312-50v13必殺問題集 & 312-50v13受験資料更新版

BONUS！！！ Topexam 312-50v13ダンプの一部を無料でダウンロード：https://drive.google.com/open?id=14SZU6wKKXSKm2anuLLdnu47HLvt0xngM

312-50v13試験資料は試験に緊密に関連しています。あなた312-50v13試験資料を勉強したら、その資料のメリットを見つけることができます。312-50v13試験資料の問題の答えを覚えると、試験に合格する可能性が大きいです。使い安ク、便利で、全面的で、全部312-50v13試験資料の特徴です。だから、312-50v13試験資料は有難い商品です。

別の人の言い回しより自分の体験感じは大切なことです。我々の希望は誠意と専業化を感じられることですなので、お客様に無料のECCouncil 312-50v13問題集デモを提供します。購買の後、行き届いたアフタサービスを続けて提供します。ECCouncil 312-50v13問題集を更新するなり、あなたのメールボックスに送付します。あなたは一年間での更新サービスを楽しみにします。

>> 312-50v13必殺問題集 <<

312-50v13受験資料更新版、312-50v13無料模擬試験

IT業界の発展とともに、IT業界で働いている人への要求がますます高くなります。競争の中で排除されないように、あなたはECCouncilの312-50v13試験に合格しなければなりません。たくさんの時間と精力で試験に合格できないという心配な心情があれば、我々Topexamにあなたを助けさせます。多くの受験生は我々のソフトでECCouncilの312-50v13試験に合格したので、我々は自信を持って我々のソフトを利用してあなたはECCouncilの312-50v13試験に合格する保障があります。

ECCouncil Certified Ethical Hacker Exam (CEHv13) 認定 312-50v13 試験問題 (Q490-Q495):

質問 # 490
Calvin, a grey-hat hacker, targets a web application that has design flaws in its authentication mechanism. He enumerates usernames from the login form of the web application, which requests users to feed data and specifies the incorrect field in case of invalid credentials. Later, Calvin uses this information to perform social engineering.
Which of the following design flaws in the authentication mechanism is exploited by Calvin?

- A. Verbose failure messages
- B. Password reset mechanism
- C. Insecure transmission of credentials
- D. User impersonation

正解：A

質問 # 491

A red team operator wants to obtain credentials from a Windows machine without touching LSASS memory due to security controls and Credential Guard. They use SSPI to generate NetNTLM responses in the logged- in user context and collect those responses for offline cracking. Which attack technique is being used?

- A. Hash injection approach using credential hashes for authentication purposes
- B. Pass-the-ticket attack method involving forged tickets for network access
- C. Replay attack attempt by reusing captured authentication traffic sequences
- D. Internal Monologue attack technique executed through OS authentication protocol manipulations

正解： D

解説：
CEH v13 discusses various credential extraction and authentication abuse techniques, including approaches that avoid LSASS memory due to modern protections like Credential Guard. The Internal Monologue technique is a specialized credential-harvesting approach that leverages the Windows SSPI authentication stack to coerce the local system into generating NetNTLM challenge-response hashes without requiring direct access to LSASS. This allows attackers to obtain legitimate NTLM responses entirely within the user's security context. These captured responses can then be cracked offline using tools such as Hashcat. Unlike replay attacks (Option B), Internal Monologue is not about reusing captured traffic. Hash injection (Option C) requires possession of NT hashes and modifies authentication tokens, which does not occur here. Pass-the- ticket (Option D) targets Kerberos, not NTLM. Therefore, the correct technique is the Internal Monologue attack.

質問 # 492

A cyber attacker has initiated a series of activities against a high-profile organization following the Cyber Kill Chain Methodology. The attacker is presently in the "Delivery" stage. As an Ethical Hacker, you are trying to anticipate the adversary's next move. What is the most probable subsequent action from the attacker based on the Cyber Kill Chain Methodology?

- A. The attacker will attempt to escalate privileges to gain complete control of the compromised system.
- B. The attacker will initiate an active connection to the target system to gather more data.
- C. The attacker will start reconnaissance to gather as much information as possible about the target.
- D. The attacker will exploit the malicious payload delivered to the target organization and establish a foothold.

正解： D

解説：
The most probable subsequent action from the attacker based on the Cyber Kill Chain Methodology is to exploit the malicious payload delivered to the target organization and establish a foothold. This option works as follows:
* The Cyber Kill Chain Methodology is a framework that describes the stages of a cyberattack from the perspective of the attacker. It helps defenders to understand the attacker's objectives, tactics, and techniques, and to design effective countermeasures. The Cyber Kill Chain Methodology consists of seven stages: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives12.
* The delivery stage is the third stage in the Cyber Kill Chain Methodology, and it involves sending or transmitting the weaponized payload to the target system. The delivery stage can use various methods, such as email attachments, web links, removable media, or network protocols. The delivery stage aims to reach the target system and bypass any security controls, such as firewalls, antivirus, or email filters12.
* The exploitation stage is the fourth stage in the Cyber Kill Chain Methodology, and it involves executing the malicious payload on the target system. The exploitation stage can use various techniques, such as buffer overflows, code injection, or privilege escalation. The exploitation stage aims to exploit a vulnerability or a weakness in the target system and gain access to its resources, such as files, processes, or memory12.
* The installation stage is the fifth stage in the Cyber Kill Chain Methodology, and it involves installing a backdoor or a malware on the target system. The installation stage can use various tools, such as rootkits, trojans, or ransomware. The installation stage aims to establish a foothold on the target system and maintain persistence, which means to survive reboots, updates, or scans12.
Therefore, the most probable subsequent action from the attacker based on the Cyber Kill Chain Methodology is to exploit the malicious payload delivered to the target organization and establish a foothold, because:
* This action follows the logical sequence of the Cyber Kill Chain Methodology, as it is the next stage after the delivery stage.
* This action is consistent with the attacker's goal, as it allows the attacker to gain access and control over the target system and prepare for further actions.
* This action is feasible, as the attacker has already delivered the malicious payload to the target system and may have bypassed some security controls.

The other options are not as probable as option B for the following reasons:
* A. The attacker will attempt to escalate privileges to gain complete control of the compromised system:
This option is possible, but not the most probable, because it is not the next stage in the Cyber Kill Chain Methodology, but rather a technique that can be used in the exploitation stage or the installation stage. Privilege escalation is a method of increasing the level of access or permissions on a system, such as from a normal user to an administrator. Privilege escalation can help the attacker to gain complete control of the compromised system, but it is not a mandatory step, as the attacker may already have sufficient privileges or may use other techniques to achieve the same goal12.
* C. The attacker will initiate an active connection to the target system to gather more data: This option is possible, but not the most probable, because it is not the next stage in the Cyber Kill Chain Methodology, but rather a technique that can be used in the command and control stage or the actions on objectives stage. An active connection is a communication channel that allows the attacker to send commands or receive data from the target system, such as a remote shell or a botnet. An active connection can help the attacker to gather more data from the target system, but it is not a necessary step, as the attacker may already have enough data or may use other techniques to obtain more data12.
* D. The attacker will start reconnaissance to gather as much information as possible about the target:
This option is not probable, because it is not the next stage in the Cyber Kill Chain Methodology, but rather the first stage. Reconnaissance is the process of collecting information about the target, such as its IP address, domain name, network structure, services, vulnerabilities, or employees. Reconnaissance is usually done before the delivery stage, as it helps the attacker to identify the target and plan the attack. Reconnaissance can be done again after the delivery stage, but it is not the most likely action, as the attacker may already have enough information or may focus on other actions12.
References:
* 1: The Cyber Kill Chain: The Seven Steps of a Cyberattack - EC-Council
* 2: Cyber Kill Chain | Lockheed Martin

質問 # 493

You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacking tool for decryption. What encryption algorithm will you be decrypting?

- A. SHA
- B. DES
- C. SSL
- D. MD4

正解： B

質問 # 494

Jacob works as a system administrator in an organization. He wants to extract the source code of a mobile application and disassemble the application to analyze its design flaws. Using this technique, he wants to fix any bugs in the application, discover underlying vulnerabilities, and improve defense strategies against attacks.
What is the technique used by Jacob in the above scenario to improve the security of the mobile application?

- A. Social engineering
- B. App sandboxing
- C. Jailbreaking
- D. Reverse engineering

正解： D

解説：
Reverse engineering is the process of analyzing compiled software to reconstruct its source code or understand its structure and functionality. In the context of mobile applications:
* It involves decompiling the APK (for Android) or IPA (for iOS) files.
* Analysts can inspect the disassembled or decompiled code.
* The goal is to uncover logic flaws, identify hardcoded secrets, debug issues, or assess security weaknesses.
According to CEH v13:
* Reverse engineering is a common security assessment method to validate code quality and investigate vulnerabilities in mobile and binary applications.
* Tools like JADX, Apktool, Hopper, and Ghidra are often used.
Incorrect Options:

* B. App sandboxing restricts app access to system resources; it's a protection mechanism, not an analysis method.
* C. Jailbreaking is the process of removing OS restrictions, not source code analysis.
* D. Social engineering manipulates human behavior, unrelated to code or binary analysis.
Reference - CEH v13 Official Courseware:
Module 17: Hacking Mobile Platforms
Section: "Mobile Application Security Testing"
Subsection: "Reverse Engineering Tools and Techniques"

質問 # 495
......

我々は312-50v13試験に失敗したら全額で返金するという承諾をしています。お客様は我々の商品を利用したら、試験の出題率は100%とはいきませんが、85%程度は出題されました、もし不幸であなたは312-50v13試験に失敗したら、あなたは失敗した成績書のスキャンを我々のメールアドレスに送って、我々は失敗の原因を問わず、あなたの支払った312-50v13問題集の金額を全額であなたに戻り返してあなたの経済損失を減少します。

312-50v13受験資料更新版: https://www.topexam.jp/312-50v13_shiken.html

また、312-50v13テスト資料ユーザーは、自分の好みに応じて選択できます、我々の提供する312-50v13試験練習問題の以下のメリット、あなたの決意を固めます、我々の312-50v13テスト練習はあなたに最も専業のガイドを提供します、心配することはないよ、TopexamのECCouncilの312-50v13試験トレーニング資料がありますから、Topexam 312-50v13受験資料更新版の試験材料は、経験豊富な専門家によって開発されています、認定試験を通して、これは312-50v13の実際の質問であり、すべてのユーザーの共通の目標であり、信頼できるヘルパーです、ECCouncil 312-50v13必殺問題集 受験生のあなたが首尾よく試験に合格することを助けるように、当社のITエリートの団体はずっと探っています。

は明確にしませんでしたが、理由を見つけるのは難しくありません、何おめでてえ、また、312-50v13テスト資料ユーザーは、自分の好みに応じて選択できます、我々の提供する312-50v13試験練習問題の以下のメリット、あなたの決意を固めます。

312-50v13最新の認定試験勉強資料、312-50v13試験内容、312-50v13出題傾向

我々の312-50v13テスト練習はあなたに最も専業のガイドを提供します、心配することはないよ、TopexamのECCouncilの312-50v13試験トレーニング資料がありますから、Topexamの試験材料は、経験豊富な専門家によって開発されています。

- 認定する312-50v13必殺問題集試験-試験の準備方法-最高の312-50v13受験資料更新版 □ ウェブサイト（ www.shikenpass.com ）を開き、➽ 312-50v13 □を検索して無料でダウンロードしてください312-50v13認証資格
- 312-50v13試験感想 □ 312-50v13試験時間 □ 312-50v13ウェブトレーニング ✴ 時間限定無料で使える“ 312-50v13 ”の試験問題は《 www.goshiken.com 》サイトで検索312-50v13試験対応
- 売れ筋ランキングナンバーワン 312-50v13 を効率よくマスター ↗ ➥ www.passtest.jp □で（ 312-50v13 ）を検索して、無料でダウンロードしてください312-50v13試験感想
- 売れ筋ランキングナンバーワン 312-50v13 を効率よくマスター □ 【 www.goshiken.com 】から簡単に▸ 312-50v13 ◂を無料でダウンロードできます312-50v13ウェブトレーニング
- 312-50v13勉強時間 □ 312-50v13ファンデーション □ 312-50v13試験感想 ↕▶ www.passtest.jp ◀には無料の □ 312-50v13 □問題集があります312-50v13問題と解答
- 売れ筋ランキングナンバーワン 312-50v13 を効率よくマスター □ 最新{ 312-50v13 }問題集ファイルは□ www.goshiken.com □にて検索312-50v13ウェブトレーニング
- 売れ筋ランキングナンバーワン 312-50v13 を効率よくマスター □ 「 www.goshiken.com 」を入力して▹ 312-50v13 ◃を検索し、無料でダウンロードしてください312-50v13問題と解答
- 312-50v13トレーニング □ 312-50v13独学書籍 □ 312-50v13試験関連赤本 □ ▶ www.goshiken.com ◀サイトにて最新▶ 312-50v13 ◀問題集をダウンロード312-50v13ファンデーション
- ハイパスレートの312-50v13必殺問題集一回合格-有難い312-50v13受験資料更新版 □ URL ▶ www.passtest.jp ◀をコピーして開き、“312-50v13 ”を検索して無料でダウンロードしてください312-50v13試験問題解説集
- 売れ筋ランキングナンバーワン 312-50v13 を効率よくマスター □ 時間限定無料で使える（ 312-50v13 ）の試験問題は ➠ www.goshiken.com □サイトで検索312-50v13実際試験
- 312-50v13参考書 □ 312-50v13日本語関連対策 □ 312-50v13シュミレーション問題集 □ 「 312-50v13 」の試験問題は { www.jpshiken.com } で無料配信中312-50v13参考書

- backloggd.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, webanalyticsbd.com, www.stes.tyc.edu.tw, Disposable vapes

無料でクラウドストレージから最新のTopexam 312-50v13 PDFダンプをダウンロードする：https://drive.google.com/open?id=14SZU6wKKXSKm2anuLLdnu47HLvt0xngM