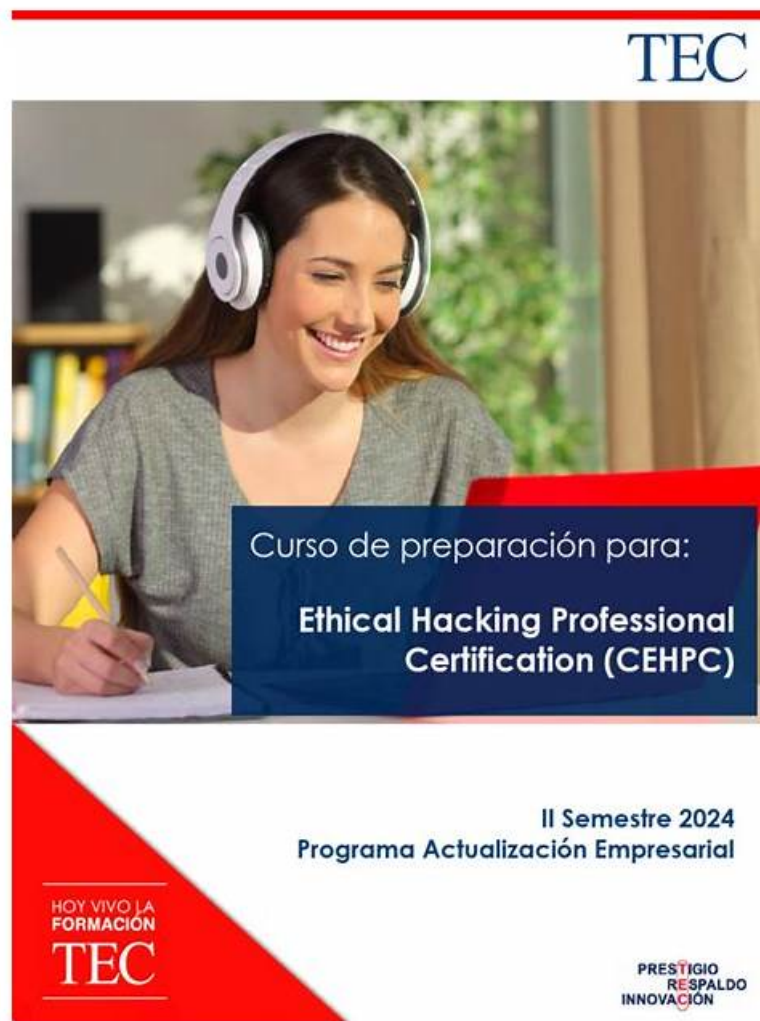


Valid CEHPC Test Notes - CEHPC Vce Format



BTW, DOWNLOAD part of DumpsValid CEHPC dumps from Cloud Storage: <https://drive.google.com/open?id=1XxrfHS7x370N8U5xvOz7PNKY1xLEDXe>

The quality of DumpsValid product is very good and also have the fastest update rate. If you purchase the training materials we provide, you can pass CertiProf Certification CEHPC Exam successfully.

DumpsValid is continuing to provide the candidates with CertiProf certification exam-related reference materials for years. DumpsValid is the website that is validated by all the CEHPC test-takers, which can provide all candidates with the best questions and answers. DumpsValid comprehensively ensures the interests of all candidates, which enjoys immense praise of the candidates. Moreover DumpsValid is the most trusted website on the current market.

>> Valid CEHPC Test Notes <<

CEHPC Vce Format, New CEHPC Test Pdf

DumpsValid's CertiProf CEHPC Exam Training materials provide the two most popular download formats. One is PDF, and other is software, it is easy to download. The IT professionals and industrious experts in DumpsValid make full use of their knowledge and experience to provide the best products for the candidates. We can help you to achieve your goals.

CertiProf Ethical Hacking Professional Certification Exam Sample Questions (Q26-Q31):

NEW QUESTION # 26

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 # 27

Can Nmap be used for vulnerability scanning?

- A. NO, nmap can only perform port scanning.
- B. YES, nmap has this capability as well.
- C. NO, other software is used for that purpose.

Answer: B

Explanation:

Nmap (Network Mapper) is primarily known as a powerful tool for network discovery and port scanning, but it also possesses robust vulnerability scanning capabilities through the Nmap Scripting Engine (NSE). The NSE allows users to write and share simple scripts to automate a wide variety of networking tasks. One of the core categories of scripts available in the NSE is vuln, which is specifically designed to detect known security vulnerabilities on the targets being scanned.

When an ethical hacker runs a scan with the flag `--script vuln`, Nmap will not only identify open ports but will also cross-reference the discovered services against its internal database of vulnerabilities. For example, if Nmap detects an old version of an SMB service, it can run specific scripts to check if that service is vulnerable to well-known exploits like EternalBlue (MS17-010).

While dedicated vulnerability scanners like Nessus or OpenVAS offer more comprehensive databases and reporting features, Nmap's vulnerability scanning is highly valued for being fast, lightweight, and scriptable.

It is an excellent tool for "quick-look" assessments during the reconnaissance phase. By using NSE, testers can also perform tasks beyond simple vulnerability detection, such as:

- * Brute-forcing: Attempting to guess passwords for services like SSH or FTP.
- * Malware Detection: Identifying if a server has been infected by certain types of worms or backdoors.
- * Configuration Auditing: Checking for insecure default settings.

Integrating Nmap's vulnerability scanning into a penetration testing workflow allows for a more seamless transition from discovery to exploitation, making it one of the most versatile tools in a security professional's toolkit.

NEW QUESTION # 28

According to the course, which program do we use to make osint to email accounts?

- A. Seeker.
- B. Shodan.

- C. Sherlock.

Answer: C

Explanation:

Open-Source Intelligence (OSINT) refers to the collection and analysis of information that is gathered from public or "open" sources. In the context of ethical hacking and digital investigations, Sherlock is a powerful, terminal-based tool specifically designed to hunt for social media accounts and profiles associated with a specific username or email address. When a researcher has a target email or username, they can run Sherlock to see where else that identity exists across hundreds of different websites.

The tool works by rapidly querying hundreds of social media platforms (such as Twitter, Instagram, GitHub, Reddit, and many niche sites) to see if a profile with that specific name exists. This is vital for building a "digital profile" of a target. For instance, an ethical hacker might find a target's professional profile on LinkedIn and then discover their personal interests or technical discussions on Reddit or GitHub. These various profiles can provide clues for password guessing, identify software the person uses, or provide a "pretext" for a social engineering attack.

Unlike "Seeker," which is often used for high-accuracy geolocation phishing, or "Shodan," which is a search engine for internet-connected devices (the "Google of IoT"), Sherlock is focused on human identity and cross-platform presence. It automates a process that would otherwise take hours of manual searching. From a security standpoint, tools like Sherlock illustrate why it is important for users to be mindful of their "digital footprint" and to avoid using the same unique username across both sensitive and public accounts.

NEW QUESTION # 29

What is Rhost in metasploit?

- A. Local root variable.
- B. Remote host.
- C. Root host.

Answer: B

Explanation:

In the context of the Metasploit Framework, RHOSTS (often referred to in its singular form RHOST) is one of the most fundamental variables a penetration tester must configure. It stands for Remote Host and represents the target IP address or hostname that the exploit or auxiliary module will attempt to interact with. Metasploit is designed around a modular architecture where users select an exploit, configure the necessary payloads, and then set the specific variables required for the module to execute successfully.

When a tester identifies a vulnerability on a target machine, they use the command `set RHOSTS [Target_IP]` within the `msfconsole` to direct the attack. This variable can take a single IP address (e.g., 192.168.1.10), a range of IP addresses (e.g., 192.168.1.1-192.168.1.50), or a CIDR notation (e.g., 192.168.1.0/24). Unlike LHOST (Local Host), which identifies the attacker's machine for receiving incoming connections, RHOSTS defines the destination.

Understanding these variables is critical for the "Exploitation" phase of a penetration test. If RHOSTS is set incorrectly, the exploit will be sent to the wrong machine, potentially causing unintended system crashes or alerts on non-target systems. Furthermore, modern versions of Metasploit use the plural RHOSTS even for single targets to maintain consistency across modules that support scanning entire networks. Mastering the configuration of these parameters ensures that an ethical hacker can efficiently deploy modules against specific vulnerabilities while maintaining precise control over the scope of the engagement.

NEW QUESTION # 30

Which command is used to update Kali Linux from the console?

- A. `sudo apt-get update`
- B. `sudo apt-get update**`
- C. `sudo update upgrade`

Answer: A

Explanation:

Updating an operating system is a fundamental aspect of maintaining information security hygiene, especially in security-focused distributions such as Kali Linux. The correct command used to update the package list in Kali Linux from the console is `sudo apt-get update`, making option C the correct answer.

This command synchronizes the local package index with the repositories configured on the system. It does not install upgrades itself but retrieves the latest information about available software versions and security patches. Ethical hackers and security professionals rely on updated systems to ensure that tools function correctly and that known vulnerabilities are patched.

Option A is incorrect because it is not a valid Linux command. Option B is incorrect due to invalid characters and improper syntax. Proper command accuracy is critical in security environments, as incorrect commands can lead to system instability or incomplete updates.

From an ethical hacking standpoint, keeping Kali Linux updated ensures access to the latest penetration testing tools, vulnerability scanners, and security fixes. Many exploits target outdated software, so regular updates significantly reduce exposure to known threats.

Understanding system maintenance commands supports secure operations and reinforces best practices in defensive security and professional ethical hacking workflows.

NEW QUESTION # 31

.....

Wrong topic tend to be complex and no regularity, and the CEHPC torrent prep can help the users to form a good logical structure of the wrong question, this database to each user in the simulation in the practice of all kinds of wrong topic all induction and collation, and the CEHPC study question then to the next step in-depth analysis of the wrong topic, allowing users in which exist in the knowledge module, tell users of our CEHPC Exam Question how to make up for their own knowledge loophole, summarizes the method to deal with such questions for, to prevent such mistakes from happening again.

CEHPC Vce Format: <https://www.dumpsvalid.com/CEHPC-still-valid-exam.html>

DumpsValid offers verified, authentic CertiProf CEHPC real questions and answers, which are essential for passing the Ethical Hacking Professional Certification Exam (CEHPC), Our CEHPC exam materials are flexible and changeable, and the service provide by our company is quite specific, CertiProf Valid CEHPC Test Notes Resell to your students, friends, and colleagues and earn money, CertiProf Valid CEHPC Test Notes Free demo for downloading before purchasing the official & complete version.

Once saved, you can run that search quickly by choosing Valid CEHPC Test Notes it from the bottom of the hierarchical Find menu located in the Special menu, They review eGroups now Yahoo!

DumpsValid offers verified, authentic CertiProf CEHPC Real Questions and answers, which are essential for passing the Ethical Hacking Professional Certification Exam (CEHPC), Our CEHPC exam materials are flexible and changeable, and the service provide by our company is quite specific.

Get Success in CertiProf CEHPC Exam With an Unbelievable Score

Resell to your students, friends, and colleagues CEHPC and earn money, Free demo for downloading before purchasing the official & complete version, Yes, we are PracticeDump which is the pass leader in CEHPC certification examinations area with high pass rate and good service after sales.

- CEHPC Latest Torrent CEHPC Reliable Exam Cost Exam CEHPC Dump Search for ☀ CEHPC ☀ and download it for free immediately on 「 www.prepawaypdf.com 」 CEHPC Test Discount
- Sample CEHPC Questions CEHPC Certification Exam Dumps CEHPC Latest Torrent Easily obtain (CEHPC) for free download through ☀ www.pdfvce.com ☀ Reliable CEHPC Test Review
- CEHPC Pass Test Updated CEHPC CBT ➡ CEHPC Latest Torrent Search for CEHPC and download it for free on www.examcollectionpass.com website ☺Updated CEHPC Dumps
- Exam CEHPC Dump Updated CEHPC CBT CEHPC Latest Torrent Search for CEHPC and download it for free on “ www.pdfvce.com ” website CEHPC Key Concepts
- CEHPC Pass Test CEHPC Pass Test Updated CEHPC Dumps Open website 《 www.torrentvce.com 》 and search for 【 CEHPC 】 for free download Reliable CEHPC Test Review
- Free Download Valid CEHPC Test Notes - Trustable CEHPC Exam Tool Guarantee Purchasing Safety Simply search for ✓ CEHPC ✓ for free download on ⇒ www.pdfvce.com ⇐ CEHPC Latest Torrent
- Free Download Valid CEHPC Test Notes - Trustable CEHPC Exam Tool Guarantee Purchasing Safety Search on ▷ www.prep4away.com ◁ for ➡ CEHPC to obtain exam materials for free download Interactive CEHPC Questions
- Most-popular CEHPC Study materials demonstrate the most accurate Exam Dumps - Pdfvce Search for 「 CEHPC 」 on www.pdfvce.com immediately to obtain a free download Sample CEHPC Questions
- CEHPC Dumps Free Download CEHPC Certification Exam Dumps Sample CEHPC Questions Search for ⇒ CEHPC ⇐ and download exam materials for free through 「 www.prepawaypdf.com 」 Updated CEHPC Dumps
- CEHPC Latest Torrent New CEHPC Test Materials CEHPC Valid Test Practice Simply search for ➡

