ISACA CCOA Learning Mode & CCOA Reliable Exam Cram

2025 Latest NewPassLeader CCOA PDF Dumps and CCOA Exam Engine Free Share: https://drive.google.com/open?id=1Bn4yd80mBEEZlmOv9L0pN3qmya-fpbo4

We offer you CCOA study guide with questions and answers, and you can practice it by concealing the answers, and when you have finished practicing, you can cancel the concealment, through the way like this, you can know the deficient knowledge for CCOA exam dumps, so that you can put your attention to the disadvantages. In addition, we also have the free demo for CCOA Study Guide for you to have a try in our website. These free demos will give you a reference of showing the mode of the complete version. If you want CCOA exam dumps, just add them into your card.

We have three versions for your practice according to your study habit. The pdf version is for you to print the CCOA Dump pdf out and you can share your CCOA exam dumps with your friends and classmates. The test engine version enables you feeling the atmosphere of formal test because it is a simulation of real test. The soft version is same as the test engine but it allows you to practice your Cybersecurity Audit real dumps in any electronic equipment.

>> ISACA CCOA Learning Mode <<

Effective CCOA Learning Mode & Leader in Qualification Exams & High-quality CCOA Reliable Exam Cram

If you are worried about your CCOA practice test and you have no much time to prepare, now you can completely rest assured it because we will offer you the most updated CCOA dumps pdf with 100% correct answers. You can save your time and money by enjoying one-year free update after purchasing our CCOA Dumps PDF. We also provide the free demo for your reference.

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	• 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	• 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 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.

ISACA Certified Cybersecurity Operations Analyst Sample Questions (Q97-Q102):

NEW QUESTION # 97
Which of the following BEST offers data encryption, authentication, and integrity of data flowing between a server and the client?

- A. Secure Sockets Layer (SSL)
- B. Transport Layer Security (TLS)
- C. Kerbcros
- D. Simple Network Management Protocol (SNMP)

Answer: B

Explanation:
Transport Layer Security (TLS)provides:
* Data Encryption:Ensures that the data transferred between the client and server is encrypted, preventing eavesdropping.
* Authentication:Verifies the identity of the server (and optionally the client) through digital certificates.
* Data Integrity:Detects any tampering with the transmitted data through cryptographic hash functions.
* Successor to SSL:TLS has largely replaced SSL due to better security protocols.
Incorrect Options:
* A. Secure Sockets Layer (SSL):Deprecated in favor of TLS.
* B. Kerberos:Primarily an authentication protocol, not used for data encryption in transit.
* D. Simple Network Management Protocol (SNMP):Used for network management, not secure data transmission.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 5, Section "Encryption Protocols," Subsection "TLS" - TLS is the recommended protocol for secure communication between clients and servers.

NEW QUESTION # 98
Which of the following services would pose the GREATEST risk when used to permit access to and from the Internet?

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

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 # 99
The user of the Accounting workstation reported thattheir calculator repeatedly opens without their input.
The following credentials are used for thisquestion.
Username:Accounting
Password:1x-4cc0unt1NG-x1
Using the provided credentials, SSH to the Accountingworkstation and generate a SHA256 checksum of the filethat triggered RuleName Suspicious PowerShell usingeither certutil or Get-FileHash of the file causing theissue. Copy the hash and paste it below.

Answer:

Explanation:
See the solution in Explanation.
Explanation:
To generate theSHA256 checksumof the file that triggeredRuleName: Suspicious PowerShellon the Accounting workstation, follow these detailed steps:
Step 1: Establish an SSH Connection
* Open a terminal on your system.
* Use the provided credentials to connect to theAccounting workstation:
ssh Accounting@<Accounting_PC_IP>
* Replace <Accounting_PC_IP> with the actual IP address of the workstation.
* Enter the password when prompted:
1x-4cc0unt1NG-x1
Step 2: Locate the Malicious File
* Navigate to the typical directory where suspicious scripts are stored:
cd C:\Users\Accounting\AppData\Roaming
* List the contents to identify the suspicious file:
dir
* Look for a file related toPowerShell(e.g., calc.ps1), as the issue involved thecalculator opening repeatedly.
Step 3: Verify the Malicious File
* To ensure it is the problematic file, check for recent modifications:
powershell
Get-ChildItem -Path "C:\Users\Accounting\AppData\Roaming" -Recurse | Where-Object { $_.LastWriteTime
-ge (Get-Date).AddDays(-1) }
* This will list files modified within the last 24 hours.
* Check file properties:
powershell
Get-Item "C:\Users\Accounting\AppData\Roaming\calc.ps1" | Format-List *
* Confirm it matches the file flagged byRuleName: Suspicious PowerShell.
Step 4: Generate the SHA256 Checksum

Method 1: Using PowerShell (Recommended)
* Run the following command to generate the hash:
powershell
Get-FileHash "C:\Users\Accounting\AppData\Roaming\calc.ps1" -Algorithm SHA256
* Output Example:
mathematica
Algorithm Hash Path
--------- ---- ----
SHA256 d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d C:
\Users\Accounting\AppData\Roaming\calc.ps1
Method 2: Using certutil (Alternative)
* Run the following command:
cmd
certutil -hashfile "C:\Users\Accounting\AppData\Roaming\calc.ps1" SHA256
* Example Output:
SHA256 hash of calc.ps1:
d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d
CertUtil: -hashfile command completed successfully.
Step 5: Copy and Paste the Hash
* Copy theSHA256 hashfrom the output and paste it as required.
Final Answer:
nginx
d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d
Step 6: Immediate Actions
* Terminate the Malicious Process:
powershell
Stop-Process -Name "powershell" -Force
* Delete the Malicious File:
powershell
Remove-Item "C:\Users\Accounting\AppData\Roaming\calc.ps1" -Force
* Disable Startup Entry:
* Check for any persistent scripts:
powershell
Get-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run"
* Remove any entries related to calc.ps1.
Step 7: Document the Incident
* Record the following:
* Filename:calc.ps1
* File Path:C:\Users\Accounting\AppData\Roaming\
* SHA256 Hash:d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d
* Date of Detection:(Today's date)

NEW QUESTION # 100
Which layer ofthe TCP/IP stack promotes the reliable transmission of data?

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

Answer: C

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 # 101
Which of the following is the PRIMARY benefit of a cybersecurity risk management program?

- A. implementation of effective controls
- B. Identification of data protection processes
- C. Reduction of compliance requirements
- D. Alignment with Industry standards

Answer: A

Explanation:
The primary benefit of a cybersecurity risk management program is theimplementation of effective controls to reduce the risk of cyber threats and vulnerabilities.
* Risk Identification and Assessment:The program identifies risks to the organization, including threats and vulnerabilities.
* Control Implementation:Based on the identified risks, appropriate security controls are put in place to mitigate them.
* Ongoing Monitoring:Ensures that implemented controls remain effective and adapt to evolving threats.
* Strategic Alignment:Helps align cybersecurity practices with organizational objectives and risk tolerance.
Incorrect Options:
* A. Identification of data protection processes:While important, it is a secondary outcome.
* B. Reduction of compliance requirements:A risk management program does not inherently reduce compliance needs.
* C. Alignment with Industry standards:This is a potential benefit but not the primary one.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 1, Section "Risk Management and Security Programs" - Effective risk management leads to the development and implementation of robust controls tailored to identified risks.

NEW QUESTION # 102
.....

The language in our ISACA CCOA test guide is easy to understand that will make any learner without any learning disabilities, whether you are a student or a in-service staff, whether you are a novice or an experienced staff who has abundant experience for many years. It should be a great wonderful idea to choose our CCOA Guide Torrent for sailing through the difficult test.

】 is best website to obtain 「 CCOA 」 for free download □CCOA Exam Practice

- CCOA Reliable Exam Questions □ CCOA Test Prep □ CCOA Regualer Update □ Immediately open [www.exam4pdf.com] and search for 「 CCOA 」 to obtain a free download □CCOA Free Download
- thevinegracecoach.com, bbs.naxshi.com, training.lightoftruthcenter.org, www.52suda.com, 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, shortcourses.russellcollege.edu.au, 58laoxiang.com, 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, Disposable vapes

P.S. Free & New CCOA dumps are available on Google Drive shared by NewPassLeader: https://drive.google.com/open?id=1Bn4yd80mBEEZlmOv9L0pN3qmya-fpbo4