212-82 Authorized Certification & Valid 212-82 Vce Dumps

BONUS!!! Download part of PracticeVCE 212-82 dumps for free: https://drive.google.com/open?id=100mc90ck8SQBmoAR4WJcIAUP1tvGFpeE

Exam candidates are susceptible to the influence of ads, so our experts' know-how is impressive to pass the 212-82 exam instead of making financial reward solely. We hypothesize that you fail the exam after using our 212-82 learning engine we can switch other versions for you or give back full refund. In such a way, our 212-82 Exam Questions can give you more choices to pass more exams and we do put our customers' interest as the first thing to consider.

ECCouncil 212-82 Exam is an essential certification for individuals who want to pursue a career in the cybersecurity field. Certified Cybersecurity Technician certification validates the candidates' knowledge and expertise in the field and enhances their professional credibility. Certified Cybersecurity Technician certification is recognized globally and opens up various job opportunities for certified professionals. Certified Cybersecurity Technician certification also demonstrates the candidates' commitment to continuous learning and professional development in the cybersecurity field.

ECCouncil 212-82 Certification Exam is an excellent way for individuals to demonstrate their knowledge and skills in cybersecurity. It is recognized by employers around the world and can help candidates stand out in a highly competitive job market. Additionally, obtaining this certification can lead to higher salaries and career advancement opportunities.

>> 212-82 Authorized Certification <<

Unparalleled 212-82 Authorized Certification – Pass 212-82 First Attempt

To succeed on the ECCouncil 212-82 exam, you require a specific ECCouncil 212-82 exam environment to practice. But before settling on any one method, you make sure that it addresses their specific concerns about the 212-82 exam, such as whether or not the platform they are joining will aid them in passing the Certified Cybersecurity Technician (212-82) exam on the first try, whether or not it will be worthwhile, and will it provide the necessary 212-82 Questions.

ECCouncil 212-82 exam is a challenging and comprehensive exam that requires candidates to have a deep understanding of cybersecurity concepts and technologies. 212-82 exam is designed to test both the theoretical knowledge and practical skills of candidates, ensuring that they are well-equipped to handle real-world cybersecurity challenges. 212-82 Exam is also updated regularly to reflect the latest developments in the field, ensuring that certified professionals are up-to-date with the latest cybersecurity trends and technologies.

ECCouncil Certified Cybersecurity Technician Sample Questions (Q155-Q160):

NEW QUESTION # 155
A disgruntled employee has set up a RAT (Remote Access Trojan) server in one of the machines in the target network to steal sensitive corporate documents. The IP address of the target machine where the RAT is installed is 20.20.10.26. Initiate a remote connection to the target machine from the "Attacker Machine-1" using the Theef client. Locate the "Sensitive Corporate Documents"

folder in the target machine's Documents directory and determine the number of files. Mint: Theef folder is located at Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Theef of the Attacker Machine1.

- A. 0
- B. 1
- C. 2
- D. 3

Answer: A

Explanation:
The number of files in the "Sensitive Corporate Documents" folder is 4. This can be verified by initiating a remote connection to the target machine from the "Attacker Machine-1" using Theef client. Theef is a Remote Access Trojan (RAT) that allows an attacker to remotely control a victim's machine and perform various malicious activities. To connect to the target machine using Theef client, one can follow these steps:
Launch Theef client from Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Theef on the "Attacker Machine-1".
Enter the IP address of the target machine (20.20.10.26) and click on Connect.
Wait for a few seconds until a connection is established and a message box appears saying "Connection Successful".
Click on OK to close the message box and access the remote desktop of the target machine.
Navigate to the Documents directory and locate the "Sensitive Corporate Documents" folder.
Open the folder and count the number of files in it. The screenshot below shows an example of performing these steps: Reference: [Theef Client Tutorial], [Screenshot of Theef client showing remote desktop and folder]

NEW QUESTION # 156
Zion belongs to a category of employees who are responsible for implementing and managing the physical security equipment installed around the facility. He was instructed by the management to check the functionality of equipment related to physical security. Identify the designation of Zion.

- A. Supervisor
- B. Safety officer
- C. Chief information security officer
- D. Guard

Answer: D

Explanation:
The correct answer is C, as it identifies the designation of Zion. A guard is a person who is responsible for implementing and managing the physical security equipment installed around the facility. A guard typically performs tasks such as:
* Checking the functionality of equipment related to physical security
* Monitoring the surveillance cameras and alarms
* Controlling the access to restricted areas
* Responding to emergencies or incidents
In the above scenario, Zion belongs to this category of employees who are responsible for implementing and managing the physical security equipment installed around the facility. Option A is incorrect, as it does not identify the designation of Zion. A supervisor is a person who is responsible for overseeing and directing the work of other employees. A supervisor typically performs tasks such as:
* Assigning tasks and responsibilities to employees
* Evaluating the performance and productivity of employees
* Providing feedback and guidance to employees
* Resolving conflicts or issues among employees
In the above scenario, Zion does not belong to this category of employees who are responsible for overseeing and directing the work of other employees. Option B is incorrect, as it does not identify the designation of Zion. A chief information security officer (CISO) is a person who is responsible for establishing and maintaining the security vision, strategy, and program for an organization. A CISO typically performs tasks such as:
* Developing and implementing security policies and standards
* Managing security risks and compliance
* Leading security teams and projects
* Communicating with senior management and stakeholders
In the above scenario, Zion does not belong to this category of employees who are responsible for establishing and maintaining the

security vision, strategy, and program for an organization. Option D is incorrect, as it does not identify the designation of Zion. A safety officer is a person who is responsible for ensuring that health and safety regulations are followed in an organization. A safety officer typically performs tasks such as:
* Conducting safety inspections and audits
* Identifying and eliminating hazards and risks
* Providing safety training and awareness
* Reporting and investigating accidents or incidents
In the above scenario, Zion does not belong to this category of employees who are responsible for ensuring that health and safety regulations are followed in an organization. References: Section 7.1

NEW QUESTION # 157

GlobalTech, a multinational corporation with over 10.000employees, has seen a surge in mobile device usage among its workforce. The IT department Is tasked with deploying a robust mobile security management solution that caters not only to the security of data but also provides flexibility in device choices and keeps administrative overhead low. Which of the following would be the best solution for GlobalTech?

- A. Containerization Solutions
- B. Unified Endpoint Management (UEM)
- C. Mobile Device Management (MDM)
- D. Mobile Application Management (MAM)

Answer: B

Explanation:
* Unified Endpoint Management (UEM) Overview:
* UEM solutions provide comprehensive management for a wide range of endpoints, including mobile devices, desktops, laptops, and even IoT devices. They integrate Mobile Device Management (MDM) and Mobile Application Management (MAM) functionalities.

NEW QUESTION # 158

Walker, a security team member at an organization, was instructed to check if a deployed cloud service is working as expected. He performed an independent examination of cloud service controls to verify adherence to standards through a review of objective evidence. Further, Walker evaluated the services provided by the CSP regarding security controls, privacy impact, and performance.
Identify the role played by Walker in the above scenario.

- A. Cloud auditor
- B. Cloud consumer
- C. Cloud provider
- D. Cloud carrier

Answer: A

Explanation:
A cloud auditor is a role played by Walker in the above scenario. A cloud auditor is a third party who examines controls of cloud computing service providers. Cloud auditor performs an audit to verify compliance with the standards and expressed his opinion through a report89. A cloud provider is an entity that provides cloud services, such as infrastructure, platform, or software, to cloud consumers10. A cloud carrier is an entity that provides connectivity and transport of cloud services between cloud providers and cloud consumers10. A cloud consumer is an entity that uses cloud services for its own purposes or on behalf of another entity

NEW QUESTION # 159

Kevin, a professional hacker, wants to penetrate CyberTech Inc.'s network. He employed a technique, using which he encoded packets with Unicode characters. The company's IDS cannot recognize the packet, but the target web server can decode them. What is the technique used by Kevin to evade the IDS system?

- A. Session splicing
- B. Desynchronization

- C. Obfuscating
- D. Urgency flag

Answer: C

Explanation:
Obfuscating is the technique used by Kevin to evade the IDS system in the above scenario.
Obfuscating is a technique that involves encoding or modifying packets or data with various methods or characters to make them unreadable or unrecognizable by an IDS (Intrusion Detection System). Obfuscating can be used to bypass or evade an IDS system that relies on signatures or patterns to detect malicious activities. Obfuscating can include encoding packets with Unicode characters, which are characters that can represent various languages and symbols. The IDS system cannot recognize the packet, but the target web server can decode them and execute them normally. Desynchronization is a technique that involves creating discrepancies or inconsistencies between the state of a connection as seen by an IDS system and the state of a connection as seen by the end hosts. Desynchronization can be used to bypass or evade an IDS system that relies on stateful inspection to track and analyze connections. Desynchronization can include sending packets with invalid sequence numbers, which are numbers that indicate the order of packets in a connection.
Session splicing is a technique that involves splitting or dividing packets or data into smaller fragments or segments to make them harder to detect by an IDS system. Session splicing can be used to bypass or evade an IDS system that relies on packet size or content to detect malicious activities. Session splicing can include sending packets with small MTU (Maximum Transmission Unit) values, which are values that indicate the maximum size of packets that can be transmitted over a network. An urgency flag is a flag in the TCP (Transmission Control Protocol) header that indicates that the data in the packet is urgent and should be processed immediately by the receiver. An urgency flag is not a technique to evade an IDS system, but it can be used to trigger an IDS system to generate an alert or a response.

NEW QUESTION # 160

......

id=100mc90ck8SQBmoAR4WJcIAUP1tvGFpeE