Up-To-Date And Verified ISACA CCOA Exam Questions For Preparation

BONUS!!! Download part of ExamsTorrent CCOA dumps for free: https://drive.google.com/open?id=1MyrjrNxK9XJb5ZOmiN4pGD_2kjbvdowF

You must hold an optimistic belief for your life. There always have solutions to the problems. We really hope that our CCOA study materials will greatly boost your confidence. In fact, many people are confused about their future and have no specific aims. Then our CCOA practice quiz can help you find your real interests. Just think about that you will get more oppotunities to bigger enterprise and better position in your career with the CCOA certification. It is quite encouraging!

ISACA CCOA Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• 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.

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	- 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.

>> CCOA Reliable Dump <<

Latest ISACA CCOA Exam Pattern & CCOA Online Training

Firstly, our company always feedbacks our candidates with highly-qualified CCOA study guide and technical excellence and continuously developing the most professional exam materials. Secondly, our CCOA study materials persist in creating a modern service oriented system and strive for providing more preferential activities for your convenience. Last but not least, we have free demos for your reference, as in the following, you can download which CCOA Exam Materials demo you like and make a choice. Therefore, you will love our CCOA study materials!

ISACA Certified Cybersecurity Operations Analyst Sample Questions (Q107-Q112):

NEW QUESTION # 107
Which type of access control can be modified by a user or data owner?

- A. Rule-based access control
- B. Role-based access control (RBAC)
- C. Discretionary access control
- D. Mandatory access control

Answer: C

Explanation:
Discretionary Access Control (DAC)allowsusers or data ownerstomodify access permissionsfor resources they own.
* Owner-Based Permissions:The resource owner decides who can access or modify the resource.
* Flexibility:Users cangrant, revoke, or change permissionsas needed.
* Common Implementation:File systems where owners set permissions for files and directories.
* Risk:Misconfigurations can lead to unauthorized access if not properly managed.
Other options analysis:
* A. Mandatory Access Control (MAC):Permissions are enforced by the system, not the user.
* B. Role-Based Access Control (RBAC):Access is based on roles, not user discretion.
* D. Rule-Based Access Control:Permissions are determined by predefined rules, not user control.
CCOA Official Review Manual, 1st Edition References:
* Chapter 7: Access Control Models:Clearly distinguishes DAC from other access control methods.
* Chapter 9: Secure Access Management:Explains how DAC is implemented and managed.

NEW QUESTION # 108
Which of the following is a network port for service message block (SMS)?

- A. 0
- B. 1
- C. 2
- D. 3

Answer: C

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 # 109
The network team has provided a PCAP file withsuspicious activity located in the Investigations folderon the Desktop titled, investigation22.pcap.
What is the filename of the webshell used to control thehost 10.10.44.200? Your response must include the fileextension.

Answer:

Explanation:
See the solution in Explanation.
Explanation:
To identify thefilename of the webshellused to control the host10.10.44.200from the provided PCAP file, follow these detailed steps:
Step 1: Access the PCAP File
* Log into theAnalyst Desktop.
* Navigate to theInvestigationsfolder located on the desktop.
* Locate the file:
investigation22.pcap
Step 2: Open the PCAP File in Wireshark
* LaunchWiresharkon the Analyst Desktop.
* Open the PCAP file:
mathematica
File > Open > Desktop > Investigations > investigation22.pcap
* ClickOpento load the file.
Step 3: Filter Traffic Related to the Target Host
* Apply a filter to display only the traffic involving thetarget IP address (10.10.44.200):
ini
ip.addr == 10.10.44.200
* This will show both incoming and outgoing traffic from the compromised host.
Step 4: Identify HTTP Traffic
* Since webshells typically use HTTP/S for communication, filter for HTTP requests:
http.request and ip.addr == 10.10.44.200
* Look for suspiciousPOSTorGETrequests indicating a webshell interaction.
Common Indicators:
* Unusual URLs:Containing scripts like cmd.php, shell.jsp, upload.asp, etc.
* POST Data:Indicating command execution.
* Response Status:HTTP 200 (Success) after sending commands.
Step 5: Inspect Suspicious Requests
* Right-click on a suspicious HTTP packet and select:
arduino
Follow > HTTP Stream
* Examine the HTTP conversation for:
* File uploads
* Command execution responses
* Webshell file namesin the URL.
Example:
makefile

```
POST /uploads/shell.jsp HTTP/1.1
Host: 10.10.44.200
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
```

Step 6: Correlate Observations

* If you identify a script like shell.jsp, verify it by checking multiple HTTP streams.
* Look for:
* Commands sent via the script.
* Response indicating successful execution or error.

Step 7: Extract and Confirm

* To confirm the filename, look for:
* Upload requests containing the webshell.
* Subsequent requests calling the same filename for command execution.
* Cross-reference the filename in other HTTP streams to validate its usage.

Step 8: Example Findings:

After analyzing the HTTP streams and reviewing requests to the host 10.10.44.200, you observe that the webshell file being used is:

shell.jsp

Final Answer:

shell.jsp

Step 9: Further Investigation

* Extract the Webshell:
* Right-click the related packet and choose:

mathematica

Export Objects > HTTP

* Save the file shell.jsp for further analysis.
* Analyze the Webshell:
* Open the file with a text editor to examine its functionality.
* Check for hardcoded credentials, IP addresses, or additional payloads.

Step 10: Documentation and Response

* Document Findings:
* Webshell Filename:shell.jsp
* Host Compromised:10.10.44.200
* Indicators:HTTP POST requests, suspicious file upload.
* Immediate Actions:
* Isolate the host10.10.44.200.
* Remove the webshell from the web server.
* Conduct aroot cause analysisto determine how it was uploaded.

NEW QUESTION # 110

A bank employee is found to beexfiltrationsensitive information by uploading it via email. Which of the following security measures would be MOST effective in detecting this type of insider threat?

- A. Intrusion detection system (IDS)
- B. Data loss prevention (DIP)
- C. Network segmentation
- D. Security information and event management (SIEM)

Answer: B

Explanation:

Data Loss Prevention (DLP) systems are specifically designed to detect and prevent unauthorized data transfers. In the context of an insider threat, where a bank employee attempts toexfiltrate sensitive information via email, DLP solutions are most effective because they:

* Monitor Data in Motion:DLP can inspect outgoing emails for sensitive content based on pre-defined rules and policies.
* Content Inspection and Filtering:It examines email attachments and the body of the message for patterns that match sensitive data (like financial records or PII).
* Real-Time Alerts:Generates alerts or blocks the transfer when sensitive data is detected.
* Granular Policies:Allows customization to restrict specific types of data transfers, including via email.

Other options analysis:

* B. Intrusion detection system (IDS):IDS monitors network traffic for signs of compromise but is not designed to inspect email

content or detect data exfiltration specifically.
* C. Network segmentation:Reduces the risk of lateral movement but does not directly monitor or prevent data exfiltration through email.
* D. Security information and event management (SIEM):SIEM can correlate events and detect anomalies but lacks the real-time data inspection that DLP offers.
CCOA Official Review Manual, 1st Edition References:
* Chapter 5: Insider Threats and Mitigation:Discusses how DLP tools are essential for detecting data exfiltration.
* Chapter 6: Threat Intelligence and Analysis:Covers data loss scenarios and the role of DLP.
* Chapter 8: Incident Detection and Response:Explains the use of DLP for detecting insider threats.

NEW QUESTION # 111

Which of the following has been defined when a disaster recovery plan (DRP) requires daily backups?

- A. Maximum tolerable downtime (MTD)
- B. Mean time to failure (MTTF)
- C. Recovery time objective (RTO|
- D. Recovery point objective {RPO)

Answer: D

Explanation:
TheRecovery Point Objective (RPO)defines themaximum acceptable amount of data lossmeasured in time before a disaster occurs.
* Daily Backups:If the DRP requiresdaily backups, the RPO is effectively set at24 hours, meaning the organization can tolerate up to one day of data loss.
* Data Preservation:Ensures that the system can recover data up to the last backup point.
* Business Continuity Planning:Helps determine how often data backups need to be performed to minimize loss.
Other options analysis:
* A. Maximum tolerable downtime (MTD):Refers to the total time a system can be down before significant impact.
* B. Recovery time objective (RTO):Defines the time needed to restore operations after an incident.
* D. Mean time to failure (MTTF):Indicates the average time a system operates before failing.
CCOA Official Review Manual, 1st Edition References:
* Chapter 5: Business Continuity and Disaster Recovery:Defines RPO and its importance in data backup strategies.
* Chapter 7: Risk Management:Discusses RPO as a key metric in disaster recovery planning.

NEW QUESTION # 112

......

To some extent, to pass the CCOA exam means that you can get a good job. The CCOA exam materials you master will be applied to your job. The possibility to enter in big and famous companies is also raised because they need outstanding talents to serve for them. Our CCOA Test Prep is compiled elaborately and will help the client a lot. Our product is of high quality and the passing rate and the hit rate are both high.

Latest CCOA Exam Pattern: https://www.examstorrent.com/CCOA-exam-dumps-torrent.html

- ISACA CCOA Dumps PDF To Gain Brilliant Result (2026) □ Download □ CCOA □ for free by simply searching on ▶ www.examcollectionpass.com ◀ □Exam CCOA Bible
- New CCOA Test Duration □ CCOA Valid Exam Question □ CCOA Valid Test Pattern □ Simply search for ▶ CCOA ◀ for free download on 「 www.pdfvce.com 」 □Valid CCOA Test Papers
- www.dumpsquestion.com ISACA CCOA Dumps PDF □ Search on ⇛ www.dumpsquestion.com ⇚ for ✔ CCOA □✔□ to obtain exam materials for free download □CCOA Test Sample Questions
- 100% Pass Quiz 2026 CCOA: Valid ISACA Certified Cybersecurity Operations Analyst Reliable Dump □ Download ➠ CCOA □ for free by simply searching on □ www.pdfvce.com □ □CCOA Valid Exam Question
- CCOA Exam Pass4sure ☢ Exam CCOA Bible □ Exam CCOA Bible □ Open □ www.practicevce.com □ and search for ➥ CCOA □ to download exam materials for free □CCOA Test Sample Questions
- CCOA Test Sample Questions □ CCOA Pdf Format □ CCOA Exam Pass4sure □ Open □ www.pdfvce.com □ and search for □ CCOA □ to download exam materials for free □Latest Braindumps CCOA Ebook
- Free PDF Quiz 2026 ISACA High-quality CCOA: ISACA Certified Cybersecurity Operations Analyst Reliable Dump □ Download ➠ CCOA □ for free by simply searching on 【 www.troytecdumps.com 】 □CCOA Pdf Format
- CCOA Best Preparation Materials □ Vce CCOA Free □ CCOA Exam Passing Score □ Search for ▶ CCOA ◀ and

download it for free immediately on [www.pdfvce.com] □CCOA Exam Pass4sure

- Latest updated CCOA Reliable Dump - The Best Assstant to help you pass CCOA: ISACA Certified Cybersecurity Operations Analyst □ Download ➡ CCOA □□□ for free by simply entering □ www.exam4labs.com □ website □ □Exam CCOA Bible
- CCOA Exam Passing Score □ CCOA Latest Braindumps Questions □ CCOA Best Preparation Materials □ Download 《 CCOA 》 for free by simply searching on 《 www.pdfvce.com 》 □CCOA Exam Passing Score
- Three Top ISACA CCOA Dumps Formats □ Search for （ CCOA ） and obtain a free download on □ www.testkingpass.com □ □Certification CCOA Questions
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 202.53.128.110, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, lms.ait.edu.za, Disposable vapes

What's more, part of that ExamsTorrent CCOA dumps now are free: https://drive.google.com/open?id=1MyrjrNxK9XJb5ZOmiN4pGD_2kjbvdowF