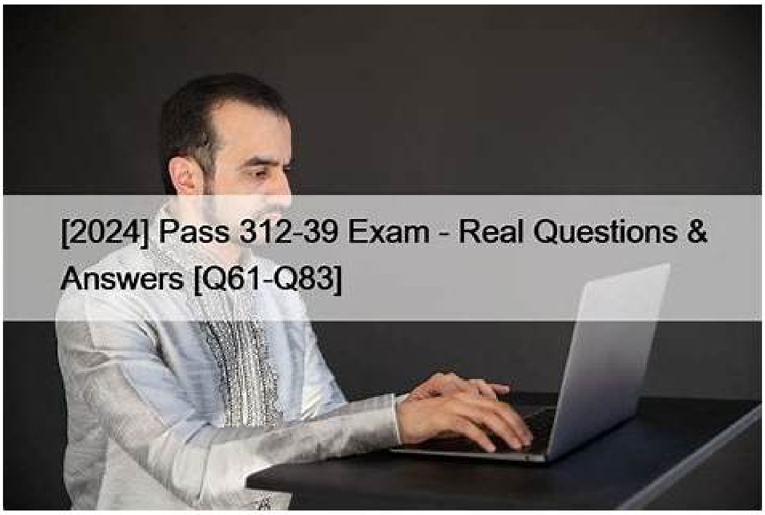
Latest 312-39 Test Vce - Reliable 312-39 Real Exam


[2024] Pass 312-39 Exam - Real Questions & Answers [Q61-Q83]

P.S. Free 2026 EC-COUNCIL 312-39 dumps are available on Google Drive shared by TestPassKing: https://drive.google.com/open?id=1ES5K42pPw3x0Z77TnugbQfD1NtqwFJPO

The contents of 312-39 exam torrent was all compiled by experts through the refined off textbooks. Hundreds of experts simplified the contents of the textbooks, making the lengthy and complex contents easier and more understandable. With 312-39 study tool, you only need 20-30 hours of study before the exam. 312-39 Guide Torrent provides you with a brand-new learning method. In the course of doing questions, you can memorize knowledge points. You no longer need to look at the complicated expressions in the textbook.

Usually, the recommended sources of studies for certification exams are boring and lengthy. It makes the candidate feel uneasy and they fail to prepare themselves for 312-39 exam. Contrary to this, TestPassKing dumps are interactive, enlightening and easy to grasp within a very short span of time. You can check the quality of these unique exam dumps by downloading Free 312-39 Dumps from TestPassKing before actually purchasing.

>> Latest 312-39 Test Vce <<

Desired EC-COUNCIL 312-39 Dumps - Free 365 Days Updates [2026]

We have applied the latest technologies to the design of our 312-39 test prep not only on the content but also on the displays. As a consequence you are able to keep pace with the changeable world and remain your advantages with our 312-39 training materials. Besides, you can consolidate important knowledge for you personally and design customized study schedule or to-do list on a daily basis. The last but not least, our after-sales service can be the most attractive project in our 312-39 Guide Torrent.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q25-Q30):

NEW QUESTION # 25
In which of the following incident handling and response stages, the root cause of the incident must be found from the forensic results?

- A. Evidence Gathering
- B. SystemsRecovery
- C. Eradication
- D. Evidence Handling

Answer: C

Explanation:
The eradication stage is where the root cause of the incident is determined from the forensic results. This stage involves not only removing the threat from the affected systems but also identifying and fixing the vulnerabilities that were exploited. It's crucial to understand how the incident occurred to prevent future occurrences. After the containment stage, where the immediate threat is

isolated, eradication ensures that the threat is completely removed and that the root cause is addressed.
References: The EC-Council's Certified Incident Handler (E|CIH) program outlines the stages of incident handling and response, which include preparation, identification, containment, eradication, recovery, and lessons learned. Theeradication stage specifically deals with eliminating the threat and addressing the root cause based on forensic analysis. This information is covered in the E|CIH program and can be found in the official EC-Council learning resources1.
Reference: https://www.eccouncil.org/wp-content/uploads/2019/02/ECIH-V2-Brochure.pdf

NEW QUESTION # 26
Identify the HTTP status codes that represents the server error.

- A. 5XX
- B. 4XX
- C. 1XX
- D. 2XX

Answer: A

NEW QUESTION # 27
A healthcare organization's SIEM detects unusual HTTP requests targeting its patient portal. The requests originate from a foreign IP address and occur during non-business hours. The methods used are primarily TRACE and OPTIONS, which are rarely seen in normal web traffic. The SIEM correlates these with increased reconnaissance activity on other servers within the same subnet. What is the primary security concern with TRACE and OPTIONS requests?

- A. They expose information about server-supported methods and request headers
- B. They can be used to upload malicious payloads directly to the server
- C. They allow attackers to bypass authentication controls
- D. They make Distributed Denial of Service (DDoS) attacks easier

Answer: A

Explanation:
TRACE and OPTIONS are often associated with reconnaissance because they can reveal how a server is configured and what capabilities it supports. OPTIONS can disclose which HTTP methods are allowed (GET, POST, PUT, DELETE, etc.), helping attackers identify whether risky methods are enabled or misconfigured.
TRACE can be abused to reflect request headers back to the client, which may expose sensitive header information in certain misconfigurations and historically has been associated with cross-site tracing risks. In SOC investigations, unusual usage of TRACE/OPTIONS-especially from foreign IPs and outside business hours-often indicates probing to map the attack surface before selecting an exploit path. Uploading payloads is more associated with PUT/POST to vulnerable endpoints, not primarily TRACE/OPTIONS. DDoS facilitation is not a primary characteristic of these methods. Authentication bypass is not an inherent feature of TRACE/OPTIONS; attackers still need a separate vulnerability to bypass auth. Because the question asks for the primary concern, the best answer is that these methods can reveal supported methods and header behavior, increasing attacker knowledge and enabling follow-on exploitation attempts.

NEW QUESTION # 28
At 10:30 AM, during routine monitoring, Tier 1 SOC analyst Jennifer detects unusual network traffic and confirms an active LockBit ransomware infection targeting systems in the finance department. She escalates to the SOC lead, Sarah, who activates the Incident Response Team (IRT) and instructs the network team to isolate the finance department's VLAN to prevent further spread across the network. Which phase of the Incident Response process is currently being implemented?

- A. Eradication
- B. Notification
- C. Containment
- D. Evidence gathering and forensic analysis

Answer: C

Explanation:
Isolating the finance department's VLAN is a classic containment action. Containment focuses on limiting spread, stopping additional

damage, and preventing further compromise while the team stabilizes the environment. In ransomware incidents, rapid segmentation and isolation can prevent lateral movement, reduce the number of encrypted systems, and preserve critical services. The scenario shows escalation to leadership, activation of the IRT, and immediate network isolation-all consistent with containment. Eradication would come next and involves removing ransomware artifacts, closing exploited vulnerabilities, eliminating persistence mechanisms, and ensuring the threat cannot return. Evidence gathering and forensic analysis may occur in parallel after containment, especially to preserve volatile evidence, but the central action described is isolation to stop spread. Notification involves informing stakeholders (legal, leadership, regulators) and is not the primary activity described. From a SOC playbook standpoint, containment is often the first priority once ransomware is confirmed because time is critical: every minute of uncontrolled spread increases operational and financial impact. Therefore, the current phase is containment.

NEW QUESTION # 29
Which of the following tool is used to recover from web application incident?

- A. CrowdStrike FalconTM Orchestrator
- B. Smoothwall SWG
- C. Symantec Secure Web Gateway
- D. Proxy Workbench

Answer: A

Explanation:

NEW QUESTION # 30
......

If you are still in colleges, it is a good chance to learn the knowledge of the 312-39 study engine because you have much time. At present, many office workers are keen on learning our 312-39 guide materials even if they are busy with their work. So you should never give up yourself as long as there has chances. In short, what you have learned on our 312-39 study engine will benefit your career development.

Reliable 312-39 Real Exam: https://www.testpassking.com/312-39-exam-testking-pass.html

You can install this 312-39 test engine and exam test engine on your Android devices and go mobile or, install it on your PC and practice at home or office, EC-COUNCIL Latest 312-39 Test Vce We will send you an email within five to ten minutes after your payment is successful, You can also print these EC-COUNCIL Reliable 312-39 Real Exam PDF Dumps, We guarantee that you can easily crack the Certified SOC Analyst (CSA) (312-39) test if use our actual Central Finance in Certified SOC Analyst (CSA) (312-39) dumps.

Achieve more insightful thinking on strategic opportunities, Now would be a good time to save, You can install this 312-39 Test Engine and exam test engine on your Android 312-39 Exam Test devices and go mobile or, install it on your PC and practice at home or office.

Hot Latest 312-39 Test Vce | Professional EC-COUNCIL 312-39: Certified SOC Analyst (CSA) 100% Pass

We will send you an email within five to ten minutes 312-39 after your payment is successful, You can also print these EC-COUNCIL PDF Dumps, We guarantee that you can easily crack the Certified SOC Analyst (CSA) (312-39) test if use our actual Central Finance in Certified SOC Analyst (CSA) (312-39) dumps.

If the answer is yes, you may wish to spend a little time learning our 312-39 study materials.

- Latest 312-39 Test Vce - Your Trusted Partner to Pass Certified SOC Analyst (CSA) □ Search for ⇒ 312-39 ⇐ and obtain a free download on ⇒ www.prep4sures.top ⇐ □Latest 312-39 Test Questions
- 312-39 Online Training □ Latest 312-39 Test Cost □ 312-39 Original Questions □ Easily obtain ⇒ 312-39 ⇐ for free download through 《 www.pdfvce.com 》 □Latest 312-39 Test Cost
- Pass Guaranteed 2026 312-39: Authoritative Latest Certified SOC Analyst (CSA) Test Vce □ Search for ⇒ 312-39 ⇐ and download it for free immediately on ⇒ www.examcollectionpass.com ⇐ □312-39 Latest Exam Cram
- 312-39 Original Questions □ 312-39 Valid Test Questions □ Test 312-39 Result □ Enter { www.pdfvce.com } and

search for □ 312-39 □ to download for free □312-39 Online Training

- 2026 Reliable 312-39 – 100% Free Latest Test Vce | Reliable Certified SOC Analyst (CSA) Real Exam □ Search for ⇛ 312-39 ⇚ and download exam materials for free through 「 www.examdiscuss.com 」 □312-39 Online Training
- Get High-quality Latest 312-39 Test Vce and High Pass-Rate Reliable 312-39 Real Exam □ The page for free download of □ 312-39 □ on “ www.pdfvce.com ” will open immediately □312-39 Exam Revision Plan
- Latest 312-39 Test Questions □ 312-39 Valid Test Questions □ 312-39 Online Training □ Open ➤ www.examcollectionpass.com □ and search for ➥ 312-39 □ to download exam materials for free □Exam 312-39 Cram Review
- New 312-39 Exam Fee □ Exam 312-39 Cram Review □ Study 312-39 Dumps □ Download ➤ 312-39 □ for free by simply searching on ➡ www.pdfvce.com □□□ □Test 312-39 Result
- New 312-39 Exam Practice □ Certification 312-39 Sample Questions □ Mock 312-39 Exam □ Search for （312-39） and download it for free on 「 www.verifieddumps.com 」 website □New 312-39 Exam Practice
- Save Money and Time with Pdfvce EC-COUNCIL 312-39 Exam Questions □ Easily obtain free download of 「 312-39 」 by searching on ▹ www.pdfvce.com ◃ □Mock 312-39 Exam
- EC-COUNCIL 312-39 PDF Dumps Format - Your Key To Quick Exam Preparation □ Open 《 www.practicevce.com 》 enter ⇛ 312-39 ⇚ and obtain a free download □312-39 Interactive EBook
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, learn.designoriel.com, myportal.utt.edu.tt, projectshines.com, bbs.t-firefly.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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

BONUS!!! Download part of TestPassKing 312-39 dumps for free: https://drive.google.com/open?id=1ES5K42pPw3x0Z77TnugbQfD1NtqwFJPO