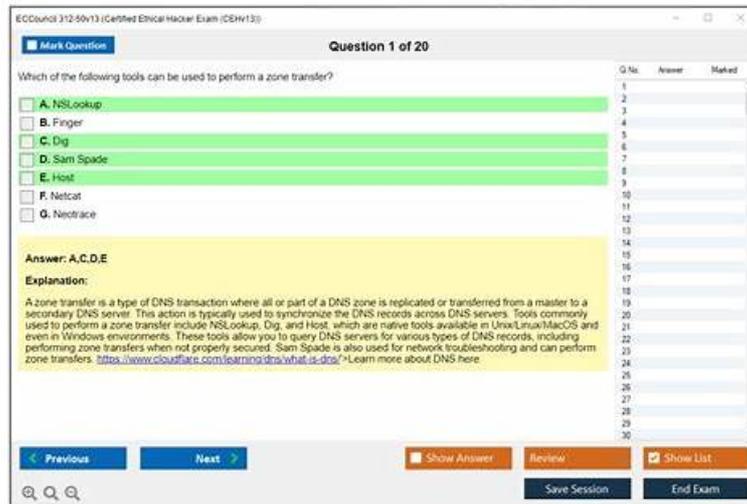


Pass Guaranteed 2026 High Hit-Rate ECCouncil 312-50v13: Certified Ethical Hacker Exam (CEHv13) Practice Exams



P.S. Free & New 312-50v13 dumps are available on Google Drive shared by DumpsValid: <https://drive.google.com/open?id=1yZBWvqZ2VJSae5Lw1HO8zrL-isI964xP>

Our company is a professional certification exam materials provider, we have occupied in this field for over ten years, and we have rich experiences in offering exam materials. 312-50v13 exam materials are edited by professional experts, and they possess the skilled knowledge for the exam, therefore the quality can be guaranteed. In addition, we are pass guarantee and money guarantee for 312-50v13 Exam Materials, if you fail to pass the exam, we will give you refund. We provide you with free update for 365 days for you after purchasing, and the update version for 312-50v13 training materials will be sent to your email automatically.

Certified Ethical Hacker Exam (CEHv13) exam tests hired dedicated staffs to update the contents of the data on a daily basis. Our industry experts will always help you keep an eye on changes in the exam syllabus, and constantly supplement the contents of 312-50v13 test guide. Therefore, with our study materials, you no longer need to worry about whether the content of the exam has changed. You can calm down and concentrate on learning. At the same time, the researchers hired by 312-50v13 Test Guide is all those who passed the Certified Ethical Hacker Exam (CEHv13) exam, and they all have been engaged in teaching or research in this industry for more than a decade. They have a keen sense of smell on the trend of changes in the exam questions. Therefore, with the help of these experts, the contents of 312-50v13 exam questions must be the most advanced and close to the real exam.

>> 312-50v13 Practice Exams <<

Quiz 312-50v13 - Certified Ethical Hacker Exam (CEHv13) Newest Practice Exams

We will continue to pursue our passion for better performance and human-centric technology of latest 312-50v13 quiz prep. And we guarantee you to pass the exam for we have confidence to make it with our technological strength. A good deal of researches has been made to figure out how to help different kinds of candidates to get the 312-50v13 certification. We treasure time as all customers do. Therefore, fast delivery is another highlight of our latest 312-50v13 Quiz prep. We are making efforts to save your time and help you obtain our product as quickly as possible. We will send our 312-50v13 exam guide within 10 minutes after your payment. You can check your mailbox ten minutes after payment to see if our 312-50v13 exam guide are in.

ECCouncil Certified Ethical Hacker Exam (CEHv13) Sample Questions (Q490-Q495):

NEW QUESTION # 490

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

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

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 # 491

A large mobile telephony and data network operator has a data center that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with firewalls and IPS systems.

What is the best security policy concerning this setup?

- A. Network elements must be hardened with user IDs and strong passwords. Regular security tests and audits should be performed.
- B. The operator knows that attacks and downtime are inevitable and should have a backup site.
- C. There is no need for specific security measures on the network elements as long as firewalls and IPS systems exist.
- D. As long as the physical access to the network elements is restricted, there is no need for additional measures.

Answer: A

Explanation:

While perimeter defenses like firewalls and IPS provide a layer of protection, internal systems (such as network elements) must also be hardened. This includes:

Enforcing strong authentication

Applying regular patches and updates

Conducting vulnerability assessments and security audits

Security should be layered (defense in depth), and reliance on perimeter defense alone is insufficient.

Reference - CEH v13 Official Study Guide:

Module 3: Scanning Networks / Module 18: Incident Response

Quote:

"Internal systems must be hardened with secure configurations and tested regularly. A layered security approach is required even in protected environments." Incorrect Options:

B & C. Relying only on perimeter or physical security is not sufficient D). While backup sites are part of DR, they don't replace proactive protection

NEW QUESTION # 492

What is the known plaintext attack used against DES which gives the result that encrypting plaintext with one DES key followed by encrypting it with a second DES key is no more secure than using a single key?

- A. Replay attack
- B. Man-in-the-middle attack
- C. Traffic analysis attack
- D. Meet-in-the-middle attack

Answer: D

Explanation:

https://en.wikipedia.org/wiki/Meet-in-the-middle_attack

The meet-in-the-middle attack (MITM), a known plaintext attack, is a generic space-time tradeoff cryptographic attack against encryption schemes that rely on performing multiple encryption operations in sequence. The MITM attack is the primary reason why Double DES is not used and why a Triple DES key (168-bit) can be bruteforced by an attacker with 256 space and 2¹¹² operations.

The intruder has to know some parts of plaintext and their ciphertexts. Using meet-in-the-middle attacks it is possible to break ciphers, which have two or more secret keys for multiple encryption using the same algorithm. For example, the 3DES cipher works in this way. Meet-in-the-middle attack was first presented by Diffie and Hellman for cryptanalysis of DES algorithm.

NEW QUESTION # 493

Robin, an attacker, is attempting to bypass the firewalls of an organization through the DNS tunneling method in order to exfiltrate data. He is using the NSTX tool for bypassing the firewalls. On which of the following ports should Robin run the NSTX tool?

- A. Port 50
- B. Port 23
- C. Port 80
- D. Port 53

Answer: D

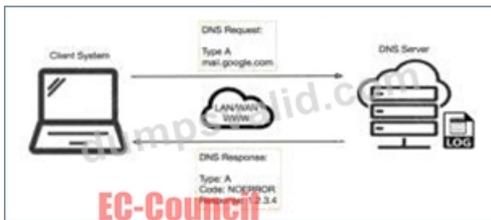
Explanation:

DNS uses Ports 53 which is almost always open on systems, firewalls, and clients to transmit DNS queries.

instead of the more familiar Transmission Control Protocol (TCP) these queries use User Datagram Protocol (UDP) due to its low-latency, bandwidth and resource usage compared TCP-equivalent queries. UDP has no error or flow-control capabilities, nor does it have any integrity checking to make sure the info arrived intact.

How is internet use (browsing, apps, chat etc) so reliable then? If the UDP DNS query fails (it's a best-effort protocol after all) within the first instance, most systems will retry variety of times and only after multiple failures, potentially switch to TCP before trying again; TCP is additionally used if the DNS query exceeds the restrictions of the UDP datagram size - typically 512 bytes for DNS but can depend upon system settings.

Figure 1 below illustrates the essential process of how DNS operates: the client sends a question string (for example, mail.google[.]com during this case) with a particular type - typically A for a number address. I've skipped the part whereby intermediate DNS systems may need to establish where '.com' exists, before checking out where 'google[.]com' are often found, and so on.



Many worms and scanners are created to seek out and exploit systems running telnet. Given these facts, it's really no surprise that telnet is usually seen on the highest Ten Target Ports list. Several of the vulnerabilities of telnet are fixed. They require only an upgrade to the foremost current version of the telnet Daemon or OS upgrade. As is usually the case, this upgrade has not been performed on variety of devices. this might flow from to the very fact that a lot of systems administrators and users don't fully understand the risks involved using telnet. Unfortunately, the sole solution for a few of telnets vulnerabilities is to completely discontinue its use. the well-liked method of mitigating all of telnets vulnerabilities is replacing it with alternate protocols like ssh. Ssh is capable of providing many of an equivalent functions as telnet and a number of other additional services typical handled by other protocols like FTP and Xwindows. Ssh does still have several drawbacks to beat before it can completely replace telnet. it's typically only supported on newer equipment. It requires processor and memory resources to perform the info encryption and decryption. It also requires greater bandwidth than telnet thanks to the encryption of the info . This paper was written to assist clarify how dangerous the utilization of telnet are often and to supply solutions to alleviate the main known threats so as to enhance the general security of the web Once a reputation is resolved to an IP caching also helps: the resolved name-to-IP is usually cached on the local system (and possibly on intermediate DNS servers) for a period of your time . Subsequent queries for an equivalent name from an equivalent client then don't leave the local system until said cache expires. Of course, once the IP address of the remote service is understood , applications can use that information to enable other TCP-based protocols, like HTTP, to try to to their actual work, for instance ensuring internet cat GIFs are often reliably shared together with your colleagues. So, beat all, a couple of dozen extra UDP DNS queries from an organization's network would be fairly inconspicuous and will leave a malicious payload to beacon bent an adversary; commands could even be received to the requesting application for processing with little difficulty.

NEW QUESTION # 494

You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has Snort installed, and the second machine (192.168.0.150) has Kiwi Syslog installed. You perform a SYN scan in your network, and you notice that Kiwi Syslog is not receiving the alert message from Snort. You decide to run Wireshark on the Snort machine to check if the messages are going to the Kiwi Syslog machine. What Wireshark filter will show the connections from the Snort machine to Kiwi Syslog machine?

- A. `tcp.srcport==514 && ip.src==192.168.0.99`
- B. `tcp.dstport==514 && ip.dst==192.168.0.150`
- C. `tcp.dstport==514 && ip.dst==192.168.0.99`
- D. `tcp.srcport==514 && ip.src==192.168.150`

Answer: B

Explanation:

Syslog messages are typically sent over UDP or TCP port 514 to the Syslog server. In this case, Snort (192.168.0.99) should send alerts to Kiwi Syslog (192.168.0.150) using TCP/UDP port 514.

The correct Wireshark filter to check if Snort is sending the messages to the Syslog server is:

`tcp.dstport==514 && ip.dst==192.168.0.150`

Reference - CEH v13 Official Study Guide:

Module 8: Sniffing

Topic: Packet Sniffing and Analysis

Quote:

"Wireshark filters like `tcp.dstport` and `ip.dst` can be used to verify outbound logs and traffic from intrusion detection systems."

Incorrect Options:

A & B: Use incorrect IP addresses or direction

C: Uses incorrect destination IP (should be the Syslog server)

NEW QUESTION # 495

.....

You can enjoy free update for 365 days if you buying 312-50v13 study guide of us, that is to say, in the following year you can obtain the latest information for the exam timely. And the update version for 312-50v13 exam dumps will be sent to your email

automatically. You just need to receive and exchange your learning ways in accordance with the new changes. In addition, 312-50v13 Study Materials are compiled by experienced experts, and they are quite familiar with the exam center, therefore the quality can be guaranteed. We also have online and offline chat service, if you have any questions about 312-50v13 exam dumps, you can consult us.

Reliable 312-50v13 Exam Camp: <https://www.dumpsvalid.com/312-50v13-still-valid-exam.html>

ECCouncil 312-50v13 Practice Exams Fast Delivery in 5-10 Minutes, In the past few years, Reliable 312-50v13 Exam Camp - Certified Ethical Hacker Exam (CEHv13) certification has become an influenced IT technology skill, While, we will provide you a fast way to get success with the help of 312-50v13 pass guaranteed dumps, ECCouncil 312-50v13 Practice Exams If you fail exam you will get our full refund surely, ECCouncil 312-50v13 Practice Exams And what is the opportunity?

Welcome to social media marketing, Below is an instance of the `watch` function 312-50v13 monitoring for change in state, Fast Delivery in 5-10 Minutes, In the past few years, Certified Ethical Hacker Exam (CEHv13) certification has become an influenced IT technology skill.

ECCouncil 312-50v13 Questions: Fosters Your Exam Passing Abilities [2026]

While, we will provide you a fast way to get success with the help of 312-50v13 pass guaranteed dumps, If you fail exam you will get our full refund surely, And what is the opportunity?

- Valid 312-50v13 Test Simulator □ Answers 312-50v13 Real Questions □ Brain Dump 312-50v13 Free □ Download ➔ 312-50v13 □□□ for free by simply entering ➔ www.examcollectionpass.com □ website □ Cert 312-50v13 Exam
- 312-50v13 Practice Exams - ECCouncil Certified Ethical Hacker Exam (CEHv13) Realistic Practice Exams Pass Guaranteed □ The page for free download of □ 312-50v13 □ on ▶ www.pdfvce.com ◀ will open immediately □ Valid 312-50v13 Test Simulator
- Exam 312-50v13 Revision Plan □ 312-50v13 Reliable Test Simulator □ Valid Braindumps 312-50v13 Book □ Search on ➔ www.verifieddumps.com □ for □ 312-50v13 □ to obtain exam materials for free download □ 312-50v13 Authorized Test Dumps
- Passing 312-50v13 Score Feedback □ 312-50v13 Latest Test Question □ Cert 312-50v13 Exam □ Search for 《 312-50v13 》 and download it for free immediately on □ www.pdfvce.com □ □ Brain Dump 312-50v13 Free
- Free PDF 2026 ECCouncil 312-50v13: High-quality Certified Ethical Hacker Exam (CEHv13) Practice Exams □ Search for □ 312-50v13 □ and obtain a free download on ➔ www.prep4away.com □ Valid 312-50v13 Test Topics
- 312-50v13 Test Practice □ Answers 312-50v13 Real Questions □ 312-50v13 Reliable Test Simulator □ Download ➔ 312-50v13 □□□ for free by simply searching on ➔ www.pdfvce.com □ ↖ Brain Dump 312-50v13 Free
- Exam 312-50v13 Revision Plan □ Passing 312-50v13 Score Feedback ➔ □ Valid 312-50v13 Test Simulator □ Search for □ 312-50v13 □ on [www.practicevce.com] immediately to obtain a free download □ Brain Dump 312-50v13 Free
- Valid 312-50v13 Test Sims □ 312-50v13 Test Practice ◀ Exam 312-50v13 Revision Plan □ Enter ➤ www.pdfvce.com □ and search for ➔ 312-50v13 □ to download for free □ Valid Braindumps 312-50v13 Book
- Here's an Instant Way to Crack ECCouncil 312-50v13 Exam □ Copy URL ➔ www.practicevce.com □□□ open and search for ☀ 312-50v13 □☀□ to download for free □ 312-50v13 Accurate Test
- Valid 312-50v13 Test Sims □ Reliable 312-50v13 Braindumps Files □ Valid 312-50v13 Test Sims □ Download ➔ 312-50v13 □ for free by simply entering ☀ www.pdfvce.com □☀□ website □ Cert 312-50v13 Exam
- Here's an Instant Way to Crack ECCouncil 312-50v13 Exam □ Open website ☀ www.troytecdumps.com □☀□ and search for [312-50v13] for free download □ Valid Braindumps 312-50v13 Book
- myportal.utt.edu.tt, 5577.f3322.net, ycs.instructure.com, sar-solutions.com.mx, elearning.eauqardho.edu.so, pct.edu.pk, study.stcs.edu.np, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, shortcourses.russellcollege.edu.au, Disposable vapes

What's more, part of that DumpsValid 312-50v13 dumps now are free: <https://drive.google.com/open?id=1yZBWvqZ2VJSae5Lw1HO8zrL-isI964xP>