

# Exam CEHPC Format | Pass CEHPC Test Guide



## 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](http://www.certiprof.com)

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

Computer brings more convenience, online access to information, published an article, watch movies, online remote virtual learning and other benefits. IT workers are becoming high-salary field in all over the world. ValidVCE releases latest and valid CEHPC Exam preparations to help candidates clear exams certainly as CertiProf certifications are outstanding and attractive. If you determine to take part in exams, our CEHPC exam preparations will be a good helper.

If you are now determined to go to research, there is still a little hesitation in product selection. CEHPC exam prep offers you a free trial version! You can choose one or more versions that you are most interested in, and then use your own judgment. CEHPC Exam Materials really hope that every user can pick the right CEHPC study guide for them. If you really lack experience, you do not know which one to choose. You can consult our professional staff.

>> Exam CEHPC Format <<

## Pass CEHPC Test Guide, Preparation CEHPC Store

This offline software works only on Windows computers and laptops. ValidVCE also offers up to 1 year of free updates, if for instance, the sections of real Ethical Hacking Professional Certification Exam examination changes after your purchase of the CEHPC practice test material. So just download actual CEHPC Exam Questions and start your journey today. It ensures that you would qualify for the CertiProf CEHPC certification exam on the maiden strive with brilliant grades.

## CertiProf Ethical Hacking Professional Certification Exam Sample Questions (Q95-Q100):

## NEW QUESTION # 95

What is Netcat?

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

**Answer: B**

Explanation:

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, including port scanning, banner grabbing, file transfers, reverse shells, bind shells, and debugging network services. It is commonly used during the reconnaissance, exploitation, and post-exploitation phases of 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 is cross-platform and 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.

## NEW QUESTION # 96

What operating system is Kali Linux based on?

- A. Arch Linux
- B. Ubuntu
- C. Debian

**Answer: C**

Explanation:

Kali Linux is based on Debian, making option C the correct answer. Debian is a stable, secure, and widely used Linux distribution known for its reliability and extensive package management system.

Kali Linux builds upon Debian's architecture and package repositories, adding hundreds of preinstalled tools specifically designed for penetration testing, digital forensics, and security auditing. Ethical hackers rely on Kali because it provides a ready-to-use environment for professional security assessments.

Option A is incorrect because Ubuntu, while also Debian-based, is not the direct base of Kali Linux. Option B is incorrect because Arch Linux uses a completely different package management and system design.

Understanding the base operating system is important for ethical hackers because it affects system administration, package management, and security updates. Kali uses Debian's APT package manager, which allows consistent updates and reliable tool maintenance.

Knowing Kali's Debian foundation helps professionals troubleshoot issues, manage dependencies, and maintain secure environments during penetration testing engagements.

## NEW QUESTION # 97

What is Masquerading?

- A. Consists of impersonating the identity of a legitimate user of a computer system or its environment.
- B. Web authentication method.
- C. A method for masking network traffic.

**Answer: A**

Explanation:

Masquerading is a sophisticated attack vector that consists of an unauthorized user or process impersonating the identity of a

legitimate user, system, or service within a computer environment. In the context of cybersecurity, the goal of masquerading is to bypass authentication controls and gain access to restricted resources or information by appearing as a trusted entity. This is often a critical step in the "Gaining Access" phase of a cyberattack, as it allows the attacker to operate under the radar of traditional security logging.

There are several ways masquerading can manifest:

- \* User Impersonation: An attacker uses stolen credentials (usernames and passwords) to log into a system as a legitimate employee.
- \* IP Spoofing: An attacker crafts network packets with a forged source IP address to make it appear as though the traffic is coming from a trusted internal machine.
- \* Email Spoofing: An attacker sends an email that appears to come from a known, trusted source (like an executive or a bank) to trick the recipient into performing an action, such as revealing a password.

Managing and mitigating the threat of masquerading requires robust "Identity and Access Management" (IAM) controls. The most effective defense is Multi-Factor Authentication (MFA). Even if an attacker successfully masquerades as a user by stealing their password, the MFA requirement provides a second layer of verification that is much harder to forge. Additionally, organizations can use "Behavioral Analytics" to detect anomalies; for example, if a user who typically logs in from London suddenly logs in from a different continent, the system can flag it as a potential masquerading attempt. By understanding that masquerading relies on the manipulation of trust and identity, ethical hackers can help organizations implement "Zero Trust" architectures, where every request is verified regardless of where it appears to originate.

## NEW QUESTION # 98

What is an XSS?

- A. It is a type of cloned website with malicious intent.
- B. It is a security vulnerability that occurs in mobile applications stealing balance or contacts.
- C. It is a security vulnerability that occurs in web applications when data provided by users is not properly filtered and malicious scripts are executed in the web browser of other users.

**Answer: C**

Explanation:

Cross-Site Scripting (XSS) is a critical security vulnerability prevalent in web applications. It occurs when an application includes untrusted data in a web page without proper validation or escaping, allowing an attacker to inject and execute malicious scripts—typically JavaScript—in the victim's web browser. Because the browser trusts the script as if it originated from the legitimate website, the script can access sensitive information stored in the browser, such as session cookies, tokens, or personal data.

There are three primary types of XSS:

- \* Stored (Persistent) XSS: The malicious script is permanently stored on the target server (e.g., in a database, in a comment field). When a victim views the page, the script executes.
- \* Reflected XSS: The script is "reflected" off a web application to the victim's browser, usually through a link containing the payload (e.g., in a URL parameter).
- \* DOM-based XSS: The vulnerability exists in the client-side code rather than the server-side code, where the script is executed by modifying the Document Object Model (DOM) environment.

Managing the threat of XSS involves implementing strict input validation and output encoding. Developers must ensure that any data provided by users is treated as "untrusted" and filtered to remove executable code before it is rendered on a page. From an ethical hacking perspective, identifying XSS is a key part of web application penetration testing. A successful XSS attack can lead to account hijacking, website defacement, or the redirection of users to malicious websites. By understanding how malicious scripts are executed in the context of other users' browsers, security professionals can better protect the integrity of web services and the privacy of their users.

## NEW QUESTION # 99

What is ZAP?

- A. It is an open-source penetration testing tool used to evaluate the security of web applications.
- B. ZAP is a closed source penetration testing tool used to evaluate online servers.
- C. 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.

**Answer: A**

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 # 100

.....

To keep constantly update can be walk in front, which is also our ValidVCE's idea. Therefore, we regularly check CEHPC exam to find whether has update or not. Once the update comes out, we will inform our customers who are using our products so that they can have a latest understanding of CEHPC Exam. All the update service is free during one year after you purchased our CEHPC exam software.

**Pass CEHPC Test Guide:** <https://www.validvce.com/CEHPC-exam-collection.html>

CertiProf Exam CEHPC Format I needed to pass the Aruba exam quickly because I had to find a well paying IT support position, Pass CEHPC Exam via Examschief CEHPC Braindumps, CEHPC exam dumps are frequently updated and reviewed for passing the exams quickly and hassle free, All the services mentioned above are to help you pass the test with our effective CEHPC training materials: Ethical Hacking Professional Certification Exam, Actually, the knowledge and perception you get from CEHPC certification may change the way you work, live, play and learn.

To a certain extent, this may result from the CEHPC fact that we are sailing uncharted waters, Store your music collection in the cloud, so you can listen anywhere, I needed to Valid CEHPC Test Cram pass the Aruba exam quickly because I had to find a well paying IT support position.

## Pass Guaranteed Efficient CEHPC - Exam Ethical Hacking Professional Certification Exam Format

Pass CEHPC Exam via Examschief CEHPC Braindumps, CEHPC exam dumps are frequently updated and reviewed for passing the exams quickly and hassle free!

All the services mentioned above are to help you pass the test with our effective CEHPC training materials: Ethical Hacking Professional Certification Exam, Actually, the knowledge and perception you get from CEHPC certification may change the way you work, live, play and learn.

- Exam CEHPC Consultant □ CEHPC Pass Guarantee □ Latest CEHPC Exam Objectives □ Search on ▷ [www.practicevce.com](http://www.practicevce.com)◀ for **【 CEHPC 】** to obtain exam materials for free download □ CEHPC Exam Cram Pdf
- Latest CEHPC Exam Objectives □ CEHPC Exam Practice □ CEHPC Latest Test Cost □ Simply search for **[ CEHPC ]** for free download on ⇒ [www.pdfvce.com](http://www.pdfvce.com) ⇐ □ Valid CEHPC Test Papers
- CEHPC Vce Exam □ New CEHPC Test Fee □ New CEHPC Learning Materials □ Search for "CEHPC" and download it for free immediately on ➡ [www.prepawaypdf.com](http://www.prepawaypdf.com) ➡ ➡ ➡ Valid CEHPC Mock Test
- New CEHPC Exam Testking □ New CEHPC Learning Materials □ Valid CEHPC Test Notes □ ➤ [www.pdfvce.com](http://www.pdfvce.com)◀ is best website to obtain ➤ CEHPC □ for free download □ New CEHPC Learning Materials
- CertiProf CEHPC Exam | Exam CEHPC Format - CEHPC: Ethical Hacking Professional Certification Exam □ The page for free download of ➤ CEHPC □ on **「 www.exam4labs.com 」** will open immediately □ CEHPC Exam Collection Pdf
- Test CEHPC Simulator □ CEHPC Vce Exam □ Reliable CEHPC Test Tips □ Download **《 CEHPC 》** for free by simply searching on ▷ [www.pdfvce.com](http://www.pdfvce.com)◀ □ CEHPC Answers Real Questions
- CertiProf CEHPC Marvelous Exam Format □ Simply search for ➤ CEHPC ➡ for free download on ➤ [www.validtorrent.com](http://www.validtorrent.com)◀ □ Trustworthy CEHPC Pdf
- CEHPC – 100% Free Exam Format | the Best Pass Ethical Hacking Professional Certification Exam Test Guide □

