Well-Prepared Top CEHPC Dumps & Leader in Qualification Exams & Trustable Reliable CEHPC Learning Materials

P.S. Free 2026 CertiProf CEHPC dumps are available on Google Drive shared by Dumps4PDF: https://drive.google.com/open?id=14zxZr3LaJYcOzPifjO1OhaHXeKrq2Ogf

Our online test engine and the windows software of the CEHPC study materials can evaluate your exercises of the virtual exam and practice exam intelligently. Our calculation system of the CEHPC study materials is designed subtly. Our evaluation process is absolutely correct. We are strictly in accordance with the detailed grading rules of the real exam. The point of every question is set separately. Once you submit your exercises of the CEHPC Study Materials, the calculation system will soon start to work.

CertiProf CEHPC Exam Overview:

Certification Vendor:	CertiProf
Exam Name:	Ethical Hacking Professional Certification
Exam Number:	CEHPC
Available Languages:	English, Spanish
Certificate Validity Period:	Not specified
Exam Price:	USD $150
Passing Score:	80% (32/40)
Exam Duration:	60 minutes
Related Certifications:	Cyber Security Foundation Professional Certification PenTester Professional Certification
Real Exam Qty:	40
Exam Format:	Multiple Choice, Closed Book
Sample Questions:	CertiProf CEHPC Sample Questions
Exam Way:	Online proctored exam
Pre Condition:	Basic computer knowledge and reading comprehension in English are recommended.
Official Syllabus URL:	https://certiprof.com/products/ethical-hacking-professional-certification-cehpc

>> Top CEHPC Dumps <<

Reliable CEHPC Learning Materials, CEHPC Cost Effective Dumps

As is known to us that pass rate is one of the most important standards when candidate choose the practice materials. The pass rate is 98.95% for CEHPC training materials, and you can pass and get a certificate successfully. In addition we also pass guarantee and

money back guarantee if you fail to pass the exam after using CEHPC Exam Dumps. Free update for one year is also available, namely in the following year, you can get latest information about the CEHPC training materials. We also have online and offline chat service to solve your confusions.

CertiProf CEHPC Exam Syllabus Topics:

Topic	Details
Topic 1	• Manage information security threats: This topic covers identifying, analyzing, and handling different types of security threats that can impact information systems and networks.
Topic 2	• 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 3	• Familiarize oneself with information security elements: This section explains the core elements of information security, including confidentiality, integrity, availability, and security governance concepts.
Topic 4	• Understand the pentesting process: This topic focuses on the complete penetration testing workflow, including planning, execution, reporting, and remediation activities.
Topic 5	• Grasp the concepts, types, and phases of ethical hacking: This domain focuses on ethical hacking fundamentals, different hacking approaches, and the various phases involved in authorized security testing.
Topic 6	• Master information security controls: This section explains administrative, technical, and physical security controls used to protect systems, networks, and organizational data.

CertiProf Ethical Hacking Professional Certification Exam Sample Questions (Q91-Q96):

NEW QUESTION # 91
Is the use of cracks good for the equipment?

- A. NO, since they are loaded with malicious software.
- B. YES, you permanently activate programs without payment.
- C. NO, since the cracks are pre-installed for the best performance of Windows servers.

Answer: A

Explanation:
"Cracks" or "Keygens" are small programs used to bypass the licensing and copy-protection mechanisms of commercial software. From a security perspective, using cracks is extremely dangerous for any computer system. Because these programs are produced by anonymous, untrusted sources and are inherently illegal, there is no accountability or quality control. Malicious actors frequently package "Trojan Horses,"
"Ransomware," or "Stealers" inside these cracks.
When a user runs a crack, they usually have to disable their antivirus software-a standard instruction provided by the malicious site to prevent the crack from being flagged. This creates a perfect window for malware to infect the host machine. Once executed, the malware can:
* Exfiltrate Data: Steal browser cookies, saved passwords, and cryptocurrency wallets.
* Create Backdoors: Allow the attacker to remotely control the computer and use it as part of a "Botnet" for DDoS attacks.
* Deploy Ransomware: Encrypt the user's files and demand payment for their release.
[Image showing a malware infection process triggered by running a fake software crack] In an enterprise environment, the use of cracked software is a major security risk that can lead to a full network compromise. Furthermore, it opens the organization to significant legal and financial penalties for copyright infringement. Ethical hackers often look for unauthorized or "pirated" software during audits as it is a common entry point for persistent threats. The perceived "saving" of not paying for software is never worth the high risk of total system compromise.

NEW QUESTION # 92
What tool would you use to scan ports?

- A. Shodan
- B. Metasploit
- C. Nmap

Answer: C

Explanation:
Nmap is the primary tool used forport scanning, making option B the correct answer. Port scanning is a core activity during the reconnaissance and scanning phases of penetration testing, where the goal is to identify open, closed, or filtered ports on target systems.
Nmap allows ethical hackers to discover which services are running, their versions, and potential misconfigurations. It supports multiple scan types, including TCP SYN scans, UDP scans, and service detection scans, making it highly versatile and efficient.
Option A is incorrect because Metasploit is primarily an exploitation framework, not a dedicated port scanner.
Option C is incorrect because Shodan is an internet-wide search engine, not a direct scanning tool used against specific targets.
Understanding port scanning is essential for identifying attack surfaces. Open ports often expose services that may contain vulnerabilities or misconfigurations. Ethical hackers use Nmap responsibly to map networks and guide further testing.
From a defensive perspective, regular port scanning helps organizations identify unnecessary services and enforce least-exposure principles. Nmap remains one of the most fundamental tools in ethical hacking and network security.

NEW QUESTION # 93
Do Google dorks show hacked computers?

- A. NO, Google dorks works to search for specific topics.
- B. YES, Google dorks hacks pages for us in order to access data.
- C. YES, Google dorks works as a backdoor to all web pages.

Answer: A

Explanation:
Google Dorking, also known as Google Hacking, is a passive reconnaissance technique that involves using advanced search operators to filter through the vast index of the Google search engine. It is important to clarify that Google Dorks do not "hack" computers or websites themselves; rather, they utilize the search engine's indexing power to find information that has already been made public-often inadvertently. By using specific strings like filetype:log, intitle:"index of", or inurl:admin, a researcher can locate sensitive directories, exposed log files, or configuration pages that were never intended to be indexed by search bots.
From a threat management perspective, Google Dorking is a double-edged sword. Ethical hackers use it during the information-gathering phase of a penetration test to see what an organization is leaking to the public web. This might include SQL error messages, which can reveal database structures, or publicly accessible backup files containing sensitive credentials. However, the tool itself is not a "backdoor" or an exploit; it is a sophisticated way of querying a database of cached website content.
If a computer or server appears in a Google Dork result, it typically means the administrator failed to configure the robots.txt file or server permissions correctly, allowing Google's crawlers to document the internal structure. Managing this threat involves regular "dorking" of one's own domain to ensure that no sensitive paths or files are visible to the public. Understanding that Google Dorks are simply advanced search queries helps security professionals realize that the "leak" occurs at the server configuration level, not within the search engine itself. Consequently, remediation focuses on tightening access controls and ensuring that internal-only resources are not reachable or indexable by external search engines.

NEW QUESTION # 94
Who uses Metasploit?

- A. Food engineers.
- B. Agricultural engineers.
- C. Cybersecurity experts.

Answer: C

Explanation:
Metasploit is a widely used penetration testing framework designed to develop, test, and execute exploit code against target

systems. It is primarily used by cybersecurity experts, including ethical hackers, penetration testers, red team members, and security researchers. Therefore, option C is the correct answer.
In the context of ethical hacking, Metasploit is most commonly used during the exploitation and post- exploitation phases of penetration testing. After reconnaissance and vulnerability scanning identify potential weaknesses, Metasploit allows security professionals to safely verify whether those vulnerabilities can be exploited in real-world scenarios. This helps organizations understand the actual risk level of discovered flaws rather than relying solely on theoretical vulnerability reports.
Metasploit provides a vast library of exploits, payloads, auxiliary modules, and post-exploitation tools. Ethical hackers use these modules in controlled environments and with proper authorization to test system defenses, validate security controls, and demonstrate attack paths to stakeholders. It is not designed for non-technical professions such as agriculture or food engineering, making options A and B incorrect.
From an ethical standpoint, Metasploit supports defensive security objectives by enabling organizations to identify weaknesses before malicious attackers do. It is frequently used in security assessments, red team exercises, and cybersecurity training programs. When used legally and responsibly, Metasploit helps improve system hardening, incident response readiness, and overall organizational security posture.

NEW QUESTION # 95
What is Whois?

- A. It is a directory by which it is possible to know where exactly the owner of a domain or IP address lives.
- B. It is a physical directory where names and ip addresses can be consulted since the beginning of the Internet.
- C. It is a public directory through which you can know "who is" the owner of a domain or IP address.

Answer: C

Explanation:
WHOIS is a query and response protocol widely used for searching databases that store the registered users or assignees of an Internet resource, such as a domain name or an IP address block. It acts as a public directory that provides essential information about the ownership and technical management of a specific online asset.
When an individual or organization registers a domain name, they are required by ICANN (Internet Corporation for Assigned Names and Numbers) to provide contact information, which is then made available through WHOIS lookups.
A standard WHOIS record typically contains:
* Registrant Information: The name and organization of the person who owns the domain.
* Administrative and Technical Contacts: Names and email addresses of the people responsible for the site's operation.
* Registrar Information: The company where the domain was purchased and the date of registration
/expiration.
* Name Servers: The servers that direct traffic for the domain.
In ethical hacking, WHOIS is a primary tool forpassive reconnaissance. It allows a tester to map out the organizational structure of a target without ever sending a packet to the target's network. For example, finding the technical contact's email address might provide a lead for a social engineering attack, or identifying the name servers might reveal the cloud provider being used. While many owners now use "WHOIS Privacy" services to hide their personal details behind a proxy, WHOIS remains a critical first step in defining the "footprint" of a target and understanding its administrative boundaries.

NEW QUESTION # 96
.....

- CEHPC Valid Learning Materials □ CEHPC Useful Dumps □ Latest Braindumps CEHPC Book □ Copy URL □ www.examcollectionpass.com □ open and search for ▸ CEHPC ◂ to download for free □CEHPC Valid Learning Materials
- Pass Guaranteed 2026 Updated CertiProf Top CEHPC Dumps □ Go to website [www.pdfvce.com] open and search for ✔ CEHPC □✔□ to download for free □Valid CEHPC Exam Cost
- CEHPC Free Brain Dumps □ CEHPC Useful Dumps □ Certification CEHPC Exam Cost □ Search for ➠ CEHPC □ and download exam materials for free through 《 www.exam4labs.com 》 □Top CEHPC Dumps
- CEHPC Reliable Test Sample □ Valid Dumps CEHPC Pdf □ CEHPC Reliable Test Sample □ Search for ▸ CEHPC ◂ and download exam materials for free through ➽ www.pdfvce.com □ □Top CEHPC Dumps
- Pass Guaranteed 2026 Updated CertiProf Top CEHPC Dumps □ Download ➡ CEHPC □□□ for free by simply entering { www.torrentvce.com } website □Top CEHPC Dumps
- app.parler.com, learn.csisafety.com.au, www.ted.com, www.grepmed.com, justpaste.me, scalar.usc.edu, justpaste.me, telegra.ph, wibki.com, www.wonderlink.de, Disposable vapes

What's more, part of that Dumps4PDF CEHPC dumps now are free: https://drive.google.com/open?id=14zxZr3LaJYcOzPifjO1OhaHXeKrq2Ogf