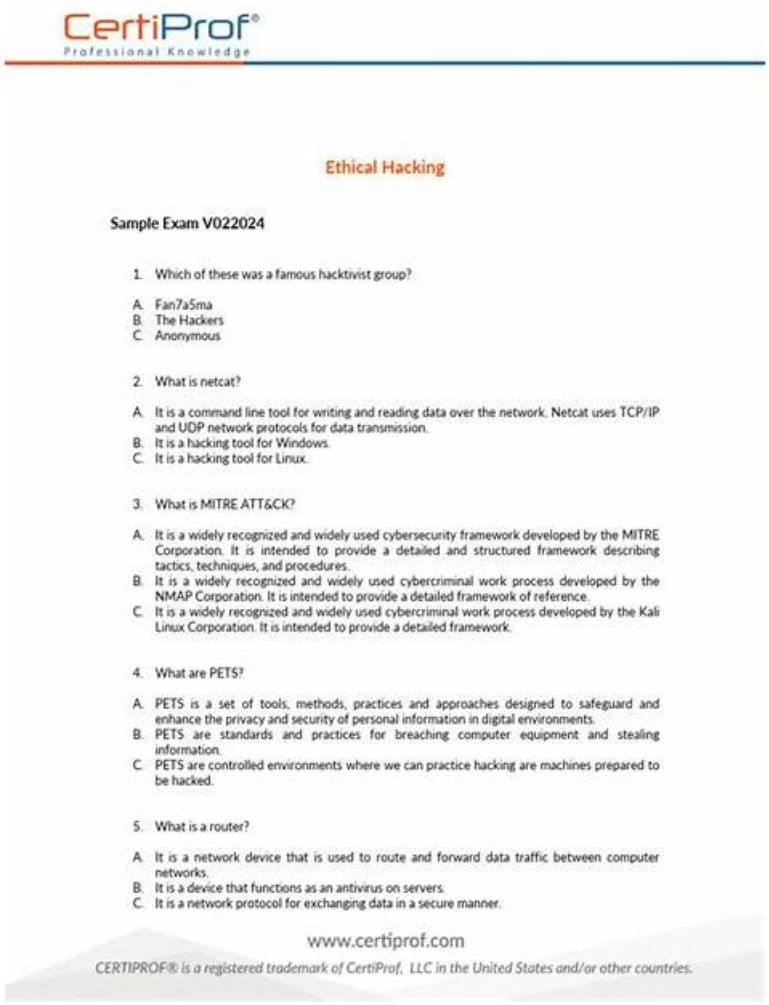
CEHPC Real Exam Questions - Detailed CEHPC Answers



CertiProf®
Professional Knowledge

Ethical Hacking

Sample Exam V022024

1. Which of these was a famous hacktivist group?

A. Fan7a5ma
B. The Hackers
C. Anonymous

2. What is netcat?

A. It is a command line tool for writing and reading data over the network. Netcat uses TCP/IP and UDP network protocols for data transmission.
B. It is a hacking tool for Windows.
C. It is a hacking tool for Linux.

3. What is MITRE ATT&CK?

A. It is a widely recognized and widely used cybersecurity framework developed by the MITRE Corporation. It is intended to provide a detailed and structured framework describing tactics, techniques, and procedures.
B. It is a widely recognized and widely used cybercriminal work process developed by the NMAP Corporation. It is intended to provide a detailed framework of reference.
C. It is a widely recognized and widely used cybercriminal work process developed by the Kali Linux Corporation. It is intended to provide a detailed framework.

4. What are PETS?

A. PETS is a set of tools, methods, practices and approaches designed to safeguard and enhance the privacy and security of personal information in digital environments.
B. PETS are standards and practices for breaching computer equipment and stealing information.
C. PETS are controlled environments where we can practice hacking are machines prepared to be hacked.

5. What is a router?

A. It is a network device that is used to route and forward data traffic between computer networks.
B. It is a device that functions as an antivirus on servers.
C. It is a network protocol for exchanging data in a secure manner.

www.certiprof.com

CERTIPROF® is a registered trademark of CertiProf, LLC in the United States and/or other countries.

P.S. Free 2026 CertiProf CEHPC dumps are available on Google Drive shared by DumpStillValid: https://drive.google.com/open?id=1RM5P9RqpXoAffsKnBpjpotDwfkD1tYcR

Have similar features to the desktop-based exam simulator Contains actual CertiProf CEHPC practice test that will help you grasp every topic Compatible with every operating system. Does not require any special plugins to operate. Creates a CEHPC Exam atmosphere making candidates more confident. Keeps track of your progress with self-analysis and Points out mistakes at the end of every attempt.

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	• Master information security controls: This section explains administrative, technical, and physical security controls used to protect systems, networks, and organizational data.
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	• 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 5	• 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 6	• Understand the pentesting process: This topic focuses on the complete penetration testing workflow, including planning, execution, reporting, and remediation activities.
Topic 7	• Master the concepts, types, and phases of pentesting: This domain covers penetration testing fundamentals, testing methodologies, and the stages involved in conducting security assessments.

Pass Guaranteed 2026 Accurate CertiProf CEHPC: Ethical Hacking Professional Certification Exam Real Exam Questions

The CertiProf job market has become so competitive and challenging. To stay competitive in the market as an experienced IT professional you have to upgrade your skills and knowledge with the Ethical Hacking Professional Certification Exam (CEHPC) certification exam. With the CEHPC exam dumps you can easily prove your skills and upgrade your knowledge. To do this you just need to enroll in the Ethical Hacking Professional Certification Exam (CEHPC) certification exam and put all your efforts to pass this challenging CertiProf CEHPC exam with good scores.

CertiProf Ethical Hacking Professional Certification Exam Sample Questions (Q21-Q26):

NEW QUESTION # 21
What is active recognition?

- A. Recognizes the target but does nothing.
- B. We only see the target without performing actions.
- C. Gathers information by interacting with the target.

Answer: C

Explanation:
Active recognition, also known as "Active Reconnaissance," is a critical phase of penetration testing where the tester gathers detailed information by directly interacting with the target system or network. Unlike
"Passive Reconnaissance," which involves collecting publicly available information from search engines (like Google Dorking) or social media without the target's knowledge, active recognition involves sending data packets to the target's infrastructure to elicit a response.
Common activities during the active recognition phase include port scanning, service version detection, and vulnerability scanning. For example, using a tool like Nmap to scan a server's open ports is a form of active recognition. The scanner sends "probes" to the server, and based on the server's reply (or lack thereof), the tester can determine which services are running (e.g., a web server on port 80 or a database on port 3306).
This phase is essential because it provides the technical "blueprint" of the target that the tester will use to plan an exploit.
However, active recognition carries a significant risk: it is much more likely to be detected by security systems like Intrusion Detection Systems (IDS) or firewalls. Because the tester is directly "knocking on the doors" of the target, their IP address and activity may be logged. In a professional pentest, the degree of
"stealth" used during active recognition is a key consideration. Testers may slow down their scans or use techniques to blend in with normal network traffic to avoid detection. For the organization, being able to detect active reconnaissance is a vital part of threat management, as it often serves as the "early warning sign" that a more sophisticated attack is being prepared. Mastering this phase allows a pentester to efficiently map the attack surface while understanding the operational limits of the target's defensive controls.

NEW QUESTION # 22
Which of the following is a Linux distribution dedicated to security auditing and penetration testing?

- A. Windows XP.
- B. Parrot OS.
- C. Hannah Montana Linux.

Answer: B

Explanation:
While Kali Linux is arguably the most recognized operating system in the cybersecurity industry, Parrot OS (Parrot Security OS) is a prominent and highly capable alternative preferred by many security professionals and ethical hackers. Developed by the Frozenbox Network, Parrot OS is based on Debian, much like Kali, but it emphasizes a different philosophy regarding system resources and privacy. Parrot OS is designed to be lightweight and highly portable, often performing better on older hardware or in virtualized environments with limited resources. It comes pre-installed with a vast repository of security tools categorized for information gathering, vulnerability analysis, exploitation, and post-exploitation.
One of the defining features of Parrot OS is its focus on developer-friendly environments and anonymity. It includes "AnonSurf," a pre-configured script that routes all system traffic through the Tor network, providing a layer of privacy for researchers conducting sensitive investigations. Additionally, Parrot OS is often praised for its "Home" edition, which serves as a secure daily-driver operating system for general use, and its
"Security" edition, which is fully loaded for penetration testing. In contrast to Kali's "root by default" history (which has since changed), Parrot OS was built from the ground up with a standard user model to improve security. For an ethical hacker, choosing between Kali and Parrot often comes down to personal preference for the desktop environment (Kali uses XFCE/GNOME/KDE, while Parrot traditionally favors MATE) and specific workflow requirements. Both systems provide the necessary toolsets-such as Nmap, Wireshark, Burp Suite, and Metasploit-to conduct comprehensive security audits across various network architectures. Understanding the landscape of security-focused distributions is vital for a professional to select the best tool for a specific operational context.

NEW QUESTION # 23
Can ransomware attacks happen to anyone or only to large companies?

- A. Only large companies with very important data.
- B. Only computers with Windows 7 and XP.
- C. We can all be infected by ransomware.

Answer: C

Explanation:
Ransomware is a pervasive and devastating form of malware that encrypts a victim's files, rendering them inaccessible until a ransom, typically in cryptocurrency, is paid to the attacker. A critical misconception in modern cybersecurity is that ransomware only targets high-value, large-scale organizations. In reality, anyonewith an internet-connected device is a potential target. While high-profile attacks on hospitals or infrastructure make the headlines, individuals, small businesses, and non-profits are frequently infected daily. Attackers utilize varied methods to spread ransomware, many of which are non-discriminatory. These include:
* Phishing: Sending mass emails with malicious attachments or links that, once clicked, execute the ransomware payload.
* Exploiting Vulnerabilities: Automated bots scan the internet for unpatched software or exposed services (like RDP) to gain entry regardless of the target's identity.
* Malvertising: Injecting malicious code into legitimate online advertising networks.
The shift toward "Ransomware-as-a-Service" (RaaS) has lowered the barrier to entry for criminals, allowing even low-skilled attackers to launch wide-reaching campaigns. For an individual, the loss of personal photos or tax documents can be just as traumatic as a data breach is for a company. Because ransomware can strike any operating system or device type, ethical hacking principles emphasize that every user must maintain a proactive defense. This includes regular data backups, keeping software updated to close security holes, and exercising extreme caution with email communication.

NEW QUESTION # 24
What is the most vulnerable within an organization?

- A. Servers.
- B. Wi-Fi network.
- C. Individuals.

Answer: C

Explanation:
In the field of cybersecurity, it is a well-established axiom thatindividuals(the human element) represent the most vulnerable link in an organization's security chain. While a company can invest millions of dollars in sophisticated firewalls, encryption, and endpoint protection, these technical controls can be completely bypassed if a human is manipulated into granting access.
The vulnerability of individuals stems from several psychological factors:
* Trust and Cooperation: Humans are naturally inclined to be helpful, which attackers exploit through social engineering.
* Lack of Awareness: Employees who are not trained in security hygiene may use weak passwords, reuse credentials across multiple sites, or fail to recognize phishing attempts.
* Fatigue and Urgency: Attackers often create a false sense of crisis (e.g., "Your account will be deleted in 1 hour") to trick users into bypassing their better judgment.
* Physical Security Risks: Common vulnerabilities include "tailgating" (following someone through a secure door) or leaving sensitive documents on a desk.
Ethical hacking documents emphasize that a "Defense in Depth" strategy must include the "Human Firewall." This involves continuous security awareness training, phishing simulations, and clearAcceptable Use Policies (AUP). Organizations that ignore the human element often find themselves victims of ransomware or data breaches despite having state-of-the-art technical defenses.
Strengthening the human link through education is the most effective way to reduce the overall attack surface of an organization.

NEW QUESTION # 25
Which of the following is a network security protocol designed to authenticate and authorize remote users to securely access network resources?

- A. SSL (Secure Sockets Layer).
- B. FTP (File Transfer Protocol).
- C. SSH (Secure Shell).

Answer: C

Explanation:
Secure Shell (SSH) is a robust cryptographic network protocol utilized for operating network services securely over an unsecured network. Its primary application is the secure remote login to computer systems by administrators and users. Unlike earlier protocols such as Telnet or rlogin, which transmitted data (including passwords) in plain text, SSH provides a secure, encrypted channel. It achieves this through a suite of cryptographic techniques that ensure theconfidentiality,integrity, andauthenticityof the data being transmitted between the client and the server.
The protocol operates using a client-server architecture, where an SSH client initiates a connection to an SSH server. SSH facilitates both authentication and authorization. Authentication is typically performed using either a password or, more securely, a public-private key pair. Once the user's identity is verified, the protocol authorizes the level of access based on the server's configuration.
Beyond simple terminal access, SSH supports secure file transfers (SFTP) and port forwarding, allowing other network protocols to be "tunneled" through its encrypted connection. From a security standpoint, while SSH is highly secure, it can be breached if misconfigured-such as by allowing weak passwords or failing to disable root login. Consequently, ethical hackers prioritize hardening SSH services as a fundamental control in protecting organizational assets.

NEW QUESTION # 26
.....

www.pass4test.com □ open and search for ⇛ CEHPC ⇚ to download for free □CEHPC Braindumps Pdf

- CEHPC pdf braindumps, CertiProf CEHPC real braindumps, CEHPC valid dumps □ Search for （ CEHPC ） and download it for free immediately on [www.pdfvce.com] □CEHPC Trustworthy Pdf
- CEHPC Trustworthy Pdf □ New CEHPC Mock Test □ CEHPC Exam Bible □ Open { www.troytecdumps.com } and search for ➤ CEHPC □ to download exam materials for free □CEHPC Braindumps Pdf
- CEHPC Reliable Exam Pdf ☎ CEHPC Exam Bible □ CEHPC Certification Training □ Search for ▹ CEHPC ◃ and download exam materials for free through ☀ www.pdfvce.com □☀□ □Practice CEHPC Tests
- Latest CEHPC Exam Topics □ CEHPC Study Tool □ New CEHPC Mock Test □ Search on ▹ www.prepawaypdf.com ◃ for [CEHPC] to obtain exam materials for free download □Pdf Demo CEHPC Download
- CEHPC Reliable Exam Pdf □ CEHPC Braindumps Pdf □ Latest CEHPC Test Notes □ Search for 【 CEHPC 】 and download it for free on { www.pdfvce.com } website □CEHPC Study Tool
- 2026 100% Free CEHPC – 100% Free Real Exam Questions | Detailed CEHPC Answers □ Open ☀ www.exam4labs.com □☀□ and search for ▹ CEHPC ◃ to download exam materials for free □CEHPC Exam Tutorials
- Best of luck in CertiProf CEHPC exam and career □ Go to website 【 www.pdfvce.com 】 open and search for ➽ CEHPC □ to download for free □CEHPC Exam Tutorials
- CEHPC Braindumps Pdf □ Reliable CEHPC Test Topics □ Latest CEHPC Test Notes ☂ Search for 「 CEHPC 」 and download exam materials for free through ➽ www.examcollectionpass.com □ □Latest CEHPC Test Notes
- www.stes.tyc.edu.tw, www.notebook.ai, www.stes.tyc.edu.tw, successflyinginstitute.com, www.stes.tyc.edu.tw, infusionmedz.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.slideshare.net, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New CEHPC dumps are available on Google Drive shared by DumpStillValid: https://drive.google.com/open?id=1RM5P9RqpXoAffsKnBpjpotDwfkD1tYcR