Specifications of ExamPrepAway ISACA CCOA Exam Preparation Material

2025 Latest ExamPrepAway CCOA PDF Dumps and CCOA Exam Engine Free Share: https://drive.google.com/open?id=10F7KDNHOdFqJstgMrBa829Grwp7ZISuy

It's time to take the ISACA CCOA practice test for self-assessment once you have prepared with CCOA PDF questions. Taking ExamPrepAway's web-based ISACA CCOA practice test is the best method to feel the real ISACA CCOA Exam scenario. ExamPrepAway offers the customizable web-based ISACA CCOA practice test that is compatible with all browsers like MS Edge, Chrome, Firefox, etc.

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	• 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 3	• 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 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	• 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.

CCOA Test Practice, Free CCOA Practice Exams

Our CCOA preparation exam have assembled a team of professional experts incorporating domestic and overseas experts and scholars to research and design related exam bank, committing great efforts to work for our candidates. Most of the experts have been studying in the professional field for many years and have accumulated much experience in our CCOA Practice Questions. So we can say that our CCOA exam questions are the first-class in the market. With our CCOA learning guide, you will get your certification by your first attempt.

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

NEW QUESTION # 97
Which of the following is the MOST effective method for identifying vulnerabilities in a remote web application?

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

Answer: B

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 # 98
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 # 99
An insecure continuous integration and continuous delivery (CI/CD) pipeline would MOST likely lead to:

- A. software Integrity failures.
- B. security monitoring failures.
- C. broken access control.
- D. browser compatibility Issues.

Answer: A

Explanation:
An insecure CI/CD pipeline can lead to software integrity failures primarily due to the risk of:
* Code Injection:Unauthenticated or poorly controlled access to the CI/CD pipeline can allow attackers to inject malicious code during build or deployment.
* Compromised Dependencies:Automated builds may incorporate malicious third-party libraries or components, compromising the final product.
* Insufficient Access Control:Without proper authentication and authorization mechanisms, unauthorized users might modify build configurations or artifacts.
* Pipeline Poisoning:Attackers can alter the pipeline to include vulnerabilities or backdoors.
Due to the above risks, software integrity can be compromised, resulting in the distribution of tampered or malicious software.
Incorrect Options:
* B. Broken access control:This is a more general web application security issue, not specific to CI/CD pipelines.
* C. Security monitoring failures:While possible, this is not the most direct consequence of CI/CD pipeline insecurities.
* D. Browser compatibility Issues:This is unrelated to CI/CD security concerns.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 6, Section "DevSecOps and CI/CD Security", Subsection "Risks and Vulnerabilities in CI /CD Pipelines" - Insecure CI/CD pipelines can compromise software integrity due to code injection and dependency attacks.

NEW QUESTION # 100
Before performing a penetration test for a client, it is MOST crucial to ensure:

- A. authorized consent is obtained.
- B. the timeframe has been determined.
- C. scope is defined.
- D. price has been estimated.

Answer: A

Explanation:
Before conducting apenetration test, themost crucial stepis to obtainauthorized consentfrom the client:
* Legal Compliance:Ensures the testing is lawful and authorized, preventing legal consequences.
* Clearance:Confirms that the client understands and agrees to the testing scope and objectives.
* Documentation:Signed agreements protect both the tester and client in case of issues during testing.

* Ethical Consideration:Performing tests without consent violates ethical hacking principles.
Incorrect Options:
* B. Determining timeframe:Important but secondary to legal consent.
* C. Defining scope:Necessary, but only after authorization.
* D. Estimating price:Relevant for contracts but not the primary security concern.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 8, Section "Ethical Hacking and Legal Considerations," Subsection "Authorization and Consent" - Proper authorization is mandatory before any penetration testing.

NEW QUESTION # 101
Robust background checks provide protection against:

- A. phishing.
- B. ransomware.
- C. distributed dental of service (DDoS) attacks.
- D. insider threats.

Answer: D

Explanation:
Robust background checks help mitigateinsider threatsby ensuring that individuals withaccess to sensitive data or critical systemsdo not have a history of risky or malicious behavior.
* Screening:Identifies red flags like past criminal activity or suspicious financial behavior.
* Trustworthiness Assessment:Ensures that employees handling sensitive information have a proven history of integrity.
* Insider Threat Mitigation:Helps reduce the risk of data theft, sabotage, or unauthorized access.
* Periodic Rechecks:Maintain ongoing security by regularly updating background checks.
Incorrect Options:
* A. DDoS attacks:Typically external; background checks do not mitigate these.
* C. Phishing:An external social engineering attack, unrelated to employee background.
* D. Ransomware:Generally spread via malicious emails or compromised systems, not insider actions.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 4, Section "Insider Threat Management," Subsection "Pre-Employment Screening" - Background checks are vital in identifying potential insider threats before hiring.

NEW QUESTION # 102
.....

www.pdfvce.com is best website to obtain ➥ CCOA for free download CCOA Reliable Test Cram

- ISACA CCOA Exam Dumps - Easiest Preparation Method [2026] Search for ➠ CCOA and download it for free on [www.pdfdumps.com] website Exam CCOA Pass4sure
- Valid ISACA Certified Cybersecurity Operations Analyst braindumps pdf - CCOA valid dumps Open website 《 www.pdfvce.com 》 and search for 「 CCOA 」 for free download Exam CCOA Testking
- CCOA Exam Consultant CCOA Exams Torrent CCOA Exams Torrent Open " www.easy4engine.com " and search for CCOA to download exam materials for free Latest CCOA Braindumps Pdf
- myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, futurewisementorhub.com, learn.smartvabna.com, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that ExamPrepAway CCOA dumps now are free: https://drive.google.com/open?id=10F7KDNHOdFqJstgMrBa829Grwp7ZISuy