

Practice CEHPC Engine, CEHPC Test Questions Vce

VCE Practice Questions with Correct Answers (Complete Solutions 2023)

What are the five sensing terms? Correct Answer Doubtful, Lost, Over, Short, Target D-LOST

What is the maximum number of targets that will be presented to an MMG platform? Correct Answer 2

Which one of the following is not a key component of threat based methodology? Correct Answer Ammunition Type

Which prerequisite should the primary evaluator meet prior to evaluating live fire gunnery? Correct Answer Be a Sergeant or above

Which of the following is not a command of execution? Correct Answer Firing

What is the eighth element in a fire command? Correct Answer Execution

MMG targets will be presented for a maximum of how many seconds in the offense? Correct Answer 50 seconds

When does time start for an offensive engagement? Correct Answer When all target(s) in the initial presentation are fully locked or first round is fired

the firer or Vehicle Commander must announce a sensing before what? Correct Answer Any Subsequent fire command
Any supplemental fire command
Terminating the engagement
ALL OF THE ABOVE

Which is not a determining factor for target prioritization when multiple targets of the same threat level are encountered? Correct Answer Engage Far targets before near targets

All targets must be presented to the firer with a minimum of how much target visibility throughout the engagement? Correct Answer 90%

Initial defilade is provided in the defense for all crews when which of the following conditions are met? Correct Answer The crew is properly positioned in their defensive firing position
All targets are in the presentation are locked
The crew has not engaged any targets currently presented
ALL OF THE ABOVE

DOWNLOAD the newest ExamsLabs CEHPC PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=19bp87Bic74dHbiMB8kJvWQ-XGjltvSdy>

The CEHPC certificate you have obtained can really prove your ability to work. Of course, our CEHPC study materials will also teach you how to improve your work efficiency. No matter how good the newcomer is, your status will not be shaken! Our CEHPC Practice Braindumps really are so powerful. If you still have concerns, you can use the free trial versions first. They are the free demos of the CEHPC exam questions for you to free download.

The price of the CEHPC test dumps is quite reasonable, no matter you are the students or the employees of the enterprise, you can afford it. CEHPC test dumps are verified by the specialists of the business, therefore the quality is ensured. Pass guarantee and money back guarantee for purchasing the CEHPC Test Dumps. Other questions or problem of the product can consult the live chat service staff or by email, we will reply you immediately.

>> Practice CEHPC Engine <<

CEHPC Test Questions Vce & Reliable CEHPC Exam Materials

Originating the CEHPC exam questions of our company from tenets of offering the most reliable backup for customers, and outstanding results have captured exam candidates' heart for their functions. Our CEHPC practice materials can be subdivided into three versions. All those versions of usage has been well-accepted by them. There is not much disparity among these versions of CEHPC simulating practice, but they do helpful to beef up your capacity and speed up you review process to master more

knowledge about the exam, so the review process will be unencumbered.

CertiProf Ethical Hacking Professional Certification Exam Sample Questions (Q97-Q102):

NEW QUESTION # 97

What is ZAP?

- A. It is a term used to describe the collection and analysis of information from publicly available sources, such as websites, social networks, government databases, news articles, among other resources freely available on the web.
- **B. It is an open-source penetration testing tool used to evaluate the security of web applications.**
- C. ZAP is a closed source penetration testing tool used to evaluate online servers.

Answer: B

Explanation:

The OWASP Zed Attack Proxy (ZAP) is one of the world's most popular free, open-source security tools for finding vulnerabilities in web applications. It is actively maintained by a global community of volunteers under the Open Web Application Security Project (OWASP). ZAP acts as a "man-in-the-middle proxy," meaning it sits between the tester's web browser and the web application being tested. This allows the tester to intercept, inspect, and even modify the requests and responses traveling between the two. ZAP provides a wide array of functionalities essential for the Web Application Pentesting process:

- * Automated Scanner: It can automatically crawl a website to find vulnerabilities like SQL injection, Cross-Site Scripting (XSS), and insecure headers.
- * Spidering: It maps out the structure of a website by following every link it finds.
- * Fuzzing: It can send many variations of malicious input to a specific field to see if it can break the application or trigger an error.
- * Active and Passive Scanning: It can passively watch traffic to find easy-to-spot issues or actively probe the server for deeper flaws.

For ethical hackers, ZAP is often compared to the commercial tool Burp Suite. While both perform similar tasks, ZAP's open-source nature and robust API make it a favorite for integrating into "DevSecOps" pipelines, where it can automatically test new code for vulnerabilities before it is deployed. Mastering ZAP is a core skill for any professional focused on securing the web-facing assets of an organization.

NEW QUESTION # 98

What is privilege escalation?

- A. A term used by hackers to describe asking compromised administrators for new permissions.
- **B. A term used in computer security to describe a situation where a user or process gains higher permissions than originally assigned.**
- C. A term used when a user formally requests elevated permissions from a system administrator.

Answer: B

Explanation:

Privilege escalation is a critical concept in ethical hacking and penetration testing that refers to a situation where a user or process gains higher-level permissions than originally authorized. This makes option A the correct answer.

Privilege escalation commonly occurs after an attacker or ethical hacker gains initial access to a system with limited privileges. The next objective is often to escalate those privileges to gain administrative or root-level access. This can be achieved through misconfigurations, vulnerable software, weak file permissions, kernel exploits, or improper access control mechanisms.

Option B is incorrect because formally requesting permissions from an administrator is a legitimate administrative process, not privilege escalation. Option C is incorrect because privilege escalation does not involve requesting permissions; it involves exploiting weaknesses to obtain them without authorization.

In penetration testing, privilege escalation is typically tested during the post-exploitation phase. Ethical hackers use it to demonstrate the potential impact of a breach, such as full system compromise, access to sensitive data, or lateral movement within a network. Understanding privilege escalation is essential for improving defensive security. By identifying and mitigating escalation paths, organizations can enforce the principle of least privilege, strengthen access controls, and reduce the impact of successful attacks. Ethical testing of privilege escalation ultimately helps organizations harden systems against real-world threats.

NEW QUESTION # 99

Security Vulnerabilities: Understanding Backdoors

- A. It is a type of hacker who exploits vulnerabilities in search of information that can compromise a company and sell this information in order to make a profit regardless of the damage it may cause to the organization.
- B. A person who creates exploits with the sole purpose of exposing existing vulnerable systems.
- C. Refers to a computer security professional or expert who uses their skills and knowledge to identify and fix vulnerabilities in systems, networks or applications for the purpose of improving security and protecting against potential cyber threats.

Answer: C

Explanation:

The term "Whitehack," more commonly known as a "White Hat Hacker," describes individuals who utilize their technical expertise for ethical and legal purposes. These professionals are the cornerstone of the ethical hacking community. They operate under a strict code of ethics and, most importantly, always obtain explicit, written permission before conducting any security assessments or penetration tests. Their primary objective is to strengthen an organization's security posture by proactively discovering vulnerabilities before malicious actors (Black Hats) can exploit them.

White Hat hackers perform various tasks, including penetration testing, vulnerability assessments, security auditing, and developing security protocols. When they identify a flaw, they do not exploit it for personal gain or damage; instead, they document the finding in a comprehensive report and provide actionable remediation advice to the organization's IT and security teams. This collaborative approach helps organizations understand their weaknesses and allocate resources effectively to mitigate risks. Many White Hat hackers are certified professionals, holding credentials such as Certified Ethical Hacker (CEH) or Offensive Security Certified Professional (OSCP). They often work as security consultants, in-house security analysts, or as part of specialized "Red Teams" that simulate real-world attacks to test defensive capabilities. By mimicking the tactics, techniques, and procedures (TTPs) of real adversaries within a controlled and authorized framework, White Hats provide invaluable insights that automated tools alone cannot achieve. Their work is essential in the modern digital landscape, where the constant evolution of threats requires a defensive strategy that is equally dynamic and informed by a deep understanding of the "hacker mindset." Ultimately, the distinction between a White Hat and other types of hackers is defined by intent, authorization, and the commitment to improving the safety of the digital ecosystem.

NEW QUESTION # 100

What tool would you use to scan ports?

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

Answer: C

Explanation:

Nmap is the primary tool used for port 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 # 101

What is a security breach?

- A. It is the hacking of the entire Internet.
- B. It's an Internet breakup.
- C. It consists of a cyber security incident that affects personal or corporate data in different ways.

Answer: C

Explanation:

A security breach is defined as a cybersecurity incident that involves the unauthorized access, disclosure, or manipulation of personal or corporate data. It represents a significant failure of an organization's security controls, leading to a compromise of confidentiality, integrity, or availability. In the context of managing information security threats, a breach is often the culmination of a successful attack chain, where a threat actor has successfully identified a vulnerability, exploited it, and bypassed the existing defense layers to reach sensitive information assets.

Breaches can manifest in various ways, ranging from the theft of customer records and financial data to the exposure of trade secrets or internal communications. They are not merely "Internet breakups" or total shutdowns of the web; rather, they are targeted incidents that affect specific entities. The impact of a security breach is multifaceted, often resulting in severe financial losses, legal liabilities under data protection regulations (such as GDPR), and long-term reputational damage.

From an ethical hacking perspective, understanding the anatomy of a breach is essential for building better detection and response mechanisms. Professionals categorize breaches based on their "attack vector," such as phishing, unpatched software, or insider threats. By simulating these breaches during a penetration test, ethical hackers can help organizations identify "indicators of compromise" (IoCs) and improve their incident response plans. Managing this threat requires a proactive stance that includes regular vulnerability assessments, robust encryption of sensitive data, and continuous monitoring of network traffic to detect unauthorized data exfiltration before it escalates into a full-scale corporate catastrophe.

NEW QUESTION # 102

.....

Before the clients purchase our CEHPC study practice guide, they can have a free trial freely. The clients can log in our company's website and visit the pages of our products. The pages of our products lists many important information about our CEHPC exam materials and they include the price, version and updated time of our products, the exam name and code, the total amount of the questions and answers, the merits of our CEHPC useful test guide and the discounts. You can have a comprehensive understanding of our CEHPC useful test guide after you see this information.

CEHPC Test Questions Vce: <https://www.examslabs.com/CertiProf/Ethical-Hacking-Professional/best-CEHPC-exam-dumps.html>

CEHPC training materials are high-quality, and you can pass the exam by using them, Through the free demo you can feel which company is strong and which CEHPC exams cram PDF is valid and accurate, With the help of our online version, you can not only practice our CEHPC exam pdf in any electronic equipment, but also make you feel the atmosphere of CEHPC actual test, And our CEHPC exam braindumps will never let you down.

That might help you deduce the answer from the information given in the question, The CertiProf CEHPC exam torrent materials we provided are the best-selling of our company.

CEHPC Training Materials are high-quality, and you can pass the exam by using them, Through the free demo you can feel which company is strong and which CEHPC exams cram PDF is valid and accurate.

CertiProf Practice CEHPC Engine: Ethical Hacking Professional Certification Exam - ExamsLabs Money Back Guaranteed

With the help of our online version, you can not only practice our CEHPC exam pdf in any electronic equipment, but also make you feel the atmosphere of CEHPC actual test.

And our CEHPC exam braindumps will never let you down, We deliver the real information to you through CEHPC test dumps with a wide variety of settings and options.

- 2026 CertiProf CEHPC: Ethical Hacking Professional Certification Exam Fantastic Practice Engine Easily obtain free download of **► CEHPC** by searching on **> www.practicevce.com <** CEHPC Reliable Dumps Free
- Ethical Hacking Professional Certification Exam study guide: exam CEHPC real vce collection Go to website **>** www.pdfvce.com open and search for CEHPC to download for free CEHPC Latest Questions
- CEHPC Exam Braindumps - CEHPC Origination Questions - CEHPC Study Guide Enter **>** www.verifiddumps.com and search for CEHPC to download for free Reliable CEHPC Exam Pdf
- 2026 CEHPC: Ethical Hacking Professional Certification Exam—High Pass-Rate Practice Engine Download CEHPC for free by simply searching on www.pdfvce.com Free CEHPC Dumps
- Free PDF 2026 Updated CertiProf CEHPC: Practice Ethical Hacking Professional Certification Exam Engine Go to website **“ www.exam4labs.com ”** open and search for **>** CEHPC to download for free New CEHPC Test Simulator
- Reliable CEHPC Exam Pdf CEHPC Reliable Dumps Free CEHPC Test Engine Version Open

