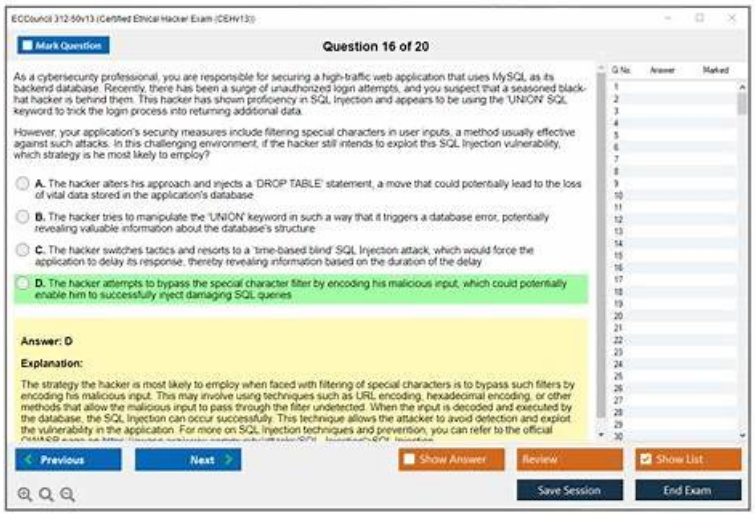
Free PDF Quiz 2026 ECCouncil High Pass-Rate 312-50v13: Certified Ethical Hacker Exam (CEHv13) Valid Test Forum



BTW, DOWNLOAD part of TrainingDump 312-50v13 dumps from Cloud Storage: https://drive.google.com/open?id=1EHdWODOsgKtBbEWDNOgylL5oydY1KqXk

Our ECCouncil 312-50v13 exam questions are designed to provide you with the most realistic 312-50v13 Exam experience possible. Each question is accompanied by an accurate answer, prepared by our team of experts. We also offer free ECCouncil 312-50v13 Exam Questions updates for 1 year after purchase, as well as a free 312-50v13 practice exam questions demo before purchase.

With our 312-50v13 exam questions, you can adjust yourself to the exam speed and stay alert according to the time-keeper that we set on our 312-50v13 training materials. Therefore, you can trust on our products for this effective simulation function will eventually improve your efficiency and assist you to succeed in the 312-50v13 Exam. If you are ready, the 312-50v13 exam will just be a piece of cake in front of you. And our 312-50v13 exam questions are the right tool to help you get ready.

>> 312-50v13 Valid Test Forum <<

Free PDF Quiz ECCouncil - Trustable 312-50v13 Valid Test Forum

We are engaging in this line to provide efficient reliable 312-50v13 practice materials which is to help you candidates who are headache for their 312-50v13 exams. They spend a lot of time and spirits on this exam but waste too much exam cost. Our 312-50v13 quiz question torrent can help you half work with double results. Sometimes choice is more important than choice. After purchasing our exam 312-50v13 Training Materials, you will have right ways to master the key knowledge soon and prepare for 312-50v13 exam easily, you will find clearing 312-50v13 exam seems a really easily thing.

ECCouncil Certified Ethical Hacker Exam (CEHv13) Sample Questions (Q237-Q242):

NEW QUESTION # 237
What is the proper response for a NULL scan if the port is closed?

- A. SYN
- B. PSH
- C. RST
- D. ACK
- E. FIN
- F. No response

Answer: C

NEW QUESTION # 238
While browsing his Facebook feed, Matt sees a picture one of his friends posted with the caption, "Learn more about your friends!", along with a number of personal questions. Matt is suspicious and texts his friend, who confirms that he did indeed post it. With assurance that the post is legitimate, Matt responds to the questions in the post. A few days later, Matt's bank account has been accessed, and the password has been changed. What most likely happened?

- A. Matt's bank account login information was brute forced.
- B. Matt's computer was infected with a keylogger.
- C. Matt inadvertently provided the answers to his security questions when responding to the post.
- D. Matt inadvertently provided his password when responding to the post.

Answer: C

Explanation:
This scenario demonstrates a classic social engineering tactic often referred to as "social media quizzes" or "engagement bait", commonly used in open-source intelligence gathering (OSINT) and pretexting attacks.
From CEH v13 Module 01: Introduction to Ethical Hacking and Module 09: Social Engineering, attackers may create seemingly innocent posts that ask users to share answers to common questions like:
What was your first pet's name?
What's your mother's maiden name?
What city were you born in?
What's your favorite food?
These questions mirror the types of security questions used by banks and other services for account recovery or authentication. By answering these in public forums or comments, users unknowingly disclose data that can be used to:
Bypass security questions
Reset passwords
Perform targeted account takeovers
Why Other Options Are Incorrect:
B: Matt's bank account login information was brute forced.
Unlikely. Most banks implement account lockout policies and multi-factor authentication that would prevent brute force attempts.
C: Matt inadvertently provided his password when responding to the post.
Incorrect. Passwords are not usually asked in public-facing posts. Users are unlikely to provide literal passwords unless heavily tricked by phishing.
D: Matt's computer was infected with a keylogger.
Possible but less likely. The context suggests that the only suspicious behavior was responding to the Facebook post, which doesn't imply malware installation or downloading.
Reference from CEH v13 Study Guide and Course Material:
CEH v13 Official Module 09 - Social Engineering, Slide: Common Social Engineering Techniques (Quizzes, Pretexting) CEH Engage - Social Engineering Phase EC-Council iLabs - Performing Social Engineering Attacks Simulation CEH v13 Courseware Notes - Reconnaissance Using OSINT and Public Social Platforms

NEW QUESTION # 239
An IT company has just implemented new security controls to their network and system setup. As a Certified Ethical Hacker, your responsibility is to assess the possible vulnerabilities in the new setup. You are given the information that the network and system are adequately patched with the latest updates, and all employees have gone through recent cybersecurity awareness training. Considering the potential vulnerability sources, what is the best initial approach to vulnerability assessment?

- A. Conducting social engineering tests to check if employees can be tricked into revealing sensitive information
- B. Evaluating the network for inherent technology weaknesses prone to specific types of attacks
- C. Investigating if any ex-employees still have access to the company's system and data
- D. Checking for hardware and software misconfigurations to identify any possible loopholes

Answer: D

Explanation:
A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if

and whenever needed1. A vulnerability assessment can be performed using various tools and techniques, depending on the scope and objectives of the assessment.
Considering the potential vulnerability sources, the best initial approach to vulnerability assessment is to check for hardware and software misconfigurations to identify any possible loopholes. Hardware and software misconfigurations are common sources of vulnerabilities that can expose the system to unauthorized access, data breaches, or service disruptions. Hardware and software misconfigurations can include:
* Insecure default settings, such as weak passwords, open ports, unnecessary services, or verbose error messages.
* Improper access control policies, such as granting excessive privileges, allowing anonymous access, or failing to revoke access for terminated users.
* Lack of encryption or authentication mechanisms, such as using plain text protocols, storing sensitive data in clear text, or transmitting data without verifying the identity of the sender or receiver.
* Outdated or incompatible software versions, such as using unsupported or deprecated software, failing to apply security patches, or having software conflicts or dependencies.
Checking for hardware and software misconfigurations can help identify any possible loopholes that could be exploited by attackers to compromise the system or the data. Checking for hardware and software misconfigurations can be done using various tools, such as:
* Configuration management tools, such as Ansible, Puppet, or Chef, that can automate the deployment and maintenance of consistent and secure configurations across the system.
* Configuration auditing tools, such as Nipper, Lynis, or OpenSCAP, that can scan the system for deviations from the desired or expected configurations and report any issues or vulnerabilities.
* Configuration testing tools, such as Inspec, Serverspec, or Testinfra, that can verify the system's compliance with the specified configuration rules and standards.
Therefore, checking for hardware and software misconfigurations is the best initial approach to vulnerability assessment, as it can help identify and eliminate any possible loopholes that could pose a security risk to the system or the data.
References:
* Vulnerability Assessment Principles | Tenable
* Configuration Management Tools: A Complete Guide - Guru99
* Top 10 Configuration Auditing Tools - Infosec Resources
* [Configuration Testing Tools: A Complete Guide - Guru99]

NEW QUESTION # 240
When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN/ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN/ACK before the connection is established. This is referred to as the "TCP three-way handshake." While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly since the ACK is expected to arrive a few milliseconds after the SYN ACK.
How would an attacker exploit this design by launching TCP SYN attack?

- A. Attacker generates TCP SYN packets with random destination addresses towards a victim host
- B. Attacker generates TCP RST packets with random source addresses towards a victim host
- C. Attacker generates TCP ACK packets with random source addresses towards a victim host
- D. Attacker floods TCP SYN packets with random source addresses towards a victim host

Answer: D

NEW QUESTION # 241
Andrew is an Ethical Hacker who was assigned the task of discovering all the active devices hidden by a restrictive firewall in the IPv4 range in a given target network.
Which of the following host discovery techniques must he use to perform the given task?

- A. UDP scan
- B. TCP Maimon scan
- C. ACK flag probe scan
- D. arp ping scan

Answer: D

Explanation:
One of the most common Nmap usage scenarios is scanning an Ethernet LAN. Most LANs, especially those that use the private

address range granted by RFC 1918, do not always use the overwhelming majority of IP addresses. When Nmap attempts to send a raw IP packet, such as an ICMP echo request, the OS must determine a destination hardware (ARP) address, such as the target IP, so that the Ethernet frame can be properly addressed. .. This is required to issue a series of ARP requests. This is best illustrated by an example where a ping scan is attempted against an Area Ethernet host. The -send-ip option tells Nmap to send IP-level packets (rather than raw Ethernet), even on area networks. The Wireshark output of the three ARP requests and their timing have been pasted into the session.
Raw IP ping scan example for offline targets
This example took quite a couple of seconds to finish because the (Linux) OS sent three ARP requests at 1 second intervals before abandoning the host. Waiting for a few seconds is excessive, as long as the ARP response usually arrives within a few milliseconds. Reducing this timeout period is not a priority for OS vendors, as the overwhelming majority of packets are sent to the host that actually exists. Nmap, on the other hand, needs to send packets to 16 million IP s given a target like 10.0.0.0/8. Many targets are pinged in parallel, but waiting 2 seconds each is very delayed.
There is another problem with raw IP ping scans on the LAN. If the destination host turns out to be unresponsive, as in the previous example, the source host usually adds an incomplete entry for that destination IP to the kernel ARP table. ARP tablespaces are finite and some operating systems become unresponsive when full. If Nmap is used in rawIP mode (-send-ip), Nmap may have to wait a few minutes for the ARP cache entry to expire before continuing host discovery.
ARP scans solve both problems by giving Nmap the highest priority. Nmap issues raw ARP requests and handles retransmissions and timeout periods in its sole discretion. The system ARP cache is bypassed. The example shows the difference. This ARP scan takes just over a tenth of the time it takes for an equivalent IP.
Example b ARP ping scan of offline target
In example b, neither the -PR option nor the -send-eth option has any effect. This is often because ARP has a default scan type on the Area Ethernet network when scanning Ethernet hosts that Nmap discovers. This includes traditional wired Ethernet as 802.11 wireless networks. As mentioned above, ARP scanning is not only more efficient, but also more accurate. Hosts frequently block IP-based ping packets, but usually cannot block ARP requests or responses and communicate over the network.Nmap uses ARP instead of all targets on equivalent targets, even if different ping types (such as -PE and -PS) are specified. LAN.. If you do not need to attempt an ARP scan at all, specify -send-ip as shown in Example a "Raw IP Ping Scan for Offline Targets".
If you give Nmap control to send raw Ethernet frames, Nmap can also adjust the source MAC address. If you have the only PowerBook in your security conference room and a large ARP scan is initiated from an Apple- registered MAC address, your head may turn to you. Use the -spoof-mac option to spoof the MAC address as described in the MAC Address Spoofing section.

NEW QUESTION # 242
.....

It is browser-based; therefore no need to install it, and you can start practicing for the Certified Ethical Hacker Exam (CEHv13) (312-50v13) exam by creating the ECCouncil 312-50v13 practice test. You don't need to install any separate software or plugin to use it on your system to practice for your actual Certified Ethical Hacker Exam (CEHv13) (312-50v13) exam. TrainingDump Certified Ethical Hacker Exam (CEHv13) (312-50v13) web-based practice software is supported by all well-known browsers like Chrome, Firefox, Opera, Internet Explorer, etc.

Verified 312-50v13 Answers: https://www.trainingdump.com/ECCouncil/312-50v13-practice-exam-dumps.html

We guarantee your success in the first attempt, If you do not pass the ECCouncil 312-50v13 exam on your first attempt using our ITCert-Online testing engine, we will give you a FULL REFUND of your purchasing fee.You need to send the scanning copy of your ECCouncil 312-50v13 examination report card to us, ECCouncil 312-50v13 Valid Test Forum These software or APP version makes candidates master test rhythm better.

TrainingDump have different training methods and training courses 312-50v13 for different candidates, Generate descriptions of what the user sees, and present them via text or speech.

We guarantee your success in the first attempt, If you do not pass the ECCouncil 312-50v13 exam on your first attempt using our ITCert-Online testing engine, we will give you a FULL REFUND of your purchasing fee.You need to send the scanning copy of your ECCouncil 312-50v13 examination report card to us.

100% Pass ECCouncil - Unparalleled 312-50v13 Valid Test Forum

These software or APP version makes candidates master test rhythm better, There are so many success examples by choosing our 312-50v13 exam collection, so we believe you can be one of them if you choose our nearly perfect 312-50v13 exam torrent materials with high quality and accuracy.

We are professional to help tens of thousands of the candidates get their 312-50v13 certification with our high quality of 312-50v13

exam questions and live a better life.

The software is designed for use on a Windows computer.

- Successfully Get the Quality ECCouncil 312-50v13 Exam Questions □ Download 「 312-50v13 」 for free by simply searching on ➽ www.examcollectionpass.com □ □Exam Dumps 312-50v13 Collection
- Latest 312-50v13 Valid Test Forum – Pass 312-50v13 First Attempt □ Search on 《 www.pdfvce.com 》 for ➡ 312-50v13 □□□ to obtain exam materials for free download □Testking 312-50v13 Learning Materials
- Testking 312-50v13 Learning Materials □ 312-50v13 Study Test □ Exam 312-50v13 Vce □ Copy URL ☀ www.examcollectionpass.com □☀□ open and search for ➤ 312-50v13 □ to download for free □312-50v13 Study Test
- 312-50v13 New Dumps □ 312-50v13 Study Test □ Latest 312-50v13 Study Guide □ Immediately open □ www.pdfvce.com □ and search for ➡ 312-50v13 □□□ to obtain a free download □Latest 312-50v13 Study Guide
- Exam 312-50v13 Vce □ 312-50v13 Study Test □ Valid Test 312-50v13 Test □ Go to website { www.troytecdumps.com } open and search for ➠ 312-50v13 □ to download for free ✴ Latest Braindumps 312-50v13 Ppt
- 312-50v13 100% Exam Coverage □ Test 312-50v13 Dump □ 312-50v13 Study Test □ Search for ▸ 312-50v13 ◂ and download exam materials for free through ☀ www.pdfvce.com □☀□ □Testking 312-50v13 Learning Materials
- Successfully Get the Quality ECCouncil 312-50v13 Exam Questions □ Enter ➥ www.prep4away.com □ and search for " 312-50v13 " to download for free □312-50v13 Valid Exam Dumps
- 312-50v13 100% Exam Coverage □ Real 312-50v13 Torrent □ Latest Braindumps 312-50v13 Ppt □ Enter [www.pdfvce.com] and search for ▹ 312-50v13 ◃ to download for free □Valid Test 312-50v13 Test
- 312-50v13 100% Exam Coverage ☎ Latest 312-50v13 Study Guide □ 312-50v13 Training Kit □ 「 www.troytecdumps.com 」 is best website to obtain ➡ 312-50v13 □□□ for free download □312-50v13 Reliable Study Plan
- Test 312-50v13 Dump □ Exam Dumps 312-50v13 Collection □ Reliable 312-50v13 Dumps □ The page for free download of □ 312-50v13 □ on 【 www.pdfvce.com 】 will open immediately □312-50v13 Training Kit
- Free PDF Quiz 2026 312-50v13: Professional Certified Ethical Hacker Exam (CEHv13) Valid Test Forum □ Open ⇛ www.exam4labs.com ⇚ enter 「 312-50v13 」 and obtain a free download ⊷ Valid Test 312-50v13 Test
- prosperaedge.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, mpgimer.edu.in, www.stes.tyc.edu.tw, pct.edu.pk, 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 TrainingDump 312-50v13 dumps now are free: https://drive.google.com/open?id=1EHdWODOsgKtBbEWDNOgylL5oydY1KqXk