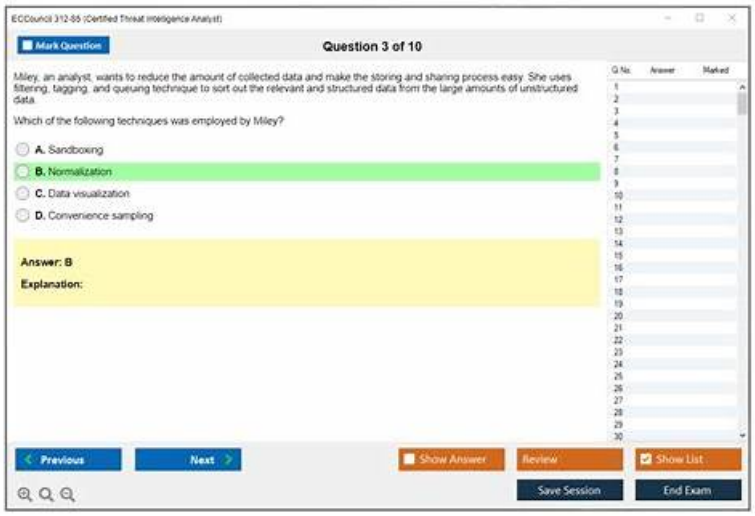
ECCouncil 312-85 Exam Questions Are Out - Download And Prepare [2026]



BTW, DOWNLOAD part of Prep4pass 312-85 dumps from Cloud Storage: https://drive.google.com/open?id=1o6f4kO1O2JP65-gCgfaxzo1N3zIM6YjK

Our 312-85 exam braindumps can lead you the best and the fastest way to reach for the certification and achieve your desired higher salary by getting a more important position in the company. Because we hold the tenet that low quality exam materials may bring discredit on the company. So we only creat the best quality of our 312-85 Study Materials to help our worthy customers pass the exam by the first attempt. Tens of thousands of our customers have passed their exam. And you will be the next one if you buy our 312-85 practice engine.

The Certified Threat Intelligence Analyst (CTIA) certification is designed to equip professionals with advanced knowledge and skills in threat intelligence. Certified Threat Intelligence Analyst certification program is offered by the International Council of Electronic Commerce Consultants (EC-Council), which is a globally recognized leader in the field of cybersecurity. The CTIA certification is designed to help professionals develop the necessary skills and knowledge to analyze, identify and prevent cyber threats in their organizations. Certified Threat Intelligence Analyst certification program covers various topics such as threat intelligence, analysis, cybercrime investigations, and much more.

>> Free 312-85 Braindumps <<

Pass Guaranteed Quiz 2026 Unparalleled ECCouncil 312-85: Free Certified Threat Intelligence Analyst Braindumps

The research and production of our 312-85 exam questions are undertaken by our first-tier expert team. The clients can have a free download and tryout of our 312-85 test practice materials before they decide to buy our products. They can use our products immediately after they pay for the 312-85 Test Practice materials successfully. There are so many advantages of our 312-85 learning guide that we can't summarize them with several simple words. You'd better look at the introduction of our 312-85 exam questions in detail as follow by yourselves.

ECCouncil 312-85 exam is designed to test the candidate's knowledge and skills in various areas related to threat intelligence. 312-85 exam consists of 100 multiple-choice questions that need to be completed within 3 hours. 312-85 exam covers topics such as the collection and analysis of intelligence data, threat intelligence methodologies, and the use of threat intelligence tools and technologies. Candidates who pass the exam earn the CTIA certification, which demonstrates their expertise in the field of threat intelligence.

The CTIA certification exam is a rigorous and challenging exam that requires candidates to demonstrate their knowledge and skills in various areas of threat intelligence. 312-85 Exam consists of 100 multiple-choice questions and must be completed within a time limit of four hours. To pass the exam, candidates must achieve a minimum score of 70%.

ECCouncil Certified Threat Intelligence Analyst Sample Questions (Q52-

Q57):

NEW QUESTION # 52
Jacob, a professional hacker, created an exact replica of an online shopping website. He copied the entire contents of the original website onto the local system that enables him to create a dummy spam website for performing social engineering attacks over the employees.
What type of technique did Jacob use for cloning the website?

- A. Data sampling
- B. Tailgating
- C. Social engineering
- D. Website mirroring

Answer: D

Explanation:
In this scenario, Jacob has copied the entire contents of a legitimate website to his local system to create a replica or duplicate version that looks exactly like the original. This process of duplicating a website by copying its structure, design, content, and files is known as website mirroring.
Website mirroring is a technique used to create an identical copy (mirror) of a real website for different purposes. In ethical use cases, organizations create mirror sites to ensure high availability, load balancing, or offline backup of web content. However, in malicious or unethical scenarios, attackers use website mirroring to replicate legitimate sites for phishing or social engineering attacks, tricking users into entering credentials, financial data, or other sensitive information.
By creating a mirrored version of an authentic site, an attacker can redirect unsuspecting victims to the fake version, which appears genuine. Victims then provide information that is captured by the attacker for malicious use. This method is commonly employed in phishing campaigns and credential harvesting operations.
Why the Other Options Are Incorrect:
* A. Data sampling:Data sampling refers to selecting a subset of data from a larger dataset for analysis or testing. It does not involve copying or cloning websites.
* C. Tailgating:Tailgating is a physical security breach technique, where an unauthorized individual follows an authorized person into a secured area without proper authentication. It is unrelated to website replication.
* D. Social engineering:Social engineering is a broader psychological manipulation technique that exploits human trust to gain confidential information. While Jacob's goal is to perform a social engineering attack using the cloned website, the method he used to create the replica is website mirroring, not social engineering itself.
Conclusion:
Jacob used website mirroring to clone the online shopping website. The mirrored site will later serve as a platform to perform social engineering attacks by deceiving employees or customers into interacting with the fake site.
Final Answer: B. Website mirroring
Explanation Reference (Based on CTIA Study Concepts):
This explanation is based on EC-Council's Certified Threat Intelligence Analyst (CTIA) study concepts under the topics of Adversary Tactics, Techniques, and Procedures (TTPs) and Threat Modeling of Infrastructure Attacks, which describe how attackers create cloned or mirrored websites to perform phishing and social engineering campaigns.

NEW QUESTION # 53
Mr. Bob, a threat analyst, is performing analysis of competing hypotheses (ACH). He has reached to a stage where he is required to apply his analysis skills effectively to reject as many hypotheses and select the best hypotheses from the identified bunch of hypotheses, and this is done with the help of listed evidence. Then, he prepares a matrix where all the screened hypotheses are placed on the top, and the listed evidence for the hypotheses are placed at the bottom.
What stage of ACH is Bob currently in?

- A. Inconsistency
- B. Diagnostics
- C. Evidence
- D. Refinement

Answer: D

Explanation:
In the Analysis of Competing Hypotheses (ACH) process, the stage where Mr. Bob is applying analysis to reject hypotheses and select the most likely one based on listed evidence, followed by preparing a matrix with screened hypotheses and evidence, is

known as the 'Refinement' stage. This stage involves refining the list of hypotheses by systematically evaluating the evidence against each hypothesis, leading to the rejection of inconsistent hypotheses and the strengthening of the most plausible ones. The preparation of a matrix helps visualize the relationship between each hypothesis and the available evidence, facilitating a more objective and structured analysis.
References:
"Psychology of Intelligence Analysis" by Richards J. Heuer, Jr., for the CIA's Center for the Study of Intelligence
"A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis" by the CIA

NEW QUESTION # 54
In which of the following attacks does the attacker exploit vulnerabilities in a computer application before the software developer can release a patch for them?

- A. Zero-day attack
- B. Advanced persistent attack
- C. Distributed network attack
- D. Active online attack

Answer: A

NEW QUESTION # 55
An analyst wants to disseminate the information effectively so that the consumers can acquire and benefit out of the intelligence. Which of the following criteria must an analyst consider in order to make the intelligence concise, to the point, accurate, and easily understandable and must consist of a right balance between tables, narrative, numbers, graphics, and multimedia?

- A. The right presentation
- B. The right order
- C. The right time
- D. The right content

Answer: A

Explanation:
For intelligence to be effectively disseminated and utilized by consumers, it must be presented in a manner that is concise, accurate, easily understandable, and engaging. This involves a careful balance of narrative, numerical data, tables, graphics, and potentially multimedia elements to convey the information clearly and compellingly. The right presentation takes into account the preferences and needs of the intelligence consumers, as well as the context andurgency of the information. By focusing on how the intelligence is presented, the analyst ensures that the content is not only consumed but also actionable, facilitating informed decision-making.

NEW QUESTION # 56
Alice, a threat intelligence analyst at HiTech Cyber Solutions, wants to gather information for identifying emerging threats to the organization and implement essential techniques to prevent their systems and networks from such attacks. Alice is searching for online sources to obtain information such as the method used to launch an attack, and techniques and tools used to perform an attack and the procedures followed for covering the tracks after an attack.
Which of the following online sources should Alice use to gather such information?

- A. Financial services
- B. Hacking forums
- C. Job sites
- D. Social network settings

Answer: B

Explanation:
Alice, looking to gather information on emerging threats including attack methods, tools, and post-attack techniques, should turn to hacking forums. These online platforms are frequented by cybercriminals and security researchers alike, where information on the latest exploits, malware, and hacking techniques is shared and discussed. Hacking forums can provide real-time insights into the tactics, techniques, and procedures (TTPs) used by threat actors, offering a valuable resource for threat intelligence analysts aiming to enhance their organization's defenses.References:

* "Hacking Forums: A Ground for Cyber Threat Intelligence," by Digital Shadows
* "The Value of Hacking Forums for Threat Intelligence," by Flashpoint

NEW QUESTION # 57
......

Test 312-85 Dumps Demo: https://www.prep4pass.com/312-85_exam-braindumps.html

What's more, part of that Prep4pass 312-85 dumps now are free: https://drive.google.com/open?id=1o6f4kO1O2JP65-gCgfaxzo1N3zIM6YjK