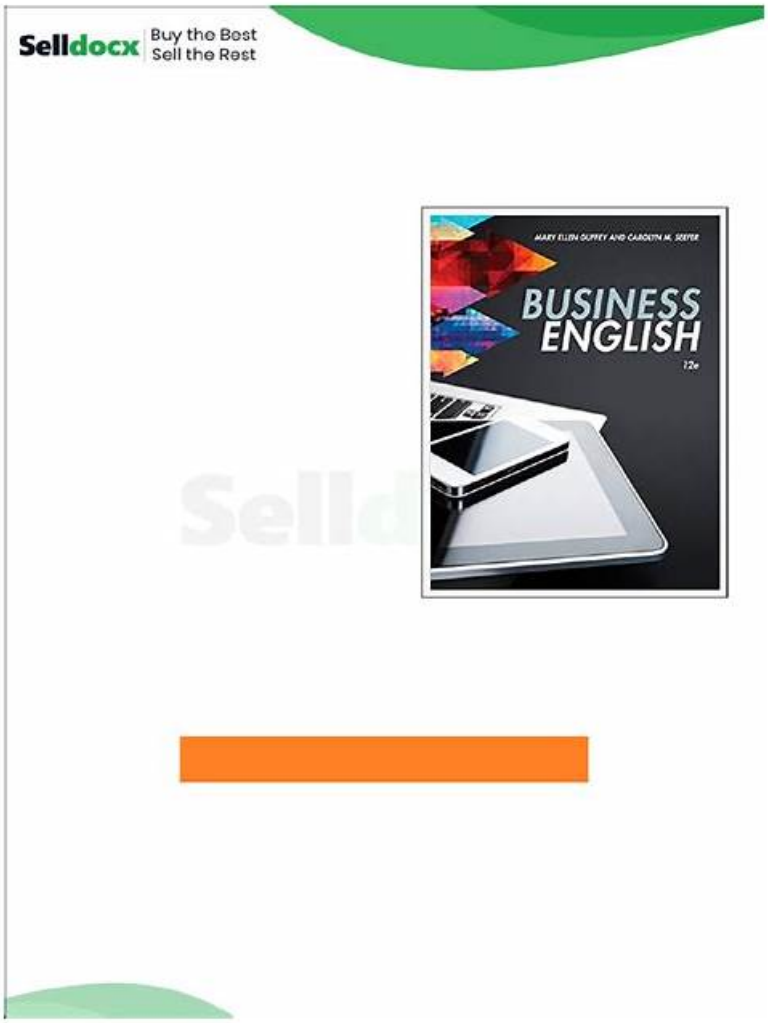
312-85 Latest Exam Testking | Printable 312-85 PDF



What's more, part of that Itexamguide 312-85 dumps now are free: https://drive.google.com/open?id=15ZUOAB9_m9gSj5GhxucLNPqU6fapG8S6

We have installed the most advanced operation system in our company which can assure you the fastest delivery speed, to be specific, you can get immediately our 312-85 training materials only within five to ten minutes after purchase after payment. At the same time, your personal information on our 312-85 Exam Questions will be encrypted automatically by our operation system as soon as you pressed the payment button, that is to say, there is really no need for you to worry about your personal information if you choose to buy the 312-85 exam practice from our company.

ECCouncil 312-85 Certification is highly valued in the cybersecurity industry and is recognized by employers worldwide. Certified Threat Intelligence Analyst certification is a testament to the candidate's skills and knowledge in the field of threat intelligence and can open up many career opportunities. Candidates who successfully pass the exam can expect to find employment in a variety of roles such as threat intelligence analyst, cybersecurity analyst, and security operations center analyst.

>> 312-85 Latest Exam Testking <<

Printable 312-85 PDF - 312-85 Valid Real Exam

As long as you follow the steps of our 312-85 quiz torrent, your mastery of knowledge will be very comprehensive and you will be very familiar with the knowledge points. This will help you pass the exam more smoothly. The 312-85 learning materials are of high quality, mainly reflected in the adoption rate. As for our 312-85 exam question, we guaranteed a higher passing rate than that of other agency. More importantly, we will promptly update our 312-85 Quiz torrent based on the progress of the letter and send it to you. 99% of people who use our 312-85 quiz torrent has passed the exam and successfully obtained their certificates, which

undoubtedly show that the passing rate of our 312-85 exam question is 99%. So our product is a good choice for you. Choose our 312-85 learning materials, you will gain a lot and lay a solid foundation for success.

ECCouncil 312-85: Certified Threat Intelligence Analyst is a highly sought-after certification for professionals in the cybersecurity industry. Certified Threat Intelligence Analyst certification is designed to equip individuals with the skills and knowledge necessary to identify and respond to threats in real-time. 312-85 Exam is tailored to test an individual's ability to analyze, interpret, and act upon threat intelligence data to protect their organization from potential cyber threats.

ECCouncil Certified Threat Intelligence Analyst Sample Questions (Q67-Q72):

NEW QUESTION # 67
Karry, a threat analyst at an XYZ organization, is performing threat intelligence analysis. During the data collection phase, he used a data collection method that involves no participants and is purely based on analysis and observation of activities and processes going on within the local boundaries of the organization.
Identify the type of data collection method used by Karry.

- A. Active data collection
- B. Raw data collection
- C. Exploited data collection
- D. Passive data collection

Answer: D

Explanation:
The described approach-non-intrusive observation without direct interaction or participants-matches the Passive Data Collection method.
Passive Data Collection involves monitoring and gathering data from systems, logs, and networks without actively probing or influencing them. It is commonly used within organizational boundaries to observe normal operations, network flows, and user behaviors.
Why the Other Options Are Incorrect:
* A. Exploited data collection: Involves data derived from external sources or compromised systems.
* B. Active data collection: Requires interaction with the environment, such as scanning or probing.
* C. Raw data collection: Refers to gathering unprocessed data, not necessarily passive.
Conclusion:
Karry used the Passive Data Collection method, which relies on observation and non-intrusive monitoring.
Final Answer: D. Passive data collection
Explanation Reference (Based on CTIA Study Concepts):
CTIA defines passive collection as observing and recording ongoing activities within an environment without direct engagement or disruption.

NEW QUESTION # 68
Jame, a professional hacker, is trying to hack the confidential information of a target organization. He identified the vulnerabilities in the target system and created a tailored deliverable malicious payload using an exploit and a backdoor to send it to the victim.
Which of the following phases of cyber kill chain methodology is Jame executing?

- A. Reconnaissance
- B. Exploitation
- C. Installation
- D. Weaponization

Answer: D

Explanation:
In the cyber kill chain methodology, the phase where Jame is creating a tailored malicious deliverable that includes an exploit and a backdoor is known as 'Weaponization'. During this phase, the attacker prepares by coupling a payload, such as a virus or worm, with an exploit into a deliverable format, intending to compromise the target's system. This step follows the initial 'Reconnaissance' phase, where the attacker gathers information on the target, and precedes the 'Delivery' phase, where the weaponized bundle is transmitted to the target. Weaponization involves the preparation of the malware to exploit the identified vulnerabilities in the target system.

References:
Lockheed Martin's Cyber Kill Chain framework
"Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," leading to the development of the Cyber Kill Chain framework

NEW QUESTION # 69
During the process of threat intelligence analysis, John, a threat analyst, successfully extracted an indication of adversary's information, such as Modus operandi, tools, communication channels, and forensics evasion strategies used by adversaries.
Identify the type of threat intelligence analysis is performed by John.

- A. Tactical threat intelligence analysis
- B. Operational threat intelligence analysis
- C. Strategic threat intelligence analysis
- D. Technical threat intelligence analysis

Answer: A

Explanation:
Tactical threat intelligence analysis focuses on the immediate, technical indicators of threats, such as the tactics, techniques, and procedures (TTPs) used by adversaries, their communication channels, the tools and software they utilize, and their strategies for evading forensic analysis. This type of analysis is crucial for operational defenses and is used by security teams to adjust their defenses against current threats. Since John successfully extracted information related to the adversaries' modus operandi, tools, communication channels, and evasion strategies, he is performing tactical threat intelligence analysis. This differs from strategic and operational threat intelligence, which focus on broader trends and specific operations, respectively, and from technical threat intelligence, which deals with technical indicators like malware signatures and IPs.
References:
"Tactical Cyber Intelligence," by Cyber Threat Intelligence Network, Inc.
"Intelligence-Driven Incident Response: Outwitting the Adversary," by Scott J. Roberts and Rebekah Brown

NEW QUESTION # 70
Bob, a threat analyst, works in an organization named TechTop. He was asked to collect intelligence to fulfil the needs and requirements of the Red Tam present within the organization.
Which of the following are the needs of a RedTeam?

- A. Intelligence related to increased attacks targeting a particular software or operating system vulnerability
- B. Intelligence that reveals risks related to various strategic business decisions
- C. Intelligence extracted latest attacks analysis on similar organizations, which includes details about latest threats and TTPs
- D. Intelligence on latest vulnerabilities, threat actors, and their tactics, techniques, and procedures (TTPs)

Answer: D

Explanation:
Red Teams are tasked with emulating potential adversaries to test and improve the security posture of an organization. They require intelligence on the latest vulnerabilities, threat actors, and their TTPs to simulate realistic attack scenarios and identify potential weaknesses in the organization's defenses. This information helps Red Teams in crafting their attack strategies to be as realistic and relevant as possible, thereby providing valuable insights into how actual attackers might exploit the organization's systems. This need contrasts with the requirements of other teams or roles within an organization, such as strategic decision-makers, who might be more interested in intelligence related to strategic risks or Blue Teams, which focus on defending against and responding to attacks.
References:
Red Team Field Manual (RTFM)
MITRE ATT&CK Framework for understanding threat actor TTPs

NEW QUESTION # 71
In which of the following storage architecture is the data stored in a localized system, server, or storage hardware and capable of storing a limited amount of data in its database and locally available for data usage?

- A. Distributed storage

- B. Object-based storage
- C. Cloud storage
- D. Centralized storage

Answer: D

Explanation:
Centralized storage architecture refers to a system where data is stored in a localized system, server, or storage hardware. This type of storage is capable of holding a limited amount of data in its database and is locally available for data usage. Centralized storage is commonly used in smaller organizations or specific departments within larger organizations where the volume of data is manageable and does not require the scalability offered by distributed or cloud storage solutions. Centralized storage systems simplify data management and access but might present challenges in terms of scalabilityand data recovery.References:
* "Data Storage Solutions for Your Business: Centralized vs. Decentralized," Techopedia
* "The Basics of Centralized Data Storage," by Margaret Rouse, SearchStorage

NEW QUESTION # 72
.....