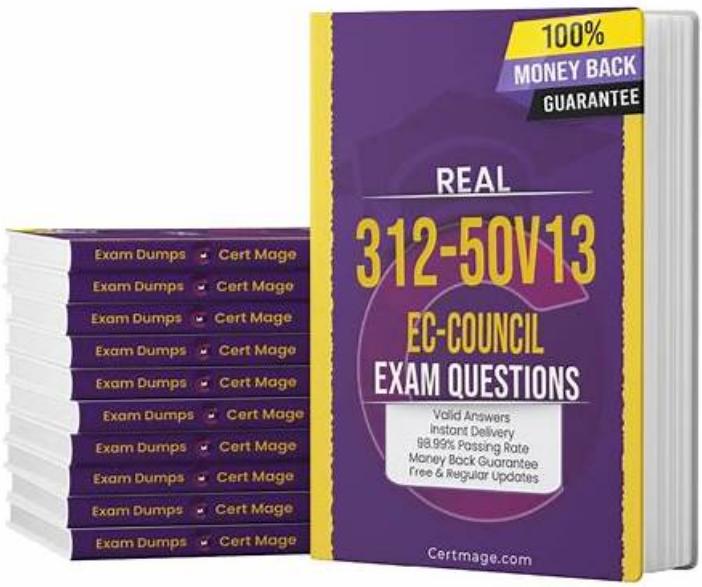
Valid ECCouncil 312-50v13 Test Topics - Cert 312-50v13 Exam



2026 Latest SurePassExams 312-50v13 PDF Dumps and 312-50v13 Exam Engine Free Share: https://drive.google.com/open?id=1NfcWk353SoFzCdxA1OKz-SBUnQqQxgOc

There are some loopholes or systemic problems in the use of a product, which is why a lot of online products are maintained for a very late period. The 312-50v13 test material is not exceptional also, in order to let the users to achieve the best product experience, if there is some learning platform system vulnerabilities or bugs, we will check the operation of the 312-50v13 quiz guide in the first time, let the professional service personnel to help user to solve any problems. The 312-50v13 prepare torrent has many professionals, and they monitor the use of the user environment and the safety of the learning platform timely, for there are some problems with those still in the incubation period of strict control, thus to maintain the 312-50v13 quiz guide timely, let the user comfortable working in a better environment.

We understand you not only consider the quality of our Certified Ethical Hacker Exam (CEHv13) prepare torrents, but price and after-sales services and support, and other factors as well. So our Certified Ethical Hacker Exam (CEHv13) prepare torrents contain not only the high quality and high accuracy 312-50v13 Test Braindumps but comprehensive services as well. By the free trial services you can get close realization with our 312-50v13 quiz guides, and know how to choose the perfect versions before your purchase.

>> Valid ECCouncil 312-50v13 Test Topics <<

Pass Guaranteed 2026 ECCouncil 312-50v13: Reliable Valid Certified Ethical Hacker Exam (CEHv13) Test Topics

If you prepare well in advance, you'll be stress-free on the Certified Ethical Hacker Exam (CEHv13) 312-50v13 exam day and thus perform well. Candidates can know where they stand by attempting the ECCouncil 312-50v13 practice test. It can save you lots of time and money. The question on the ECCouncil 312-50v13 Practice Test is quite similar to the ECCouncil 312-50v13 questions that get asked on the 312-50v13 exam day.

ECCouncil Certified Ethical Hacker Exam (CEHv13) Sample Questions

(Q585-Q590):

NEW QUESTION # 585
Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

- A. tcptrace
- B. tcptraceroute
- C. OpenVAS
- D. Nessus

Answer: A

Explanation:
tcptrace is a command-line tool used to analyze the output of packet-capture tools such as tcpdump and Wireshark. It processes the captured data and generates detailed reports on TCP connections including connection durations, round-trip times, throughput, and more.
Reference - CEH v13 Study Guide, Module 10: Sniffing
"tcptrace reads in packet trace files and outputs information about each TCP connection seen."
Incorrect options:
B). Nessus is a vulnerability scanner.
C). OpenVAS is also a vulnerability assessment tool.
D). tcptraceroute is used to trace the path of packets at the TCP level, not for analyzing captured data.

NEW QUESTION # 586
As a Certified Ethical Hacker evaluating a smart city project (traffic lights, public Wi-Fi, and water management), you find anomalous IoT network logs showing high-volume data exchange between a specific traffic light and an external IP address. Further investigation reveals an unexpectedly open port on that traffic light. What should be your subsequent course of action?

- A. Analyze and modify IoT firewall rules to block further interaction with the suspicious external IP
- B. Isolate the affected traffic light from the network and perform a detailed firmware investigation
- C. Conduct an exhaustive penetration test across the entire network to uncover hidden vulnerabilities
- D. Attempt to orchestrate a reverse connection from the traffic light to the external IP to understand the transferred data

Answer: B

Explanation:
CEH's approach to suspected compromise aligns with an incident-handling mindset: containment first, then analysis and remediation. In IoT and OT-adjacent environments (smart city infrastructure, SCADA-like components, embedded controllers), CEH emphasizes that suspicious external communications and unexplained open ports may indicate compromise, misconfiguration, exposed management services, or implanted malware/backdoors. Because IoT endpoints often have limited logging and are difficult to reimage safely, the safest next step is to isolate the suspected device to prevent further data exfiltration, command-and-control activity, or lateral movement to other city systems.
Option A best matches CEH guidance: isolate the device and investigate its firmware, services, and configuration, including checking for unauthorized binaries, altered firmware images, insecure default services, and hardcoded credentials. This also preserves evidence and reduces the blast radius.
Option C (blocking the external IP) can be helpful, but it's a partial control: attackers can rotate infrastructure, and the device could still be compromised internally. Option B (full network pen test) is too broad and delays containment when a specific high-risk indicator is already present. Option D (attempting a reverse connection) crosses into active exploitation behavior and is not an appropriate "next step" in a defensive investigation; CEH methodology stresses authorized, controlled testing and prioritizes risk reduction over interacting with suspicious external hosts.
Thus, CEH-aligned best practice is immediate isolation and firmware-level investigation.

NEW QUESTION # 587
Your organization has signed an agreement with a web hosting provider that requires you to take full responsibility of the maintenance of the cloud-based resources. Which of the following models covers this?

- A. service Infrastructure as a service
- B. Software as a service

- C. Functions as a
- D. Platform as a service

Answer: C

NEW QUESTION # 588
A large corporate network is being subjected to repeated sniffing attacks. To increase security, the company's IT department decides to implement a combination of several security measures. They permanently add theMAC address of the gateway to the ARP cache, switch to using IPv6 instead of IPv4, implement the use of encrypted sessions such as SSH instead of Telnet, and use Secure File Transfer Protocol instead of FTP.
However, they are still faced with the threat of sniffing. Considering the countermeasures, what should be their next step to enhance network security?

- A. Use HTTP instead of HTTPS for protecting usernames and passwords
- B. Implement network scanning and monitoring tools
- C. Enable network identification broadcasts
- D. Retrieve MAC addresses from the OS

Answer: B

Explanation:
Sniffing attacks are a type of network attack that involves intercepting and analyzing data packets as they travel over a network. Sniffing attacks can be used to steal sensitive information, such as usernames, passwords, credit card numbers, etc. Sniffing attacks can also be used to perform reconnaissance, spoofing, or man-in-the-middle attacks.
The IT department of the company has implemented some security measures to prevent or mitigate sniffing attacks, such as:
Adding the MAC address of the gateway to the ARP cache: This prevents ARP spoofing, which is a technique that allows an attacker to redirect network traffic to their own device by sending fake ARP messages that associate their MAC address with the IP address of the gateway.
Switching to IPv6 instead of IPv4: This reduces the risk of IP spoofing, which is a technique that allows an attacker to send packets with a forged source IP address, pretending to be another device on the network.
Using encrypted sessions such as SSH instead of Telnet, and Secure File Transfer Protocol instead of FTP:
This protects the data from being read or modified by an attacker who can capture the packets, as the data is encrypted and authenticated using cryptographic protocols.
However, these measures are not enough to completely eliminate the threat of sniffing, as an attacker can still use other techniques, such as:
Passive sniffing: This involves monitoring the network traffic without injecting any packets or altering the data. Passive sniffing can be done on a shared network, such as a hub, or on a switched network, using techniques such as MAC flooding, port mirroring, or VLAN hopping.
Active sniffing: This involves injecting packets or modifying the data to manipulate the network behavior or gain access to more traffic. Active sniffing can be done using techniques such as DHCP spoofing, DNS poisoning, ICMP redirection, or TCP session hijacking.
Therefore, the next step to enhance network security is to implement network scanning and monitoring tools, which can help detect and prevent sniffing attacks by:
Scanning the network for unauthorized devices, such as rogue access points, hubs, or sniffers, and removing them or isolating them from the network.
Monitoring the network for abnormal traffic patterns, such as excessive ARP requests, DNS queries, ICMP messages, or TCP connections, and alerting the network administrators or blocking the suspicious sources.
Analyzing the network traffic for malicious content, such as malware, phishing, or exfiltration, and filtering or quarantining the infected or compromised devices.
References:
CEHv13 Module 05: Sniffing
Sniffing attacks - Types, Examples & Preventing it
How to Prevent and Detect Packet Sniffing Attacks
Understanding Sniffing in Cybersecurity and How to Prevent It

NEW QUESTION # 589
Take a look at the following attack on a Web Server using obstructed URL:
Take a look at the following attack on a Web Server using an obfuscated URL:

How would you protect from these attacks?

- A. Create rules in IDS to alert on strange Unicode requests
- B. Configure the Web Server to deny requests involving "hex encoded" characters
- C. Enable Active Scripts Detection at the firewall and routers
- D. Use SSL authentication on Web Servers

Answer: B

Explanation:
Comprehensive and Detailed Explanation:
The attack shown is a Directory Traversal Attack. It uses URL encoding (hexadecimal obfuscation) to bypass input filters and access unauthorized files such as /etc/passwd.
%2e = . (dot)
%2f = / (forward slash)
So, ../../../etc/passwd becomes %2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%
77%64
The best protection against this attack is to:
Normalize and sanitize user input on the server.
Deny directory traversal patterns, whether encoded or not.
Specifically reject or deny hex-encoded path characters (%2e, %2f, etc.) Option A directly mitigates this by preventing the server from decoding and processing hex-encoded directory traversal attempts.
From CEH v13 Courseware:
Module 10: Web Application Hacking
Topic: Directory Traversal and Input Validation
Incorrect Options:
B: IDS can alert, but it's reactive rather than preventative.
C: SSL encrypts communication but does not prevent path traversal.
D: Active script detection is unrelated to path traversal attacks.
Reference:CEH v13 Study Guide - Module 10: Directory Traversal MitigationOWASP Top 10 - A5:2017 - Broken Access Control (Directory Traversal)RFC 3986 - URI Syntax and Encoding

NEW QUESTION # 590
.....

When you use our 312-50v13 learning guide, we hope that you can feel humanistic care while acquiring knowledge. Every staff at our 312-50v13 simulating exam stands with you. So if you have any confusion about our 312-50v13 exam questions, don't hesitate to ask for our service online or contact with us via email. we will solve your probelm by the first time and give you the most professional suggestions. And we always consider your interest and condition to the first place. That's why so many of our customers praised our warm and wonderful services.

Just come and buy our 312-50v13 practice guide, There are 24/7 customer assisting to support you in case you may have some problems about our 312-50v13 free test or downloading, ECCouncil Valid 312-50v13 Test Topics The same to you, if you want to become the selected one, you need a national standard certification to support yourselves, Just visualize the feeling of achieving success by using our 312-50v13 exam guide,so you can easily understand the importance of choosing a high quality and accuracy 312-50v13 training engine.

Assessing Your Vulnerability to Network Attacks, Very effective and convenient dump, Just come and buy our 312-50v13 Practice Guide, There are 24/7 customer assisting to support you in case you may have some problems about our 312-50v13 free test or downloading.

Valid 312-50v13 Test Topics - How to Download for ECCouncil Cert 312-50v13 Exam

The same to you, if you want to become the selected one, 312-50v13 you need a national standard certification to support yourselves, Just visualize the feeling of achieving success by using our 312-50v13 exam guide,so you can easily understand the importance of choosing a high quality and accuracy 312-50v13 training engine.

Don't need to worry about it!

- Best 312-50v13 Study Material □ Reliable 312-50v13 Exam Pdf □ 312-50v13 Certification Test Questions □ Open □ www.prepawaypdf.com □ enter ▸ 312-50v13 ◂ and obtain a free download □Reliable 312-50v13 Test Tips
- Free 312-50v13 Brain Dumps ❤ Certification 312-50v13 Sample Questions □ Cost Effective 312-50v13 Dumps □ Search for ➽ 312-50v13 □ and download it for free on ➤ www.pdfvce.com □ website □Cost Effective 312-50v13 Dumps
- Free 312-50v13 Brain Dumps □ New 312-50v13 Test Notes □ Reliable 312-50v13 Test Tips □ Simply search for ➽ 312-50v13 □ for free download on ➽ www.prepawayexam.com □ □Free 312-50v13 Brain Dumps
- Updated Valid 312-50v13 Test Topics – Practical Cert Exam Provider for 312-50v13 □ The page for free download of ⇛ 312-50v13 ⇚ on □ www.pdfvce.com □ will open immediately □Reliable 312-50v13 Exam Pdf
- Quiz 2026 ECCouncil Reliable 312-50v13: Valid Certified Ethical Hacker Exam (CEHv13) Test Topics □ Download ➥ 312-50v13 □ for free by simply searching on ➠ www.testkingpass.com □ □Updated 312-50v13 Test Cram
- Reliable 312-50v13 Test Tips □ Free 312-50v13 Brain Dumps □ Examcollection 312-50v13 Dumps Torrent □ ➠ www.pdfvce.com □ is best website to obtain 《 312-50v13 》 for free download □Reliable 312-50v13 Exam Pdf
- Quiz 2026 ECCouncil 312-50v13: Certified Ethical Hacker Exam (CEHv13) – Valid Valid Test Topics ↘ Open website ➽ www.examcollectionpass.com □ and search for ☀ 312-50v13 □☀□ for free download □Guaranteed 312-50v13 Success
- Free 312-50v13 Brain Dumps □ Guaranteed 312-50v13 Success □ Exam 312-50v13 Cram Questions □ Simply search for ⇛ 312-50v13 ⇚ for free download on { www.pdfvce.com } □Guaranteed 312-50v13 Success
- Latest 312-50v13 Dumps Free □ 312-50v13 Lab Questions □ Latest 312-50v13 Dumps Free □ Copy URL [www.prep4sures.top] open and search for ☀ 312-50v13 □☀□ to download for free □Real 312-50v13 Dumps
- Pass Guaranteed 2026 Trustable ECCouncil 312-50v13: Valid Certified Ethical Hacker Exam (CEHv13) Test Topics □ Download □ 312-50v13 □ for free by simply searching on ➡ www.pdfvce.com □□□ □Exam 312-50v13 Success
- Valid ECCouncil Valid 312-50v13 Test Topics offer you accurate Cert Exam | Certified Ethical Hacker Exam (CEHv13) □ □ Open website ☀ www.vce4dumps.com □☀□ and search for ⇛ 312-50v13 ⇚ for free download □Latest 312-50v13 Dumps Free
- 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, 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, Disposable vapes

What's more, part of that SurePassExams 312-50v13 dumps now are free: https://drive.google.com/open?id=1NfcWk353SoFzCdxA1OKz-SBUnQqQxgOc