212-89在線題庫，212-89真題材料

BONUS!!! 免費下載VCESoft 212-89考試題庫的完整版：https://drive.google.com/open?id=1uq-Hbuuq_fG6c4RCUsueILUxHgRITCaL

沒有人除外，我們VCESoft保證你100%的比例， 今天你選擇VCESoft，選擇你要開始的訓練，並通過你的下一次的考題，你將得到最好的資源與市場的相關性和可靠性保證。VCESoft EC-COUNCIL的212-89考題和答案反映的問題問212-89考試。

要參加ECIH v2考試，考生必須擁有至少兩年的信息安全或相關領域的經驗。他們還必須完成EC-Council官方培訓課程或EC-Council認可的培訓中心的培訓。該課程涵蓋考試所包含的所有主題，並為考生提供通過考試所需的知識和技能。

認證考試由 50 道選擇題組成，考生有 2 小時的時間作答。考試合格分數為 70%，通過考試者將獲得 EC-COUNCIL 的數字徽章和證書。認證有效期為三年，考生必須通過重新參加考試或完成持續教育學分以更新認證。

>> 212-89在線題庫 <<

212-89真題材料 - 最新212-89試題

我們都知道，在互聯網普及的時代，需要什麼資訊那是非常簡單的事情，不過缺乏的是品質及適用性的問題。許多人在網路上搜尋EC-COUNCIL的212-89考試認證培訓資料，卻不知道該如何去相信，在這裏，我向大家推薦VCESoft EC-COUNCIL的212-89考試認證培訓資料，它在互聯網上點擊率購買率好評率都是最高的，VCESoft EC-COUNCIL的212-89考試認證培訓資料有部分免費的試用考題及答案，你們可以先試用後決定買不買，這樣就知道VCESoft所有的是不是真實的。

EC-Council Certified Incident Handler（ECIH v2）考試旨在提供實踐經驗和知識，處理各種類型的事故，包括網絡安全事故、惡意代碼事故和內部攻擊威脅。該考試由國際電子商務顧問委員會（EC-Council）主辦，該委員會是信息安全認證的主要提供者。

最新的 ECIH Certification 212-89 免費考試真題 (Q253-Q258):

問題 #253
Daniel, a SOC analyst, detects multiple incoming TCP requests to the organization's mail server from different IPs. However, none of the requests complete the handshake. He suspects a potential attempt to exhaust server resources and confirms this with netstat logs. Which type of protocol-level incident is Daniel identifying?

- A. DNS cache poisoning
- B. TCP session hijacking
- C. SYN flood attack
- D. UDP reflection

答案：C

解題說明：
Comprehensive and Detailed Explanation (ECIH-aligned):
This scenario describes a SYN flood attack, a classic protocol-level Denial-of-Service technique covered in the ECIH Network

Security Incidents module. In a SYN flood, attackers send a large volume of TCP SYN packets but never complete the three-way handshake, leaving the server waiting for responses and exhausting connection resources.
Option D is correct because incomplete TCP handshakes, half-open connections, and resource exhaustion are defining characteristics of SYN flood attacks. The presence of multiple source IPs further suggests a distributed attack.
Option A involves taking over an existing session, not exhausting resources. Option B applies to UDP-based amplification attacks. Option C affects DNS resolution, not TCP handshakes.
ECIH stresses that early identification of SYN floods allows defenders to deploy SYN cookies, rate limiting, and upstream filtering. Recognizing handshake anomalies is therefore critical in protecting service availability.

問題 #254
Which of the following is NOT part of the static data collection process?

- A. Evidence acquisition
- B. Password protection
- C. Evidence examination
- D. System preservation

答案：B

問題 #255
An incident handler is analyzing email headers to uncover suspicious emails.
Which of the following tools would he/she use in order to accomplish this task?

- A. Go phish
- B. Barracuda Email Security Gateway
- C. SPAMfighter
- D. Mx Toolbox

答案：D

問題 #256
You are a systems administrator for a company. You are accessing your file server remotely for maintenance.
Suddenly, you are unable to access the server. After contacting others in your department, you find out that they cannot access the file server either. You can ping the file serverbut not connect to it via RDP. You check the Active Directory Server, and all is well. You check the email server and find that emails are sent and received normally. What is the most likely issue?

- A. An admin account issue
- B. A denial-of-service issue
- C. An e-mail service issue
- D. The file server has shut down

答案：B

解題說明：
In this scenario, the inability to access the file server via Remote Desktop Protocol (RDP), despite the server being pingable and other services functioning normally, suggests a service-specific disruption rather than a complete system shutdown or broader network issue. This pattern is indicative of a denial-of-service (DoS) attack targeted at the file server's RDP service or network congestion that specifically affects RDP connectivity. A DoS attack aims to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. The fact that other services (like email) are operational rules out broader system or admin account issues, pointing towards a specific problem with accessing the file server, most likely due to a denial-of-service condition.References:Incident Handler (ECIH v3) courses teach systems administrators and security professionals to diagnose and respond to various security incidents, including DoS attacks, by understanding symptoms and isolating issues based on the services affected.

問題 #257
Which of the following options describes common characteristics of phishing emails?

- A. Written in French
- B. Urgency, threatening, or promising subject lines
- C. Sent from friends or colleagues
- D. No BCC fields

答案：B

解題說明：
Phishing emails often share common characteristics designed to manipulate the recipient into taking immediate action. One of the hallmark features is the use of urgency, threatening language, or promising subject lines in the emails. These tactics are intended to create a sense of urgency or fear, compelling the recipient to respond quickly without giving due consideration to the legitimacy of the email. Phishing emails may claim that the recipient's account has been compromised, that they need to confirm personal information immediately, or that they have won a prize. The goal is to trick the recipient into clicking on malicious links, opening attachments, or providing sensitive information.
References:The Certified Incident Handler (ECIH v3) program by EC-Council covers the identification and handling of phishing incidents, including the analysis of phishing emails and the importance of educating users on recognizing and responding to phishing attempts.

問題 #258
.....