

熱門的212-82在線題庫，全面覆蓋212-82考試知識點



P.S. Testpdf在Google Drive上分享了免費的2026 ECCouncil 212-82考試題庫：<https://drive.google.com/open?id=1ug5e28uZd1A1BF78JhKlPPB4CqBzRnJg>

212-82 認證對於雇員和雇主來說都有好處。對雇員來說，它包括技術可信度、繼續教育和事業升遷的機會，更多的工作滿足感。但是 ECCouncil 212-82 考試是考生所能接受的考試，對有心應考的人來說，實在是不小的負擔。若第一次沒通過，又需一大筆的費用重考。如果您正在準備 ECCouncil 的 212-82 考試以獲得適當的知識和技能，Testpdf 考題網的練習題和答案，為您節約寶貴的時間以及金錢并順利通過考試。

ECCouncil 212-82 認證考試，也被稱為認證的網絡安全技術人員（CCT）考試，旨在測試個人在網絡安全領域的知識和技能。考試涵蓋各種主題，如網絡安全，威脅管理，漏洞評估和事件響應。該認證非常適合想要開始從事網絡安全職業的個人，或想要增強其在該領域的知識和技能的 IT 專業人士。CCT 認證是供應商中立的，這意味著它不與任何特定的技術或平台相關聯，對於任何對網絡安全感興趣的人來說都是一個有價值的認證。

>> 212-82 在線題庫 <<

高命中率的212-82題庫平臺 - 最新的212-82認證新題庫已出

你對自己現在的工作滿意嗎？對自己正在做的事情滿意嗎？想不想提升自己的水準呢？多掌握一些對工作有用的技能吧。那麼，在 IT 領域工作的你，當然是應該選擇參加 IT 認定考試獲得認證資格了。因為這樣可以更好地提升你自己。而且，最重要的是，你也可以向別人證明你掌握了更多的工作技能。那麼，快來參加 ECCouncil 的 212-82 考試吧。這個考試可以幫助你實現你自己的願望。對通過這個考試沒有信心也沒關係。因為你可以來 Testpdf 找到你想要的幫手和準備考試的工具。Testpdf 的考試資料一定能幫助你獲得 212-82 考試的認證資格。

ECCouncil 212-82: 認證網絡安全技術師考試是對於想要成為網絡安全專業人員的個人而言，是一個有價值的認證。這是一個全球認可的認證，能夠展示在各個網絡安全領域的能力。通過此認證，個人可以提高其在這個領域的技能和知識，進而推進自己的職業生涯。對於那些對於追求網絡安全職業生涯或提升其現有技能有興趣的人而言，這是一個絕佳的選擇。

在成功通過 ECCouncil 212-82（認證網絡安全技術人員）認證後，候選人將能夠熟練部署網絡安全解決方案，以預防、檢測和應對各種網絡威脅。此外，獲得認證的個人將通過在各種組織中擔任網絡安全分析師、技術人員或工程師等職位，來推動自己在網絡安全行業中的職業發展。

最新的 Cyber Technician (CCT) 212-82 免費考試真題 (Q32-Q37):

問題 #32

Grace, an online shopping enthusiast, purchased a smart TV using her debit card. During online payment, Grace's browser redirected her from the e-commerce website to a third-party payment gateway, where she provided her debit card details and the OTP received on her registered mobile phone. After completing the transaction, Grace logged into her online bank account and verified the current balance in her savings account, identify the state of data being processed between the e-commerce website and payment gateway in the above scenario.

- A. Data in transit
- B. Data in inactive

- C. Data at rest
- D. Data in use

答案： A

解題說明：

Data in transit is the state of data being processed between the e-commerce website and payment gateway in the above scenario. Data in transit is the data that is moving from one location to another over a network, such as the internet. Data in transit can be vulnerable to interception, modification, or theft by unauthorized parties. Therefore, data in transit should be protected using encryption, authentication, and secure protocols. Reference: Data in Transit

問題 #33

A company decided to implement the cloud infrastructure within its corporate firewall to secure sensitive data from external access. The company invested heavily in creating a cloud architecture within its premises to manage full control over its corporate data. Which of the following types of cloud deployment models did the company implement in this scenario?

- A. Multi cloud
- B. Community cloud
- C. Private cloud
- D. Public cloud

答案： C

解題說明：

Private cloud is the type of cloud deployment model that the company implemented in this scenario. Cloud computing is a model that provides on-demand access to shared and scalable computing resources, such as servers, storage, networks, applications, etc., over the internet or a network. Cloud computing can have different types based on its service or deployment model. A cloud deployment model defines how and where the cloud infrastructure and services are hosted and accessed. A cloud deployment model can have different types, such as public cloud, private cloud, hybrid cloud, community cloud, etc. A private cloud is a type of cloud deployment model that provides exclusive access to cloud infrastructure and services to a single organization or entity. A private cloud can be hosted within or outside the organization's premises and managed by the organization or a third-party provider. A private cloud can be used to secure sensitive data from external access and maintain full control over the corporate data. In the scenario, the company decided to implement the cloud infrastructure within its corporate firewall to secure sensitive data from external access. The company invested heavily in creating a cloud architecture within its premises to manage full control over its corporate data. This means that the company implemented a private cloud for this purpose. A multi-cloud is not a type of cloud deployment model, but a term that describes a strategy that uses multiple public or private clouds from different providers for different purposes or functions. A public cloud is a type of cloud deployment model that provides open access to cloud infrastructure and services to multiple organizations or entities over the internet. A public cloud can be hosted and managed by a third-party provider that owns and operates the cloud infrastructure and services. A community cloud is a type of cloud deployment model that provides shared access to cloud infrastructure and services to multiple organizations or entities that have common interests or goals.

問題 #34

An MNC hired Brandon, a network defender, to establish secured VPN communication between the company's remote offices. For this purpose, Brandon employed a VPN topology where all the remote offices communicate with the corporate office but communication between the remote offices is denied.

Identify the VPN topology employed by Brandon in the above scenario.

- A. Star topology
- B. Point-to-Point VPN topology
- C. Hub-and-Spoke VPN topology
- D. Full-mesh VPN topology

答案： C

解題說明：

A hub-and-spoke VPN topology is a type of VPN topology where all the remote offices communicate with the corporate office, but communication between the remote offices is denied.

The corporate office acts as the hub, and the remote offices act as the spokes. This topology reduces the number of VPN tunnels

required and simplifies the management of VPN policies. A point-to-point VPN topology is a type of VPN topology where two endpoints establish a direct VPN connection. A star topology is a type of VPN topology where one endpoint acts as the central node and connects to multiple other endpoints. A full-mesh VPN topology is a type of VPN topology where every endpoint connects to every other endpoint.

問題 #35

Initiate an SSH Connection to a machine that has SSH enabled in the network. After connecting to the machine find the file flag.txt and choose the content hidden in the file. Credentials for SSH login are provided below:

Hint:

Username: sam

Password: admin@123

- A. bob2@sam
- B. sam@bob
- C. bob@sam
- D. sam2@bob

答案： C

解題說明：

Quid pro quo is the social engineering technique that Johnson employed in the above scenario. Social engineering is a technique that involves manipulating or deceiving people into performing actions or revealing information that can be used for malicious purposes. Social engineering can be performed through various methods, such as phone calls, emails, websites, etc. Quid pro quo is a social engineering method that involves offering a service or a benefit in exchange for information or access. Quid pro quo can be used to trick victims into believing that they are receiving help or assistance from a legitimate source, while in fact they are compromising their security or privacy. In the scenario, Johnson performed quid pro quo by claiming himself to represent a technical support team from a vendor and offering to help sibertech.org with a server issue, while in fact he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical information to Johnson's machine. Diversion theft is a social engineering method that involves diverting the delivery or shipment of goods or assets to a different location or destination. Elicitation is a social engineering method that involves extracting information from a target by engaging them in a conversation or an interaction. Phishing is a social engineering method that involves sending fraudulent emails or messages that appear to come from a trusted source, such as a bank, a company, or a person, and asking the recipient to click on a link, open an attachment, or provide personal or financial information.

問題 #36

You are the Lead Cybersecurity Specialist at GlobalTech, a multinational tech conglomerate renowned for its avant-garde technological solutions in the aerospace and defense sector. The organization's reputation stands on the innovative technologies it pioneers, many of which are nation's top secrets.

Late on a Sunday night, you are alerted about suspicious activities on a server holding the schematics and project details for a groundbreaking missile defense system. The indicators suggest a complex, multi-stage cyberattack that managed to bypass traditional security measures. Preliminary investigations reveal that the cybercriminals might have used an Insider's credentials, further complicating the breach. Given the extremely sensitive nature of the data involved, a leak could have severe national security implications and irreparably tarnish the company's reputation. Considering the potential gravity and intricacies of this security incident, what immediate action should you undertake to handle this situation effectively, safeguard crucial data, and minimize potential fallout?

- A. Inform the top executive board and legal team about the breach. Prepare a public statement to ensure shareholders and clients are kept in the loop about the incident and the measures being undertaken.
- B. Initiate the incident response protocol, focusing on immediate containment by isolating the impacted server. Concurrently, assess the breadth and depth of the breach by examining network logs and affected systems.
- C. Notify federal agencies about the potential breach of national security. Work in tandem with them to ensure all necessary measures are taken to prevent further data exfiltration and protect national interests.
- D. Engage with an external specialized cybersecurity firm to conduct a parallel investigation, leveraging its expertise to identify the culprits and understand the breach's modus operandi.

答案： B

解題說明：

In the event of a cyberattack involving highly sensitive data, such as a missile defense system, the immediate focus should be on

