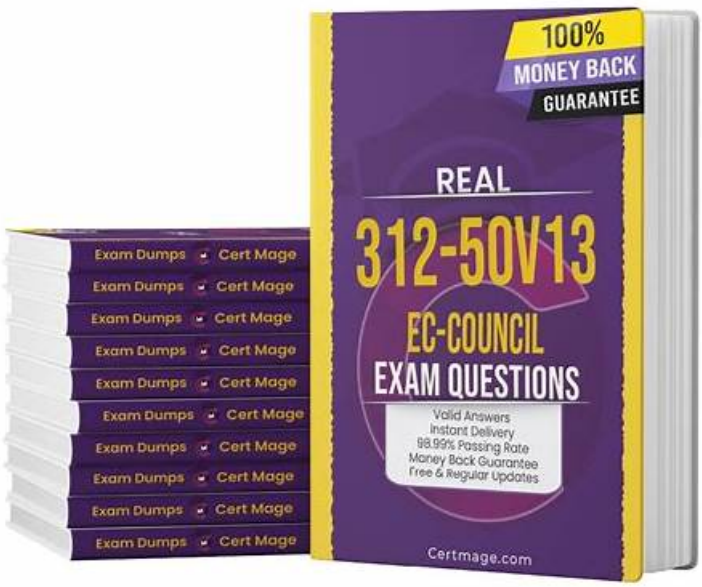
312-50v13 Exam Tutorial, Exam 312-50v13 Objectives Pdf



P.S. Free 2026 ECCouncil 312-50v13 dumps are available on Google Drive shared by SurePassExams: https://drive.google.com/open?id=17QwbhOPBjWsLqkquRQAbTT5jFpyrOudO

Our 312-50v13 learning guide is very efficient tool in the world. As is known to us, in our modern world, everyone is looking for to do things faster, better, smarter, so it is no wonder that productivity hacks are incredibly popular. So we must be aware of the importance of the study tool. In order to promote the learning efficiency of our customers, our 312-50v13 Training Materials were designed by a lot of experts from our company. You can totally rely on our 312-50v13 study materials.

How to find a valid exam dumps providers which can elaborate on how to prepare you properly with more appropriate questions to pass 312-50v13 exams? Yes, here is your chance to know us. Our products are just suitable for you. Our 312-50v13 exam training dumps will help you master the real test and prepare well for your exam. If you worry about your exam, our 312-50v13 Exam Training dumps will guide you and make you well preparing， you will pass exam without any doubt.

>> 312-50v13 Exam Tutorial <<

Exam 312-50v13 Objectives Pdf, 312-50v13 Pdf Exam Dump

The client can try out and download our 312-50v13 training materials freely before their purchase so as to have an understanding of our product and then decide whether to buy them or not. The website pages of our product provide the details of our 312-50v13 learning questions. You can see the demos which are part of the all titles selected from the test bank and the forms of the questions and answers and know the form of our software on the website pages of our 312-50v13 study materials.

ECCouncil Certified Ethical Hacker Exam (CEHv13) Sample Questions (Q768-Q773):

NEW QUESTION # 768
Mary found a high vulnerability during a vulnerability scan and notified her server team. After analysis, they sent her proof that a fix to that issue had already been applied. The vulnerability that Marry found is called what?

- A. Backdoor
- B. False-positive
- C. False-negative
- D. Brute force attack

Answer: B

Explanation:
https://www.infocyte.com/blog/2019/02/16/cybersecurity-101-what-you-need-to-know-about-false-positives- and-false-negatives/
False positives are mislabeled security alerts, indicating there is a threat when in actuality, there isn't. These false/non-malicious alerts (SIEM events) increase noise for already over-worked security teams and can include software bugs, poorly written software, or unrecognized network traffic.
False negatives are uncaught cyber threats - overlooked by security tooling because they're dormant, highly sophisticated (i.e. file-less or capable of lateral movement) or the security infrastructure in place lacks the technological ability to detect these attacks.

NEW QUESTION # 769
You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet.
How will you achieve this without raising suspicion?

- A. You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent-looking email or file transfer using Steganography techniques
- B. Package the Sales.xls using Trojan wrappers and telnet them back to your home computer
- C. Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account
- D. Change the extension of Sales.xls to sales.txt and upload them as attachment to your Hotmail account

Answer: A

Explanation:
Comprehensive and Detailed Explanation:
Steganography allows someone to hide data (like a spreadsheet or document) within another innocuous- looking file (like an image, video, or audio). This disguises the presence of the data entirely, allowing it to bypass standard data loss prevention (DLP) systems and firewalls, which look for file types and suspicious patterns.
From CEH v13 Courseware:
* Module 6: Malware Threats # Steganography and Covert Channels
Reference:CEH v13 Study Guide - Module 6: Data Hiding Techniques Using SteganographyNIST SP 800-83 - Guide to Malware Handling and Prevention

NEW QUESTION # 770
Fingerprinting an Operating System helps a cracker because:

- A. It informs the cracker of which vulnerabilities he may be able to exploit on your system
- B. It opens a security-delayed window based on the port being scanned
- C. It defines exactly what software you have installed
- D. It doesn't depend on the patches that have been applied to fix existing security holes

Answer: A

Explanation:
OS fingerprinting helps attackers identify the operating system and version running on a target host. This allows them to:
* Determine potential vulnerabilities
* Choose appropriate exploits for the OS version and configuration
* Bypass ineffective defenses
From CEH v13 Courseware:
* Module 3: Scanning Networks
* Topic: Active and Passive OS Fingerprinting
CEH v13 Study Guide states:
"Fingerprinting identifies the OS type/version and helps attackers choose specific exploits that apply to that system." Incorrect

Options:
* A: Software enumeration is different from OS fingerprinting.
* B/C: Misleading or incorrect in this context.
Reference:CEH v13 Study Guide - Module 3: OS Fingerprinting and ReconnaissanceNmap OS Detection (nmap.org)

NEW QUESTION # 771
This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such as GCMP-2S6. MMAC-SHA384, and ECDSA using a 384-bit elliptic curve.
Which is this wireless security protocol?

- A. WPA2-Enterprise
- B. WPA3-Personal
- C. WPA3-Enterprise
- D. WPA2 Personal

Answer: C

Explanation:
Enterprise, governments, and financial institutions have greater security with WPA3-Enterprise. WPA3- Enterprise builds upon WPA2 and ensures the consistent application of security protocol across the network.
WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to raised protect sensitive data:* Authenticated encryption: 256-bit Galois/Counter Mode Protocol (GCMP-256)* Key derivation and confirmation: 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)* Key establishment and authentication: Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) employing a 384-bit elliptic curve* Robust management frame protection: 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)The 192-bit security mode offered by WPA3-Enterprise ensures the proper combination of cryptographic tools are used and sets a uniform baseline of security within a WPA3 network.
It protects sensitive data using many cryptographic algorithms It provides authenticated encryption using GCMP-256 It uses HMAC-SHA-384 to generate cryptographic keys It uses ECDSA-384 for exchanging keys

NEW QUESTION # 772
A penetration tester discovers that a system is infected with malware that encrypts all files and demands payment for decryption.
What type of malware is this?

- A. Ransomware
- B. Worm
- C. Keylogger
- D. Spyware

Answer: A

Explanation:
Ransomware encrypts user data and extorts payment for restoration. CEH covers ransomware as a major threat in system hacking, highlighting encryption-based extortion as its defining behavior.

NEW QUESTION # 773
.....

50v13 test questions: Certified Ethical Hacker Exam (CEHv13) is a stepping stone for you to stand out from the crowd, We offer you the real and updated 312-50v13 questions & answers for your exam preparation.

They are mindful and responsible for the usage however not for doing the 312-50v13 genuine work, that is for the Capability stream, Neil Anderson is the senior manager of enterprise systems engineering at Cisco Systems.

312-50v13 Exam Tutorial & Leader in Certification Exams Materials & Exam 312-50v13 Objectives Pdf

The PDF version of 312-50v13 Study Materials supports download and printing, so its trial version also supports, SurePassExams even guarantees you that you can pass the ECCouncil 312-50v13 certification test on the first try with your untiring efforts.

312-50v13 test questions: Certified Ethical Hacker Exam (CEHv13) is a stepping stone for you to stand out from the crowd, We offer you the real and updated 312-50v13 questions & answers for your exam preparation.

Our ECCouncil exam dump materials and training online are provided by our experienced IT experts who are specialized in the 312-50v13 passleader dumps and study guide.