

New CertiProf CEHPC Exam Online & Latest CEHPC Exam Objectives



You must have felt the changes in the labor market. Today's businesses require us to have more skills and require us to do more in the shortest possible time. We are really burdened with too much pressure. CEHPC simulating exam may give us some help. With our CEHPC Study Materials, we can get the CEHPC certificate in the shortest possible time. And our pass rate is high as 98% to 100% which is unbeatable in the market.

It is known to us that getting the CEHPC certification is not easy for a lot of people, but we are glad to tell you good news. The CEHPC study materials from our company can help you get the certification in a short time. Now we are willing to let you know our CEHPC Practice Questions in detail on the website, we hope that you can spare your valuable time to have a look to our products. Please believe that we will not let you down.

>> New CertiProf CEHPC Exam Online <<

Quiz 2026 CertiProf CEHPC Marvelous New Exam Online

In order to let customers understand our CEHPC exam dumps better, our company will provide customers with a trail version. And the trail version is free for customers. The trail version will offer demo to customers, it means customers can study the demo of our CEHPC Exam Torrent for free. If you use our CEHPC test quiz, we believe you will know fully well that our product is of superior quality, other products can't be compared with it. Don't hesitate, just buy our CEHPC test quiz!

CertiProf Ethical Hacking Professional Certification Exam Sample Questions (Q104-Q109):

NEW QUESTION # 104

What is a Stored Cross-Site Scripting Attack (Stored XSS)?

- A. The source code of the page, this can be html or javascript.
- **B. The malicious code is permanently stored on the server.**
- C. In this type of attack, the malicious code is sent to the web server via an HTTP request. The server then processes the request and returns a response that includes the malicious code.

Answer: B

Explanation:

Persistent Cross-Site Scripting (XSS), also known as Stored XSS, is one of the most dangerous forms of web application vulnerabilities. It occurs when a web application receives data from a user and stores it permanently in its backend database or filesystem without proper sanitization or encoding. Common vectors for persistent XSS include comment sections, user profiles, message boards, and "Contact Us" forms. Unlike Reflected XSS, where the payload is included in a specific URL and only affects the user who clicks that link, a persistent XSS payload is served automatically to every user who visits the affected page. When an attacker successfully injects a malicious script (typically JavaScript), the server "remembers" this script. Every time a legitimate user requests the page where the data is displayed, the server includes the malicious code in the HTML response. The user's browser, trusting the source, executes the script. This can lead to devastating consequences, such as session hijacking through the theft of session cookies, account takeover, or the redirection of users to malicious websites. From an ethical hacking perspective, identifying persistent XSS involves testing all input fields that result in data being displayed later. Mitigation strategies focus on the principle of "filter input, escape output." Input should be validated against a strict whitelist of allowed characters, and any data rendered in the browser must be context-aware encoded (e.g., converting < to <) to prevent the browser from interpreting the data as executable code. Because the payload is stored on the server, this vulnerability represents a significant risk to the entire user base of an organization, making it a high-priority finding in any security assessment.

NEW QUESTION # 105

What is privilege escalation?

- A. Is the term used when you request elevated permissions to your account with the administrator.
- **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. It is the term used by major hackers to refer to the request for new permissions to your account with hacked administrators.

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 # 106

What is Nmap?

- A. It is a Linux-based tool that works specifically to exploit computer vulnerabilities.
- **B. It is an open-source command-line tool used to scan IP addresses and ports on a network and to detect services, operating systems, and running applications.**
- C. It is a program used only for pinging computers within a network or work environment.

Answer: B

Explanation:

Nmap, also known as Network Mapper, is a widely used open-source tool in ethical hacking and penetration testing. It plays a critical role during the reconnaissance and scanning phases of ethical hacking, where the primary goal is to collect information about

target systems in a legal and authorized manner. Ethical hackers rely on Nmap to understand the structure and exposure of a network before moving forward with deeper security testing.

The tool works by sending various types of packets to target hosts and analyzing the responses. Based on these responses, Nmap can identify active hosts, open and closed ports, running services, service versions, operating systems, and even certain firewall and intrusion detection configurations. This information is essential for identifying potential weaknesses such as unnecessary open ports, misconfigured services, or outdated software.

Option A correctly defines Nmap because it accurately reflects its purpose as a scanning and discovery tool rather than an exploitation utility. Option B is incorrect because Nmap does not exploit vulnerabilities; exploitation is typically performed using specialized frameworks such as vulnerability scanners or exploitation platforms. Option C is also incorrect because although Nmap can perform host discovery similar to ping, it offers far more advanced capabilities than simple network reachability checks.

From an ethical hacking perspective, Nmap supports preventive and defensive security objectives. By revealing network visibility issues and configuration flaws, it enables organizations to harden systems, reduce attack surfaces, and comply with security best practices. When used ethically and with proper authorization, Nmap is a foundational tool for strengthening information security.

NEW QUESTION # 107

What is a remote exploit?

- A. It is a type of computer attack that targets vulnerabilities present in an operating system, application or software in a local environment.
- B. It is a type of social engineering attack for all types of users.
- C. It is a type of computer attack in which a hacker or attacker attempts to exploit vulnerabilities in a computer system, network or application from a remote location.

Answer: C

Explanation:

A remote exploit is a sophisticated attack vector where a threat actor manipulates a vulnerability in a system over a network—typically the internet—without having prior physical or local access to the target machine.

This type of exploit is highly dangerous because the attacker can be located anywhere in the world, making it difficult to trace or physically stop. Remote exploits usually target services that are "listening" for incoming connections, such as web servers (HTTP/HTTPS), database servers (SQL), or remote desktop protocols (RDP).

The mechanism of a remote exploit often involves sending specially crafted data packets to a service to trigger a specific flaw, such as a buffer overflow or an injection vulnerability. If successful, the exploit can allow the attacker to execute arbitrary code with the same privileges as the service being attacked. This is often the first step in a larger attack chain, where the remote exploit provides the "initial access" needed to drop malware or pivot further into the internal network.

To manage and mitigate the risks associated with remote exploits, organizations must focus on "Attack Surface Reduction." This involves closing unnecessary ports, implementing robust firewalls, and using Intrusion Detection Systems (IDS) to flag suspicious network traffic. Patch management is the most effective defense, as most remote exploits target known vulnerabilities that have available security updates. Ethical hackers use remote exploits during penetration tests to demonstrate the exposure of an organization's perimeter. By identifying these external-facing weaknesses, they help the organization prioritize defenses on the services most likely to be targeted by global threat actors.

NEW QUESTION # 108

What is netcat?

- A. It is a hacking tool for Windows.
- B. It is a hacking tool for Linux.
- C. It is a versatile, open-source network tool used for reading and writing data over network connections.

Answer: C

Explanation:

Netcat, often referred to as the "Swiss Army Knife" of networking, is a powerful and versatile utility that uses TCP or UDP protocols to read and write data across network connections. It is a foundational tool for both system administrators and security professionals because of its ability to perform a wide variety of tasks with minimal overhead. While it is natively a Linux tool, versions like `ncat` (distributed with Nmap) make it available across all major operating systems.

In the context of ethical hacking, Netcat is used for:

* Port Scanning: It can be used as a lightweight port scanner to check for open services on a target.

* Banner Grabbing: By connecting to a specific port, testers can capture the "banner" or header sent by a service to identify its

software version.

* File Transfer: It can push files from one machine to another without needing FTP or SMB protocols.

* Creating Backdoors and Shells: Netcat is the primary tool used to establish Bind Shells or Reverse Shells during the exploitation phase of a pentest. An attacker can set Netcat to "listen" on a port and execute a shell (like /bin/bash or cmd.exe) whenever someone connects to it.

Its simplicity is its greatest strength; it can be scripted into complex automated tasks or used manually for quick troubleshooting. Because Netcat can be used to bypass security controls and establish unauthorized access, security teams often monitor for its presence or execution on sensitive servers. Understanding how to use and defend against Netcat is a core requirement for any information security expert.

NEW QUESTION # 109

.....

If you want to give up your certificate exams as you fail CEHPC exam or feel it too difficult, please think about its advantages after you obtain a CertiProf certification. Many special positions require employees to have a qualification. If you think it is very difficult for you to pass exams, our CEHPC Valid Exam Cram PDF can help you to achieve your goal. Our exam materials are collected from the real test center and edited by our experienced experts. If you need 100% passing rate, our CEHPC valid exam cram PDF can help you.

Latest CEHPC Exam Objectives: <https://www.it-tests.com/CEHPC.html>

With the high quality and high passing rate of our CEHPC test questions: Ethical Hacking Professional Certification Exam, we promised that our CEHPC training online questions are the best for your reference. We are constantly improving and just want to give you the best CEHPC learning braindumps. These CEHPC exam questions features are valid, updated, and real CertiProf CEHPC exam questions, availability of CertiProf CEHPC exam questions in three different formats. If you failed to do so then the customer gets a full refund from It-Tests Latest CEHPC Exam Objectives according to the terms and conditions.

Much of the work was performed in a lab environment with the hardware Latest CEHPC Exam Objectives engineers. From there, it's a matter of how, when, and where to showcase your abilities to prospective employers.

With the high quality and high passing rate of our CEHPC Test Questions: Ethical Hacking Professional Certification Exam, we promised that our CEHPC training online questions are the best for your reference.

CertiProf CEHPC Exam | New CEHPC Exam Online - Updated Download Latest CEHPC Exam Objectives

We are constantly improving and just want to give you the best CEHPC learning braindumps. These CEHPC exam questions features are valid, updated, and real CertiProf CEHPC exam questions, availability of CertiProf CEHPC exam questions in three different formats.

If you failed to do so then the customer gets a full refund from It-Tests CEHPC according to the terms and conditions. Of course, they have worked hard, but having a competent assistant is also one of the important factors.

- Frequent CEHPC Update ☐ Vce CEHPC Format ☐ CEHPC Certification Test Questions ☐ Search for > CEHPC < and download it for free immediately on ✓ www.prepawayexam.com ☐ ✓ ☐ Vce CEHPC Format
- New CEHPC Mock Exam ☐ CEHPC Reliable Exam Bootcamp ☐ CEHPC Valid Real Exam ☐ Download > CEHPC ☐ for free by simply entering ➡ www.pdfvce.com ☐ website ☐ Pass CEHPC Exam
- Pass Guaranteed 2026 CertiProf CEHPC: High Hit-Rate New Ethical Hacking Professional Certification Exam Exam Online ☐ Search on ➡ www.prep4sures.top ☐ for > CEHPC < to obtain exam materials for free download ☐ CEHPC Latest Learning Materials
- CEHPC Latest Learning Materials ☐ New CEHPC Mock Exam ☐ Practice CEHPC Engine ☐ Search for > CEHPC < and download exam materials for free through ➡ www.pdfvce.com ☐ ☐ Latest CEHPC Braindumps Free
- Latest CEHPC Exam Discount ☐ Vce CEHPC Format ☐ CEHPC Valid Real Exam ☐ Download [CEHPC] for free by simply searching on > www.dumpsquestion.com ☐ ☐ CEHPC Valid Dumps Ppt
- CEHPC Certification Test Questions ☐ Latest CEHPC Exam Discount ☐ Vce CEHPC Format ☐ Immediately open ☐ www.pdfvce.com ☐ and search for ☐ CEHPC ☐ to obtain a free download ☐ CEHPC Download Pdf
- CEHPC Certification Test Questions ☐ CEHPC Reliable Exam Bootcamp ☐ CEHPC Latest Learning Materials ☐ Open ☐ www.exam4labs.com ☐ and search for ➡ CEHPC ☐ ☐ ☐ to download exam materials for free ☐ Training CEHPC Kit
- Prepare with updated CertiProf CEHPC dumps - Get up to 1 year of free updates ☐ Search for ☀ CEHPC ☐ ☀ ☐ and

- CEHPC Trustworthy Exam Content ➡ New CEHPC Mock Exam ☐ CEHPC Study Test ☐ ⇒ www.practicevce.com
 ⇐ is best website to obtain ➡ CEHPC ☐ for free download ☐ CEHPC Valid Dumps Ppt
- Latest CEHPC Exam Discount ☐ CEHPC Dumps Free Download ☐ CEHPC Reliable Exam Bootcamp ☐
 Immediately open [www.pdfvce.com] and search for **【 CEHPC 】** to obtain a free download ☐ CEHPC Study Test
- Pass CEHPC Exam ☐ CEHPC Study Test ☐ CEHPC Latest Learning Materials ☐ Easily obtain free download of ➡
 CEHPC ☐ by searching on { www.vce4dumps.com } ☐ Training CEHPC Kit
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt,
myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw,
onlinecourse.essinstitute.in, www.stes.tyc.edu.tw, udrive242.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt,
myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt,
myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw,
 Disposable vapes