

Exam 212-82 Exercise & 212-82 Vce File



What's more, part of that PassSureExam 212-82 dumps now are free: <https://drive.google.com/open?id=1rCU1jqttOxagL9MAlgdyEqCPZTH-wcRq>

The product is made in three different formats to help customers with different preparation styles meet their needs. One of these formats is ECCouncil 212-82 Dumps PDF file which is printable and portable. Users can take Certified Cybersecurity Technician (212-82) PDF questions anywhere and use them anytime.

One of the key benefits of the ECCouncil 212-82 Certification is that it is recognized by many employers in the cybersecurity industry. Certified Cybersecurity Technician certification can help individuals stand out from other job applicants and demonstrate their commitment to the field of cybersecurity.

>> Exam 212-82 Exercise <<

212-82 Vce File | Latest 212-82 Exam Notes

Once you get the ECCouncil 212-82 certificate, you can quickly quit your current job and then change a desirable job. The ECCouncil 212-82 certificate can prove that you are a competent person. So it is easy for you to pass the interview and get the job. The assistance of our 212-82 practice quiz will change your life a lot.

ECCouncil 212-82 Exam is challenging and requires extensive preparation. Candidates need to have a thorough understanding of cybersecurity concepts, tools, and techniques to pass the exam. Certified Cybersecurity Technician certification exam is designed to ensure that only the most qualified and skilled cybersecurity professionals earn the certification. The ECCouncil provides various training resources and study materials to help candidates prepare for the exam.

ECCouncil Certified Cybersecurity Technician Sample Questions (Q91-Q96):

NEW QUESTION # 91

A threat intelligence feed data file has been acquired and stored in the Documents folder of Attacker Machine-1 (File Name: Threatfeed.txt). You are a cybersecurity technician working for an ABC organization. Your organization has assigned you a task to analyze the data and submit a report on the threat landscape. Select the IP address linked with <http://securityabc.s21sec.com>

- A. 5.9.200.150
- B. 5.9.200.200
- C. 5.9.188.148
- D. 5.9.110.120

Answer: C

NEW QUESTION # 92

Mark, a security analyst, was tasked with performing threat hunting to detect imminent threats in an organization's network. He generated a hypothesis based on the observations in the initial step and started the threat hunting process using existing data collected

from DNS and proxy logs.

Identify the type of threat hunting method employed by Mark in the above scenario.

- A. TTP-driven hunting
- B. Hybrid hunting
- C. Entity-driven hunting
- D. Data-driven hunting

Answer: D

NEW QUESTION # 93

As a network security analyst for a video game development company, you are responsible for monitoring the traffic patterns on the development server used by programmers. During business hours, you notice a steady stream of data packets moving between the server and internal programmer workstations. Most of this traffic is utilizing TCP connections on port 22 (SSH) and port 5900 (VNC).

Based on this scenario, what does it describe?

- A. Traffic seems normal SSH and VNC are commonly used by programmers for secure remote access and collaboration.
- B. Traffic appears suspicious - The presence of encrypted connections might indicate attempts to conceal malicious activities.
- C. Traffic is because of malware infection - Frequently used SSH & VNC Ports could indicate malware spreading through the Network.
- D. The situation is inconclusive - Further investigation is necessary to determine the nature of the traffic.

Answer: A

NEW QUESTION # 94

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

Answer: A

NEW QUESTION # 95

TechTYendz, a leading tech company, is moving towards the final stages of developing a new cloud-based web application aimed at real-time data processing for financial transactions. Given the criticality of data and the high user volume expected. TechTYendz's security team is keen on employing rigorous application security testing techniques. The team decides to carry out a series of tests using tools that can best mimic potential real-world attacks on the application. The team's main concern Is to detect vulnerabilities In the system, including those stemming from configuration errors, software bugs, and faulty APIs. The security experts have shortlisted four testing tools and techniques. Which of the following would be the MOST comprehensive method to ensure a thorough assessment of the application's security?

- A. Conducting a manual penetration test focusing only on the user interface and transaction modules.
- B. Implementing a tool that combines both SAST and DAST features for a more holistic security overview.
- C. Employing dynamic application security testing (DAST) tools that analyze running applications in realtime.
- D. Utilizing static application security testing (SAST) tools to scan the source code for vulnerabilities.

Answer: B

Explanation:

For comprehensive application security testing, combining Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) provides the best coverage:

* Static Application Security Testing (SAST):

* Source Code Analysis: Scans the source code to identify vulnerabilities such as code injection, buffer overflows, and insecure APIs.

* Early Detection: Allows developers to fix vulnerabilities early in the development lifecycle.

* Dynamic Application Security Testing (DAST):

* Runtime Analysis: Tests the running application for vulnerabilities, including issues related to configuration, authentication, and authorization.

* Real-World Attacks: Simulates real-world attacks to identify how the application behaves under different threat scenarios.

* Combined Approach:

* Holistic Security: Using both SAST and DAST provides a thorough security assessment, covering both code-level and runtime vulnerabilities.

* Comprehensive Coverage: Ensures that both internal code issues and external attack vectors are addressed.

References:

* OWASP Guide on SAST and DAST: OWASP

* NIST Application Security Guidelines:NIST SP 800-53

NEW QUESTION # 96

• • • • •

212-82 Vce File: <https://www.passsureexam.com/212-82-pass4sure-exam-dumps.html>

DOWNLOAD the newest PassSureExam 212-82 PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=1rCU1jqttOxagL9MAlgdyEqCPZTH-wcRq>