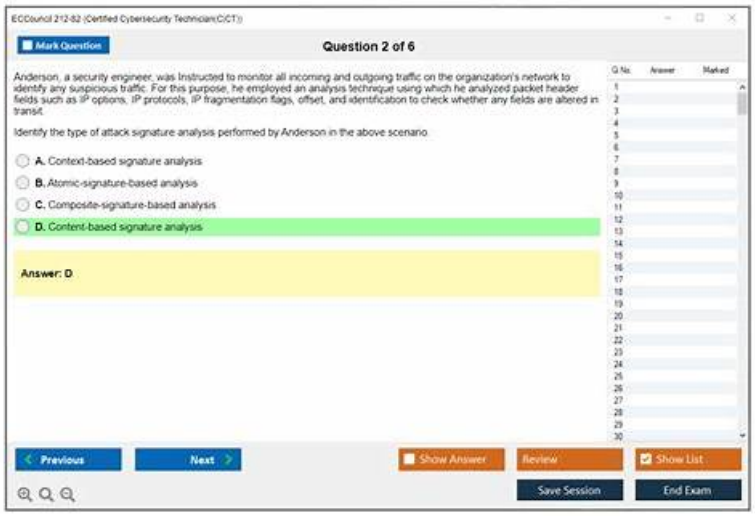
Free PDF Quiz 212-82 - Latest Latest Certified Cybersecurity Technician Test Cram



BTW, DOWNLOAD part of BraindumpsIT 212-82 dumps from Cloud Storage: https://drive.google.com/open?id=14AJUakN00Qtfq0ekB0BskrXcwpqvb9BP

Do you have the plan to accept this challenge? Looking for a proven and quick method to pass this challenge ECCouncil 212-82 exam? If your answer is yes then you do not need to go anywhere. Just visit the BraindumpsIT and explore the top features of valid, updated, and real ECCouncil 212-82 Dumps.

The ECCouncil 212-82 Exam covers a wide range of topics, including network security, cryptography, and ethical hacking. Candidates will be expected to demonstrate their understanding of these topics through a series of multiple-choice questions and practical exercises.

>> Latest 212-82 Test Cram <<

Authoritative Latest 212-82 Test Cram & Leading Offer in Qualification Exams & Trusted ECCouncil Certified Cybersecurity Technician

Maybe you are busy with working every day without the help of our 212-82 learning materials. The heavy work leaves you with no time to attend to study. It doesn't matter. Our 212-82 learning materials can help you squeeze your time out and allow you to improve your knowledge and skills while having work experience. And there are three versions of our 212-82 Exam Questions for you to choose according to your interests and hobbies.

The Certified Cybersecurity Technician certification program covers a broad range of topics, including network security, operating system security, cryptography, and incident response. 212-82 exam is designed to assess the candidate's knowledge of these topics and their ability to apply that knowledge in real-world situations. Certified Cybersecurity Technician certification program is designed to help cybersecurity professionals advance their careers by demonstrating their proficiency in these areas.

The EC-Council 212-82 (Certified Cybersecurity Technician) exam is a certification exam that is designed to test the candidate's knowledge and skills in the field of cybersecurity. 212-82 exam is created by the International Council of E-Commerce Consultants, also known as EC-Council, which is a global leader in cybersecurity certification programs. Certified Cybersecurity Technician certification is vendor-neutral, meaning that it is not affiliated with any particular technology or solution.

ECCouncil Certified Cybersecurity Technician Sample Questions (Q71-Q76):

NEW QUESTION # 71
An MNC hired Brandon, a network defender, to establish secured VPN communication between the company's remote offices. For this purpose, Brandon employed a VPN topology where all the remote offices communicate with the corporate office but communication between the remote offices is denied.

Identify the VPN topology employed by Brandon in the above scenario.

- A. Point-to-Point VPN topology
- B. Hub-and-Spoke VPN topology
- C. Full-mesh VPN topology
- D. Star topology

Answer: B

Explanation:
A hub-and-spoke VPN topology is a type of VPN topology where all the remote offices communicate with the corporate office, but communication between the remote offices is denied.
The corporate office acts as the hub, and the remote offices act as the spokes. This topology reduces the number of VPN tunnels required and simplifies the management of VPN policies. A point-to-point VPN topology is a type of VPN topology where two endpoints establish a direct VPN connection. A star topology is a type of VPN topology where one endpoint acts as the central node and connects to multiple other endpoints. A full-mesh VPN topology is a type of VPN topology where every endpoint connects to every other endpoint.

NEW QUESTION # 72
You are the lead cybersecurity specialist at a cutting-edge tech organization that specializes In developing artificial intelligence (Al)products for clients across various sectors. Given the sensitivity and proprietary nature of your products, ensuring top-notch security is of paramount importance. Late one evening, you receive an alert from your threat Intelligence platform about potential vulnerabilities In one of the third-party components your Al products heavily rely upon.
This component is known to have integration points with several key systems within your organization. Any successful exploitation of this vulnerability could grant attackers unparalleled access to proprietary algorithms and client-specific modifications, which could be catastrophic in the wrong hands.
While you are analyzing the threat's details, a member of your team identifies several unusual patterns of data access, suggesting that the vulnerability might already have been exploited. The potential breach's initial footprint suggests a highly sophisticated actor, possibly even a nation- state entity. Given the gravity of the situation and the potential consequences of a full-blown breach, what should be your immediate course of action to address the incident and ensure minimal risk exposure?

- A. Initiate an emergency patching protocol, immediately updating all instances of the vulnerable component across your infrastructure and closely monitor the network for further unusual activities.
- B. Alert the organization s legal and PR teams, preparing a communication strategy to notify clients and the public about the potential breach, ensuring transparency and proactive damage control.
- C. Engage an external cybersecurity consultancy with expertise in nation-state level threats.
  Collaborate to devise a mitigation strategy while also running parallel investigations to understand the full scope of the breach.
- D. Disconnect the potentially compromised systems from the network, archive all logs and related data for future analysis, and shift core services to backup systems ensuring business continuity.

Answer: D

NEW QUESTION # 73
A pfSense firewall has been configured to block a web application www.abchacker.com. Perform an analysis on the rules set by the admin and select the protocol which has been used to apply the rule.
Hint: Firewall login credentials are given below:
Username: admin
Password: admin@l23

- A. FTP
- B. POP3
- C. ARP
- D. TCP/UDP

Answer: D

Explanation:
TCP/UDP is the protocol that has been used to apply the rule to block the web application www.abchacker.com in the above scenario. pfSense is a firewall and router software that can be installed on a computer or a device to protect a network from various

threats and attacks. pfSense can be configured to block or allow traffic based on various criteria, such as source, destination, port, protocol, etc. pfSense rules are applied to traffic in the order they appear in the firewall configuration . To perform an analysis on the rules set by the admin, one has to follow these steps:
Open a web browser and type 20.20.10.26
Press Enter key to access the pfSense web interface.
Enter admin as username and admin@l23 as password.
Click on Login button.
Click on Firewall menu and select Rules option.
Click on LAN tab and observe the rules applied to LAN interface.
The rules applied to LAN interface are:

Action	Interface	Protocol	Source	Port	Destination	Port	Description
Block	LAN	TCP/UDP	any	any	www.abchacker.com	any	Block abchacker website
Pass	LAN	any	any	any	any	any	Default allow LAN to any rule

The first rule blocks any traffic from LAN interface to www.abchacker.com website using TCP/UDP protocol. The second rule allows any traffic from LAN interface to any destination using any protocol. Since the first rule appears before the second rule, it has higher priority and will be applied first. Therefore, TCP/UDP is the protocol that has been used to apply the rule to block the web application www.abchacker.com. POP3 (Post Office Protocol 3) is a protocol that allows downloading emails from a mail server to a client device. FTP (File Transfer Protocol) is a protocol that allows transferring files between a client and a server over a network. ARP (Address Resolution Protocol) is a protocol that resolves IP addresses to MAC (Media Access Control) addresses on a network.

NEW QUESTION # 74
NexaCorp. an enterprise with a robust Linux infrastructure, has been facing consistent downtimes without any apparent reasons. The company's initial investigation suggests possible unauthorized system-level changes.
NexaCorp's IT team realizes that It needs to monitor andanalyze system logs more efficiently to pinpoint the cause. What would be the optimal approach for NexaCorp to monitor and analyze its Linux system logs to detect and prevent unauthorized changes?

- A. Monitor and analyze the /var/)og/syslog file daily for any unusual activities.
- B. Implement a SIEM system that centralizes, correlates, and analyzes logs in real-time.
- C. Set up an automated script to send alerts if the last' command shows unexpected users.
- D. Only focus on monitoring SSH logs since most changes likely come through remote access.

Answer: B

Explanation:
For NexaCorp to effectively monitor and analyze system logs, implementing a Security Information and Event Management (SIEM) system is the optimal approach:
* SIEM Overview: SIEM systems collect, normalize, and analyze log data from various sources in real-time.
* Benefits:
* Centralization: Aggregates logs from all systems into a single platform.
* Correlation: Identifies patterns and correlates events from different sources to detect anomalies.
* Implementation Steps:
* Select a SIEM Solution: Choose a suitable SIEM tool (e.g., Splunk, ELK Stack, QRadar).
* Integration: Configure the SIEM to collect logs from all relevant systems.
* Alerting and Reporting: Set up alerts for suspicious activities and generate periodic reports.
References:
* SIEM Basics: Link
* Implementing SIEM: Link

NEW QUESTION # 75
Stella purchased a smartwatch online using her debit card. After making payment for the product through the payment gateway, she

received a transaction text message with a deducted and available balance from her bank.
Identify the information security element that ensures that Stella's transaction status is immediately reflected in her bank account in this scenario.

- A. Availability
- B. Integrity
- C. Non-repudiation
- D. Confidentiality

Answer: A

Explanation:
Availability is the information security element that ensures that Stella's transaction status is immediately reflected in her bank account in this scenario. Information security is the practice of protecting information and information systems from unauthorized access, use, disclosure, modification, or destruction. Information security can be based on three fundamental principles: confidentiality, integrity, and availability.
Confidentiality is the principle that ensures that information is accessible only to authorized parties and not disclosed to unauthorized parties. Integrity is the principle that ensures that information is accurate, complete, and consistent and not altered or corrupted by unauthorized parties. Availability is the principle that ensures that information and information systems are accessible and usable by authorized parties when needed. In the scenario, Stella purchased a smartwatch online using her debit card. After making payment for the product through the payment gateway, she received a transaction text message with a deducted and available balance from her bank. This means that her transaction status was immediately reflected in her bank account, which indicates that availability was ensured by her bank's information system.

NEW QUESTION # 76
.....