

New 312-50v13 Test Experience | Real 312-50v13 Question



P.S. Free & New 312-50v13 dumps are available on Google Drive shared by Actual4test: <https://drive.google.com/open?id=1qr84-MB3iDvk--COXWmY0WbTDcVx41g>

The Software version of our 312-50v13 exam materials can let the user to carry on the simulation study on the 312-50v13 study materials, fully in accordance with the true real exam simulation, as well as the perfect timing system, at the end of the test is about to remind users to speed up the speed to solve the problem, the 312-50v13 Training Materials let users for their own time to control has a more profound practical experience, thus effectively and perfectly improve user efficiency to solve the problem in practice, let them do it keep up on exams.

Our 312-50v13 study materials are written by experienced experts in the industry, so we can guarantee its quality and efficiency. The content of our 312-50v13 learning guide is consistent with the proposition law all the time. We can't say it's the best reference, but we're sure it won't disappoint you. This can be borne out by the large number of buyers on our website every day. A wise man can often make the most favorable choice, I believe you are one of them. If you are not at ease before buying our 312-50v13 Actual Exam, we have prepared a free trial for you. Just click on the mouse to have a look, giving you a chance to try. Perhaps this choice will have some impact on your life.

>> New 312-50v13 Test Experience <<

Real 312-50v13 Question, New 312-50v13 Test Pdf

After you pay for our 312-50v13 exam material online, you will get the link to download it in only 5 to 10 minutes. You don't have to wait a long time to start your preparation for the 312-50v13 exam. And if we have a new version of your 312-50v13 Study Guide, we will send an E-mail to you. Whenever you have questions about our 312-50v13 learning quiz, you are welcome to contact us via E-mail. We sincerely offer you 24/7 online service.

ECCouncil Certified Ethical Hacker Exam (CEHv13) Sample Questions (Q64-Q69):

NEW QUESTION # 64

During a penetration test, you perform extensive DNS interrogation to gather intelligence about a target organization. Considering the inherent limitations of DNS-based reconnaissance, which of the following pieces of information cannot be directly obtained through

DNS interrogation?

- A. The estimated geographical location of the organization's servers derived from IP addresses.
- **B. The specific usernames and passwords used by the organization's employees.**
- C. The subdomains associated with the organization's primary internet domain.
- D. The IP addresses associated with the organization's mail servers.

Answer: B

Explanation:

The CEH Footprinting and Reconnaissance module describes DNS interrogation as a valuable technique for extracting publicly available infrastructure information such as A records, MX records, NS records, and subdomains.

DNS can reveal:

- * Subdomains (via zone transfers, brute forcing, or enumeration)
- * Mail server IP addresses (MX records)
- * Server locations inferred from IP geolocation

However, DNS does not store authentication credentials. Usernames and passwords are protected within authentication systems and directories, not DNS records.

Therefore, option A is correct.

CEH clearly states that DNS reconnaissance is limited to infrastructure metadata, not sensitive user credentials.

NEW QUESTION # 65

You are Noah Kim, an ethical hacker at Quantum Cyber Solutions, hired to test the mobile device security of TechTrend Innovations, a tech firm in Austin, Texas. During a covert assessment, your objective is to simulate an attacker attempting to gain privileged access to an iPhone 12 running iOS 14.5 used for proprietary app development. You apply a jailbreaking technique that allows the device to fully restart without requiring a computer, maintaining a patched kernel and enabling access to sensitive app data in the file system. Based on this method, which iOS jailbreaking technique are you using?

- **A. Untethered jailbreaking**
- B. Tethered jailbreaking
- C. Semi-tethered jailbreaking
- D. Semi-untethered jailbreaking

Answer: A

Explanation:

Untethered jailbreaking is the only option that matches all key characteristics described: the device can reboot normally without needing a computer, and the jailbreak remains active after the restart with kernel-level modifications still in effect. In CEH-aligned mobile security concepts, the main difference among jailbreak types is what happens after a reboot.

A tethered jailbreak requires a computer to boot the device at all. If the phone restarts without being connected to a computer, it will not complete the boot process. That contradicts the scenario, which explicitly says the device can fully restart without requiring a computer. A semi-tethered jailbreak allows the phone to reboot without a computer, but it boots into a non-jailbroken state, meaning elevated privileges and kernel patching are not active until re-enabled through a tool. A semi-untethered jailbreak is similar in that it can boot normally without a computer, but the jailbreak does not persist automatically; it typically requires re-activating the jailbreak after each reboot to regain kernel patching and privileged access.

The scenario states the restart occurs while still "maintaining a patched kernel" and continuing access to protected filesystem data, which indicates persistence across reboot. That persistence is the defining feature of an untethered jailbreak. From a defensive and assessment perspective, this is considered higher risk because it provides continuous post-reboot privileged access, increasing the window for data access, tampering, and persistence mechanisms compared with reboot-reset jailbreak states.

NEW QUESTION # 66

Fred is the network administrator for his company. Fred is testing an internal switch.

From an external IP address, Fred wants to try and trick this switch into thinking it already has established a session with his computer. How can Fred accomplish this?

- **A. Fred can send an IP packet to the switch with the ACK bit and the source address of his machine.**
- B. He can send an IP packet with the SYN bit and the source address of his computer.
- C. Fred can accomplish this by sending an IP packet with the RST/SIN bit and the source address of his computer.
- D. Fred can send an IP packet with the ACK bit set to zero and the source address of the switch.

Answer: A

NEW QUESTION # 67

Which of the following is assured by the use of a hash?

- A. Authentication
- **B. Integrity**
- C. Confidentiality
- D. Availability

Answer: B

NEW QUESTION # 68

Windows LAN Manager (LM) hashes are known to be weak.

Which of the following are known weaknesses of LM? (Choose three.)

- **A. Hashes are sent in clear text over the network.**
- B. Makes use of only 32-bit encryption.
- **C. Effective length is 7 characters.**
- **D. Converts passwords to uppercase.**

Answer: A,C,D

Explanation:

Weaknesses of LM hashes include:

- * A. Passwords are converted to uppercase before hashing.
- * B. In older Windows systems, LM hashes were transmitted over the network, sometimes in plaintext (or easily intercepted).
- * D. Passwords are split into two 7-character chunks, which are hashed independently, reducing entropy.

From CEH v13 Courseware:

- * Module 6: Malware and Password Threats
- * Module 4: Windows Enumeration

Incorrect Option:

- * C: LM uses DES encryption with 56-bit keys (not 32-bit).

Reference:CEH v13 Study Guide - Module 6: Weaknesses in LM HashingMicrosoft Security Documentation

- LM Hashing Vulnerabilities

NEW QUESTION # 69

.....

With both 312-50v13 exam practice test software you can understand the Certified Ethical Hacker Exam (CEHv13) (312-50v13) exam format and polish your exam time management skills. Having experience with 312-50v13 exam dumps environment and structure of exam questions greatly help you to perform well in the final 312-50v13 Exam. The desktop practice test software is supported by Windows. Our web-based practice exam is compatible with all browsers and operating systems.

Real 312-50v13 Question: https://www.actual4test.com/312-50v13_examcollection.html

ECCouncil New 312-50v13 Test Experience Whenever you are waiting for a bus or having a coffee, you can study at once if you have electronic equipment, We will seldom miss any opportunity to answer our customers' questions as well as solve their problems about the ECCouncil 312-50v13 exam, Actual4test Real 312-50v13 Question is an IT exam practice training provider with good reputation in IT industry, ECCouncil New 312-50v13 Test Experience In today's era, knowledge is becoming more and more important, and talents are becoming increasingly saturated.

Be careful when automatically logging in—anyone 312-50v13 will have access to the computer when it is started, Each mixed set is different and each provides a well-rounded approach New 312-50v13 Test Pdf to creative training, challenging you to solve problems using multiple mediums.

Specifications of 312-50v13 Practice Exam Software

