CertiProf CEHPC試験感想 & CEHPC的中合格問題集

進歩を続けることは、すべての人にとって非常に良いことです。継続的に自分自身を改善するために最善を尽くすと、お金、幸福、良い仕事などを含め、たくさん収穫することになります。当社のCEHPC準備試験は、進歩を続けるのに役立ちます。私たちのCEHPC学習教材を選択すると、あなたの欠点を克服し、永続的な人になることは非常に簡単であることがわかります。 CEHPC試験問題を購入することに決めた場合、CEHPC試験に合格し、短時間で正常に認定を取得できる可能性があります。

CertiProf CEHPC 認定試験の出題範囲:

トピック	出題範囲
トピック 1	• Understand current security trends: This topic covers the latest cybersecurity trends, emerging threats, and evolving attack techniques affecting modern organizations and systems.
トピック 2	• Understand the pentesting process: This topic focuses on the complete penetration testing workflow, including planning, execution, reporting, and remediation activities.
トピック 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.
トピック 4	• 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.

>> CertiProf CEHPC試験感想 <<

CEHPC的中合格問題集 & CEHPC英語版

私たちのウェブサイトから見ると、CEHPC学習教材は3つのバージョンがあります。PDF、ソフトウェアとオンライン版です。CEHPC PDF版は印刷できます。ソフトウェアとオンライン版はコンピュータで使用できます。

コンピュータで学ぶことが難しい場合は、CEHPC学習教材の印刷資料で勉強できます。また、CEHPC学習教材の価格は合理的に設定されています。

CertiProf Ethical Hacking Professional Certification Exam 認定 CEHPC 試験問題 (Q71-Q76):

質問 # 71
As pentester can we exploit any vulnerability regardless of the affectations?

- A. NO, since performing these acts without consent is a crime.
- B. YES, we have all the power to perform these processes without consent.
- C. YES, we have all the freedom.

正解：A

解説：
The defining characteristic that separates a professional penetration tester from a criminal hacker islegal authorization and consent. In the pentesting process, it is strictly prohibited to exploit any vulnerability without the explicit, written consent of the system owner. Performing such acts without authorization-even if the intent is to "help"-is a criminal offense in most jurisdictions and can lead to severe legal consequences, including fines and imprisonment.
Before any testing begins, a "Rules of Engagement" (RoE) and a "Statement of Work" (SoW) must be signed.
These documents define the scope of the test: which systems can be touched, which exploits are allowed, and what hours the testing can take place. A pentester must also consider "affectations," meaning the potential impact on business operations. If exploiting a vulnerability has a high risk of crashing a production server or corrupting critical data, the tester must consult with the client before proceeding.
Ethical hacking is built on a foundation of trust and professional integrity. A pentester's goal is to improve security, not to disrupt business or act recklessly. If a critical vulnerability is found, the ethical response is to document it and inform the client immediately so it can be fixed. This disciplined approach ensures that the pentesting process remains a valuable security tool rather than a liability, reinforcing the fact that professional power in this field must always be balanced by strict adherence to legal and ethical standards.

質問 # 72
Do hackers only use Linux?

- A. Linux and Windows only.
- B. Yes, since Linux is the only platform that works correctly for these tasks.
- C. No, hackers use all operating systems.

正解：C

解説：
While Linux distributions like Kali Linux and Parrot OS are highly favored by the security community due to their open-source nature and pre-installed toolkits, it is a misconception that hackers exclusively use Linux.
Malicious actors and ethical hackers alike utilizeall operating systems, including Windows, macOS, and mobile platforms (Android/iOS), depending on their specific objectives.
The choice of operating system is often driven by the "Target Environment." For example:
* Windows: Many hackers use Windows because it is the most prevalent OS in corporate environments.
To develop effective exploits for Windows-based active directories or software, it is often necessary to work within a Windows environment using tools like PowerShell and the .NET framework.
* macOS: This platform is popular among researchers and developers due to its Unix-based core combined with a high-end commercial interface, allowing for a seamless transition between development and security tasks.
* Linux: Linux remains the "OS of choice" for heavy networking tasks, server-side exploits, and automated scripts because of its transparency and the power of its terminal.
Furthermore, hackers often use specialized hardware or mobile devices to conduct "War Driving" (scanning for Wi-Fi) or "Skimming" attacks. In a modern penetration test, a professional might use a Linux machine for reconnaissance, a Windows machine for testing Active Directory vulnerabilities, and a mobile device for testing application security. An effective hacker must be cross-platform proficient, understanding the unique vulnerabilities and command-line interfaces of every major operating system to successfully navigate a target's network.

質問 # 73
Can the FTP protocol be breached?

- A. Yes, using appropriate attack techniques.
- B. Yes, by asking the administrator for credentials.
- C. No, FTP is very secure.

正解：A

解説：
Yes, the FTP protocol can be breached, making option B the correct answer. FTP transmits usernames, passwords, and datain clear text, which makes it highly vulnerable to interception and attack.
Attackers can exploit FTP through techniques such as credential sniffing, brute-force attacks, anonymous access abuse, and man-in-the-middle attacks. Ethical hackers frequently demonstrate FTP weaknesses during penetration testing to highlight the risks of using outdated protocols.
Option A is incorrect because asking for credentials is not an attack technique. Option C is incorrect because FTP is considered insecure by modern security standards.
From a defensive standpoint, FTP should be replaced with secure alternatives such asSFTP or FTPS, which encrypt authentication and data transfers. Ethical hackers use FTP breach demonstrations to encourage protocol modernization and better access controls. Understanding insecure protocols is essential for managing information security threats. Eliminating weak services like FTP significantly reduces an organization's attack surface and exposure to credential compromise.

質問 # 74
Can Kali Linux only be used by criminals?

- A. NO, it can be used by cybersecurity enthusiasts.
- B. YES, criminal acts are carried out with it.
- C. YES, it is a prohibited system.

正解：A

解説：
Kali Linux is a specialized, Debian-derived Linux distribution designed specifically for digital forensics and penetration testing. While it is true that the tools included in Kali Linux can be used for criminal activities (Option A), the operating system itself is a legitimate professional tool used worldwide by cybersecurity enthusiasts, ethical hackers, and security researchers. Its primary purpose is to provide a comprehensive environment pre-loaded with hundreds of security tools for tasks like vulnerability analysis, wireless attacks, and web application testing.
The distinction between a criminal act and ethical hacking lies in "authorization" and "intent" rather than the tools used. Ethical hackers use Kali Linux to perform authorized security audits to help organizations identify and fix vulnerabilities before they are exploited by real-world attackers. For example, tools like Nmap or Metasploit are essential for a penetration tester to map a network and verify the effectiveness of existing security controls.
Furthermore, Kali Linux is an essential educational resource. It allows students to learn about the "phases of hacking"-reconnaissance, scanning, and gaining access-in a controlled, legal environment. Many cybersecurity certifications, such as the OSCP (Offensive Security Certified Professional), are built around the proficiency of using this system. Claiming it is a "prohibited system" (Option B) is factually incorrect; it is an open-source project maintained by Offensive Security and is legal to download and use for legitimate security research and defense. By mastering Kali Linux, security professionals can better understand the techniques used by adversaries, allowing them to build more resilient and secure digital infrastructures.

質問 # 75
What is Netcat?

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

正解：C

解説：
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.

質問 # 76
.....

10年以上のビジネス経験により、当社のCEHPCテストトレントは、顧客の購入体験を非常に重要視していました。電子製品の購入速度を心配する必要はありません。弊社では、CEHPC試験準備の信頼性を長期間にわたって評価および評価し、保証された購入スキームを提案するために尽力しています。必要な場合は、CEHPCテストトレントを使用するためのリモートオンラインガイダンスも利用できます。通常、購入後数分でCEHPC練習問題を効率よく取得できます。