CertiProf CEHPC PDF Questions - Ensure Your Success In Exam

BONUS!!! Download part of TestInsides CEHPC dumps for free: https://drive.google.com/open?id=1iYeoP4IwuWtZcrEgWxAeP-h7x3_nSyIt

Our CEHPC practice engine boosts both the high passing rate which is about 98%-100% and the high hit rate to have few difficulties to pass the test. Our CEHPC exam simulation is compiled based on the resources from the authorized experts' diligent working and the real exam and confer to the past years' exam papers thus they are very practical. So the content of the CEHPC Learning Materials is quite fully covered and completed. And we will update it to be the latest.

CertiProf CEHPC Exam Syllabus Topics:

Topic	Details
Topic 1	• Understand the pentesting process: This topic focuses on the complete penetration testing workflow, including planning, execution, reporting, and remediation activities.
Topic 2	• Manage information security threats: This topic covers identifying, analyzing, and handling different types of security threats that can impact information systems and networks.
Topic 3	• Develop strategies for understanding, managing, and mitigating attack vectors: This section explains how attackers exploit vulnerabilities and how organizations can reduce risks through effective mitigation strategies.
Topic 4	• Master information security controls: This section explains administrative, technical, and physical security controls used to protect systems, networks, and organizational data.
Topic 5	• Understand current security trends: This topic covers the latest cybersecurity trends, emerging threats, and evolving attack techniques affecting modern organizations and systems.

Topic 6	• Familiarize oneself with information security elements: This section explains the core elements of information security, including confidentiality, integrity, availability, and security governance concepts.

>> Latest CEHPC Practice Materials <<

CEHPC Exam Objectives - CEHPC Valid Exam Vce

The Software version of our CEHPC exam materials can let the user to carry on the simulation study on the CEHPC 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 CEHPC 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.

CertiProf Ethical Hacking Professional Certification Exam Sample Questions (Q108-Q113):

NEW QUESTION # 108
What is active reconnaissance?

- A. Recognizes the target but does nothing.
- B. Gathers information by directly interacting with the target.
- C. Observes the target without performing any direct actions.

Answer: B

Explanation:
Active reconnaissance is a phase of ethical hacking in which information is gathered bydirectly interacting with the target system. This makes option C the correct answer. Unlike passive reconnaissance, active reconnaissance involves sending requests, probes, or packets to the target to elicit responses that reveal useful technical details.
Common active reconnaissance techniques includeport scanning,service enumeration,banner grabbing,DNS queries, andnetwork mapping. These methods help ethical hackers identify open ports, running services, operating systems, and potential vulnerabilities.
Active reconnaissance is typically conducted after passive techniques have provided initial intelligence.
Option A is incorrect because recognizing a target without action does not describe reconnaissance behavior.
Option B is also incorrect because observing without interaction definespassive reconnaissance, not active reconnaissance.
From an ethical hacking perspective, active reconnaissance is more intrusive and therefore more likely to be detected by intrusion detection systems or firewalls. Because of this, it must always be performed withexplicit authorization. Despite the increased risk of detection, active reconnaissance provides far more accurate and actionable information, making it essential for effective penetration testing.
Understanding the distinction between active and passive reconnaissance helps security professionals choose the correct techniques based on scope, authorization, and risk tolerance. Properly managed, active reconnaissance enables organizations to identify weaknesses early and strengthen their defensive security posture.

NEW QUESTION # 109
When critical vulnerabilities are detected, what should be done?

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

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 # 110
What is Netcat?

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

Answer: B

Explanation:
Netcat, often referred to as the"Swiss Army knife of networking,"is a versatile, open-source tool used for reading from and writing to network connections using TCP or UDP. This makes option B the correct answer.
Netcat is widely used in ethical hacking, penetration testing, and system administration due to its flexibility and simplicity.
Netcat can perform a wide range of networking tasks, includingport scanning, banner grabbing, file transfers, reverse shells, bind shells, and debugging network services. It is commonly used during thereconnaissance, exploitation, and post-exploitation phasesof ethical hacking. Because of its ability to create raw network connections, it can simulate both client and server behavior.
Option A and option C are incorrect because Netcat iscross-platformand works on Linux, Windows, macOS, and other Unix-like systems. It is not limited to a single operating system, nor is it exclusively a hacking tool; it is also used legitimately by network administrators for troubleshooting and testing.
From a defensive security perspective, understanding Netcat is important because attackers frequently abuse it to establish unauthorized communication channels or backdoors. Ethical hackers use Netcat responsibly to demonstrate how weak configurations or exposed services can be exploited.
By identifying improper Netcat usage during assessments, organizations can improve monitoring, restrict unnecessary outbound connections, and strengthen endpoint security controls.

NEW QUESTION # 111
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 # 112
What tool would you use to search for hidden directories or files?

- A. Shodan
- B. Ping
- C. Dirb

Answer: C

Explanation:
DIRB is a specializedweb content scanning toolused in ethical hacking and penetration testing to discoverhidden directories and fileson web servers. It operates by performing adictionary-based brute-force attackagainst a target website, attempting to access directories and files that are not publicly linked but may still be accessible. This makes option A the correct answer.
DIRB is typically used during theweb application reconnaissance and enumeration phasesof penetration testing. Ethical hackers rely on it to uncover misconfigurations such as exposed admin panels, backup files, configuration files, or outdated directories that could lead to further compromise. These hidden resources often exist due to poor security practices or improper cleanup during development.
Option B, Shodan, is incorrect because Shodan is a search engine used to discover internet-connected devices and services, not hidden directories within a specific website. Option C, Ping, is also incorrect because it is a network utility used only to test host reachability and does not interact with web servers at the application layer.
From a defensive security perspective, DIRB helps organizations identify unnecessary exposure in web environments. Discovering hidden directories allows administrators to remove, restrict, or secure them before attackers exploit them. When used ethically and with authorization, DIRB is a powerful tool for improving web application security and reducing attack surfaces.

NEW QUESTION # 113
.....

Our CEHPC test prep is of high quality. The passing rate and the hit rate are both high. The passing rate is about 98%-100%. We can guarantee that you have a very high possibility to pass the exam. The CEHPC guide torrent is compiled by the experts and approved by the professionals with rich experiences. The CEHPC prep torrent is the products of high quality complied elaborately and gone through strict analysis and summary according to previous exam papers and the popular trend in the industry. The language of the CEHPC exam material is simple and easy to be understood.

- Valid CEHPC Test Labs □ CEHPC Reliable Dumps Questions □ Valid Test CEHPC Test □ Search for ✔ CEHPC □✔□ and download exam materials for free through 《 www.examcollectionpass.com 》 ↗Test CEHPC Lab Questions
- CEHPC Free Download Pdf □ New CEHPC Exam Topics □ Valid Test CEHPC Test □ Open ➡ www.pdfvce.com □□□ and search for （ CEHPC ） to download exam materials for free □CEHPC Actual Test Answers
- Updated CertiProf CEHPC Questions - Fast Track To Get Success □ Open website （ www.pass4test.com ） and search for ➤ CEHPC □ for free download □Latest CEHPC Test Online
- 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, laylajhlu789824.atualblog.com, isaiahjwjf422945.signalwiki.com, theresauisy424994.blogsuperapp.com, ledbookmark.com, get-social-now.com, henridouk711299.blogdemls.com, finniansjyu957305.blog-gold.com, aishaitgg870024.theisblog.com, poppiemoua556251.wikienlightenment.com, Disposable vapes

BONUS!!! Download part of TestInsides CEHPC dumps for free: https://drive.google.com/open?id=1iYeoP4IwuWtZcrEgWxAeP-h7x3_nSyIt