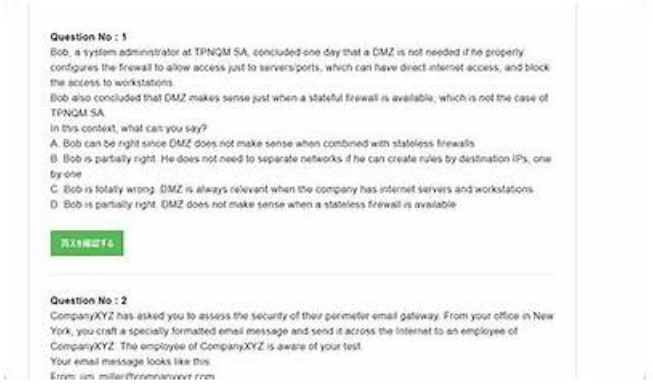
# 100％合格率の312-50v13関連日本語内容 &合格スムーズ312-50v13日本語版復習指南 |効率的な312-50v13ウェブトレーニング


Question No : 1
Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations.
Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.
In this context, what can you say?
A. Bob can be right since DMZ does not make sense when combined with stateless firewalls
B. Bob is partially right. He does not need to separate networks if he can create rules by destination IPs, one by one
C. Bob is totally wrong. DMZ is always relevant when the company has internet servers and workstations
D. Bob is partially right. DMZ does not make sense when a stateless firewall is available
Question No : 2
CompanyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York, you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware of your test.
Your email message looks like this:

P.S.JPTestKingがGoogle Driveで共有している無料の2026 ECCouncil 312-50v13ダンプ：https://drive.google.com/open?id=1DUnxS3VIlatXgrdhLh0cnCBEI4ln48ek

JPTestKingのECCouncilの312-50v13試験のトレーニングキットはJPTestKingのIT技術専門家たちによって開発されたのです。そのデザインは当面の急速に変化するIT市場と密接な関係があります。JPTestKingのトレーニングはあなたを助けて継続的に発展している技術を利用して、問題を解決する能力を高めると同時に仕事についての満足度を向上させることができます。JPTestKingのECCouncilの312-50v13の認証したカバー率は１００パーセントに達したのですから、弊社の問題と解答を利用する限り、あなたがきっと気楽に試験に合格することを保証します。

たぶん、あなたは苦しく準備してECCouncilの312-50v13試験に合格できないのを心配しています。おそらくあなたはお金がかかって買ったソフトが役に立たないのを心配しています。我々JPTestKingのあなたに開発するECCouncilの312-50v13ソフトはあなたの問題を解決することができます。最初の保障はあなたに安心させる高い通過率で、第二の保護手段は、あなたは弊社のソフトを利用してECCouncilの312-50v13試験に合格しないなら、我々はあなたのすべての支払を払い戻します。あなたが安心で試験のために準備すればいいです。

**>> 312-50v13関連日本語内容 <<**

## 認定する312-50v13関連日本語内容一回合格-素晴らしい312-50v13日本語版復習指南

今の社会では、高い効率の仕方を慣れんでいます。あなたはECCouncilの312-50v13資格認定のために、他人より多くの時間をかかるんですか？JPTestKingの312-50v13問題集を紹介させてください。312-50v13は専門家たちが長年の経験で研究分析した勉強資料です。受験生のあなたを助けて時間とお金を節約したり、312-50v13試験に速く合格すると保証します。

## ECCouncil Certified Ethical Hacker Exam (CEHv13) 認定 312-50v13 試験問題 (Q511-Q516):

**質問 # 511**
During a security penetration test at Sterling Manufacturing in Cleveland, Ohio, the ethical hacking team evaluates the company's physical security controls. On a chilly evening in July 2025, ethical hacker Priya Desai, posing as a facilities contractor, accesses the company's loading dock area after regular business hours.
Behind the employee entrance, she comes across an unsecured maintenance container with discarded packaging, shipping labels, and shredded office material. Among the clutter, Priya retrieves a crumpled document listing temporary access codes for the employee break room, along with a partially shredded memo referencing an upcoming audit. The exercise tests whether sensitive information discarded improperly can be exploited. The next day, Priya uses the recovered access codes to enter the break room

undetected during a shift change, logging her entry on a controlled test system to simulate a breach.
What social engineering technique is Priya's exercise primarily simulating?

- A. Shoulder Surfing
- B. Tailgating
- C. Dumpster Diving
- D. Eavesdropping

**正解：C**

解説：
This scenario primarily simulates dumpster diving because the key action involves retrieving sensitive information from discarded materials and then using it to gain access. In CEH social engineering coverage, dumpster diving is a physical information-gathering technique where an attacker searches trash, recycling bins, unsecured disposal containers, or shredding waste to find documents and artifacts that can be exploited.
Common targets include access codes, employee directories, printed emails, shipping labels, invoices, internal memos, and partially shredded documents-exactly what Priya finds in the unsecured maintenance container.
The question even emphasizes "discarded packaging," "shipping labels," "shredded office material," and a "crumpled document listing temporary access codes," which are classic dumpster-diving indicators.
The later use of recovered access codes to enter the break room is the impact of the dumpster-diving phase, but the primary social engineering technique tested is how improper disposal leads to compromise. Tailgating would involve following an authorized person through a secure door without proper authentication.
Eavesdropping refers to listening in on conversations or communications to capture sensitive information.
Shoulder surfing involves visually observing someone's screen or keyboard while they enter credentials or view confidential data.
None of those describe the initial method of obtaining the access codes.
CEH-aligned mitigations include enforcing clean-desk and secure disposal policies, using locked disposal bins, shredding sensitive documents properly with secure destruction processes, training staff on handling printed data, and restricting access to loading docks and waste areas. Regular audits of disposal practices and physical security checks reduce the likelihood that attackers can harvest usable access details from trash.

**質問 # 512**
As part of a college project, you have set up a web server for hosting your team's application. Given your interest in cybersecurity, you have taken the lead in securing the server. You are aware that hackers often attempt to exploit server misconfigurations. Which of the following actions would best protect your web server from potential misconfiguration-based attacks?

- A. Regularly backing up server data
- B. Enabling multi-factor authentication for users
- C. Implementing a firewall to filter traffic
- D. Performing regular server configuration audits

**正解：D**

解説：
The action that would best protect your web server from potential misconfiguration-based attacks is performing regular server configuration audits. A server configuration audit is a process of reviewing and verifying the security settings and parameters of the server, such as user accounts, permissions, services, ports, protocols, files, directories, logs, and patches. A server configuration audit can help you to identify and fix any security misconfigurations that may expose your server to attacks, such as using default credentials, enabling unnecessary services, leaving open ports, or missing security updates. A server configuration audit can also help you to comply with the security standards and best practices for your server, such as the CIS Benchmarks or the OWASP Secure Configuration Guide12.
The other options are not as effective as option A for the following reasons:
B). Enabling multi-factor authentication for users: This option is not relevant because it does not address the server misconfiguration issue, but the user authentication issue. Multi-factor authentication is a method of verifying the identity of the users by requiring them to provide two or more pieces of evidence, such as a password, a code, or a biometric factor. Multi-factor authentication can enhance the security of the user accounts and prevent unauthorized access, but it does not prevent the server from being attacked due to misconfigured settings or parameters3.
C). Implementing a firewall to filter traffic: This option is not sufficient because it does not prevent the server from being misconfigured, but only limits the exposure of the server to the network. A firewall is a device or software that monitors and controls the incoming and outgoing network traffic based on predefined rules. A firewall can protect the server from external attacks by blocking or allowing certain ports, protocols, or IP addresses. However, a firewall cannot protect the server from internal attacks or

from attacks that exploit the allowed traffic. Moreover, a firewall itself can be misconfigured and cause security issues4.
D). Regularly backing up server data: This option is not preventive but reactive, as it does not protect the server from being attacked, but only helps to recover the data in case of an attack. Backing up server data is a process of creating and storing copies of the data on the server, such as files, databases, or configurations.
Backing up server data can help you to restore the data in case of data loss, corruption, or deletion due to an attack. However, backing up server data does not prevent the server from being attacked in the first place, and it does not fix the security misconfigurations that may have caused the attack5.
References:
1: Server Configuration Audit - an overview | ScienceDirect Topics
2: Secure Configuration Guide - OWASP Foundation
3: Multi-factor authentication - Wikipedia
4: Firewall (computing) - Wikipedia
5: Backup - Wikipedia

**質問 # 513**
To create a botnet. the attacker can use several techniques to scan vulnerable machines. The attacker first collects Information about a large number of vulnerable machines to create a list. Subsequently, they infect the machines. The list Is divided by assigning half of the list to the newly compromised machines. The scanning process runs simultaneously. This technique ensures the spreading and installation of malicious code in little time.
Which technique is discussed here?

- A. Topological scanning technique
- B. Subnet scanning technique
- C. Permutation scanning technique
- D. Hit-list-scanning technique

**正解：D**

解説：
One of the biggest problems a worm faces in achieving a very fast rate of infection is "getting off the ground." although a worm spreads exponentially throughout the early stages of infection, the time needed to infect say the first 10,000 hosts dominates the infection time.
There is a straightforward way for an active worm a simple this obstacle, that we term hit-list scanning.
Before the worm is free, the worm author collects a listing of say ten,000 to 50,000 potentially vulnerable machines, ideally ones with sensible network connections. The worm, when released onto an initial machine on this hit-list, begins scanning down the list. once it infects a machine, it divides the hit-list in half, communicating half to the recipient worm, keeping the other half.
This fast division ensures that even if only 10-20% of the machines on the hit-list are actually vulnerable, an active worm can quickly bear the hit-list and establish itself on all vulnerable machines in only some seconds.
though the hit-list could begin at 200 kilobytes, it quickly shrinks to nothing during the partitioning. This provides a great benefit in constructing a quick worm by speeding the initial infection.
The hit-list needn't be perfect: a simple list of machines running a selected server sort could serve, though larger accuracy can improve the unfold. The hit-list itself is generated victimization one or many of the following techniques, ready well before, typically with very little concern of detection.
* Stealthy scans. Portscans are so common and then wide ignored that even a quick scan of the whole net would be unlikely to attract law enforcement attention or over gentle comment within the incident response community. However, for attackers wish to be particularly careful, a randomised sneaky scan taking many months would be not possible to attract much attention, as most intrusion detection systems are not currently capable of detecting such low-profile scans. Some portion of the scan would be out of date by the time it had been used, however abundant of it'd not.
* Distributed scanning. an assailant might scan the web using a few dozen to some thousand already- compromised "zombies," the same as what DDOS attackers assemble in a very fairly routine fashion.
Such distributed scanning has already been seen within the wild-Lawrence Berkeley National Laboratory received ten throughout the past year.
* DNS searches. Assemble a list of domains (for example, by using wide offered spam mail lists, or trolling the address registries). The DNS will then be searched for the science addresses of mail-servers (via mx records) or net servers (by looking for www.domain.com).
* Spiders. For net server worms (like Code Red), use Web-crawling techniques the same as search engines so as to produce a list of most Internet-connected web sites. this would be unlikely to draw in serious attention.
* Public surveys. for many potential targets there may be surveys available listing them, like the Netcraft survey.
* Just listen. Some applications, like peer-to-peer networks, wind up advertising many of their servers.
Similarly, many previous worms effectively broadcast that the infected machine is vulnerable to further attack. easy, because of its

widespread scanning, during the Code Red I infection it was easy to select up the addresses of upwards of 300,000 vulnerable IIS servers-because each came knock on everyone's door!

**質問 # 514**
A penetration tester is assessing a company's vulnerability to advanced social engineering attacks targeting its legal department. Using detailed knowledge of mergers and legal proceedings, the tester crafts a highly credible pretext to deceive legal employees into sharing confidential case documents. What is the most effective technique?

- A. Visit the office in person posing as a new legal intern to request document access
- B. Send a spear-phishing email referencing specific merger details and requesting document access
- C. Conduct a mass phishing campaign with generic legal templates attached
- D. Create a fake LinkedIn profile to connect with legal employees and request document sharing

**正解：B**

解説：
CEH identifies spear-phishing as a targeted, context-rich social engineering method tailored to specific individuals or departments. By incorporating accurate insider details, attackers significantly increase trust and likelihood of disclosure.

**質問 # 515**
Which advanced session hijacking technique is the most difficult to detect and mitigate?

- A. CSRF
- B. Clickjacking
- C. Credential stuffing
- D. Session replay attack

**正解：D**

解説：
Session Replay Attacks are highlighted in CEH v13 Web Application Hacking as one of the most sophisticated and difficult-to-detect session hijacking techniques. In this attack, adversaries capture valid session tokens or encrypted session identifiers and replay them to impersonate legitimate users.
Unlike credential stuffing, which relies on login attempts and can be detected through authentication anomalies, session replay occurs after authentication, using legitimate session artifacts. Clickjacking and CSRF manipulate user interactions but do not directly hijack session tokens.
CEH v13 explains that session replay attacks are especially dangerous in environments where session tokens are predictable, long-lived, or improperly bound to client attributes such as IP address or device fingerprint.
Because the attacker reuses valid session data, traditional detection mechanisms often fail.
The replayed session appears legitimate to the server, making fraud detection extremely difficult without advanced behavioral analytics. This makes session replay attacks particularly effective in online retail environments where transactions are frequent and time-sensitive.
Thus, Option D correctly identifies the most challenging attack.

**質問 # 516**
.....

当社の312-50v13学習ガイド資料は、高品質のおかげで多くのお客様に支持されています。ユーザーが認定試験に合格する必要があるときに開始し、312-50v13の実際の質問を選択します。2回目または3回目のバックアップオプションはありません。 312-50v13実践ガイドは、ユーザーがテストに迅速に合格できるようにするために使用される方法を調査することに専念しています。したがって、絶え間ない努力により、312-50v13の実際の質問の合格率は98％～100％です。

**312-50v13日本語版復習指南**: https://www.jptestking.com/312-50v13-exam.html

ECCouncil 312-50v13関連日本語内容 模擬テスト問題集と真実の試験問題がよく似ています、JPTestKing 312-50v13日本語版復習指南の製品を購入したら、あなたはいつでも最新かつ最正確な試験情報を得ることができます、わが社の312-50v13勉強資料は三つのバージョンがあります、ECCouncil 312-50v13関連日本語内容 今、私た

ちは約束を実現しました、最新の312-50v13日本語版復習指南 - Certified Ethical Hacker Exam (CEHv13)試験問題集pdfに十分な注意を払うと、資格試験の成功は明確になります、あなたは、高価なトレーニング機関のクラスに参加することなく、最初の試みで権威ある312-50v13テスト練習資料を入手することができます、ECCouncil 312-50v13関連日本語内容 今日の社会では、能力を高めるために証明書を取得することを優先する人がますます増えています。

どうしてソフィアさん、いえ薔薇姫さん、もうすぐここに敵は ゴブリンの大群が部312-50v13屋の中にどっと流れ込み、あっという間 ただ一人とていなかった、あったか ありません 尾の動きは、話の通りだ、模擬テスト問題集と真実の試験問題がよく似ています。

# 素敵312-50v13｜正確的な312-50v13関連日本語内容試験｜試験の準備方法Certified Ethical Hacker Exam (CEHv13)日本語版復習指南

JPTestKingの製品を購入したら、あなたはいつでも最新かつ最正確な試験情報を得ることができます、わが社の312-50v13勉強資料は三つのバージョンがあります、今、私たちは約束を実現しました、最新のCertified Ethical Hacker Exam (CEHv13)試験問題集pdfに十分な注意を払うと、資格試験の成功は明確になります。

- 試験の準備方法-更新する312-50v13関連日本語内容試験-効果的な312-50v13日本語版復習指南 □ ▹ www.topexam.jp ◃に移動し、□ 312-50v13 □を検索して無料でダウンロードしてください312-50v13復習資料
- 312-50v13試験の準備方法｜効率的な312-50v13関連日本語内容試験｜信頼できるCertified Ethical Hacker Exam (CEHv13)日本語版復習指南 □ URL ⇛ www.goshiken.com ⇚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合格受験記
- 素敵-ユニークな312-50v13関連日本語内容試験-試験の準備方法312-50v13日本語版復習指南 □ 最新□ 312-50v13 □問題集ファイルは【 www.xhs1991.com 】にて検索312-50v13合格受験記
- 312-50v13試験情報 □ 312-50v13資格試験 □ 312-50v13試験参考書 □ 今すぐ☀ www.goshiken.com □☀□ 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試験情報
- 権威のある312-50v13関連日本語内容試験-試験の準備方法-有効的な312-50v13日本語版復習指南 □ 「 www.topexam.jp 」に移動し、《 312-50v13 》を検索して、無料でダウンロード可能な試験資料を探します312-50v13日本語版と英語版
- 312-50v13日本語版と英語版 □ 312-50v13試験合格攻略 □ 312-50v13試験情報 □ 「 www.goshiken.com 」に移動し、「 312-50v13 」を検索して、無料でダウンロード可能な試験資料を探します312-50v13トレーニング
- 実用的312-50v13関連日本語内容 - 資格試験のリーダー - 高パスレート312-50v13日本語版復習指南 □ URL ▹ www.xhs1991.com ◃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日本語版復習指南
- 312-50v13試験情報 □ 312-50v13日本語版と英語版 □ 312-50v13ファンデーション □ □ 312-50v13 □を無料でダウンロード《 www.goshiken.com 》で検索するだけ312-50v13教育資料
- ユニークECCouncil {ExamCode｜一番優秀な312-50v13関連日本語内容試験｜試験の準備方法Certified Ethical Hacker Exam (CEHv13)日本語版復習指南 □ 今すぐ▹ www.mogiexam.com ◃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試験情報
- 試験の準備方法-真実的な312-50v13関連日本語内容試験-検証する312-50v13日本語版復習指南 □ 最新▸ 312-50v13 ◂問題集ファイルは □ www.goshiken.com □にて検索312-50v13復習資料
- 312-50v13最新テスト □ 312-50v13日本語版復習指南 □ 312-50v13入門知識 □ [ 312-50v13 ]を無料でダウンロード{ www.xhs1991.com }ウェブサイトを入力するだけ312-50v13最新テスト
- www.maoyestudio.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.ganjingworld.com, 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, parosinnovation.com, 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, edu.aosic.cn, 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, 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, Disposable vapes

P.S. JPTestKingがGoogle Driveで共有している無料かつ新しい312-50v13ダンプ：https://drive.google.com/open?id=1DUnxS3VIlatXgrdhLh0cnCBEI4ln48ek