

212-82 Pass Rate, Certification 212-82 Exam Infor

EC-Council CCT 212-82 Certification Exam Questions and Answers PDF

EC-Council 212-82 Exam Guide

www.EduSum.com
Get complete detail on 212-82 exam guide to crack EC-Council Certified Cybersecurity Technician. You can collect all information on 212-82 tutorial, practice test, books, study material, exam questions, and syllabus. Firm your knowledge on EC-Council Certified Cybersecurity Technician and get ready to crack 212-82 certification. Explore all information on 212-82 exam with number of questions, passing percentage and time duration to complete test.

2025 Latest PDF4Test 212-82 PDF Dumps and 212-82 Exam Engine Free Share: https://drive.google.com/open?id=1zHOfMrRe3cqbOX_7ErvdHuZ-nFMGPKzL

PDF4Test is a leading provider of top-quality Certified Cybersecurity Technician (212-82) preparation material for the 212-82 test. Our Certified Cybersecurity Technician (212-82) exam questions are designed to help customers get success on the first try. These latest ECCouncil 212-82 Questions are the result of extensive research by a team of professionals with years of experience.

To qualify for the CCT certification, candidates must have a minimum of six months of experience in the IT or cybersecurity field. Certified Cybersecurity Technician certification covers a wide range of topics such as intrusion detection and prevention, security architecture and operations, and vulnerability management. 212-82 Exam comprises of 50 multiple-choice questions, and test-takers have 60 minutes to complete it.

>> 212-82 Pass Rate <<

Certification 212-82 Exam Infor | New 212-82 Test Registration

Our customer service staff will be patient to help you to solve them. At the same time, if you have problems with downloading and installing, Certified Cybersecurity Technician torrent prep also has dedicated staff that can provide you with remote online guidance. In order to allow you to use our products with confidence, 212-82 Test Guide provide you with a 100% pass rate guarantee. Once you unfortunately fail the exam, we will give you a full refund, and our refund process is very simple.

The Certified Cybersecurity Technician certification process involves taking the exam after completing the required training. The training can be obtained through various means, such as online courses or classroom instruction. The training covers all the topics included in the exam and is designed to prepare individuals to pass the exam and obtain the certification.

ECCouncil Certified Cybersecurity Technician Sample Questions (Q90-Q95):

NEW QUESTION # 90

Sam, a software engineer, visited an organization to give a demonstration on a software tool that helps in business development. The administrator at the organization created a least privileged account on a system and allocated that system to Sam for the demonstration. Using this account, Sam can only access the files that are required for the demonstration and cannot open any other file in the system.

Which of the following types of accounts the organization has given to Sam in the above scenario?

- A. User account
- B. Service account
- C. Administrator account
- D. Guest account

Answer: D

Explanation:

The correct answer is B, as it identifies the type of account that the organization has given to Sam in the above scenario. A guest account is a type of account that allows temporary or limited access to a system or network for visitors or users who do not belong to the organization. A guest account typically has minimal privileges and permissions and can only access certain files or applications. In the above scenario, the organization has given Sam a guest account for the demonstration. Using this account, Sam can only access the files that are required for the demonstration and cannot open any other file in the system. Option A is incorrect, as it does not identify the type of account that the organization has given to Sam in the above scenario. A service account is a type of account that allows applications or services to run on a system or network under a specific identity. A service account typically has high privileges and permissions and can access various files or applications. In the above scenario, the organization has not given Sam a service account for the demonstration. Option C is incorrect, as it does not identify the type of account that the organization has given to Sam in the above scenario. A user account is a type of account that allows regular access to a system or network for employees or members of an organization. A user account typically has moderate privileges and permissions and can access various files or applications depending on their role. In the above scenario, the organization has not given Sam a user account for the demonstration. Option D is incorrect, as it does not identify the type of account that the organization has given to Sam in the above scenario. An administrator account is a type of account that allows full access to a system or network for administrators or managers of an organization. An administrator account typically has the highest privileges and permissions and can access and modify any files or applications. In the above scenario, the organization has not given Sam an administrator account for the demonstration.

References: , Section 4.1

NEW QUESTION # 91

An organization divided its IT infrastructure into multiple departments to ensure secure connections for data access. To provide high-speed data access, the administrator implemented a RAID level that broke data into sections and stored them across multiple drives. The storage capacity of this RAID level was equal to the sum of disk capacities in the set. which of the following RAID levels was implemented by the administrator in the above scenario?

- A. RAID Level 0
- B. RAID Level 1
- C. RAID Level 3
- D. RAID Level 5

Answer: A

Explanation:

RAID Level 0 is the RAID level that was implemented by the administrator in the above scenario. RAID Level 0 is also known as striping, which breaks data into sections and stores them across multiple drives. RAID Level 0 provides high-speed data access and increases performance, but it does not provide any redundancy or fault tolerance. The storage capacity of RAID Level 0 is equal to the sum of disk capacities in the set.

References: RAID Level 0

NEW QUESTION # 92

Desmond, a forensic officer, was investigating a compromised machine involved in various online attacks. For this purpose.

Desmond employed a forensic tool to extract and analyze computer-based evidence to retrieve information related to websites accessed from the victim machine. Identify the computer-created evidence retrieved by Desmond in this scenario.

- A. Documents
- B. Compressed files
- C. Address books
- D. Cookies

Answer: D

Explanation:

Cookies are the computer-created evidence retrieved by Desmond in this scenario. Cookies are small files that are stored on a user's computer by a web browser when the user visits a website. Cookies can contain information such as user preferences, login details, browsing history, or tracking data. Cookies can be used to extract and analyze computer-based evidence to retrieve information related to websites accessed from the victim machine². References: Cookies

NEW QUESTION # 93

Jane is a newly appointed Chief Financial Officer at BigTech Corp. Within a week, she receives an email from a sender posing as the company's CEO, instructing her to make an urgent wire transfer. Suspicious. Jane decides to verify the request's authenticity. She receives another email from the same sender, now attaching a seemingly scanned image of the CEO's handwritten note. Simultaneously, she gets a call from an 'IT support' representative, instructing her to click on the attached image to download a 'security patch'. Concerned. Jane must determine which social engineering tactics she encountered.

- A. Baiting via the handwritten note image and preloading through the 'IT support' call.
- B. Spear phishing through the CEO impersonation email and vishing via the 'IT support' call.
- C. Spear phishing through both the emails and quizzing via the 'IT support' call.
- D. Phishing through the CEO impersonation email and baiting via the 'IT support' call.

Answer: B

Explanation:

Jane encountered a combination of social engineering tactics:

* Spear Phishing:

* CEO Impersonation Email: The initial email and the follow-up with the scanned image of the CEO's handwritten note are examples of spear phishing, where attackers target specific individuals with tailored messages to gain their trust and extract sensitive information.

* Vishing:

* 'IT Support' Call: The phone call from the supposed 'IT support' representative asking Jane to download a 'security patch' is a form of vishing (voice phishing). This tactic involves using phone calls to trick victims into revealing sensitive information or performing actions that compromise security.

References:

* Social Engineering Techniques: SANS Institute Reading Room

* Phishing and Vishing Explained: Norton Security

NEW QUESTION # 94

In a multinational corporation, the IT department implemented a new network security protocol for their global data centers. This protocol was designed to enhance security measures by incorporating advanced access control principles. The protocol employs a combination of methods to ensure that only authorized personnel can access sensitive data. Recently, an incident occurred where an unauthorized user gained access to confidential data. The security team discovered that the intruder exploited a specific aspect of the access control system. Which aspect of the access control principles, terminologies, and models was most likely exploited?

- A. Role-Based Access Control (RBAC), where access is given based on the roles within the organization.
- B. Mandatory Access Control (MAC), where access decisions are made based on predefined rules set by the system's administrator.
- C. Discretionary Access Control (DAC), where the resource owner decides on the access permissions.
- D. Attribute-Based Access Control (ABAC), where access decisions are made based on a set of policies and attributes.

Answer: C

Explanation:

The incident likely exploited a weakness inherent in Discretionary Access Control (DAC). Here's an explanation:

* DAC Overview: In DAC, resource owners determine who has access to their resources. This model is flexible but can be prone to misconfigurations.

* Weaknesses:

* Ownership Rights: Users with ownership rights can inadvertently or maliciously grant access to unauthorized users.

* Human Error: High reliance on correct permission settings by individual users.

* Incident Scenario:

* An unauthorized user gained access, possibly due to a misconfigured or overly permissive access setting by the resource owner.

* This highlights the risk of relying solely on user discretion for access control.

References:

* DAC Model Explanation:Link

* SANS Institute on DAC: Link

NEW QUESTION # 95

...

Certification 212-82 Exam Infor: <https://www.pdf4test.com/212-82-dump-torrent.html>

BONUS!!! Download part of PDF4Test 212-82 dumps for free: <https://drive.google.com/open?>

id=1zHOfMrRe3cqbOX_7ErvdHuZ-nFMGPKzL