312-50v13 Pruefungssimulationen & 312-50v13 German

Außerdem sind jetzt einige Teile dieser ITZert 312-50v13 Prüfungsfragen kostenlos erhältlich: https://drive.google.com/open?id=1C17lX00PIuu6irxaHLlzNr5azyQ-Vq0a

Im Informationszeitalter kümmern sich viele Leute um die IT-Branche. Aber es fehlen trozt den vielen Exzellenten doch IT-Fachleute. Viele Firmen stellen ihre Angestellte nach ihren Fragenkataloge Zertifikaten ein. Deshalb sind die Zertifikate bei den Firmen sehr beliebt. Aber es ist nicht so leicht, diese Zertifikate zu erhalten. Die ECCouncil 312-50v13 Zertifizierungsprüfung ist eine schwierige Zertifizierungsprüfung. Obwohl viele Menschen beteiligen sich an der ECCouncil 312-50v13 Zertifizierungsprüfung, ist jedoch die Pass-Quote eher niedrig.

Vorm Kauf der Dumps zur 312-50v13 Zertifizierungsprüfung von ITZert können Sie unsere Demo kostenlos als Probe herunterladen.

>> 312-50v13 Pruefungssimulationen <<

312-50v13 German, 312-50v13 Zertifizierungsprüfung

Seit Jahren gilt ITZert als der beste Partner für die IT-Prüfungsteilnehmer. Sie bietet reichliche Ressourcen der Prüfungsunterlagen. Die Bestehensquote der Kunden, die ECCouncil 312-50v13 Prüfungssoftware benutzt haben, erreicht eine Höhe von fast 100%. Diese befriedigte Feedbacks geben wir mehr Motivation, die zuverlässige Qualität von ECCouncil 312-50v13 weiter zu versichern. Wir wünschen Ihnen, durch das Bestehen der ECCouncil 312-50v13 das Gefühl des Erfolgs empfinden, weil es uns auch das Gefühl des Erfolges mitbringt.

ECCouncil Certified Ethical Hacker Exam (CEHv13) 312-50v13 Prüfungsfragen mit Lösungen (Q787-Q792):

787. Frage
Self-replicating malware causes redundant traffic, crashes, and spreads autonomously. What malware type is responsible, and how should it be handled?

- A. Ransomware - disconnect, back up data, decrypt
- B. Trojan - scan systems and patch
- C. Rootkit - reboot and deploy scanner
- D. Worm - isolate systems, scan network, update OS

Antwort: D

Begründung:
This scenario describes a worm infection, as defined in CEH v13 Malware Threats. Worms are self- replicating malware that spread autonomously across networks without user interaction. Their propagation often results in excessive network traffic, system crashes,

and resource exhaustion, which aligns with the symptoms described.
CEH v13 differentiates worms from other malware:
* Ransomware encrypts data but does not self-propagate aggressively.
* Trojans require user execution.
* Rootkits focus on stealth and persistence rather than replication.
The appropriate response prioritizes containment and eradication. Quarantining affected systems prevents further spread. A network-wide antivirus sweep with updated signatures removes known worm variants.
Updating operating systems closes vulnerabilities that worms exploit for propagation.
CEH v13 stresses rapid isolation and patching as critical measures to control worm outbreaks and restore network stability.
Therefore, Option A is correct.

788. Frage
A malware analyst finds JavaScript and /OpenAction keywords in a suspicious PDF using pdfid. What should be the next step to assess the potential impact?

- A. Extract and analyze stream objects using PDFStreamDumper
- B. Upload the file to VirusTotal
- C. Compute file hashes for signature matching

Antwort: A

Begründung:
CEH's Malware Analysis module outlines a structured approach:
* Identify suspicious indicators (e.g., JavaScript, OpenAction)
* Extract and analyze embedded objects
* Determine behavior and exploit logic
PDFStreamDumper allows analysts to extract JavaScript code and embedded objects for detailed inspection.
Option B is correct.
Option A is useful but insufficient for deep analysis.
Option C only aids identification, not behavior understanding.

789. Frage
You are a cybersecurity consultant for a global organization. The organization has adopted a Bring Your Own Device (BYOD)policy, but they have recently experienced a phishing incident where an employee's device was compromised. In the investigation, you discovered that the phishing attack occurred through a third-party email app that the employee had installed. Given the need to balance security and user autonomy under the BYOD policy, how should the organization mitigate the risk of such incidents? Moreover, consider a measure that would prevent similar attacks without overly restricting the use of personal devices.

- A. Provide employees with corporate-owned devices for work-related tasks.
- B. Implement a mobile device management solution that restricts the installation of non-approved applications.
- C. Require all employee devices to use a company-provided VPN for internet access.
- D. Conduct regular cybersecurity awareness training, focusing on phishing attacks.

Antwort: D

Begründung:
The best measure to prevent similar attacks without overly restricting the use of personal devices is to conduct regular cybersecurity awareness training, focusing on phishing attacks. Cybersecurity awareness training is a process of educating and empowering employees on the best practices and behaviors to protect themselves and the organization from cyber threats, such as phishing, malware, ransomware, or data breaches. Cybersecurity awareness training can help the organization mitigate the risk of phishing incidents by providing the following benefits12:
* It can increase the knowledge and skills of employees on how to identify and avoid phishing emails, messages, or links, such as by checking the sender, the subject, the content, the attachments, and the URL of the message, and by verifying the legitimacy and authenticity of the message before responding or clicking.
* It can enhance the attitude and culture of employees on the importance and responsibility of cybersecurity, such as by encouraging them to report any suspicious or malicious activity, to follow the security policies and guidelines, and to seek help or guidance when in doubt or trouble.
* It can reduce the human error and negligence that are often the main causes of phishing incidents, such as by reminding employees to update their devices and applications, to use strong and unique passwords, to enable multi-factor authentication, and to backup

their data regularly.
The other options are not as optimal as option D for the following reasons:
* A. Provide employees with corporate-owned devices for work-related tasks: This option is not feasible because it contradicts the BYOD policy, which allows employees to use their personal devices for work- related tasks. Providing employees with corporate-owned devices would require the organization to incur additional costs and resources, such as purchasing, maintaining, and securing the devices, as well as training and supporting the employees on how to use them. Moreover, providing employees with corporate-owned devices would not necessarily prevent phishing incidents, as the devices could still be compromised by phishing emails, messages, or links, unless the organization implements strict security controls and policies on the devices, which may limit the user autonomy and productivity3.
* B. Implement a mobile device management solution that restricts the installation of non-approved applications: This option is not desirable because it violates the user autonomy and privacy under the BYOD policy, which allows employees to use their personal devices for both personal and professional purposes. Implementing a mobile device management solution that restricts the installation of non- approved applications would require the organization to monitor and control the devices of the employees, which may raise legal and ethical issues, such as data ownership, consent, and compliance. Furthermore, implementing a mobile device management solution that restricts the installation of non-approved applications would not completely prevent phishing incidents, as the employees could still receive phishing emails, messages, or links through the approved applications, unless the organization implements strict security controls and policies on the applications, which may affect the user experience and functionality4.
* C. Require all employee devices to use a company-provided VPN for internet access: This option is not sufficient because it does not address the root cause of phishing incidents, which is the human factor.
Requiring all employee devices to use a company-provided VPN for internet access would provide the organization with some benefits, such as encrypting the network traffic, hiding the IP address, and bypassing geo-restrictions. However, requiring all employee devices to use a company-provided VPN for internet access would not prevent phishing incidents, as the employees could still fall victim to phishing emails, messages, or links that lure them to malicious websites or applications, unless the organization implements strict security controls and policies on the VPN, which may affect the network performance and reliability.
References:
* 1: What is Cybersecurity Awareness Training? | Definition, Benefits & Best Practices | Kaspersky
* 2: How to Prevent Phishing Attacks with Security Awareness Training | Infosec
* 3: BYOD vs. Corporate-Owned Devices: Pros and Cons | Bitglass
* 4: Mobile Device Management (MDM) | OWASP Foundation
* : What is a VPN and why do you need one? Everything you need to know | ZDNet

790. Frage
Which of the following is a low-tech way of gaining unauthorized access to systems?

- A. Sniffing
- B. Social Engineering
- C. Eavesdropping
- D. Scanning

Antwort: B

Begründung:
Social engineering is a non-technical attack that manipulates human behavior to gain access to systems or data. It often involves deception (e.g., phishing, pretexting, baiting) and requires no technical expertise or tools, making it a low-tech yet highly effective method.
Reference - CEH v13 Official Study Guide:
Module 9: Social Engineering
Quote:
"Social engineering exploits human psychology and trust to gain unauthorized access. It is considered a low- tech method because it does not require technical means." Incorrect Options Explained:
B: Eavesdropping may require technical tools to intercept data.
C: Scanning involves active use of tools to find vulnerabilities.
D: Sniffing is technical and requires tools to capture network traffic.

791. Frage
A penetration tester suspects that a web application's user profile page is vulnerable to SQL injection, as it uses the userID parameter in SQL queries without proper sanitization. Which technique should the tester use to confirm the vulnerability?

- A. Modify the userID parameter in the URL to ' OR '1'='1 and check if it returns multiple profiles
- B. Use the userID parameter to perform a brute-force attack on the admin login page
- C. Attempt a directory traversal attack using the userID parameter
- D. Inject HTML code into the userID parameter to test for Cross-Site Scripting (XSS)

Antwort: A

Begründung:
CEH describes SQL injection testing as a core part of web application assessment. One of the first and safest validation techniques is using a tautology-based SQL injection payload, such as ' OR '1'='1. If the application concatenates user input directly into SQL queries, such an input will cause the query to always evaluate as true, often returning additional records such as multiple user profiles. This confirms the presence of SQL injection without causing destructive effects like dropping tables. Testing XSS does not validate SQL injection, brute-forcing credentials is unrelated, and directory traversal attacks target file path manipulation rather than backend queries. CEH emphasizes avoiding destructive queries and starting with non-intrusive injection payloads that reveal improper input sanitization, making ' OR '1'='1 the correct technique for confirming SQL injection vulnerabilities in URL parameters.

792. Frage
.....

- Sie können so einfach wie möglich - 312-50v13 bestehen! □ Suchen Sie einfach auf ▷ www.zertpruefung.ch ◁ nach kostenloser Download von ➡ 312-50v13 □□□ □312-50v13 Examsfragen
- 312-50v13 Pruefungssimulationen □ 312-50v13 Pruefungssimulationen □ 312-50v13 Quizfragen Und Antworten □ Erhalten Sie den kostenlosen Download von ➡ 312-50v13 □□□ mühelos über ☀ www.itzert.com □☀□ □312-50v13 Examsfragen
- 312-50v13 Certified Ethical Hacker Exam (CEHv13) Pass4sure Zertifizierung - Certified Ethical Hacker Exam (CEHv13) zuverlässige Prüfung Übung □ Suchen Sie jetzt auf ⇛ www.zertsoft.com ⇚ nach ☀ 312-50v13 □☀□ um den kostenlosen Download zu erhalten □312-50v13 Vorbereitungsfragen
- Die seit kurzem aktuellsten ECCouncil 312-50v13 Prüfungsinformationen, 100% Garantie für Ihen Erfolg in der Prüfungen! □ □ Suchen Sie jetzt auf □ www.itzert.com □ nach 《 312-50v13 》 und laden Sie es kostenlos herunter □312-50v13 Lernhilfe
- 312-50v13 Zertifizierungsprüfung ↘ 312-50v13 Quizfragen Und Antworten □ 312-50v13 Prüfungsfrage □ ✔ www.deutschpruefung.com □✔□ ist die beste Webseite um den kostenlosen Download von ▸ 312-50v13 ◂ zu erhalten □ □312-50v13 Quizfragen Und Antworten
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, ccinst.in, offensonline.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

P.S. Kostenlose 2026 ECCouncil 312-50v13 Prüfungsfragen sind auf Google Drive freigegeben von ITZert verfügbar: https://drive.google.com/open?id=1C17lX00PIuu6irxaHLlzNr5azyQ-Vq0a