CertiProf's CEHPC Exam Questions Come with Realistic Practice and Accurate Answers

One more thing to give you an idea about the top features of Ethical Hacking Professional Certification Exam (CEHPC) exam questions before purchasing, the ActualTestsIT are offering free ActualTestsIT CEHPC Exam Questions demo download facility. This facility is being offered in all three ActualTestsIT CEHPC exam practice question formats.

The world is changing rapidly and the requirements to the employees are higher than ever before. If you want to find an ideal job and earn a high income you must boost good working abilities and profound major knowledge. Passing CEHPC certification can help you realize your dreams. If you buy our product, we will provide you with the best Ethical Hacking Professional study materials and it can help you obtain CEHPCcertification. Our product is of high quality and our service is perfect.

>> CEHPC Dumps Vce <<

Latest CertiProf CEHPC Exam Pdf - Real CEHPC Dumps

We have a special technical customer service staff to solve all kinds of consumers' problems on our CEHPC exam questions. If you have questions when installing or using our CEHPC practice engine, you can always contact our customer service staff via email or online consultation. They will solve your questions about CEHPC Preparation materials with enthusiasm and professionalism, giving you a timely response whenever you contact them.

CertiProf Ethical Hacking Professional Certification Exam Sample Questions (Q16-Q21):

NEW QUESTION # 16
What is Nessus used for?

- A. To scan a network or system for vulnerabilities.
- B. To watch videos on a blocked network.
- C. For automated hacking.

Answer: A

Explanation:
Nessus is a globally recognized, industry-standardvulnerability scannerused by security professionals to identify security flaws in a network, operating system, or application. Developed by Tenable, it is a comprehensive tool that automates the process of finding weaknesses such as unpatched software, weak passwords, misconfigurations, and "zero-day" vulnerabilities.
Nessus operates by probing a target system and comparing the results against an extensive, constantly updated database of thousands of known vulnerabilities (plugins). The scanning process typically involves:
* Host Discovery: Identifying which devices are active on the network.

* Port Scanning: Checking for open services and identifying their versions.
* Vulnerability Assessment: Running specific checks to see if those services are susceptible to known exploits.
* Compliance Auditing: Ensuring that systems meet specific security standards like PCI DSS or HIPAA.
Unlike "automated hacking" tools that focus on exploitation, Nessus is adiagnostic tool. It provides detailed reports that categorize vulnerabilities by severity (Critical, High, Medium, Low) and offers specific remediation advice on how to fix the issues. In a professional penetration test, Nessus is used during the
"Vulnerability Analysis" phase to provide a broad map of the target's weaknesses. This allows the tester to prioritize which flaws to attempt to exploit manually. Regular use of Nessus is a cornerstone of any proactive vulnerability management program.

NEW QUESTION # 17
What is privilege escalation?

- A. It is the term used by major hackers to refer to the request for new permissions to your account with hacked administrators.
- B. A term used in computer security to describe the situation in which a user or process acquires greater permissions or privileges than they originally had.
- C. Is the term used when you request elevated permissions to your account with the administrator.

Answer: B

Explanation:
Privilege escalation is a critical phase in the cyber-attack lifecycle where an adversary seeks to expand their influence within a target environment after gaining an initial foothold. In standard security architectures, users are granted the "least privilege" necessary to perform their duties; however, attackers aim to bypass these restrictions to access sensitive data or execute restricted commands. This process is categorized into two distinct dimensions: horizontal and vertical escalation.
Horizontal privilege escalation(also known as lateral movement) occurs when an attacker gains access to resources belonging to another user with a similar level of permissions. This is often achieved through credential theft, session hijacking, or exploiting vulnerabilities in peer-level applications. While the attacker's authorization level remains the same, their reach increases as they assume different identities.
Vertical privilege escalation, or privilege elevation, is the process of moving from a standard user account to one with higher administrative or "root" privileges. This typically involves exploiting system bugs, misconfigurations, or unpatched vulnerabilities in the kernel or operating system. For instance, an attacker might use an exploit to trick a high-privileged service into executing malicious code on their behalf. Gaining root or administrator status is often the ultimate goal for an attacker, as it provides unrestricted control over the entire system, allowing for the deployment of malware, modification of security logs, and total data exfiltration. Effective defense against this threat involves implementing zero-trust architectures, rigorous patch management, and continuous monitoring for unauthorized permission changes.

NEW QUESTION # 18
What is a hacktivist?

- A. Refers to politicians who get involved in social issues by being in the news.
- B. They use their computer skills to steal sensitive information, to infect computer systems, to restrict access to a system.
- C. Refers to hacking into a computer system for political or social purposes. A hacktivist breaks into a computer system, but always with the aim of influencing ideological, religious, political or social causes.

Answer: C

Explanation:
Hacktivism is a modern security trend that sits at the intersection of computer hacking and social activism. A "hacktivist" is an individual or a member of a group who uses their technical expertise to gain unauthorized access to systems or disrupt digital services to promote a specific political, social, or ideological agenda.
Unlike traditional cybercriminals who are typically motivated by financial gain, or state-sponsored actors seeking geopolitical intelligence, hacktivists act as "digital protesters." Their goal is often to draw public attention to perceived injustices, government policies, or corporate misconduct.
Common tactics used by hacktivists include Distributed Denial of Service (DDoS) attacks to take down a target's website, "defacing" web pages with political messages, or leaking confidential internal documents (often referred to as "doxxing") to embarrass or expose the target. High-profile groups like Anonymous or WikiLeaks are frequently cited as examples of this phenomenon. While the hacktivist might believe their actions are morally justified by their cause-be it environmental protection, free speech, or human rights- their actions remain illegal under most international and domestic computer crime laws because they involve

unauthorized access or disruption of service.
From a defensive standpoint, hacktivism represents a unique threat profile. Organizations must monitor the social and political climate to gauge if they might become a target of a hacktivist campaign. For instance, a company involved in a controversial project might see a sudden surge in scan attempts or phishing attacks.
Understanding hacktivism is essential for modern threat intelligence, as it requires security teams to look beyond technical vulnerabilities and consider the reputational and ideological factors that might drive an attack. This trend highlights how the digital realm has become a primary battlefield for social discourse and political conflict in the 21st century.

NEW QUESTION # 19
What is a reverse shell?

- A. It refers to a process in which the victim's machine initiates a connection back to the attacker's machine to receive commands.
- B. A common Linux command-line console.
- C. It refers to when the terminal is run with root privileges.

Answer: A

Explanation:
A reverse shell is a technique used in ethical hacking and penetration testing where the target (victim) system initiates a connection back to the attacker's system, allowing the attacker to execute commands remotely. This makes option C the correct answer.
Unlike a bind shell, where the victim opens a listening port, a reverse shell is particularly effective in environments protected by firewalls or Network Address Translation (NAT). Since outbound connections are often allowed, the victim system connects outward to the attacker, bypassing many network restrictions.
Ethical hackers commonly use reverse shells during the exploitation and post-exploitation phases of penetration testing to maintain access to compromised systems.
Option A is incorrect because running a terminal as root does not define a reverse shell. Option B is incorrect because a reverse shell is not a standard command-line interface but rather a remote command execution channel.
From an ethical hacking perspective, reverse shells help demonstrate the real-world impact of vulnerabilities such as command injection, remote code execution, or misconfigured services. Once established, a reverse shell may allow privilege escalation, lateral movement, or data exfiltration-highlighting serious security risks.
Understanding reverse shells is essential for both attackers and defenders. Defenders can mitigate reverse shell attacks by implementing strict egress filtering, intrusion detection systems, endpoint protection, and proper system hardening. Ethical testing of reverse shells enables organizations to identify weaknesses and improve overall security posture.

NEW QUESTION # 20
What is ransomware?

- A. A security protocol to protect confidential data.
- B. A type of malicious software that encrypts files and demands a ransom for their release.
- C. A cloud backup service.

Answer: B

Explanation:
Ransomware is one of the most destructive and prevalent information security threats facing organizations today. It is a specific type of malicious software (malware) designed to encrypt a victim's files, making them inaccessible to the legitimate user. Once the encryption process is complete, the software displays a notification-often referred to as a "ransom note"-demanding a payment, usually in an untraceable cryptocurrency like Bitcoin, in exchange for the decryption key required to release the files.
Managing the threat of ransomware requires a comprehensive understanding of its delivery mechanisms. Most infections occur through phishing emails containing malicious attachments or links, or by exploiting vulnerabilities in exposed remote access services like RDP (Remote Desktop Protocol). Once the ransomware is executed, it often attempts to spread laterally through the network to encrypt as many machines and backups as possible, maximizing the pressure on the organization to pay.
From an ethical hacking standpoint, the defense against ransomware is focused on "Resilience and Recovery." Since technical controls can sometimes be bypassed, having an "air-gapped" or offline backup strategy is the only 100% effective way to recover data without paying the attackers. Furthermore, security professionals emphasize the importance of "Endpoint Detection and Response" (EDR) tools that can identify the rapid, unauthorized encryption of files and kill the malicious process before it completes.
Ransomware represents a shift in cybercrime from data theft to data "kidnapping," highlighting that even if data isn't stolen, its unavailability can cause catastrophic operational failure. Organizations must view ransomware not just as a virus, but as a business

continuity threat that demands rigorous patching, user training, and robust incident response planning.

NEW QUESTION # 21
......

Maybe most of people prefer to use the computer when they are study, but we have to admit that many people want to learn buy the paper, because they think that studying on the computer too much does harm to their eyes. CEHPC test questions have the function of supporting printing in order to meet the need of customers. You can print our CEHPC Exam Question on papers after you have downloaded it successfully. It not only can help you protect your eyes, but also it will be very convenient for you to make notes. We believe that you will like our CEHPC exam prep.

Latest CEHPC Exam Pdf: https://www.actualtestsit.com/CertiProf/CEHPC-exam-prep-dumps.html

CertiProf CEHPC Dumps Vce This version just can run on web browser, For your convenience, ActualTestsIT gives you a chance to try a free demo of CertiProf CEHPC exam questions, which means you can buy the product once you are satisfied with the features and you think it can actually help you to pass your certification exam, With our motto "Sincerity and Quality", we will try our best to provide the big-league CEHPC exam questions for our valued customers like you.

Design, Features, and Applicability of Solaris File Systems, Long CEHPC List Selector, This version just can run on web browser, For your convenience, ActualTestsIT gives you a chance to try a free demo of CertiProf CEHPC Exam Questions, which means you can buy the product once you are satisfied with the features and you think it can actually help you to pass your certification exam.

Reliable CertiProf CEHPC PDF Questions Pass Exam With Confidence

With our motto "Sincerity and Quality", we will try our best to provide the big-league CEHPC exam questions for our valued customers like you, If you want to use our CEHPC study materials on your phone at any time, then APP version is your best choice as long as you have browsers on your phone.

Now hurry to download free demo, you will believe your choice can't be wrong.

- 2026 Valid 100% Free CEHPC – 100% Free Dumps Vce | Latest CEHPC Exam Pdf □ Open website □ www.pass4test.com □ and search for ➤ CEHPC □ for free download □CEHPC Valid Dumps Sheet
- Some Top Features of Pdfvce CertiProf CEHPC Exam Practice Questions □ Open website 【 www.pdfvce.com 】 and search for ⇛ CEHPC ⇚ for free download □Latest CEHPC Exam Duration
- The Best Accurate CEHPC Dumps Vce – Find Shortcut to Pass CEHPC Exam □ Easily obtain [CEHPC] for free download through ➤ www.practicevce.com □ □Test CEHPC Voucher
- Pdf CEHPC Torrent □ CEHPC Valid Dumps Sheet □ Latest CEHPC Dumps Sheet □ Easily obtain free download of （CEHPC） by searching on 【 www.pdfvce.com 】 □Latest CEHPC Exam Duration
- Trustworthy CEHPC Exam Torrent □ CEHPC Valid Dumps Sheet ☀ Latest CEHPC Exam Duration □ Open ✔ www.practicevce.com □✔□ and search for ➥ CEHPC □ to download exam materials for free □CEHPC Valid Dumps Sheet
- Reliable Study CEHPC Questions □ Valid CEHPC Test Vce □ New CEHPC Test Format □ Easily obtain free download of ➡ CEHPC □□□ by searching on ⇛ www.pdfvce.com ⇚ □Valid CEHPC Exam Camp
- Features of CertiProf CEHPC PDF Dumps Formate □ Search for 【 CEHPC 】 and download it for free immediately on ➤ www.examdiscuss.com □ □Best CEHPC Practice
- Reliable Study CEHPC Questions □ New CEHPC Test Format □ Latest CEHPC Dumps Sheet □ Open website ✔ www.pdfvce.com □✔□ and search for [CEHPC] for free download □CEHPC Reliable Test Question
- Test CEHPC Voucher □ CEHPC Exam Simulator Online □ Test CEHPC Voucher □ Download ➡ CEHPC □□□ for free by simply entering □ www.easy4engine.com □ website □Test CEHPC Duration
- 2026 Valid 100% Free CEHPC – 100% Free Dumps Vce | Latest CEHPC Exam Pdf □ Open ➤ www.pdfvce.com □ and search for " CEHPC " to download exam materials for free □Valuable CEHPC Feedback
- Pass4sure CEHPC dumps - CertiProf CEHPC sure practice dumps □ Easily obtain ➤ CEHPC □ for free download through 【 www.pdfdumps.com 】 □Valid CEHPC Test Vce
- 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, mytlearnu.com, myportal.utt.edu.tt,

myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes