100% Pass Latest CCOA - Valid ISACA Certified Cybersecurity Operations Analyst Exam Sims

BONUS!!! Download part of ExamDiscuss CCOA dumps for free: https://drive.google.com/open?id=1Xul4bDKIoo9wAT24SZSuKmRHrokD5Gc1

Advancement in CCOA information and communications technology generates huge potential for moving business and production up the value-chain, and improving the quality of life of citizens. And there is no doubt that you can get all kinds of information in cyber space now, CCOA latest torrent is not an exception. I strongly recommend the CCOA Study Materials compiled by our company for you, the advantages of our CCOA exam questions are too many to enumerate. And if you have a try on our CCOA exam questions, you will love to buy it.

Evaluate your own mistakes each time you attempt the desktop ISACA Certified Cybersecurity Operations Analyst (CCOA) practice exam. It expertly is designed CCOA practice test software supervised by a team of professionals. There is 24/7 customer service to help you in any situation. You can customize your desired CCOA Exam conditions like exam length and the number of questions.

>> Valid CCOA Exam Sims <<

ISACA CCOA Valid Exam Sims - CCOA Latest Study Plan

Compared to other products in the industry, our CCOA actual exam has a higher pass rate. If you really want to pass the exam, this must be the one that makes you feel the most suitable and effective. According the data which is provided and tested by our loyal customers, our pass rate of the CCOA Exam Questions is high as 98% to 100%. It is hard to find such high pass rate in the market. And the quality of the CCOA training guide won't let you down.

ISACA CCOA Exam Syllabus Topics:

Topic	Details

Topic 1	• Cybersecurity Principles and Risk: This section of the exam measures the skills of a Cybersecurity Specialist and covers core cybersecurity principles and risk management strategies. It includes assessing vulnerabilities, threat analysis, and understanding regulatory compliance frameworks. The section emphasizes evaluating risks and applying appropriate measures to mitigate potential threats to organizational assets.
Topic 2	• Technology Essentials: This section of the exam measures skills of a Cybersecurity Specialist and covers the foundational technologies and principles that form the backbone of cybersecurity. It includes topics like hardware and software configurations, network protocols, cloud infrastructure, and essential tools. The focus is on understanding the technical landscape and how these elements interconnect to ensure secure operations.
Topic 3	• Adversarial Tactics, Techniques, and Procedures: This section of the exam measures the skills of a Cybersecurity Analyst and covers the tactics, techniques, and procedures used by adversaries to compromise systems. It includes identifying methods of attack, such as phishing, malware, and social engineering, and understanding how these techniques can be detected and thwarted.
Topic 4	• Securing Assets: This section of the exam measures skills of a Cybersecurity Specialist and covers the methods and strategies used to secure organizational assets. It includes topics like endpoint security, data protection, encryption techniques, and securing network infrastructure. The goal is to ensure that sensitive information and resources are properly protected from external and internal threats.
Topic 5	• Incident Detection and Response: This section of the exam measures the skills of a Cybersecurity Analyst and focuses on detecting security incidents and responding appropriately. It includes understanding security monitoring tools, analyzing logs, and identifying indicators of compromise. The section emphasizes how to react to security breaches quickly and efficiently to minimize damage and restore operations.

ISACA Certified Cybersecurity Operations Analyst Sample Questions (Q62-Q67):

NEW QUESTION # 62
The network team has provided a PCAP file withsuspicious activity located in the Investigations folderon the Desktop titled, investigation22.pcap.
What date was the webshell accessed? Enter the formatas YYYY-MM-DD.

Answer:

Explanation:
See the solution in Explanation.
Explanation:
To determine thedate the webshell was accessedfrom theinvestigation22.pcapfile, follow these detailed steps:
Step 1: Access the PCAP File
* Log into the Analyst Desktop.
* Navigate to theInvestigationsfolder on the desktop.
* Locate the file:
investigation22.pcap
Step 2: Open the PCAP File in Wireshark
* LaunchWireshark.
* Open the PCAP file:
mathematica
File > Open > Desktop > Investigations > investigation22.pcap
* ClickOpento load the file.
Step 3: Filter for Webshell Traffic
* Since webshells typically useHTTP/Sto communicate, apply a filter:
http.request or http.response
* Alternatively, if you know the IP of the compromised host (e.g.,10.10.44.200), use:
nginx
http and ip.addr == 10.10.44.200

* PressEnterto apply the filter.
Step 4: Identify Webshell Activity
* Look for HTTP requests that include:
* Common Webshell Filenames:shell.jsp, cmd.php, backdoor.aspx, etc.
* Suspicious HTTP Methods:MainlyPOSTorGET.
* Right-click a suspicious packet and choose:
arduino
Follow > HTTP Stream
* Inspect the HTTP headers and content to confirm the presence of a webshell.
Step 5: Extract the Access Date
* Look at theHTTP request/response header.
* Find theDatefield orTimestampof the packet:
* Wireshark displays timestamps on the left by default.
* Confirm theHTTP streamincludes commands or uploads to the webshell.
Example HTTP Stream:
POST /uploads/shell.jsp HTTP/1.1
Host: 10.10.44.200
User-Agent: Mozilla/5.0
Date: Mon, 2024-03-18 14:35:22 GMT
Step 6: Verify the Correct Date
* Double-check other HTTP requests or responses related to the webshell.
* Make sure thedate fieldis consistent across multiple requests to the same file.
2024-03-18
Step 7: Document the Finding
* Date of Access:2024-03-18
* Filename:shell.jsp (as identified earlier)
* Compromised Host:10.10.44.200
* Method of Access:HTTP POST
Step 8: Next Steps
* Isolate the Affected Host:
* Remove the compromised server from the network.
* Remove the Webshell:
rm /path/to/webshell/shell.jsp
* Analyze Web Server Logs:
* Correlate timestamps with access logs to identify the initial compromise.
* Implement WAF Rules:
* Block suspicious patterns related to file uploads and webshell execution.

NEW QUESTION # 63
Which layer ofthe TCP/IP stack promotes the reliable transmission of data?

- A. Internet
- B. Link
- C. Application
- D. Transport

Answer: D

Explanation:
TheTransport layerof theTCP/IP stackis responsible for thereliable transmission of databetween hosts.
* Protocols:IncludesTCP (Transmission Control Protocol)andUDP (User Datagram Protocol).
* Reliable Data Delivery:TCP ensures data integrity and order through sequencing, error checking, and acknowledgment.
* Flow Control and Congestion Handling:Uses mechanisms likewindowingto manage data flow efficiently.
* Connection-Oriented Communication:Establishes a session between sender and receiver for reliable data transfer.
Other options analysis:
* A. Link:Deals with physical connectivity and media access.
* B. Internet:Handles logical addressing and routing.
* C. Application:Facilitates user interactions and application-specific protocols (like HTTP, FTP).
CCOA Official Review Manual, 1st Edition References:
* Chapter 4: Network Protocols and Layers:Details the role of the Transport layer in reliable data transmission.

* Chapter 6: TCP/IP Protocol Suite:Explains the functions of each layer.

NEW QUESTION # 64
Which of the following should be the ULTIMATE outcome of adopting enterprise governance of information and technology in cybersecurity?

- A. Value creation
- B. Resource optimization
- C. Risk optimization
- D. Business resilience

Answer: A

Explanation:
Theultimate outcome of adopting enterprise governance of information and technologyin cybersecurity is value creationbecause:
* Strategic Alignment:Ensures that cybersecurity initiatives support business objectives.
* Efficient Use of Resources:Enhances operational efficiency by integrating security practices seamlessly.
* Risk Optimization:Minimizes the risk impact on business operations while maintaining productivity.
* Business Enablement:Strengthens trust with stakeholders by demonstrating robust governance and security.
Other options analysis:
* A. Business resilience:Important, but resilience is part of value creation, not the sole outcome.
* B. Risk optimization:A component of governance but not the final goal.
* C. Resource optimization:Helps achieve value but is not the ultimate outcome.
CCOA Official Review Manual, 1st Edition References:
* Chapter 2: Cyber Governance and Strategy:Explains how value creation is the core goal of governance.
* Chapter 10: Strategic IT and Cybersecurity Alignment:Discusses balancing security with business value.

NEW QUESTION # 65
Which ofthe following is a type of middleware used to manage distributed transactions?

- A. Transaction processing monitor
- B. Remote procedure call
- C. Object request broker
- D. Message-oriented middleware

Answer: A

Explanation:
ATransaction Processing Monitor (TPM)is a type of middleware that manages and coordinates distributed transactions across multiple systems.
* Core Functionality:Ensures data consistency and integrity during complex transactions that span various databases or applications.
* Transactional Integrity:Provides rollback and commit capabilities in case of errors or failures.
* Common Use Cases:Banking systems, online booking platforms, and financial applications.
Incorrect Options:
* A. Message-oriented middleware:Primarily used for asynchronous message processing, not transaction management.
* C. Remote procedure call (RPC):Facilitates communication between systems but does not manage transactions.
* D. Object request broker:Manages object communication but lacks transaction processing capabilities.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 7, Section "Middleware Components," Subsection "Transaction Processing Middleware" - TPMs handle distributed transactions to ensure consistency across various systems.

NEW QUESTION # 66
Which of the following is a network port for service message block (SMS)?

- A. 0
- B. 1
- C. 2

- D. 3

Answer: D

Explanation:
Port445is used byServer Message Block (SMB)protocol:
* SMB Functionality:Allows file sharing, printer sharing, and access to network resources.
* Protocol:Operates over TCP, typically on Windows systems.
* Security Concerns:Often targeted for attacks like EternalBlue, which was exploited by the WannaCry ransomware.
* Common Vulnerabilities:SMBv1 is outdated and vulnerable; it is recommended to use SMBv2 or SMBv3.
Incorrect Options:
* B. 143:Used by IMAP for email retrieval.
* C. 389:Used by LDAP for directory services.
* D. 22:Used by SSH for secure remote access.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 5, Section "Common Network Ports and Services," Subsection "SMB and Network File Sharing" - Port 445 is commonly used for SMB file sharing on Windows networks.

NEW QUESTION # 67
.....

What's more, part of that ExamDiscuss CCOA dumps now are free: https://drive.google.com/open?id=1Xul4bDKIoo9wAT24SZSuKmRHrokD5Gc1