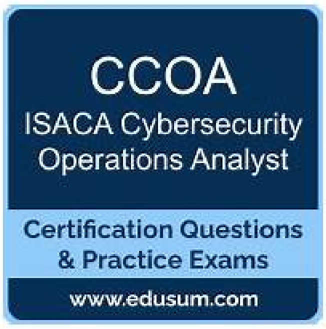
CCOA Test Vce - CCOA Real Question


CCOA
ISACA Cybersecurity Operations Analyst
Certification Questions & Practice Exams
www.edusum.com

P.S. Free 2025 ISACA CCOA dumps are available on Google Drive shared by PassLeaderVCE: https://drive.google.com/open?id=1XCUAZIafy_5EzsyY-SowjzfBMVQv_BNW

Our CCOA exam questions are designed from the customer's perspective, and experts that we employed will update our CCOA learning materials according to changing trends to ensure the high quality of the CCOA practice materials. What are you still waiting for? Choosing our CCOA guide questions and work for getting the certificate, you will make your life more colorful and successful.

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	• 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 3	• 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 4	• 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 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.

>> CCOA Test Vce <<

Trust CCOA Test Vce, Pass The ISACA Certified Cybersecurity Operations Analyst

PassLeaderVCE is professional platform to establish for compiling ISACA exam materials for candidates, and we aim to help you to pass the examination as well as getting the related certification in a more efficient and easier way. Our answers and questions are compiled elaborately and easy to be mastered. Because our CCOA Test Braindumps are highly efficient and the passing rate is very high you can pass the exam fluently and easily with little time and energy needed.

ISACA Certified Cybersecurity Operations Analyst Sample Questions (Q41-Q46):

NEW QUESTION # 41
Which of the following services would pose the GREATEST risk when used to permit access to and from the Internet?

- A. Server Message Block (5MB) on TCP 445
- B. Remote Desktop Protocol (RDP) on TCP 3389
- C. Domain Name Service (DNS) on UOP 53
- D. File Transfer Protocol(FTP) on TCP 21

Answer: B

Explanation:
Remote Desktop Protocol (RDP)poses the greatest risk when exposed to the internet because:
* Common Attack Vector:Frequently targeted in brute-force attacks and ransomware campaigns.
* Privilege Escalation:If compromised, attackers can gain full control of the target system.
* Vulnerability History:RDP services have been exploited in numerous attacks (e.g., BlueKeep).
* Exploitation Risk:Directly exposing RDP to the internet without proper safeguards (like VPNs or MFA) is extremely risky.
Incorrect Options:
* A. SMB on TCP 445:Risky, but usually confined to internal networks.
* B. FTP on TCP 21:Unencrypted but less risky compared to RDP for remote control.
* C. DNS on UDP 53:Used for name resolution; rarely exploited for direct system access.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 5, Section "Remote Access Security," Subsection "RDP Risks" - Exposing RDP to the internet presents a critical security risk due to its susceptibility to brute-force and exploitation attacks.

NEW QUESTION # 42
Which of the following is foundational for implementing a Zero Trust model?

- A. Robust network monitoring
- B. Comprehensive process documentation
- C. Identity and access management (IAM) controls
- D. Routine vulnerability and penetration testing

Answer: C

Explanation:
Implementing aZero Trust modelfundamentally requires robustIdentity and Access Management (IAM) controls because:
* Zero Trust Principles:Never trust, always verify; enforce least privilege.
* Identity-Centric Security:Strong IAM practices ensure that only authenticated and authorized users can access resources.
* Multi-Factor Authentication (MFA):Verifying user identities at each access point.
* Granular Access Control:Assigning minimal necessary privileges based on verified identity.
* Continuous Monitoring:Continuously assessing user behavior and access patterns.
Other options analysis:
* A. Comprehensive process documentation:Helpful but not foundational for Zero Trust.
* B. Robust network monitoring:Supports Zero Trust but is not the core principle.
* C. Routine vulnerability and penetration testing:Important for security but not specifically for Zero Trust.
CCOA Official Review Manual, 1st Edition References:
* Chapter 7: Access Control and Identity Management:Emphasizes the role of IAM in Zero Trust architecture.
* Chapter 10: Secure Network Architecture:Discusses how Zero Trust integrates IAM.

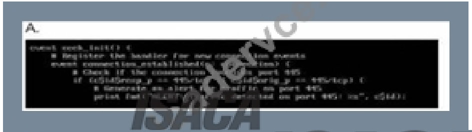
NEW QUESTION # 43
Which of the following controls would BEST prevent an attacker from accessing sensitive data from files or disk images that have been obtained either physically or via the network?

- A. Endpoint detection and response (EOR)
- B. Next generation antivirus
- C. Data loss prevention (DLP)
- D. Encryption of data at rest

Answer: D

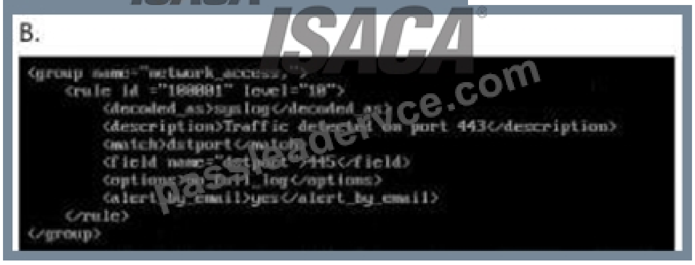
Explanation:
Encryption of data at restis the best control to protectsensitive data from unauthorized access, even if physical or network access to the disk or file is obtained.
* Protection:Data remains unreadable without the proper encryption keys.
* Scenarios:Protects data from theft due to lost devices or compromised servers.
* Compliance:Often mandated by regulations (e.g., GDPR, HIPAA).
Incorrect Options:
* A. Next-generation antivirus:Detects malware, not data protection.
* B. Data loss prevention (DLP):Prevents data exfiltration but does not protect data at rest.
* C. Endpoint detection and response (EDR):Monitors suspicious activity but does not secure stored data.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 6, Section "Data Security Strategies," Subsection "Encryption Techniques" - Encryption of data at rest is essential for protecting sensitive information.

NEW QUESTION # 44
Which ruleset can be applied in the /home/administrator/hids/ruleset/rules directory?
Double-click each image to view it larger.



A.

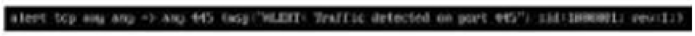
```
event zeek_init() {
    # Register the handler for new connection events
    event connection_established(c: connection) {
        # Check if the connection is to port 445
        if (c$id$resp_p == 445/tcp || c$id$orig_p == 445/tcp) {
            # Generate an alert for traffic on port 445
            print fmt("ALERT: Traffic detected on port 445: %s", c$id);
```



B.

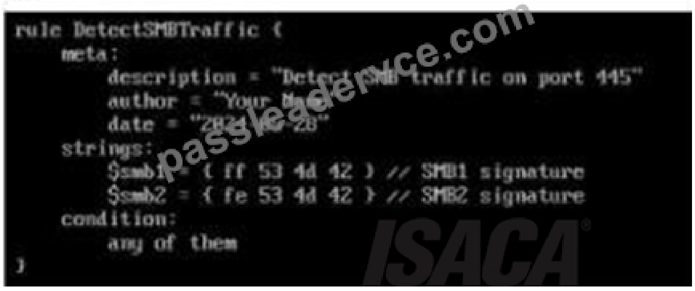
```
<group name="network_access,">
    <rule id ="100001" level="10">
        <decoded_as>syslog</decoded_as>
        <description>Traffic detected on port 443</description>
        <match>dstport</match>
        <field name="dstport">445</field>
        <options>no_full_log</options>
        <alert_by_email>yes</alert_by_email>
    </rule>
</group>
```

C.



```
alert tcp any any -> any 445 (msg:"ALERT: Traffic detected on port 445"; sid:1000001; rev:1;)
```

D.



```
rule DetectSMBTraffic {
    meta:
        description = "Detect SMB traffic on port 445"
        author = "Your Name"
        date = "2024-[illegible]-28"
    strings:
        $smb1 = { ff 53 4d 42 } // SMB1 signature
        $smb2 = { fe 53 4d 42 } // SMB2 signature
    condition:
        any of them
}
```

- A. Option A
- B. Option C
- C. Option B
- D. Option D

Answer: C

Explanation:
Step 1: Understand the Question Context
The question is asking whichruleset can be appliedin the following directory:
/home/administrator/hids/ruleset/rules
This is typically the directory forHost Intrusion Detection System (HIDS)rulesets.
Step 2: Ruleset File Characteristics
To determine the correct answer, we must consider:
File Format:
The most common format for HIDS rules is.rules.
Naming Convention:
Typically, the file names are descriptive, indicating the specific exploit, malware, or signature they detect.
Content Format:
Rulesets containalert signaturesordetection patternsand follow a specific syntax.
Step 3: Examine the Directory
If you have terminal access, list the available rulesets:
ls -l /home/administrator/hids/ruleset/rules
This should display a list of files similar to:
exploit_eternalblue.rules
malware_detection.rules
network_intrusion.rules
default.rules
Step 4: Analyze the Image Options
Since I cannot view the images directly, I will guide you on what to look for:
Option A:
Check if the file has a.rulesextension.
Look for keywords like"exploit","intrusion", or"malware".
Option B:
Verify if it mentionsEternalBlue,SMB, or other exploits.
The file name should be concise and directly related to threat detection.
Option C:
Look for generic names like"default.rules"or"base.rules".
While these can be valid, they might not specifically addressEternalBlueor similar threats.
Option D:
Avoid files with non-standard extensions (e.g., .conf, .txt).
Rulesets must specifically have.rulesas the extension.
Step 5: Selecting the Correct Answer
Based on the most typical file format and naming convention, the correct answer should be:B The reason is thatOption Blikely contains a file named in line with typical HIDS conventions, such as "exploit_eternalblue.rules"or similar, which matches the context given.
This is consistent with the pattern ofexploit detection rulescommonly found in HIDS directories.

NEW QUESTION # 45
A cybersecurity analyst has discovered a vulnerability in an organization's web application. Which ofthe following should be done FIRST to address this vulnerability?

- A. Immediately shut down the web application to prevent exploitation.
- B. Restart the web server hosting the web application.
- C. Attempt to exploit the vulnerability to determine its severity.
- D. Follow the organization's incident response management procedures.

Answer: D

Explanation:
When a cybersecurity analyst discovers a vulnerability, thefirst stepis to follow theorganization's incident response procedures.
* Consistency:Ensures that the vulnerability is handled systematically and consistently.
* Risk Mitigation:Prevents hasty actions that could disrupt services or result in data loss.
* Documentation:Helps record the discovery, assessment, and remediation steps for future reference.
* Coordination:Involves relevant stakeholders, including IT, security teams, and management.
Incorrect Options:
* A. Restart the web server:May cause service disruption and does not address the root cause.
* B. Shut down the application:Premature without assessing the severity and impact.
* D. Attempt to exploit the vulnerability:This should be part of the risk assessment after following the response protocol.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 6, Section "Incident Response and Management," Subsection "Initial Response Procedures" - Follow established protocols to ensure controlled and coordinated action.

NEW QUESTION # 46
......

Our ISACA Certified Cybersecurity Operations Analyst (CCOA) practice exam can be modified in terms of length of time and number of questions to help you prepare for the ISACA real test. We're certain that our CCOA Questions are quite similar to those on CCOA real exam since we regularly update and refine the product based on the latest exam content.

CCOA Real Question: https://www.passleadervce.com/Cybersecurity-Audit/reliable-CCOA-exam-learning-guide.html

- Reliable CCOA Braindumps Ebook □ Practice CCOA Exam Fee □ Hot CCOA Spot Questions □ Easily obtain free download of 【 CCOA 】 by searching on { www.exam4labs.com } □CCOA Reliable Exam Topics
- Quiz 2026 CCOA: Fantastic ISACA Certified Cybersecurity Operations Analyst Test Vce □ Download ➡ CCOA □□□ for free by simply entering □ www.pdfvce.com □ website □CCOA Exam Passing Score
- CCOA Exam Tests □ Composite Test CCOA Price □ Certification CCOA Cost □ Immediately open ▸ www.vce4dumps.com ◂ and search for □ CCOA □ to obtain a free download □CCOA Test Pdf
- CCOA Reliable Exam Cram □ CCOA Exam Passing Score □ CCOA Study Tool □ Open website ➤ www.pdfvce.com □ and search for ➡ CCOA □□□ for free download □CCOA Test Pdf
- Avail Reliable CCOA Test Vce to Pass CCOA on the First Attempt □ Search on 「 www.troytecdumps.com 」 for ➽ CCOA □ to obtain exam materials for free download □Composite Test CCOA Price
- CCOA Exam Tests □ CCOA Test Pdf □ Reliable CCOA Braindumps Ebook □ Open 【 www.pdfvce.com 】 and search for ▸ CCOA ◂ to download exam materials for free □New CCOA Cram Materials
- Valid ISACA CCOA Exam Question Free Updates For 1 year □ Go to website ⇒ www.testkingpass.com ⇐ open and search for ▹ CCOA ◃ to download for free □CCOA Study Tool
- CCOA Guide Braindumps Is Typically Beneficial for CCOA Exam - Pdfvce □ Enter □ www.pdfvce.com □ and search for □ CCOA □ to download for free □Practice CCOA Exam Fee
- CCOA Actual Test □ New CCOA Cram Materials □ Composite Test CCOA Price □ Search on ➤ www.prepawayexam.com □ for 【 CCOA 】 to obtain exam materials for free download □CCOA Latest Test Question
- Testking CCOA Exam Questions □ Reliable CCOA Braindumps Ebook □ CCOA Reliable Exam Topics □ Easily obtain free download of ➡ CCOA □□□ by searching on ➤ www.pdfvce.com □ □CCOA Actual Test
- CCOA Latest Test Answers □ CCOA Reliable Exam Topics □ CCOA Reliable Exam Online □ Copy URL ⇒ www.examcollectionpass.com ⇐ open and search for （ CCOA ） to download for free □CCOA Reliable Exam Topics
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, lms.ait.edu.za, 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, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt,