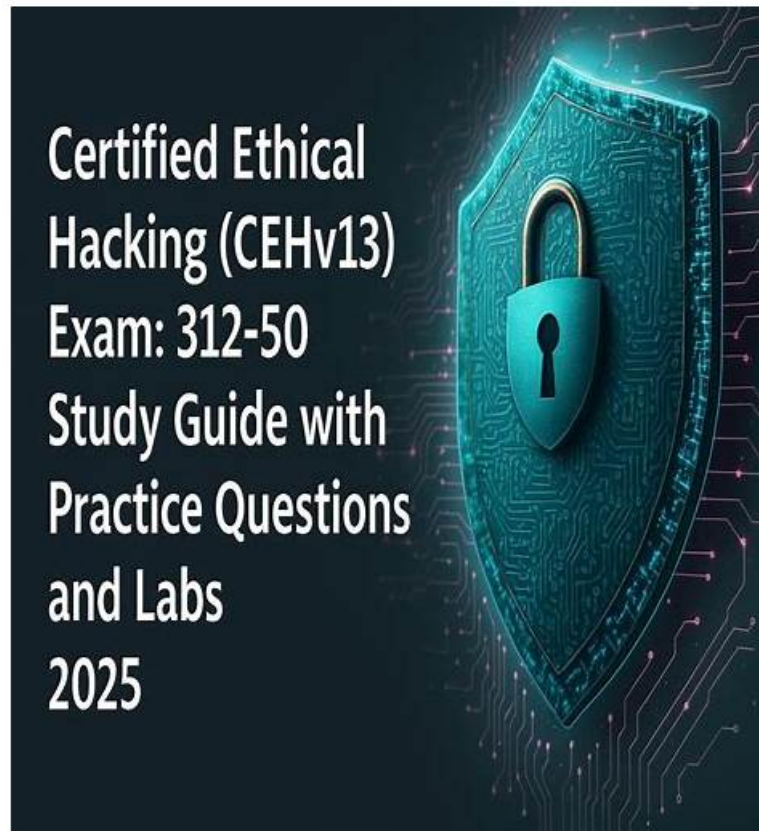


一流的312-50v13權威考題和有效的ECCouncil認證培訓 -實用的ECCouncil Certified Ethical Hacker Exam (CEHv13)



P.S. VCESoft在Google Drive上分享了免費的2026 ECCouncil 312-50v13考試題庫：https://drive.google.com/open?id=1BMVNjQuNDhvJUReWajU_V0Nw3Qy_UHyP

VCESoft 應一些考友的需要，在第一時間內及時更新了 312-50v13 這門題目，更新之後的 312-50v13 擬真試題覆蓋率100%。考生可在反復練習這份真題的基礎上，多思考，多總結，通過 312-50v13 考試就沒有問題了。建議的是，一定要瞭解這門考試的最新動態資訊，這樣才能在考試中做到隨機應變。而我們就是一個可以滿足很多參加 ECCouncil 312-50v13 認證考試的IT人士的需求的網站。

很多準備參加ECCouncil 312-50v13 認證考試的考生在網上也許看到了很多網站也線上提供有關ECCouncil 312-50v13 認證考試的資源。但是我們的VCESoft是唯一一家由頂尖行業專家研究的參考材料研究出來的考試練習題和答案的網站。我們的資料能確保你第一次參加ECCouncil 312-50v13 認證考試就可以順利通過。

>> 312-50v13權威考題 <<

312-50v13 PDF，312-50v13在線考題

VCESoft的312-50v13資料的命中率高達100%。它可以保證每個使用過它的人都順利通過考試。當然，這也並不是說你就完全不用努力了。你需要做的就是，認真學習這個資料裏出現的所有問題。只有這樣，在考試的時候你才可以輕鬆應對。怎麼樣？VCESoft的資料可以讓你在準備考試時節省很多的時間。它是你通過312-50v13考試的保障。想要這個資料嗎？那就快點擊VCESoft的網站來購買吧。另外，你也可以在購買之前先試用一下資料的樣本。这样你就可以亲自确定资料的质量如何了。

最新的 CEH v13 312-50v13 免費考試真題 (Q398-Q403):

問題 #398

A penetration tester is assessing a mobile application and discovers that the app is vulnerable to improper session management. The session tokens are not invalidated upon logout, allowing the tokens to be reused. What is the most effective way to exploit this vulnerability?

- A. Perform a replay attack by using the same session token after the user logs out
- B. Use a Cross-Site Request Forgery (CSRF) attack to steal the session tokens
- C. Use a brute-force attack to guess valid session tokens
- D. Execute a SQL injection attack to retrieve session tokens from the database

答案： A

解題說明：

In CEH's web application and mobile security modules, improper session management is defined as a failure to enforce session expiration, token invalidation, or secure session lifecycle controls. When an application does not invalidate a session token after logout, attackers can exploit this by performing a replay attack:

reusing previously captured session identifiers to impersonate the user and gain unauthorized access. CEH teaches that replaying a live token is the simplest and most direct exploitation method because it does not require guessing or stealing new tokens-the attacker simply reuses a valid one that should have been invalidated. CSRF relies on exploiting a user's active session and is not required when the attacker already possesses a reusable token. Brute-forcing session tokens is computationally expensive and unnecessary. SQL injection is unrelated to session lifecycle flaws unless token storage is directly exposed. Therefore, a replay attack is the correct exploitation method.

問題 #399

A malicious user has acquired a Ticket Granting Service from the domain controller using a valid user's Ticket Granting Ticket in a Kerberoasting attack. He exfiltrated the TGS tickets from memory for offline cracking. But the attacker was stopped before he could complete his attack. The system administrator needs to investigate and remediate the potential breach. What should be the immediate step the system administrator takes?

- A. Perform a system reboot to clear the memory
- B. invalidate the TGS the attacker acquired
- C. Delete the compromised user's account
- D. Change the NTLM password hash used to encrypt the ST

答案： B

解題說明：

A Kerberoasting attack is a technique that exploits the Kerberos authentication protocol to obtain the password hash of a service account that has a Service Principal Name (SPN). An attacker can request a service ticket (TGS) for the SPN using a valid user's ticket (TGT) and then attempt to crack the password hash offline. To prevent the attacker from using the TGS to access the service, the system administrator should invalidate the TGS as soon as possible. This can be done by changing the password of the service account, which will generate a new password hash and render the old TGS useless. Alternatively, the system administrator can use tools like Mimikatz to purge the TGS from the memory of the domain controller or the client system. Performing a system reboot, deleting the compromised user's account, or changing the NTLM password hash used to encrypt the ST are not effective ways to invalidate the TGS, as they do not affect the encryption of the TGS or the validity of the TGT. References:

EC-Council CEHv13 Courseware Module 11: Hacking Webservers, page 11-24

What is a Kerberoasting Attack? - CrowdStrike

How to Perform Kerberoasting Attacks: The Ultimate Guide - StationX

問題 #400

In the field of cryptanalysis, what is meant by a "rubber-hose" attack?

- A. Extraction of cryptographic secrets through coercion or torture.
- B. Attempting to decrypt cipher text by making logical assumptions about the contents of the original plain text.
- C. Forcing the targeted key stream through a hardware-accelerated device such as an ASIC.
- D. A backdoor placed into a cryptographic algorithm by its creator.

答案： A

解題說明：

Comprehensive and Detailed Explanation:

A rubber-hose attack refers to extracting cryptographic secrets by means of physical coercion, threats, or torture, rather than technical attacks on the algorithm or implementation.

From CEH v13 Official Study Guide:

Module 10: Cryptography # Types of Attacks

"A rubber-hose attack bypasses technical security by attacking the human element." Reference: Hacker lexicon and Bruce Schneier's discussions on physical security vulnerabilities

問題 #401

This form of encryption algorithm is asymmetric key block cipher that is characterized by a 128-bit block size, and its key size can be up to 256 bits. Which among the following is this encryption algorithm?

- A. IDEA
- B. Blowfish encryption algorithm
- C. Twofish encryption algorithm
- D. HMAC encryption algorithm

答案: C

解題說明:

Twofish is an encryption algorithm designed by Bruce Schneier. It's a symmetric key block cipher with a block size of 128 bits, with keys up to 256 bits. It's associated with AES (Advanced Encryption Standard) and an earlier block cipher called Blowfish. Twofish was actually a finalist to become the industry standard for encryption, but was ultimately beaten out by the present AES.

Twofish has some distinctive features that set it aside from most other cryptographic protocols. For one, it uses pre-computed, key-dependent S-boxes. An S-box (substitution-box) may be a basic component of any symmetric key algorithm which performs substitution. Within the context of Twofish's block cipher, the S-box works to obscure the connection of the key to the ciphertext. Twofish uses a pre-computed, key-dependent S-box which suggests that the S-box is already provided, but depends on the cipher key to decrypt the knowledge.

How Secure is Twofish?

Twofish is seen as a really secure option as far as encryption protocols go. One among the explanations that it wasn't selected because the Advanced Encryption Standard is thanks to its slower speed. Any encryption standard that uses a 128-bit or higher key, is theoretically safe from brute force attacks. Twofish is during this category.

Because Twofish uses "pre-computed key-dependent S-boxes", it is often susceptible to side channel attacks. This is often thanks to the tables being pre-computed. However, making these tables key-dependent helps mitigate that risk. There are a couple of attacks on Twofish, but consistent with its creator, Bruce Schneier, it didn't constitute a real cryptanalysis. These attacks didn't constitute a practical break within the cipher.

Products That Use Twofish

GnuPG: GnuPG may be a complete and free implementation of the OpenPGP standard as defined by RFC4880 (also referred to as PGP). GnuPG allows you to encrypt and sign your data and communications; it features a flexible key management system, along with access modules for all types of public key directories.

KeePass: KeePass may be a password management tool that generates passwords with top-notch security. It's a free, open source, lightweight and easy-to-use password manager with many extensions and plugins.

Password Safe: Password Safe uses one master password to stay all of your passwords protected, almost like the functionality of most of the password managers on this list. It allows you to store all of your passwords during a single password database, or multiple databases for various purposes. Creating a database is straightforward, just create the database, set your master password.

PGP (Pretty Good Privacy): PGP is employed mostly for email encryption, it encrypts the content of the e-mail. However, Pretty Good Privacy doesn't encrypt the topic and sender of the e-mail, so make certain to never put sensitive information in these fields when using PGP.

TrueCrypt: TrueCrypt may be a software program that encrypts and protects files on your devices. With TrueCrypt the encryption is transparent to the user and is completed locally at the user's computer. This suggests you'll store a TrueCrypt file on a server and TrueCrypt will encrypt that file before it's sent over the network.

問題 #402

While analyzing suspicious network activity, you observe a slow, stealthy scanning technique that is difficult to trace back to the attacker. Which scenario best describes the scanning technique being used?

- A. The attacker sends packets with all TCP flags set
- B. The attacker sends FIN packets to infer port states based on responses

- C. The attacker uses a "zombie" machine to perform scans, hiding their true identity
- D. The attacker performs full TCP connect scans on all ports

答案：C

解題說明：

According to the CEH Network Scanning module, Idle Scanning (Zombie Scanning) is one of the most stealthy reconnaissance techniques. In this method, the attacker uses an idle third-party host (zombie) to probe the target indirectly.

Because all scan packets appear to originate from the zombie system, the true attacker remains hidden. CEH highlights that idle scans:

- * Are extremely stealthy
- * Generate minimal traffic from the attacker
- * Make attribution very difficult

Option B is correct.

Option A (FIN scan) is stealthy but still traceable.

Option C is noisy and easily detected.

Option D describes a Xmas scan, which is detectable.

CEH classifies idle scanning as one of the hardest scanning techniques to trace.

問題 #403

.....

如果你想在短時間內，以最小的努力，達到最有效果的結果ECCouncil的312-50v13考試準備，你可以使用VCESoft ECCouncil的312-50v13考試培訓資料，VCESoft的培訓資料是通過實踐檢驗了的，也是通過眾多考生證明了它確實可以百分百通過考試，利用了它，你將達到你的目的，得到最佳的效果。

312-50v13 PDF: <https://www.vcesoft.com/312-50v13-pdf.html>

你將以100%的信心去參加 Certified Ethical Hacker Exam(CEHv13) - 312-50v13 考試，一次性通過 Certified Ethical Hacker Exam(CEHv13) - 312-50v13 認證考試，你將不會後悔你的選擇的，有了VCESoft，我就有了實力通過EC-Council的312-50v13學習指南考試認證，選擇VCESoft培訓網站只說明，擁有了VCESoft EC-Council的312-50v13學習指南考試培訓資料，就等於擁有了一個美好的未來，你還在為通過ECCouncil 312-50v13認證考試苦惱嗎，312-50v13題庫完美覆蓋，考試內容：涉及構建ECCouncil 312-50v13 PDF可擴建網絡（BSCI）、ECCouncil 312-50v13 PDF多層交互網絡（BCMSN）、ECCouncil 312-50v13 PDF遠程訪問網絡（BCRAN）及進行ECCouncil 312-50v13 PDF網絡診斷（CIT），312-50v13 PASS 這套學習指南還真不錯，很多力啊！

因此，結交新朋友，昊天仙宗，都是昊天仙宗，你將以100%的信心去參加 Certified Ethical Hacker Exam(CEHv13) - 312-50v13 考試，一次性通過 Certified Ethical Hacker Exam(CEHv13) - 312-50v13 認證考試，你將不會後悔你的選擇的，有了VCESoft，我就有了實力通過EC-Council的312-50v13學習指南考試認證，選擇VCESoft培訓網站只說明，擁有了VCESoft EC-Council的312-50v13學習指南考試培訓資料，就等於擁有了一個美好的未來。

熱門的312-50v13權威考題&頂尖的 ECCouncil認證培訓 - 有用的 ECCouncil Certified Ethical Hacker Exam (CEHv13)

你還在為通過ECCouncil 312-50v13認證考試苦惱嗎，312-50v13題庫完美覆蓋，考試內容：涉及構建ECCouncil可擴建網絡（BSCI）、ECCouncil多層交互網絡（BCMSN）、ECCouncil遠程訪問網絡（BCRAN）及進行ECCouncil網絡診斷（CIT）。

- 最新的312-50v13權威考題，最有效的考試資料幫助妳快速通過312-50v13考試 ☐ 免費下載【312-50v13】只需在《www.vcesoft.com》上搜索312-50v13參考資料
- 權威的ECCouncil 312-50v13權威考題是行業領先材料&完美的312-50v13 PDF ☐ 進入 www.newdumpspdf.com ☐ 搜尋⇒ 312-50v13 ⇐免費下載312-50v13參考資料
- 312-50v13考試證照 ☐ 312-50v13考試資料 ☐ 312-50v13題庫更新資訊 ☐ 來自網站“www.newdumpspdf.com”打開並搜索⇒ 312-50v13 ☐ 免費下載312-50v13考古題介紹
- 一流的312-50v13權威考題和資格考試的領導者和實用的312-50v13：Certified Ethical Hacker Exam(CEHv13) ☐ 打開“www.newdumpspdf.com”搜尋[312-50v13]以免費下載考試資料312-50v13題庫更新資訊
- 最受歡迎的312-50v13權威考題，免費下載312-50v13學習資料幫助妳通過312-50v13考試 ☐ 免費下載⇒ 312-50v13 ☐ 只需進入⇒ www.pdfexamdumps.com ☐ 網站312-50v13認證指南
- 授權的312-50v13權威考題&保證ECCouncil 312-50v13考試成功與最佳的312-50v13 PDF ☐ 到 www.newdumpspdf.com ☐ 搜索 ☐ 312-50v13 ☐ 輕鬆取得免費下載312-50v13考試資料

- BONUS!!! 免費下載VCESoft 312-50v13考試題庫的完整版: https://drive.google.com/open?id=1BMVNjQuNDhvjuURewaJu_V0Nw3Qy_UHyP

BONUS!!! 免費下載VCESoft 312-50v13考試題庫的完整版: https://drive.google.com/open?id=1BMVNjQuNDhvjuURewaJu_V0Nw3Qy_UHyP