

Quiz CertiProf - Newest CEHPC - New Ethical Hacking Professional Certification Exam Test Questions



BONUS!!! Download part of RealVCE CEHPC dumps for free: https://drive.google.com/open?id=1NkcKGVSSQf5pZEQVwuDIPrdQrFzIZI_m

You can avail all the above-mentioned characteristics of the desktop software in this web-based CertiProf CEHPC practice test. While you appear in the CertiProf CEHPC real examination, you will feel the same environment you faced during our CertiProf CEHPC practice test.

The CEHPC certification costs somewhere between 100\$ and 1000\$. Thus we save your amount by offering the best prep material with up to 1 year of free updates so that you pass the exam on the first attempt without having to retry, saving your time, effort, and money! RealVCE offers the CertiProf CEHPC Dumps at a very cheap price.

>> New CEHPC Test Questions <<

CEHPC Exam Consultant | Test CEHPC Cram

Our CertiProf CEHPC study guide is the most reliable and popular exam product in the market for we only sell the latest CEHPC practice engine to our clients and you can have a free trial before your purchase. Our CertiProf CEHPC training materials are full of the latest exam questions and answers to handle the exact exam you are going to face. With the help of our CEHPC Learning Engine, you will find to pass the exam is just like having a piece of cake.

CertiProf Ethical Hacking Professional Certification Exam Sample Questions (Q105-Q110):

NEW QUESTION # 105

What is a reverse shell?

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

Answer: A

Explanation:

A reverse shell is a fundamental technique used during the "Gaining Access" and "Maintaining Access" phases of a penetration test. In a standard (bind) shell, the attacker connects to a specific port on the victim's machine to gain command-line access. However, most modern firewalls block incoming connections to unauthorized ports. To bypass this, a reverse shell reverses the connection logic: the victim's machine is tricked into initiating an outgoing connection to the attacker's machine, which is "listening" for the call. This technique is highly effective because firewalls are typically much more permissive with "egress" (outgoing) traffic than with "ingress" (incoming) traffic. For example, an attacker might host a listener on port 443 (HTTPS). Since most organizations allow internal machines to browse the web over port 443, the firewall perceives the reverse shell connection as standard web traffic and allows it to pass. Once the connection is established, the attacker has a terminal interface on the victim's machine, allowing them to execute commands remotely.

In professional pentesting, establishing a reverse shell is often the primary goal of an exploit. It provides the "foothold" needed for lateral movement and privilege escalation. Common tools used to create reverse shells include Netcat (nc), Bash, and Python scripts. To defend against this, organizations must implement "Egress Filtering," which restricts outgoing traffic to only known, necessary destinations. Security professionals also monitor for "long-lived" connections to unusual IP addresses, as these can be a tell-tale sign of an active reverse shell. Understanding how these connections manipulate network policy is crucial for any ethical hacker seeking to demonstrate how internal systems can be compromised despite robust perimeter defenses.

NEW QUESTION # 106

Can all computers be hacked?

- A. No, only computers that are not updated with security patches and have exposed ports can be hacked.
- **B. Yes, all computers are hackable.**
- C. Yes, all computer equipment can be hacked without any complications.

Answer: B

Explanation:

From a cybersecurity and ethical hacking perspective, the most accurate answer is option C: yes, all computers are hackable. This does not mean that all systems are easily compromised, but rather that no system is 100% secure under all circumstances.

Security is a matter of risk management, not absolute prevention. Even fully patched systems with strong security controls may be vulnerable to zero-day exploits, misconfigurations, supply-chain attacks, physical access threats, or human factors such as social engineering. Ethical hackers assess these risks to determine how systems could be compromised under realistic threat scenarios.

Option A is incorrect because even updated systems with minimal exposure can still be attacked through advanced techniques.

Option B is incorrect because hacking is not always easy or without complications; strong defenses significantly increase the difficulty.

Understanding this concept is critical in modern security strategy. Ethical hacking promotes defense in depth, continuous monitoring, regular testing, and user awareness rather than reliance on a single control.

Acknowledging that all systems are potentially hackable encourages proactive security practices, timely patching, strong authentication, network segmentation, and incident response planning. Ethical hackers help organizations identify weaknesses early, reduce risk, and improve resilience against evolving cyber threats.

NEW QUESTION # 107

What is ethical responsibility in hacking?

- A. Ensuring that scanning is performed without permission and for illegitimate purposes.
- **B. Ensuring that scanning and testing are performed with proper authorization and for legitimate purposes.**
- C. Performing scanning activities with technical knowledge only.

Answer: B

Explanation:

Ethical responsibility in hacking refers to the obligation to perform all security testing activities legally, transparently, and with explicit authorization, making option B the correct answer. Ethical hacking is not defined solely by technical skill, but by adherence to legal boundaries, professional conduct, and organizational policies.

Ethical hackers must always obtain written permission before conducting reconnaissance, scanning, or exploitation activities. This authorization clearly defines the scope, targets, and limitations of the engagement.

Without permission, even basic scanning activities may be considered illegal or unethical, regardless of intent.

Option A is incorrect because technical knowledge alone does not make hacking ethical. Skills must be applied responsibly. Option C is incorrect because performing scans without permission is a violation of ethical and legal standards and may result in criminal charges.

From an ethical hacking perspective, responsibility also includes responsible disclosure, minimizing impact, protecting sensitive data, and reporting findings accurately. Ethical hackers must avoid data misuse, service disruption, or unnecessary system damage. Understanding ethical responsibility is foundational to professional cybersecurity practice. It distinguishes ethical hackers from malicious actors and ensures that security testing contributes positively to risk reduction, compliance, and organizational trust.

NEW QUESTION # 108

When critical vulnerabilities are detected, what should be done?

- A. Inform the corresponding area for a prompt solution.
- B. Exploit it and extract as much information as possible.
- C. Document the problem and do nothing.

Answer: A

Explanation:

In the professional penetration testing process, the discovery of a "critical" vulnerability—one that could lead to immediate system compromise or data loss—triggers a specific ethical and procedural response. While the ultimate goal of a pentest is to find weaknesses, the primary duty of an ethical hacker is to ensure the safety and security of the client's environment. Therefore, when a critical flaw is identified, the tester must immediately inform the relevant stakeholders or technical teams so that a prompt solution or "hotfix" can be implemented.

This immediate reporting deviates from the standard "end-of-test" report delivery because critical vulnerabilities represent an "active risk". If a tester finds an unpatched, high-impact vulnerability that is publicly known, there is a high probability that a real attacker could exploit it while the pentest is still ongoing. By notifying the client immediately, the tester helps mitigate the risk of an actual breach occurring during the assessment. This process is often detailed in the "Rules of Engagement" (RoE) agreed upon before the test begins.

Once the "corresponding area" (such as the DevOps or Security Operations team) is informed, the tester documents the vulnerability with clear reproduction steps and remediation advice. The tester may then be asked to "re-test" the vulnerability after the fix has been applied to verify its effectiveness. This highlights the collaborative nature of ethical hacking: it is not just about "breaking in" (Option B), but about the strategic management of risk. Professionalism in pentesting is defined by this commitment to communication and the proactive protection of the client's assets, ensuring that vulnerabilities are closed as quickly as possible to minimize the window of opportunity for malicious actors.

NEW QUESTION # 109

What is malware?

- A. Refers to any software specifically designed to damage, infect, steal data or otherwise cause a nuisance to a device, network or system without the owner's consent.
- B. Refers to any software specifically designed to protect, safeguard and store data on a device, network or system.
- C. It is an Antivirus for servers especially.

Answer: A

Explanation:

Malware, short for "malicious software," is a broad category of software specifically engineered to perform unauthorized and often harmful actions on a computer system, network, or device. Its primary characteristic is that it operates without the owner's consent. Malware is the primary tool used by cybercriminals to achieve various objectives, ranging from financial gain to corporate espionage and simple disruption.

Malware encompasses several distinct types, each with its own method of infection and goal:

* Viruses and Worms: Designed to spread from one file or computer to another, often damaging data or consuming network bandwidth along the way.

* Trojan Horses: Programs that disguise themselves as legitimate software to trick users into installing them, only to reveal a malicious "payload" once active.

* Ransomware: Encrypts the victim's data and demands payment for the decryption key.

* Spyware and Stealers: Secretly monitor user activity or steal sensitive information like passwords and credit card numbers.

* Rootkits: Specialized malware designed to provide high-level "root" access while remaining hidden from the operating system and antivirus software.

Ethical hackers study malware to understand how to defend against it. This involves analyzing "Attack Vectors" (how malware enters a system), "Persistence Mechanisms" (how it stays there), and "Command and Control" (how it communicates with the attacker). Protecting against malware requires a multi-layered defense strategy, including updated antivirus software, strict Acceptable Use Policies (AUP), and regular vulnerability scanning to close the gaps that malware exploits to infect systems.

NEW QUESTION # 110

.....

CEHPC study dumps always managed to build an excellent relationship with our users through the mutual respect and attention we provide to everyone. We sincerely hope our CEHPC study dumps will help you to pass the CEHPC Exam in a shortest time, we aimed to help you save more time. Once you purchase our CEHPC study dumps, we will send to your mailbox within 5-10 minutes, if there are some problem, please contact with us.

CEHPC Exam Consultant: https://www.realvce.com/CEHPC_free-dumps.html

CertiProf New CEHPC Test Questions We are waiting to your reply, To choose RealVCE's CertiProf CEHPC exam training materials, and it is equivalent to have a better future, We believe in offering assistance to customers regarding each and every query about CertiProf CEHPC Brain Dumps, CertiProf New CEHPC Test Questions With a high pass rate as 98% to 100%, you will be bound to pass the exam, I believe that no one can know the CEHPC exam questions better than them.

Now, here comes the good news for you, He closes CEHPC with a formula for determining what you can do in a volatile work environment, We are waiting to your reply, To choose RealVCE's CertiProf CEHPC Exam Training materials, and it is equivalent to have a better future.

New CEHPC Test Questions 100% Pass | The Best Ethical Hacking Professional Certification Exam Exam Consultant Pass for sure

We believe in offering assistance to customers regarding each and every query about CertiProf CEHPC Brain Dumps, With a high pass rate as 98% to 100%, you will be bound to pass the exam.

I believe that no one can know the CEHPC exam questions better than them.

- Place Your Order and Download CertiProf CEHPC Actual Questions Instantly Search for ⇒ CEHPC ⇐ on (www.practicevce.com) immediately to obtain a free download CEHPC Download Demo
- Pass Guaranteed First-grade CertiProf CEHPC - New Ethical Hacking Professional Certification Exam Test Questions Open ➔ www.pdfvce.com enter ▶ CEHPC ◀ and obtain a free download Download CEHPC Demo
- CEHPC training exam pdf - CEHPC real valid dumps Open website www.pdfdumps.com and search for ➤ CEHPC for free download CEHPC Exam Learning
- CEHPC Valid Braindumps Free Valid Braindumps CEHPC Files Valid Braindumps CEHPC Files Download ⇒ CEHPC ⇐ for free by simply entering ➤ www.pdfvce.com website CEHPC Pdf Dumps
- Place Your Order and Download CertiProf CEHPC Actual Questions Instantly Search on ✓ www.testkingpass.com ✓ for **【 CEHPC 】** to obtain exam materials for free download Pass Leader CEHPC Dumps
- CEHPC Reliable Mock Test CEHPC Test Registration CEHPC Valid Braindumps Free Search for ☀ CEHPC ☀ and obtain a free download on ➔ www.pdfvce.com Related CEHPC Exams
- Pass Guaranteed First-grade CertiProf CEHPC - New Ethical Hacking Professional Certification Exam Test Questions Search for ➔ CEHPC and download it for free immediately on www.examcollectionpass.com Download CEHPC Demo
- CEHPC Exam Duration CEHPC Exam Duration CEHPC Valid Braindumps Free Search for ➔ CEHPC and easily obtain a free download on (www.pdfvce.com) CEHPC Test Registration
- CEHPC Latest Dump CEHPC New Study Guide Related CEHPC Exams Search on (www.troytecdumps.com) for ➔ CEHPC to obtain exam materials for free download CEHPC Valid Exam Answers
- CEHPC Reliable Mock Test Valid Test CEHPC Test New CEHPC Dumps Ebook Open (www.pdfvce.com) enter CEHPC and obtain a free download Download CEHPC Demo
- CEHPC training exam pdf - CEHPC real valid dumps Easily obtain > CEHPC < for free download through “ www.prep4sures.top ” CEHPC Exam Learning
- telegra.ph, www.stes.tyc.edu.tw, www.grepmed.com, www.stes.tyc.edu.tw, graphiskill.com, mutouzyz.com, bbs.t-firefly.com, vkurbakov.alboompro.com, www.stes.tyc.edu.tw, hhi.instructure.com, Disposable vapes

P.S. Free 2026 CertiProf CEHPC dumps are available on Google Drive shared by RealVCE: <https://drive.google.com/open?>

id=1NkcKGVsQ5pZEqVwuDlPrdQrFzI_m