不會測試站點處理負載的能力，滲透測試人員可能會進

行拒絕服務攻擊，但通常不會。模糊器發送隨機輸入來測試應用程序如何

處理意外輸入，而不是依賴於極端負載。它們可能有助於測試可能導致拒

絕服務情況的缺陷，但該問題專門詢問基於負載的情況，而不是軟件缺陷。

問題 46

tb787631.CISSPPT3E.c06.046

以下哪項不是軟件測試過程中通常要測試的接口？

A. 原料藥

B. 網絡接口

C. 用戶界面

D. 物理接口

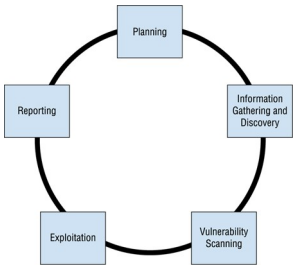
您回答錯誤。

在執行軟件測試時，應用程序編程接口 (API)、用戶界面 (UI) 和物理接口都是重要的測試對象。網絡接口不是軟件測試中測試的典型接口列表的一部分。

問題 47

tb787631.CISSPPT3E.c06.041

請參考以下場景。Chris 使用此處所示的標準滲透測試方法。使用此方法和您的滲透測試知識來回答有關滲透測試期間工具使用的問題。



在發現過程中最有可能使用以下哪種工具？

A. Nessus

B.約翰

C、Nmap

D、沒人

你回答正確！

發現可以包括主動發現和被動發現。端口掃描通常在發現期間進行，以評估目標提供的服務，nmap 是用於此目的的最流行的工具之一。Nessus

和 Nikto 可能在漏洞掃描階段使用，密碼破解器 john 可用於在利用階段

恢復密碼。

問題 48

tb787631.CISSPPT3E.c06.088

Diana 聘請了第三方審計員，並希望向第三方發布審計證明，但不包括審計細節。她應該請求哪種類型的 SSAE 18 SOC 報告？

A.SOC 1

B、SOC 2

C、SOC 3

D.SOC 4

你回答正確！

Diana 應索取 SOC 3 報告，該報告旨在分發給第三方。它們包括審計員

的意見和管理斷言，以及有關服務組織的信息。SOC3 報告專門用於外

部發布，這與 SOC 1（財務報告）和 SOC 2（機密安全和隱私）約定不

同。

問題 49

tb787631.CISSPPT3E.c06.060

Kelly 的團隊對他們發布的每個補丁進行回歸測試。他們應該維護哪些關鍵績效指標來衡量測試的有效性？

A.修復漏洞的時間

B. 缺陷復發率的度量

C. 加權風險趨勢

D. 衡量他們測試的具體覆蓋範圍

你回答正確！

Kelly’s team is using regression testing, which is intended to prevent the recurrence of issues. This means that measuring the rate of defect recurrence is an appropriate measure for their work. Time to remediate vulnerabilities is associated with activities like patching, rather than preparing the patch, whereas a weighted risk trend is used to measure risk over time to an organization. Finally, specific coverage may be useful to determine if they are fully testing their effort, but regression testing is more specifically covered by defect recurrence rates.

Question 50

tb787631.CISSPPT3E.c06.079

Please refer to the following scenario:

- Ben’s organization has begun to use STRIDE to assess its software and has identified threat agents and the business impacts that these threats could have. Now they are working to identify appropriate controls for the issues they have identified.

Ben’s team is attempting to categorize a transaction identification issue that is caused by use of a symmetric key shared by multiple servers. What STRIDE category should this fall into?

A. Information disclosure

B. Denial of service

C. Tampering

D. Repudiation

You Answered Incorrectly.

Since a shared symmetric key could be used by any of the servers, transaction identification problems caused by a shared key are likely to involve a repudiation issue. If encrypted transactions cannot be uniquely

identified by a server, they cannot be proved to have come from a specific server.

Question 51

tb787631.CISSPPT3E.c06.007

Morgan 正在實施一個漏洞管理系統，該系統使用基於標準的組件對其發現的漏洞進行評分和評估。以下哪項最常用於提供漏洞的嚴重性評分？

A、CCE

B、CVSS

C、持續專業教育

D. 橢圓形

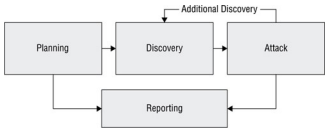
你回答正確！

CVSS，Common Vulnerability Scoring System，用於描述安全漏洞的嚴重程度。CCE 是 Common Configuration Enumeration，一種針對配置問題的命名系統。CPE 是 Common Platform Enumeration，它命名操作系統、應用程序和設備。OVAL 是一種描述安全測試過程的語言。

問題 52

tb787631.CISSPPT3E.c06.097

請參考以下場景。NIST 特別出版物 800-115，信息安全測試和評估技術指南，提供了 NIST 的滲透測試流程。使用此圖像以及您的滲透測試知識來回答問題。



資料來源：NIST SP 800-115。

以下哪項不是發現階段的一部分？

A.主機名和 IP 地址信息收集

B. 服務信息抓取

C. 垃圾箱潛水

D. 權限提升

你回答正確！

權限升級發生在滲透測試的攻擊階段。主機和服務信息收集，以及垃圾箱挖掘等可以提供有關組織、其係統和安全信息的活動，都是發現階段的一部分。

問題 53

tb787631.CISSPPT3E.c06.058

Jim 正在幫助他的組織決定在整個國際組織中使用的審計標準。以下哪一項不是 Jim 的組織可能在其審計中使用的 IT 標準？

A.COBIT

B. SSAE-18

C、ITIL

D. ISO 27001

您回答錯誤。

ITIL 最初代表 IT Infrastructure Library，是一套 IT 服務管理實踐，通常不用於審計。COBIT，或信息和相關技術的控制目標，ISO 27001 和 SSAE-18，或第 18 號鑑證業務標準聲明，都用於審計。

問題 54

tb787631.CISSPPT3E.c06.001

在端口掃描期間，Susan 發現一個系統在 TCP、UDP 137–139 和 TCP 445 以及 TCP 1433 上運行服務。如果她連接到機器，她可能會找到什麼類型的系統？

A. Linux 電子郵件服務器

B. Windows SQL 服務器

C. 一個 Linux 文件服務器

D. Windows 工作站

你回答正確！

TCP 和 UDP 端口 137–139 用於 NetBIOS 服務，而 445 用於 Active

Directory。TCP 1433 是 Microsoft SQL 的默認端口，表明這可能是提供

SQL 服務的 Windows 服務器。

問題 55

tb787631.CISSPPT3E.c06.034

為什麼除了實施無線入侵檢測系統等無線安全技術外還要進行被動掃描？

A. 它可以幫助識別惡意設備。

B. 可以通過腳本攻擊來測試無線網絡的安全性。

C. 它們在每個無線信道上停留的時間很短，可以讓它們捕獲更多的數據包。

D. 他們可以幫助測試無線 IDS 或 IPS 系統。

你回答正確！

被動掃描可以通過捕獲與已部署設備不匹配的 MAC 地址供應

商 ID、通過硬件地址驗證系統是否與組織擁有的硬件清單相匹

配以及通過監控惡意 SSID 或連接來幫助識別惡意設備。

腳本攻擊是主動掃描的一部分，而不是被動掃描，主動掃描對測

試 IDS 或 IPS 系統很有用，而被動掃描不會被檢測系統檢測到 。

最後，較短的駐留時間實際上可能會錯過麻煩的流量，因此平衡

駐留時間與覆蓋範圍對於被動無線掃描工作是必要的。

問題 56

tb787631.CISSPPT3E.c06.076

在查看訪問日誌期間，亞歷克斯注意到米歇爾每天早上 8 點登錄她在紐約的工作站，但她被記錄為每天凌晨 3 點後不久登錄她所在部門的主要 Web 應用程序。Alex 可能遇到過哪些常見的日誌記錄問題？

A. 日誌格式不一致

B.修改日誌

C. 不一致的時間戳

D. 多個日誌源

你回答正確！

Inconsistent timestamps are a common problem, often caused by

improperly set time zones or due to differences in how system clocks are

set. In this case, a consistent time difference often indicates that one system uses local time, and the other is using Greenwich mean time (GMT). Logs from multiple sources tend to cause problems with centralization and collection, whereas different log formats can create challenges in parsing log data. Finally, modified logs are often a sign of intrusion or malicious intent.

Question 57

tb787631.CISSPPT3E.c06.003

During a port scan, Naomi found TCP port 443 open on a system. Which tool is best suited to scanning the service that is most likely running on that port?

A. zzuf
B. Nikto
C. Metasploit
D. sqlmap

You Answered Correctly!

TCP 端口 443 通常表示 HTTPS 服務器。Nikto 可用於漏洞掃描 Web 服務器和應用程序，是列出的 Web 服務器的最佳選擇。Metasploit 包括一些掃描功能，但不是專門用於漏洞掃描的工具。zzuf 是一個模糊測試工具，與漏洞掃描無關，而 sqlmap 是一個 SQL 注入測試工具。

問題 58

tb787631.CISSPPT3E.c06.099

請參考以下場景。NIST 特別出版物 800-115，信息安全測試和評估技術指南，提供了 NIST 的滲透測試流程。使用此圖像以及您的滲透測試知識來回答問題。

資料來源：NIST SP 800-115。

以下哪項不是滲透測試報告的典型部分？

A. 已識別漏洞列表

B. 測試期間收集的所有敏感數據

C. 對發現的每個問題的風險評級

D. 針對已查明問題的緩解指南

您回答錯誤。

滲透測試報告通常不包括評估期間捕獲的特定數據，因為報告的讀者可能

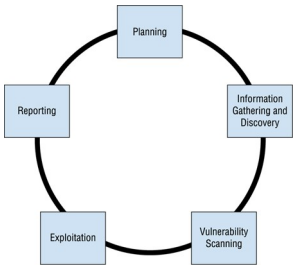
未被授權訪問所有數據，並且報告的暴露可能會給組織帶來額外的問題。

發現的問題列表、風險評級和補救指南都是滲透測試報告的常見部分。

問題 59

tb787631.CISSPPT3E.c06.042

請參考以下場景。Chris 使用此處所示的標準滲透測試方法。使用此方法和您的滲透測試知識來回答有關滲透測試期間工具使用的問題。



為了確保報告階段不會出現問題，在計劃期間解決這些問題中的哪一個是最重要的？

A. 使用哪種 CVE 格式

B. 漏洞數據將如何存儲和發送

C. 哪些目標是禁區

D. 報告應該有多長

你回答正確！

滲透測試報告通常包含的信息如果被意外洩露或被盜，可能會導致額外的

暴露。因此，確定漏洞數據的存儲和發送方式至關重要。越界目標的問題

更有可能導致漏洞評估和利用階段出現問題，報告的長度不應受到限制，

而應與實現測試目標所需的長度保持一致。

問題 60

tb787631.CISSPPT3E.c06.068

在對他的網絡進行端口掃描期間，亞歷克斯發現他所在組織的辦公室中有許多主機在 TCP 端口 80、443、515 和 9100 上響應。Alex 可能會發現什麼類型的設備？

A. 網絡服務器

B、文件服務器

C. 無線接入點

D. 打印機

你回答正確！

啟用網絡的打印機通常通過 TCP 515 和 9100 提供服務，並且在 TCP

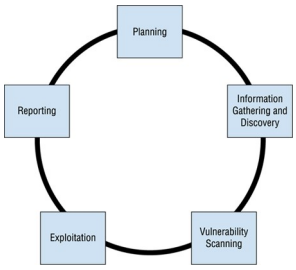
80 和 443 上具有非安全和安全的啟用 Web 的管理界面。Web 服務器、

訪問點和文件服務器通常不會在 LPR 和 LPD 端口上提供服務（515 和 9100）。

問題 61

tb787631.CISSPPT3E.c06.040

請參考以下場景。Chris 使用此處所示的標準滲透測試方法。使用此方法和您的滲透測試知識來回答有關滲透測試期間工具使用的問題。



在第 1 階段（規劃）中什麼任務最重要？

A. 建立測試實驗室

B. 獲得授權

C. 收集適當的工具

D. 確定測試是白盒、黑盒還是灰盒

你回答正確！

獲得授權是規劃階段最關鍵的因素。許可和“出獄卡”表明組織領導層意識到滲透測試可能導致的問題，是任何滲透測試的第一步。收集工具和建立

實驗室，以及確定將進行何種類型的測試，都很重要，但未經許可不得發

生任何事情。

第 62 題

tb787631.CISSPPT3E.c06.056

如果 Kara 主要關心的是阻止與服務器的管理連接，那麼她應該阻止哪個端口？

A.22

B. 80

C.443

D. 1433

你回答正確！

安全外殼 (SSH) 協議使用端口 22 進行管理連接。如果 Kara 想要限制管

理連接，她應該阻止對該端口的訪問。

問題 63

tb787631.CISSPPT3E.c06.036

什麼術語描述了旨在發現補丁或配置更改引入的新錯誤的軟件測試？

A. 非回歸測試

B. 進化測試

C. 冒煙測試

D. 回歸測試

您回答錯誤。

回歸測試是一種功能或單元測試，用於確保更改沒有引入新問題的測試。

非回歸測試檢查更改是否產生了預期的效果，冒煙測試側重於對關鍵功能

有影響的簡單問題，而進化測試不是一種軟件測試技術。

第 64 題

tb787631.CISSPPT3E.c06.075

Windows 系統重啟時，會生成什麼類型的日誌？

A、錯誤

B. 警告

三、信息

D. 故障審核

您回答錯誤。

重新啟動 Windows 機器會產生一個信息日誌條目。Windows 定義了五

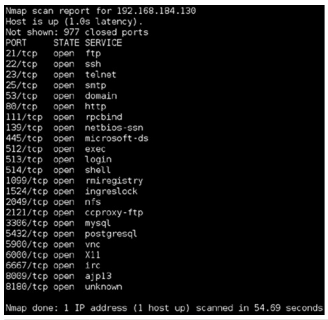
種類型的事件：錯誤，表示重大問題；警告，可能表明未來的問題；描述

成功操作的信息；成功審計，記錄成功的安全訪問；和失敗審計，記錄失敗的安全訪問嘗試。

問題 65

tb787631.CISSPPT3E.c06.084

請參考以下場景。在端口掃描期間，Ben 使用 nmap 的默認設置並看到以下結果。



如果 Ben 正在進行滲透測試，他在收到這些結果後下一步應該做什麼？

A. 使用網絡瀏覽器連接到網絡服務器。

B. 通過 Telnet 連接以測試易受攻擊的帳戶。

C. 確定感興趣的端口以進行進一步掃描。

D. 對打開的數據庫使用 sqlmap。

你回答正確！

在使用 nmap 等端口掃描工具掃描開放端口後，滲透測試人員將識別感興趣的端口，然後進行漏洞掃描以確定哪些服務可能存在漏洞。這將執行

許多與通過 Web 服務器連接相同的活動，並且通常比嘗試通過 Telnet

手動測試易受攻擊的帳戶更有用。sqlmap 通常會在漏洞掃描程序識別出

有關服務的附加信息後使用，並且漏洞掃描程序通常會提供範圍更廣的有

用信息。

第 66 題

tb787631.CISSPPT3E.c06.011

在一個工作日中途，流行的 Apache Web 服務器出現了一個零日漏洞。作為一名信息安全分析師，Jacob 需要快速掃描他的網絡以確定哪些服務器容易受到問題的影響。Jacob 快速識別易受攻擊系統的最佳途徑是什麼？

A. 立即對所有服務器運行 Nessus 以確定哪些系統易受攻擊。

B.查看 CVE 數據庫，查找漏洞信息和補丁信息。

C. 創建自定義 IDS 或 IPS 簽名。

D. 識別受影響的版本並使用自動掃描儀檢查該版本號的系統。

您回答錯誤。

在許多情況下，當最初報告漏洞利用時，沒有針對漏洞掃描程序的預置簽

名或檢測，並且 CVE 數據庫可能不會立即獲得有關攻擊的信息。Jacob

的最佳選擇是快速收集信息並根據當前配置檢查可能存在漏洞的服務器。

隨著更多信息可用，簽名和 CVE 信息可能會被發布。不幸的是，對於

Jacob 而言，IDS 和 IPS 簽名只能檢測攻擊，而不會檢測系統是否易受

攻擊，除非他看到系統正在被利用。

問題 67

tb787631.CISSPPT3E.c06.043

在驗證代碼測試套件的工作時，通常使用哪四種類型的覆蓋標準？

A. 輸入、語句、分支和條件覆蓋
B. 函數、語句、分支和條件覆蓋
C. API、分支、邊界和條件覆蓋
D. 邊界、分支、循環和條件覆蓋

你回答正確！

代碼覆蓋率測試最頻繁地要求調用每個函數，執行每個語句，充分探索所

有分支，並且評估每個條件的所有可能性。API、輸入和循環測試不是常

見類型的代碼覆蓋測試措施。

第 68 題

tb787631.CISSPPT3E.c06.012

使用什麼類型的測試來確保單獨開發的軟件模塊正確交換數據？

A. 模糊測試

B、動態測試

C、接口測試

D. API 校驗和

你回答正確！

接口測試用於確保軟件模塊正確地滿足接口規範，從而正確地交換數據。

動態測試在運行環境中測試軟件，而模糊測試是一種動態測試，它將無效

輸入提供給正在運行的軟件以測試錯誤和輸入處理。API 校驗和不是測

試技術。

第 69 題

tb787631.CISSPPT3E.c06.064

請參考以下場景：

- 蘇珊是她公司質量保證團隊的負責人。該團隊的任務是測試他們公司核心軟件產品的主要版本。

作為代碼覆蓋率測試的一部分，Susan 的團隊使用日誌記錄和跟踪工具在非生產環境中運行分析。由於運行環境的這種變化，以下哪種類型的代碼問題最有可能在測試過程中被遺漏？

A. 邊界檢查不當

B. 輸入驗證

C. 競爭條件

D. 指針操作

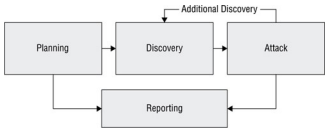
你回答正確！

在代碼中插入儀器的測試環境和代碼的生產環境的變化可以掩蓋與時間相關的問題，如競爭條件。邊界檢查、輸入驗證和指針操作都與編碼問題相關，而不是環境問題，並且更有可能在測試環境中被發現。

第 70 題

tb787631.CISSPPT3E.c06.098

請參考以下場景。NIST 特別出版物 800-115，信息安全測試和評估技術指南，提供了 NIST 的滲透測試流程。使用此圖像以及您的滲透測試知識來回答問題。



資料來源：NIST SP 800-115。

NIST 指定了四個攻擊階段步驟：獲取訪問權限、提升權限、系統瀏覽和安裝其他工具。一旦攻擊者安裝了額外的工具，滲透測試人員通常會回到哪個階段？

A. 發現

B. 獲得訪問權

C. 提升權限

D、系統瀏覽

您回答錯誤。

一旦安裝了額外的工具，滲透測試人員通常會使用它們來獲得額外的訪問權限。他們可以從那裡進一步提升權限、搜索新目標或數據，並再次安裝更多工具，以允許他們進一步轉向基礎設施或系統。

第 71 題

tb787631.CISSPPT3E.c06.045

在查看日誌時，為所有用戶使用唯一的用戶 ID 提供什麼？

A. 保密

B. 誠信

C. 可用性

D. 問責制

您回答錯誤。

唯一的用戶 ID 與可審計的日誌配對時提供責任，以提供特定用戶採取的

任何給定操作。機密性、可用性和完整性可以通過其他方式提供，例如加

密、系統設計和數字簽名。

第 72 題

tb787631.CISSPPT3E.c06.087

Lucca 正在審查他的組織的災難恢復過程數據，並註意到公司主要網站的 MTD 是兩個小時。當他進行測試和驗證時，他對站點的 RTO 了解多少？

A. 需要少於兩個小時。

B. 至少需要兩個小時。

C. MTD 太短，需要更長。

D. RTO 太短，需要加長。

你回答正確！

當 Lucca 查看恢復時間目標 (RTO) 數據時，他需要確保根據兩小時的最

大可容忍停機時間 (MTD)，組織可以在不到兩小時的時間內從中斷中恢

復。

第 73 題

tb787631.CISSPPT3E.c06.091

Josh 公司的總裁擔心加密惡意軟件的顯著增加正在影響他們所在行業的其他公司。她已要求 John 確保公司的數據在惡意軟件攻擊並加密其生產系統時能夠恢復。Josh 需要執行什麼流程才能告訴她公司在承保範圍內？

A. 加密所有敏感數據。

B. 散列組織的所有數據以檢測加密惡意軟件。

C. 執行備份驗證。

D. 使用反加密技術來防止惡意軟件加密驅動器。

你回答正確！

Josh 的最佳答案是驗證組織是否擁有安全可用的備份。如果加密惡意軟件攻擊，最好的解決辦法是擁有您可以依賴的備份並且不會加密，這意味著系統分離並且可能需要進行版本控制，以便未加密的備份不會被加密的備份替換，因此無法訪問版本。加密敏感數據不會阻止攻擊者對其進行重新加密，從而使其無法訪問。散列法檢測攻擊不會阻止它或使恢復成為可能，並且反加密技術會執行選項建議不存在的操作。

第 74 題

tb787631.CISSPPT3E.c06.032

Angela 想要使用自動化工具測試 Web 瀏覽器對意外數據的處理能力。她應該選擇什麼工具？

A.Nmap

B.zzuf

C. Nessus

D、沒人

你回答正確！

zzuf 是列表中唯一的模糊器，zzuf 專門設計用於通過修改應用程序的網絡和文件輸入來與 Web 瀏覽器、圖像查看器和類似軟件等工具配合使用。

Nmap 是端口掃描器，Nessus 是漏洞掃描器，Nikto 是 Web 服務器掃描器。

第 75 題

tb787631.CISSPPT3E.c06.089

在查看其組織的新應用程序的軟件測試輸出時，Madhuri 注意到該應用程序產生了錯誤，其中包括向 Web 應用程序測試人員顯示的目錄和文件信息。她應該在關於申請的報告中包括什麼問題？

A. 它沒有執行正確的異常處理。

B. 軟件沒有正確處理誤用案例測試。

C.調試語句需要去掉。

D. 由於錯誤，代碼沒有經過全面測試。

您回答錯誤。

向最終用戶顯示有關代碼的錯誤信息，尤其是包含目錄和文件信息，意味著應用程序未執行正確的異常處理。應該以管理員可以處理的方式記錄或記錄錯誤，但最終用戶（和攻擊者！）不應該看到該信息。該軟件可能會正確處理誤用，因為該問題不會說明這是由於正常測試還是誤用測試引起的。沒有關於導致輸出的調試代碼的信息，問題中也沒有註明測試覆蓋率。

第 76 題

tb787631.CISSPPT3E.c06.081

Chris 正在解決其組織的 SIEM 報告問題。分析問題後，他認為不同系統的日誌條目的時間戳不一致。他可以使用什麼協議來解決這個問題？

A、SSH
B、FTP
C、TLS
D、NTP

你回答正確！

網絡時間協議 (NTP) 允許系統時鐘與標準化時間源同步。Secure Shell (SSH) 協議提供與服務器的加密管理連接。文件傳輸協議 (FTP) 用於數據交換。傳輸層安全性 (TLS) 是一種加密過程，用於保護通過網絡傳輸的信息。

第 77 題

tb787631.CISSPPT3E.c06.057

在第三方審核期間，Jim 的公司收到一份調查結果，其中指出：“管理員應每天檢查備份成功和失敗日誌，並及時採取措施解決報告的異常情況。” 這一發現表明什麼潛在問題？

A. 管理員不知道備份是成功還是失敗。
B. 備份可能沒有正確記錄。
C. 備份可能無法使用。
D. 備份日誌可能沒有被正確審查。

您回答錯誤。

審計結果表明備份管理員可能沒有監控備份日誌並根據他們報告的內容採

取適當的措施，從而導致備份可能無法使用。審查、記錄或了解備份成功

或失敗的問題不如沒有可用備份重要。

第 78 題

tb787631.CISSPPT3E.c06.048

Susan 正在查看軟件測試覆蓋率數據，看到如下圖所示的信息。關於這個測試過程，她能確定什麼？ (選擇所有適用的答案。)

A. 測試沒有完全覆蓋。

B. 測試 4 無故障完成。

C. 測試 2 未能成功運行。

D. 測試需要進行第五次。

你回答正確！

測試 2 的完全失敗可能是由於測試運行失敗，但測試整體顯示持續改進 ，

測試 4 完全成功。此時，大多數測試過程會認為測試已完成。這不顯示

覆蓋率，如果第四次測試成功，則沒有理由運行第五次運行。

第 79 題

tb787631.CISSPPT3E.c06.028

Jim 使用一種工具掃描系統中的可用服務，然後連接到這些服務以收集橫幅信息以確定正在運行的服務版本。然後它會提供一份報告，詳細說明它收集的內容，結果基於服務指紋識別、橫幅信息以及它收集的類似詳細信息以及 CVE 信息。吉姆使用什麼類型的工具？

A.端口掃描器

B. 服務驗證器

C. 漏洞掃描器

D.補丁管理工具

您回答錯誤。

沒有訪問機器的管理權限或不使用代理的漏洞掃描器掃描遠程機器以收集信息，包括來自查詢和連接響應的指紋、來自服務的橫幅信息和相關數據。

CVE 信息即 Common Vulnerability and Exposure 信息，或漏洞信息。

端口掃描器收集有關打開哪些服務端口的信息，儘管一些端口掃描器模糊了端口掃描器和漏洞掃描器之間的界限。補丁管理工具通常作為系統上的

代理運行，以允許它們監控補丁級別並根據需要更新系統。服務驗證通常

涉及測試服務的功能，而不是其橫幅和響應模式。

問題 80

tb787631.CISSPPT3E.c06.073

Jim 正在設計他的組織的日誌管理系統，並且知道他需要仔細計劃以處理組織的日誌數據。以下哪項不是吉姆應該關注的因素？

A.日誌數據量

B. 缺乏足夠的日誌源

C. 數據存儲安全要求

D、網絡帶寬

您回答錯誤。

沒有足夠的日誌源並不是日誌管理系統設計中的常見考慮因素，儘管對於

無法捕獲所需數據的安全管理人員來說，這可能是一個擔憂。日誌管理系

統設計必須考慮日誌數據量及其消耗的網絡帶寬、數據的安全性以及分析

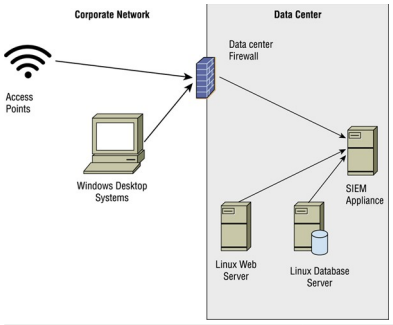
數據所需的工作量。

問題 81

tb787631.CISSPPT3E.c06.019

請參考以下場景：

- Jennifer 工作的公司實施了中央日誌記錄基礎設施，如下圖所示。使用此圖和您對日誌系統的了解來回答以下問題。



在正常操作期間，Jennifer 的團隊使用 SIEM 設備來監控通過系統日誌接收到的異常。顯示的哪個系統本身不支持系統日誌事件？

A. 企業無線接入點

B. Windows 桌面系統

C. Linux 網絡服務器

D. 企業防火牆設備

你回答正確！

Windows 系統以 Windows 本機日誌記錄格式生成日誌。要發送系統日誌事件，Windows 系統需要輔助應用程序或工具。企業無線接入點、防火牆和 Linux 系統通常都支持系統日誌。

問題 82

tb787631.CISSPPT3E.c06.090

在執行滲透測試之前應該進行的第一步是什麼？

A. 數據收集

B、端口掃描

C. 獲得許可

D、規劃

您回答錯誤。

滲透測試最重要的第一步是獲得許可。一旦獲得許可，就可以開始規劃、

數據收集以及端口掃描等實際測試要素。

問題 83

tb787631.CISSPPT3E.c06.078

請參考以下場景：

- Ben 的組織已開始使用 STRIDE 來評估其軟件，並確定了威脅代理和這些威脅可能產生的業務影響。現在他們正在努力為他們發現的問題確定適當的控制措施。

Ben 的開發團隊需要解決導致特權提升威脅的授權問題。以下哪項控制措施最適合此類問題？

A. 啟用審計和日誌記錄。

B. 基於角色的訪問控制用於特定的操作。

C. 啟用數據類型和格式檢查。

D. 用戶輸入根據白名單進行測試。

您回答錯誤。

Microsoft 的 STRIDE 威脅評估模型將威脅分為六類之一：

- 欺騙——涉及用戶憑據和身份驗證或偽造合法通信的威脅
- 篡改——涉及惡意修改數據的威脅
- 否認——導致用戶無法拒絕的行為發生的威脅
- 信息洩露——涉及將數據暴露給未經授權的個人的威脅
- 拒絕服務——拒絕為合法用戶提供服務的威脅
- 特權提升——為未授權用戶提供更高特權的威脅

對特定操作使用基於角色的訪問控制 (RBAC) 將有助於確保用戶無法執行他們不應執行的操作。審核和日誌記錄可以幫助檢測濫用，但不能阻止濫用；數據類型、格式檢查和白名單都有助於

防止 SQL 注入和緩衝區溢出攻擊等攻擊，但並不直接針對授權

問題。

問題 84

tb787631.CISSPPT3E.c06.069

Nikto、Burp Suite 和 Wapiti 都是哪種工具的例子？

A. Web 應用漏洞掃描器

B.代碼審查工具

C. 漏洞掃描器

D. 端口掃描器

你回答正確！

Nikto、Burp Suite 和 Wapiti 都是 Web 應用程序漏洞掃描器，是專為掃

描 Web 服務器和應用程序而設計的工具。雖然它們與更廣泛的漏洞掃描

器和端口掃描工具共享一些功能，但它們的關注範圍更窄，並且通常比漏

洞掃描器具有更深入的功能。

問題 85

tb787631.CISSPPT3E.c06.006

Susan 需要掃描系統中的漏洞，她想使用開源工具遠程測試系統。以下哪些工具可以滿足她的要求並允許進行漏洞掃描？

A.Nmap

B.OpenVAS

C、MBSA

D. Nessus

你回答正確！

OpenVAS 是一個開源漏洞掃描工具，它將向 Susan 提供一份漏洞報告，該漏洞報告可以從基於網絡的遠程掃描中識別出來。Nmap 是一個開源的端口掃描器。Microsoft Baseline Security Analyzer (MBSA) 和 Nessus 都是閉源工具，儘管 Nessus 最初是開源的。

問題 86

tb787631.CISSPPT3E.c06.013

Selah 想要向想要使用其組織的雲服務的客戶提供安全評估信息。她應該選擇以下哪個選項才能確保最大數量的客戶對評估信息感到滿意？

A. 使用內部審計團隊根據內部指標進行自我評估。

B. 使用第三方審核員。

C. 使用了解系統的內部技術人員。

D. 使用內部審計團隊根據 COBIT 等通用標准進行自我評估。

你回答正確！

在向第三方提供審計和合規信息時，聘請知名公司的第三方審計師通常是

最佳選擇。Selah 可以聘請合適的供應商進行 SOC 2 類型 II 約定，作為

向她的客戶提供詳細信息的合理選擇的一個例子。按照 COBIT 這樣的通

用標准進行評估的內部員工將是此列表中下一個最可接受的選項，內部標

準的用處不如它。最後，內部非審計人員在這種情況下是最沒有用的。

問題 87

tb787631.CISSPPT3E.c06.066

Andrea 作為其組織的 CI/CD 管道的一部分運行的自動化代碼測試和集成出錯了。如果公司需要代碼立即上線，Andrea 應該如何處理代碼？

A. 手動繞過測試。

B. 查看錯誤日誌以確定問題。

C. 重新運行測試以查看它是否有效。

D. 將代碼發回給開發人員進行修復。

您回答錯誤。

雖然處理錯誤和異常可能是一門藝術，但在這種情況下要做的第一件事是

查看錯誤日誌和通知，試圖找出問題所在。從那裡，Andrea 可以決定修

復問題、發回代碼進行修復或採取其他行動。如果錯誤發生在測試完成後

並且與流程或其他非關鍵元素有關，她甚至可能會選擇轉發代碼，但只有

在她絕對確定情況確實如此時才會這樣做。

問題 88

tb787631.CISSPPT3E.c06.054

Michelle 正在進行定量業務影響評估，並希望收集數據以確定停機的美元成本。她需要從前一年的中斷中獲得哪些信息來計算這些中斷對企業造成的成本？（選擇所有符合條件的。）

A. 業務中斷的總時間

B. 從停電中恢復的人員工作小時數

C. 中斷期間每小時損失的業務（以美元計）

D. 員工每小時平均工資

你回答正確！

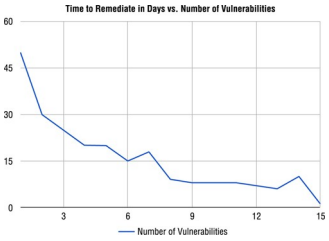
所有這些對於業務影響分析都很重要，可以收集停機總成本。當企業無法

經營時，企業會虧損，但員工時間和精力的支出也是一個重要的考慮因素 。

問題 89

tb787631.CISSPPT3E.c06.044

作為安全經理角色的一部分，Jacob 向其組織的管理團隊提供了以下圖表。他為他們提供什麼類型的測量？



A. 覆蓋率衡量標準

B. 關鍵績效指標

C. 生存時間指標

D. 業務關鍵性指標

您回答錯誤。

修復漏洞的時間是安全團隊常用的關鍵績效指標。生存時間衡量數據包可

以在躍點中存在多長時間，業務關鍵性是用於確定服務或系統對組織的重

要性的衡量標準，覆蓋率用於衡量代碼測試的有效性。

問題 90

tb787631.CISSPPT3E.c06.072

Susan 需要確保她的電子商務應用程序組件之間的交互都得到正確處理。她打算驗證整個基礎設施中的通信、錯誤處理和會話管理功能。她計劃進行什麼類型的測試？

A. 誤用案例測試
B. 模糊測試
C. 回歸測試
D、接口測試

您回答錯誤。

Susan 正在進行接口測試。接口測試涉及測試系統或應用程序組件以確保它們一起正常工作。誤用案例測試側重於攻擊者如何濫用應用程序而不測試正常案例。模糊測試會嘗試發送意外輸入並可能參與接口測試，但它不會涵蓋所有問題。回歸測試是在測試更改時進行的，用於確保應用程序或系統的功能與更新或更改之前一樣。

問題 91

tb787631.CISSPPT3E.c06.037

以下哪個工具無法為滲透測試人員識別目標操作系統？

A.Nmap

B. Nessus

C、沒人

D.sqlmap

您回答錯誤。

Nmap、Nessus 和 Nikto 都具有操作系統指紋識別或其他操作系統識別功能。sqlmap 旨在執行 SQL 注入漏洞的自動檢測和測試，不提供操作系統檢測。

問題 92

tb787631.CISSPPT3E.c06.025

專注於系統不應允許的功能的測試是哪種測試的示例？

A. 用例測試

B、人工測試

C. 誤用案例測試

D、動態測試

你回答正確！

測試系統如何被濫用或濫用測試側重於組織不希望的行為或與系統或應用

程序的正常功能背道而馳的行為。用例測試用於驗證所需功能是否有效。

動態測試用於確定代碼如何處理隨時間變化的變量，而手動測試正是它的

含義：手動測試代碼。

問題 93

tb787631.CISSPPT3E.c06.029

Emily 構建了一個腳本，用於將數據發送到她正在測試的 Web 應用程序。每次腳本運行時，它都會發送一系列交易，其中包含符合 Web 應用程序預期要求的數據，以驗證它是否響應典型的客戶行為。她使用什麼類型的交易，這是什麼類型的測試？

A. 綜合、被動監測
B. 綜合用例測試
C. 實際動態監測
D. 實際的，模糊測試

你回答正確！

Emily 正在使用合成事務，它可以使用記錄的或生成的事務，並且正在

進行用例測試以驗證應用程序是否正確響應實際用例。實際數據和動態監

控都不是行業術語。模糊測試涉及向程序發送意外輸入以查看其響應方式。

被動監控使用網絡分路器或其他捕獲技術來監控系統或應用程序的實際流量。

問題 94

tb787631.CISSPPT3E.c06.067

Michelle 想比較她在數據中心發現的漏洞，依據是漏洞的可利用程度、漏洞利用代碼是否存在以及補救的難易程度。她應該使用什麼評分系統來比較這些漏洞指標？

A、CSV
B、NVD
C、VSS
D、CVSS

你回答正確！

通用漏洞評分系統 (CVSS) 包括用於可利用性、影響、漏洞利用代碼的成熟程度以及如何修復漏洞的指標和計算工具，以及根據用戶的獨特需求對漏洞進行評分的方法。NVD 是國家漏洞數據庫，CSV 是逗號分隔值

的縮寫，而 Visual SourceSafe (VSS) 是與軟件開發而非漏洞管理相關的無關術語。

問題 95

tb787631.CISSPPT3E.c06.014

Yasmine 被要求考慮破壞和攻擊模擬系統。她應該尋找什麼類型的系統？

A. 旨在幫助管理事件的工單和變更管理系統

B. 為藍隊運行事件響應模擬以測試他們技能的系統

C. 將紅藍團隊技術與自動化相結合的系統

D. 安全運營和響應 (SOAR) 系統

你回答正確！

BAS 或突破和攻擊模擬系統是將紅隊（攻擊）和藍隊（防禦）技術與自動化相結合的系統，以在針對您的環境運行時模擬高級持續威脅和其他高級威脅參與者。這允許在一個環境中復制和評估各種威脅，而無需像人員配備齊全的紫色團隊那樣多的開銷。

問題 96

tb787631.CISSPPT3E.c06.053

哪個 NIST 特別出版物涵蓋了安全和隱私控制的評估？

A. 800-12

B. 800-53A

C.800-34

D.800-86

你回答正確！

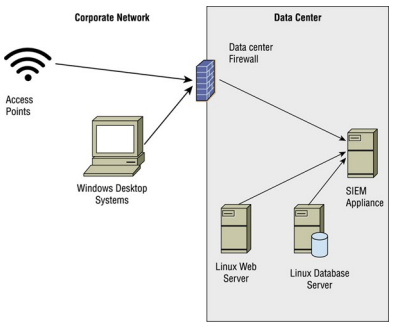
NIST SP 800-53A 的標題是“評估聯邦信息系統和組織中的安全和隱私控制：制定有效的評估計劃”，涵蓋了評估和衡量控制的方法。NIST 800-12 是對計算機安全的介紹，800-34 涵蓋應急計劃，800-86 是“將取證技術集成到事件響應中的指南”。

問題 97

tb787631.CISSPPT3E.c06.020

請參考以下場景：

- Jennifer 工作的公司實施了中央日誌記錄基礎設施，如下圖所示。使用此圖和您對日誌系統的了解來回答以下問題。



組織應該為圖中顯示的每個設備使用什麼技術來確保日誌可以在整個基礎設施中按時間排序？

A. 系統日誌

B、NTP

C. 日誌同步

D. 快照

你回答正確！

網絡時間協議 (NTP) 可以確保系統使用相同的時間，從而允許在整個集

中式日誌記錄基礎架構中對日誌進行時間排序。Syslog 是系統將日誌發

送到日誌服務器的一種方式，不會解決時間順序問題。logsync 和 SNAP

都不是行業術語。

問題 98

tb787631.CISSPPT3E.c06.055

如果 Kara 最關心的是防止竊聽攻擊，她應該阻止哪個端口？

A.22

B. 80

C.443

D. 1433

你回答正確！

HTTP 協議使用端口 80 進行未加密的 Web 通信。如果 Kara 想要防止

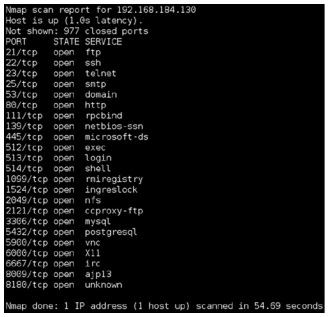
竊聽，她應該封鎖這個端口並限制 Web 訪問端口 443 上的加密 HTTPS

連接。

問題 99

tb787631.CISSPPT3E.c06.086

請參考以下場景。在端口掃描期間，Ben 使用 nmap 的默認設置並看到以下結果。



本的經理對他的掃描範圍表示擔憂。為什麼他的經理會有這種擔憂？

A. Ben 沒有測試 UDP 服務。

B. Ben 沒有發現“知名端口”之外的端口。

C. Ben 沒有執行操作系統指紋識別。

D. Ben 只測試了有限數量的端口。

您回答錯誤。

默認情況下，Nmap 僅掃描 1000 個 TCP 和 UDP 端口，包括“知名”端口

0-1024 範圍之外的端口。通過使用 nmap 的默認值，Ben 錯過了

64,535 個端口。操作系統指紋不會覆蓋更多端口，但會提供對掃描系統

上運行的操作系統的最佳猜測。