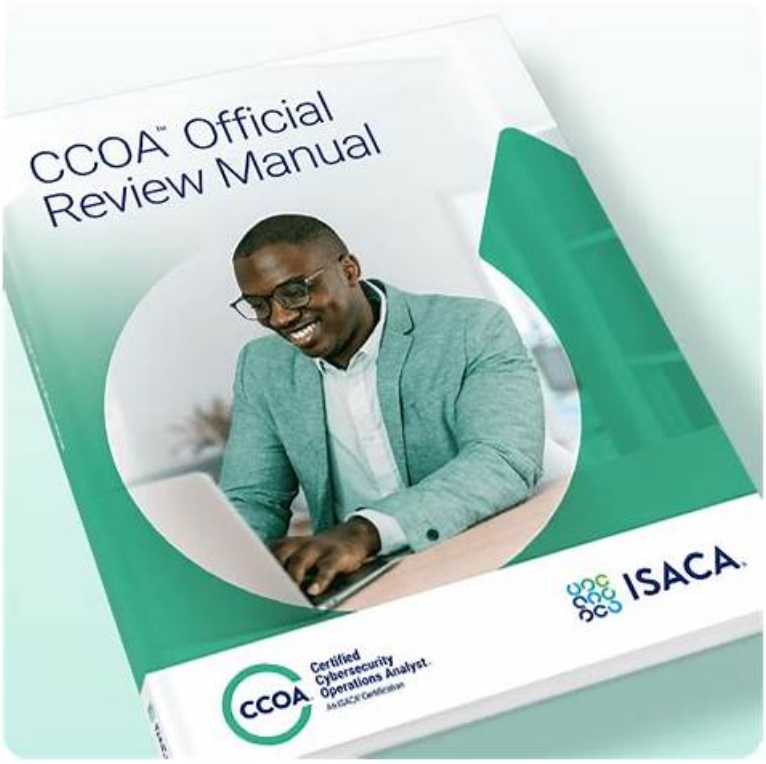
ISACA CCOA PDF Guide | CCOA Demo Test



What's more, part of that Pass4SureQuiz CCOA dumps now are free: https://drive.google.com/open?id=1dV8fosIo_cWNH0RBrA9te2Dt26OMTtOI

We provide 3 versions of our CCOA exam torrent and they include PDF version, PC version, APP online version. Each version's functions and using method are different and you can choose the most convenient version which is suitable for your practical situation. For example, the PDF version is convenient for you to download and print our CCOA Test Torrent and is suitable for browsing learning. If you use the PDF version you can print our CCOA guide torrent on the papers. The PC version of our CCOA exam questions can stimulate the real exam's environment.

ISACA CCOA Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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.

CCOA Demo Test, Test CCOA Simulator

Which kind of CCOA certificate is most authorized, efficient and useful? We recommend you the CCOA certificate because it can prove that you are competent in some area and boost outstanding abilities. If you buy our CCOA Study Materials you will pass the test smoothly and easily. We boost professional expert team to organize and compile the CCOA training guide diligently and provide the great service.

ISACA Certified Cybersecurity Operations Analyst Sample Questions (Q110-Q115):

NEW QUESTION # 110
Which of the following is the MOST effective method for identifying vulnerabilities in a remote web application?

- A. Source code review
- B. Dynamic application security testing (DA5T)
- C. Penetration testing
- D. Static application security testing (SAST)

Answer: C

Explanation:
The most effective method for identifying vulnerabilities in aremote web applicationispenetration testing.
* Realistic Simulation:Penetration testing simulates real-world attack scenarios to find vulnerabilities.
* Dynamic Testing:Actively exploits potential weaknesses rather than just identifying them statically.
* Comprehensive Coverage:Tests the application from an external attacker's perspective, including authentication bypass, input validation flaws, and configuration issues.
* Manual Validation:Can verify exploitability, unlike automated tools.
Incorrect Options:
* A. Source code review:Effective but only finds issues in the code, not in the live environment.
* B. Dynamic application security testing (DAST):Useful but more automated and less thorough than penetration testing.
* D. Static application security testing (SAST):Focuses on source code analysis, not the deployed application.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 6, Section "Application Security Testing Methods" - Penetration testing is crucial for identifying vulnerabilities in remote applications through real-world attack simulation.

NEW QUESTION # 111
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 # 112
Which of the following roles typically performs routine vulnerability scans?

- A. IT auditor
- B. Incident response manager
- C. Information security manager
- D. IT security specialist

Answer: D

Explanation:
AnIT security specialistis responsible forperforming routine vulnerability scansas part of maintaining the organization's security posture. Their primary tasks include:
* Vulnerability Assessment:Using automated tools to detect security flaws in networks, applications, and systems.
* Regular Scanning:Running scheduled scans to identify new vulnerabilities introduced through updates or configuration changes.
* Reporting:Analyzing scan results and providing reports to management and security teams.
* Remediation Support:Working with IT staff to patch or mitigate identified vulnerabilities.
Other options analysis:
* A. Incident response manager:Primarily focuses on responding to security incidents, not performing routine scans.
* B. Information security manager:Manages the overall security program but does not typically conduct scans.
* C. IT auditor:Reviews the effectiveness of security controls but does not directly perform scanning.
CCOA Official Review Manual, 1st Edition References:
* Chapter 6: Vulnerability and Patch Management:Outlines the responsibilities of IT security specialists in conducting vulnerability assessments.
* Chapter 8: Threat and Vulnerability Assessment:Discusses the role of specialists in maintaining security baselines.

NEW QUESTION # 113
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 # 114
Following a ransomware incident, the network teamprovided a PCAP file, titled ransom.pcap, located in theInvestigations folder on the Desktop.
What is the name of the file containing the ransomwaredemand? Your response must include the fileextension.

Answer:

Explanation:
See the solution in Explanation.
Explanation:
To identify thefilename containing the ransomware demandfrom theransom.pcapfile, follow these detailed steps:
Step 1: Access the PCAP File
* Log into the Analyst Desktop.
* Navigate to theInvestigationsfolder located on the desktop.
* Locate the file:
ransom.pcap
Step 2: Open the PCAP File in Wireshark
* LaunchWireshark.
* Open the PCAP file:
mathematica
File > Open > Desktop > Investigations > ransom.pcap
* ClickOpento load the file.
Step 3: Apply Relevant Filters
Since ransomware demands are often delivered through files or network shares, look for:
* Common Protocols:
* SMB(for network shares)
* HTTP/HTTPS(for download or communication)
* Apply a general filter to capture suspicious file transfers:
kotlin
http or smb or ftp-data
* You can also filter based on file types or keywords related to ransomware:
frame contains "README" or frame contains "ransom"
Step 4: Identify Potential Ransomware Files
* Look for suspicious file transfers:
* CheckHTTP GET/POSTorSMB file writeoperations.
* Analyze File Names:
* Ransom notes commonly use filenames such as:
* README.txt
* DECRYPT_INSTRUCTIONS.html
* HELP_DECRYPT.txt
* Right-click on any suspicious packet and select:
arduino
Follow > TCP Stream
* Inspect the content to see if it contains a ransom note or instructions.
Step 5: Extract the File
* If you find a packet with afile transfer, extract it:
mathematica
File > Export Objects > HTTP or SMB
* Save the suspicious file to analyze its contents.
Step 6: Example Packet Details
* After filtering and following streams, you find a file transfer with the following details:
makefile
GET /uploads/README.txt HTTP/1.1
Host: 10.10.44.200

User-Agent: Mozilla/5.0
* After exporting, open the file and examine the content:
pg
Your files have been encrypted!
To recover them, you must pay in Bitcoin.
Read this file carefully for payment instructions.
README.txt
Step 7: Confirm and Document
* File Name:README.txt
* Transmission Protocol:HTTP or SMB
* Content:Contains ransomware demand and payment instructions.
Step 8: Immediate Actions
* Isolate Infected Systems:
* Disconnect compromised hosts from the network.
* Preserve the PCAP and Extracted File:
* Store them securely for forensic analysis.
* Analyze the Ransomware Note:
* Look for:
* Bitcoin addresses
* Contact instructions
* Identifiers for ransomware family
Step 9: Report the Incident
* Include the following details:
* Filename:README.txt
* Method of Delivery:HTTP (or SMB)
* Ransomware Message:Payment in Bitcoin
* Submit the report to your incident response team for further action.

NEW QUESTION # 115
.....

Our CCOA exam guide has high quality of service. We provide 24-hour online service on the CCOA training engine. If you have any questions in the course of using the bank, you can contact us by email. We will provide you with excellent after-sales service with the utmost patience and attitude. And we will give you detailed solutions to any problems that arise during the course of using the CCOA learning braindumps. And our CCOA study materials welcome your supervision and criticism.

- 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, pct.edu.pk, knowara.com, wkwjhskssksbg.pointblog.net, arcoasiscareacademy.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, www.stes.tyc.edu.tw, lms.ait.edu.za, Disposable vapes

What's more, part of that Pass4SureQuiz CCOA dumps now are free: https://drive.google.com/open?id=1dV8fosIo_cWNH0RBrA9te2Dt26OMTtOI