312-85 Certification Test Answers, 312-85 Exam Certification Cost

P.S. Free & New 312-85 dumps are available on Google Drive shared by ITPassLeader: https://drive.google.com/open?id=1_VBqTi7KysNA64n1EH9hvuvO72YwaVtk

As long as you bought our 312-85 practice guide, then you will find that it cost little time and efforts to learn. You can have a quick revision of the 312-85 learning quiz in your spare time. Also, you can memorize the knowledge quickly. There almost have no troubles to your normal life. You can make use of your spare moment to study our 312-85 Preparation questions. The results will become better with your constant exercises. Please have a brave attempt.

Candidates who pass the CTIA exam receive the Certified Threat Intelligence Analyst certification, which is recognized globally as a mark of excellence in threat intelligence. Certified Threat Intelligence Analyst certification demonstrates that the candidate has the knowledge and skills to identify and mitigate threats, protect critical assets, and enhance their organization's overall cybersecurity posture.

>> 312-85 Certification Test Answers <<

Three High in Demand ECCouncil 312-85 Exam Questions Formats

ITPassLeader also provides easy to use 312-85 practice test brain dump preparation software for 312-85. Moreover, after the date of purchase of the 312-85 testing engine, you will receive free updates for 90 days. The 312-85 dumps practice test software is easy to install and has a simple interface. The practice test software for 312-85 Exam provides a real feel of an exam and allows you to test your skills for the exam. The 312-85 software comes with multiple features including the self-assessment feature. You will get free updates for 90 days after the purchase date that will allow you to get latest and well-curated questions for the 312-85 exam.

To become a Certified Threat Intelligence Analyst, candidates must pass the 312-85 Exam. 312-85 exam consists of 100 multiple-choice questions and has a duration of four hours. Candidates must achieve a passing score of 70% or higher to earn the certification. 312-85 exam is available in multiple languages, including English, Spanish, Portuguese, and Chinese.

To be eligible to take the CTIA certification exam, candidates must have at least two years of experience in the field of cybersecurity and must have completed a training program that covers the exam objectives. Certified Threat Intelligence Analyst certification exam is a four-hour, multiple-choice test that consists of 100 questions. The passing score for the exam is 70%. Upon passing the exam, candidates will receive the CTIA certification, which is valid for three years. To maintain their certification, candidates must earn 60 continuing education credits during the three-year period.

ECCouncil Certified Threat Intelligence Analyst Sample Questions (Q15-Q20):

NEW QUESTION # 15
John, a professional hacker, is trying to perform APT attack on the target organization network. He gains access to a single system of a target organization and tries to obtain administrative login credentials to gain further access to the systems in the network using various techniques.
What phase of the advanced persistent threat lifecycle is John currently in?

- A. Expansion
- B. Initial intrusion
- C. Search and exfiltration
- D. Persistence

Answer: A

NEW QUESTION # 16
A threat analyst obtains an intelligence related to a threat, where the data is sent in the form of a connection request from a remote host to the server. From this data, he obtains only the IP address of the source and destination but no contextual information. While processing this data, he obtains contextual information stating that multiple connection requests from different geo-locations are received by the server within a short time span, and as a result, the server is stressed and gradually its performance has reduced. He further performed analysis on the information based on the past and present experience and concludes the attack experienced by the client organization.
Which of the following attacks is performed on the client organization?

- A. Distributed Denial-of-Service (DDoS) attack
- B. Bandwidth attack
- C. MAC spoofing attack
- D. DHCP attacks

Answer: A

Explanation:
The attack described, where multiple connection requests from different geo-locations are received by a server within a short time span leading to stress and reduced performance, is indicative of a Distributed Denial-of-Service (DDoS) attack. In a DDoS attack, the attacker floods the target's resources (such as a server) with excessive requests from multiple sources, making it difficult for the server to handle legitimate traffic, leading to degradation or outright unavailability of service. The use of multiple geo-locations for the attack sources is a common characteristic of DDoS attacks, making them harder to mitigate.References:
* "Understanding Denial-of-Service Attacks," US-CERT
* "DDoS Quick Guide," DHS/NCCIC

NEW QUESTION # 17
Daniel is a professional hacker whose aim is to attack a system to steal data and money for profit. He performs hacking to obtain confidential data such as social security numbers, personally identifiable information (PII) of an employee, and credit card information. After obtaining confidential data, he further sells the information on the black market to make money.
Daniel comes under which of the following types of threat actor.

- A. Insider threat
- B. Organized hackers
- C. State-sponsored hackers
- D. Industrial spies

Answer: B

Explanation:
Daniel's activities align with those typically associated with organized hackers. Organized hackers or cybercriminals work in groups with the primary goal of financial gain through illegal activities such as stealing and selling data. These groups often target large amounts of data, including personal and financial information, which they can monetize by selling on the black market or dark web. Unlike industrial spies who focuson corporate espionage or state-sponsored hackers who are backed by nation-states for political or military objectives, organized hackers are motivated by profit. Insider threats, on the other hand, come from within the organization and might not always be motivated by financial gain. The actions described in the scenario-targeting personal and financial information for sale-best fit the modus operandi of organized cybercriminal groups.References:

* ENISA (European Union Agency for Cybersecurity) Threat Landscape Report
* Verizon Data Breach Investigations Report

NEW QUESTION # 18
Henry. a threat intelligence analyst at ABC Inc., is working on a threat intelligence program. He was assigned to work on establishing criteria for prioritization of intelligence needs and requirements.
Which of the following considerations must be employed by Henry to prioritize intelligence requirements?

- A. Understand data reliability
- B. Develop a collection plan
- C. Understand frequency and impact of a threat
- D. Produce actionable data

Answer: C

Explanation:
When prioritizing intelligence requirements, it is crucial to understand the frequency and impact of various threats. This approach helps in allocating resources effectively, focusing on threats that are both likely to occur and that would have significant consequences if they did. By assessing threats based on these criteria, Henry can ensure that the threat intelligence program addresses the most pressing and potentially damaging threats first, thereby enhancing the organization's security posture. This prioritization is essential for effective threat management and for ensuring that the most critical threats are addressed promptly.References:
* "Cyber Threat Intelligence: Prioritizing and Using CTI Effectively," by SANS Institute
* "Threat Intelligence: What It Is, and How to Use It Effectively," by Gartner

NEW QUESTION # 19
Tyrion, a professional hacker, is targeting an organization to steal confidential information. He wants to perform website footprinting to obtain the following information, which is hidden in the web page header.
Connection status and content type
Accept-ranges and last-modified information
X-powered-by information
Web server in use and its version
Which of the following tools should the Tyrion use to view header content?

- A. Vanguard enforcer
- B. AutoShun
- C. Hydra
- D. Burp suite

Answer: D

Explanation:
Burp Suite is a comprehensive tool used for web application security testing, which includes functionality for viewing and manipulating the HTTP/HTTPS headers of web page requests and responses. This makes it an ideal tool for someone like Tyrion, who is looking to perform website footprinting to gather information hidden in the web page header, such as connection status, content type, server information, and other metadata that can reveal details about the web server and its configuration. Burp Suite allows users to intercept, analyze, and modify traffic between the browser and the web server, which is crucial for uncovering such hidden information.
References:
"Burp Suite Essentials" by Akash Mahajan
Official Burp Suite Documentation

NEW QUESTION # 20
.....