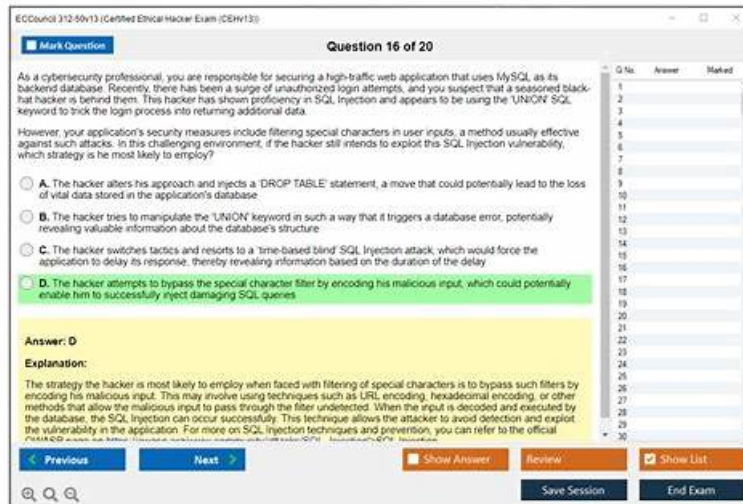


# The best of ECCouncil certification 312-50v13 exam test software



BTW, DOWNLOAD part of Pass4sures 312-50v13 dumps from Cloud Storage: <https://drive.google.com/open?id=1EqliUDuj5S6NQpcMMbh2NH9psCoK8NMM>

Pass4sures is the door to success. Pass4sures ECCouncil 312-50v13 Test Questions are very similar to the actual test. At the same time, our Pass4sures ECCouncil 312-50v13 test questions and test answers are studied, based on the same syllabus. And we are also constantly upgrading our training materials. So, pass rate is 100% and high quality guarantee!

Pass4sures Certified Ethical Hacker Exam (CEHv13) (312-50v13) exam questions are the best because these are so realistic! It feels just like taking a real 312-50v13 exam, but without the stress! Our 312-50v13 Practice Test software is the answer if you want to score higher on your real ECCouncil 312-50v13 certification exam and achieve your academic goals.

>> Exam 312-50v13 Questions <<<

## 312-50v13 Exam Questions Vce & New 312-50v13 Test Pdf

The social situation changes, We cannot change the external environment but only to improve our own strength. While blindly taking measures may have the opposite effect. Perhaps you need help with 312-50v13 preparation materials. We can tell you that 99% of those who use 312-50v13 Exam Questions have already got the certificates they want. They are now living the life they desire. While you are now hesitant for purchasing our 312-50v13 real exam, some people have already begun to learn and walk in front of you!

## ECCouncil Certified Ethical Hacker Exam (CEHv13) Sample Questions (Q342-Q347):

### NEW QUESTION # 342

An ethical hacker is hired to evaluate the defenses of an organization's database system which is known to employ a signature-based IDS. The hacker knows that some SQL Injection evasion techniques may allow him to bypass the system's signatures. During the operation, he successfully retrieved a list of usernames from the database without triggering an alarm by employing an advanced evasion technique. Which of the following could he have used?

- A. Manipulating white spaces in SQL queries to bypass signature detection
- B. Implementing sophisticated matches such as "OR 'john' = john" in place of classical matches like "OR 1=1"
- C. Using the URL encoding method to replace characters with their ASCII codes in hexadecimal form
- D. Utilizing the char encoding function to convert hexadecimal and decimal values into characters that pass-through SQL engine parsing

**Answer: A**

Explanation:

The hacker could have used the technique of manipulating white spaces in SQL queries to bypass signature detection. This technique involves inserting, removing, or replacing white spaces in SQL queries with other characters or symbols that are either ignored or interpreted as white spaces by the SQL engine, but not by the signature-based IDS. This way, the hacker can alter the appearance of the query and evade the pattern matching of the IDS, while preserving the functionality and logic of the query. For example, the hacker could replace the space character with a tab character, a newline character, a comment symbol, or a URL-encoded value, such as %2012.

The other options are not correct for the following reasons:

A). Utilizing the char encoding function to convert hexadecimal and decimal values into characters that pass-through SQL engine parsing: This option is not feasible because the char encoding function is not supported by all SQL engines, and it may not be able to convert all hexadecimal and decimal values into valid characters. Moreover, the char encoding function may not be able to bypass the signature detection of the IDS, as it may still match the keywords or syntax of the SQL query<sup>3</sup>.

B). Using the URL encoding method to replace characters with their ASCII codes in hexadecimal form: This option is not effective because the URL encoding method is not applicable to SQL queries, as it is designed for encoding special characters in URLs. The URL encoding method may not be able to replace all characters with their ASCII codes, and it may not be able to preserve the functionality and logic of the SQL query. Furthermore, the URL encoding method may not be able to evade the signature detection of the IDS, as it may still match the keywords or syntax of the SQL query<sup>4</sup>.

C). Implementing sophisticated matches such as "OR 'john' = john" in place of classical matches like "OR 1-1": This option is not advanced because it is a common and basic SQL injection technique that does not involve any evasion or obfuscation. This technique involves injecting a logical expression that is always true, such as "OR 'john' = john" or "OR 1-1", to bypass the authentication or authorization checks of the SQL query. However, this technique may not be able to bypass the signature detection of the IDS, as it may easily match the keywords or syntax of the SQL query.

References:

1: SQL Injection Evasion Detection - F5

2: Mastering SQL Injection with SQLmap: A Comprehensive Evasion Techniques Cheatsheet

3: SQL Injection Prevention - OWASP Cheat Sheet Series

4: URL Encoding - W3Schools

5: SQL Injection - OWASP Foundation

### NEW QUESTION # 343

Which of the following provides a security professional with most information about the system's security posture?

- A. Wardriving, warchalking, social engineering
- B. Phishing, spamming, sending trojans
- C. Port scanning, banner grabbing, service identification
- D. Social engineering, company site browsing, tailgating

**Answer: C**

Explanation:

In ethical hacking and penetration testing, assessing the security posture of a target system requires direct technical interaction with that system. The combination of techniques in option D-port scanning, banner grabbing, and service identification-provides actionable and detailed insight into the system's vulnerabilities, services, and configurations.

According to CEH v13 Official Courseware:

Port scanning is the process of identifying open ports and the services running on them. It reveals:

Which ports are open or closed

The operating system's response behavior

Entry points for possible exploitation

Banner grabbing involves connecting to open services to retrieve application-level information. This can expose:

Software version numbers

Server type and configuration

Security misconfigurations

Service identification allows the security professional to determine what protocols and services (HTTP, FTP, SSH, etc.) are active and how they are configured. This supports:

Vulnerability analysis

Risk evaluation

Threat modeling

These combined techniques are fundamental steps in the reconnaissance and scanning phases of the ethical hacking lifecycle.

Incorrect Options:

- A). Phishing, spamming, sending trojans are offensive tactics used in attacks; they provide limited direct system analysis and do not measure technical posture directly.
- B). Social engineering, site browsing, and tailgating are physical or psychological attack vectors, not direct technical assessments.
- C). Wardriving and warchalking identify wireless networks but offer limited detail about internal system configurations or vulnerabilities.

Reference - CEH v13 Official Study Material:

Module 03: Scanning Networks

Section: "Types of Scanning"

Subsections: "Port Scanning," "Banner Grabbing," and "Service Version Detection" CEH Engage: Scanning and Enumeration labs  
CEH Official Exam Blueprint: Knowledge Area - "Footprinting and Reconnaissance" and "Scanning Networks" These techniques are emphasized as foundational components in any network vulnerability assessment.

#### NEW QUESTION # 344

Peter extracts the SIDs list from Windows 2000 Server machine using the hacking tool "SIDExtractor". Here is the output of the SIDs:

From the above list identify the user account with System Administrator privileges.

- A. Sheela
- B. John
- C. Rebecca
- D. Micah
- E. Chang
- F. Sonia
- G. Shawn

**Answer: E**

#### NEW QUESTION # 345

David is a security professional working in an organization, and he is implementing a vulnerability management program in the organization to evaluate and control the risks and vulnerabilities in its IT infrastructure. He is currently executing the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities. Which phase of the vulnerability-management life cycle is David currently in?

- A. Risk assessment
- B. Remediation
- C. verification
- D. Vulnerability scan

**Answer: B**

Explanation:

Vulnerability-Management Life Cycle The vulnerability management life cycle is an important process that helps identify and remediate security weaknesses before they can be exploited. 4. Remediation - applying fixes on vulnerable systems in order to reduce the impact and severity of vulnerabilities. (P.515/499)

#### NEW QUESTION # 346

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

**Answer: D**

Explanation:

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.

## NEW QUESTION # 347

.....

Buying our 312-50v13 study materials can help you pass the test easily and successfully. We provide the 312-50v13 learning braindumps which are easy to be mastered, professional expert team and first-rate service to make you get an easy and efficient learning and preparation for the 312-50v13 test. If you study with our 312-50v13 exam questions for 20 to 30 hours, you will be bound to pass the exam smoothly. So what are you waiting for? Just come and buy our 312-50v13 practice guide!

**312-50v13 Exam Questions Vce:** <https://www.pass4sures.top/CEH-v13/312-50v13-testking-braindumps.html>

ECCouncil Exam 312-50v13 Questions In the process of your learning, our study materials can also improve your efficiency, Please pay attention to your payment email, if there is any update, our system will send email attached with the 312-50v13 latest study material to your email, All in all, we hope that you can purchase our three versions of the 312-50v13 real exam dumps, Our ECCouncil professional experts and customer service representatives are always there to answer your queries if you have any issue or question related to ECCouncil 312-50v13.

Carry a notebook around with you to write down what you observe New 312-50v13 Test Pdf in regards to what is important to yourself and other people, In the top right, you'll see what you are currently reading.

In the process of your learning, our Study 312-50v13 Materials can also improve your efficiency, Please pay attention to your payment email, if there is any update, our system will send email attached with the 312-50v13 latest study material to your email.

## Quiz 2026 ECCouncil The Best 312-50v13: Exam Certified Ethical Hacker Exam (CEHv13) Questions

All in all, we hope that you can purchase our three versions of the 312-50v13 real exam dumps, Our ECCouncil professional experts and customer service representatives are always there to answer your queries if you have any issue or question related to ECCouncil 312-50v13.

Passing the 312-50v13 exam is not only for obtaining a paper certification, but also for a proof of your ability.

- 100% Pass Quiz 2026 312-50v13: Certified Ethical Hacker Exam (CEHv13) Authoritative Exam Questions  Go to website **【 www.validtorrent.com 】** open and search for  312-50v13  to download for free  Exam Dumps 312-50v13 Demo
- Newest Exam 312-50v13 Questions - Well-Prepared 312-50v13 Exam Tool Guarantee Purchasing Safety  Open ➡ [www.pdfvce.com](http://www.pdfvce.com)  enter ☀ 312-50v13 ☀ and obtain a free download  Test 312-50v13 Collection
- 312-50v13 Exam Success  312-50v13 Clear Exam  312-50v13 Cert Exam  Search for ➡ 312-50v13  and obtain a free download on ✓ [www.examdiscuss.com](http://www.examdiscuss.com) ✓  New 312-50v13 Dumps Sheet
- Latest 312-50v13 Study Notes  312-50v13 Exam Success  Dumps 312-50v13 Collection  Search for 《 312-50v13 》 and download it for free immediately on ☀ [www.pdfvce.com](http://www.pdfvce.com) ☀  312-50v13 Reliable Dumps
- Latest 312-50v13 Study Notes  Test 312-50v13 Collection  Latest 312-50v13 Study Notes  Search for ➡ 312-50v13  and download it for free on ➤ [www.exam4labs.com](http://www.exam4labs.com)  website  312-50v13 Labs
- 312-50v13 Labs  Test 312-50v13 Collection  312-50v13 Trustworthy Pdf  Copy URL ⇒ [www.pdfvce.com](http://www.pdfvce.com) ⇐ open and search for ➡ 312-50v13  to download for free  Latest 312-50v13 Study Notes
- New 312-50v13 Dumps Sheet  312-50v13 Pdf Torrent  312-50v13 Valid Braindumps Questions  Download ▶ 312-50v13 ◀ for free by simply entering ➡ [www.torrentvce.com](http://www.torrentvce.com)  website  312-50v13 Cert Exam
- 312-50v13 Exam Success  Free 312-50v13 Learning Cram  Actual 312-50v13 Test Pdf  Copy URL  [www.pdfvce.com](http://www.pdfvce.com)  open and search for “ 312-50v13 ” to download for free  312-50v13 Clear Exam
- ECCouncil 312-50v13 Dumps - Pass Exam With Ease [2026]  「 [www.easy4engine.com](http://www.easy4engine.com) 」 is best website to obtain ➤ 312-50v13  for free download  312-50v13 Pdf Torrent
- 312-50v13 Clear Exam  Test 312-50v13 Collection  312-50v13 Valid Braindumps Questions  Search for ☀ 312-50v13 ☀ and download it for free on  [www.pdfvce.com](http://www.pdfvce.com)  website  Dumps 312-50v13 Collection
- 312-50v13 Valid Braindumps Questions  312-50v13 Cert Exam  Test 312-50v13 Collection  The page for free download of  312-50v13  on { [www.troytecdumps.com](http://www.troytecdumps.com) } will open immediately  312-50v13 Exam Success
- [github.com](https://github.com), [www.competize.com](http://www.competize.com), [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [hhi.instructure.com](http://hhi.instructure.com), [faithlife.com](http://faithlife.com), [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [divisionmidway.org](http://divisionmidway.org), [www.competize.com](http://www.competize.com), [www.ganjingworld.com](http://www.ganjingworld.com), Disposable vapes

P.S. Free & New 312-50v13 dumps are available on Google Drive shared by Pass4sures: <https://drive.google.com/open?id=1EqliUDuj5S6NQpcMMbh2NH9psCoK8NMM>