CCOA Valid Dumps Questions | CCOA Exam Certification Cost

What's more, part of that ActualCollection CCOA dumps now are free: https://drive.google.com/open?id=1dr5LcVI0IPtAB-JlF3LjdsZFFYBl4ToD

With the high pass rate as 98% to 100%, we are confident to claim that our high quality and high efficiency of our CCOA exam guide is unparalleled in the market. We provide the latest and exact CCOA practice quiz to our customers and you will be grateful if you choose our CCOA Study Materials and gain what you are expecting in the shortest time. Besides, you have the chance to experience the real exam in advance with the Software version of our CCOA practice materials.

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	• 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 3	• 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 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	• 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.

CCOA Exam Certification Cost | Free Sample CCOA Questions

The customers can immediately start using the ISACA Certified Cybersecurity Operations Analyst (CCOA) exam dumps of ActualCollection after buying it. In this way, one can save time and instantly embark on the journey of CCOA test preparation. 24/7 customer service is also available at ActualCollection. Feel free to reach our customer support team if you have any questions about our CCOA Exam Preparation material.

ISACA Certified Cybersecurity Operations Analyst Sample Questions (Q19-Q24):

NEW QUESTION # 19
The CISO has received a bulletin from law enforcementauthorities warning that the enterprise may be at risk ofattack from a specific threat actor. Review the bulletin named CCOA Threat Bulletin.pdf on the Desktop.
Which of the following domain name(s) from the CCOAThreat Bulletin.pdf was contacted between 12:10 AMto 12:12 AM (Absolute) on August 17, 2024?

Answer:

Explanation:
See the solution in Explanation.
Explanation:
Step 1: Understand the Objective
Objective:
* Identify thedomain name(s)that werecontactedbetween:
12:10 AM to 12:12 AM on August 17, 2024
* Source of information:
CCOA Threat Bulletin.pdf
* File location:
~/Desktop/CCOA Threat Bulletin.pdf
Step 2: Prepare for Investigation
2.1: Ensure Access to the File
* Check if the PDF exists:
ls ~/Desktop | grep "CCOA Threat Bulletin.pdf"
* Open the file to inspect:
xdg-open ~/Desktop/CCOA\ Threat\ Bulletin.pdf
* Alternatively, convert to plain text for easier analysis:
pdftotext ~/Desktop/CCOA\ Threat\ Bulletin.pdf ~/Desktop/threat_bulletin.txt cat ~/Desktop/threat_bulletin.txt
2.2: Analyze the Content
* Look for domain names listed in the bulletin.
* Make note ofany domainsorURLsmentioned as IoCs (Indicators of Compromise).
* Example:
suspicious-domain.com
malicious-actor.net
threat-site.xyz

Step 3: Locate Network Logs
3.1: Find the Logs Directory
* The logs could be located in one of the following directories:
/var/log/
/home/administrator/hids/logs/
/var/log/httpd/
/var/log/nginx/
* Navigate to the likely directory:
cd /var/log/
ls -l
* Identify relevant network or DNS logs:
ls -l | grep -E "dns|network|http|nginx"
Step 4: Search Logs for Domain Contacts
4.1: Use the Grep Command to Filter Relevant Timeframe
* Since we are looking for connections between12:10 AM to 12:12 AMonAugust 17, 2024:
grep "2024-08-17 00:1[0-2]" /var/log/dns.log
* Explanation:
* grep "2024-08-17 00:1[0-2]": Matches timestamps between00:10and00:12.
* Replace dns.log with the actual log file name, if different.
4.2: Further Filter for Domain Names
* To specifically filter out the domains listed in the bulletin:
grep -E "(suspicious-domain.com|malicious-actor.net|threat-site.xyz)" /var/log/dns.log
* If the logs are in another file, adjust the file path:
grep -E "(suspicious-domain.com|malicious-actor.net|threat-site.xyz)" /var/log/nginx/access.log Step 5: Correlate Domains and Timeframe
5.1: Extract and Format Relevant Results
* Combine the commands to get time-specific domain hits:
grep "2024-08-17 00:1[0-2]" /var/log/dns.log | grep -E "(suspicious-domain.com|malicious-actor.net|threat- site.xyz)"
* Sample Output:
2024-08-17 00:11:32 suspicious-domain.com accessed by 192.168.1.50
2024-08-17 00:12:01 malicious-actor.net accessed by 192.168.1.75
* Interpretation:
* The command revealswhich domain(s)were contacted during the specified time.
Step 6: Verification and Documentation
6.1: Verify Domain Matches
* Cross-check the domains in the log output against those listed in theCCOA Threat Bulletin.pdf.
* Ensure that the time matches the specified range.
6.2: Save the Results for Reporting
* Save the output to a file:
grep "2024-08-17 00:1[0-2]" /var/log/dns.log | grep -E "(suspicious-domain.com|malicious-actor.net|threat- site.xyz)" > ~/Desktop/domain_hits.txt
* Review the saved file:
cat ~/Desktop/domain_hits.txt
Step 7: Report the Findings
Final Answer:
* Domain(s) Contacted:
* suspicious-domain.com
* malicious-actor.net
* Time of Contact:
* Between 12:10 AM to 12:12 AM on August 17, 2024
* Reasoning:
* Matched thelog timestampsanddomain nameswith the threat bulletin.
Step 8: Recommendations:
* Immediate Block:
* Add the identified domains to theblockliston firewalls and intrusion detection systems.
* Monitor for Further Activity:
* Keep monitoring logs for any further connection attempts to the same domains.
* Perform IOC Scanning:
* Check hosts that communicated with these domains for possible compromise.
* Incident Report:
* Document the findings and mitigation actions in theincident response log.

NEW QUESTION # 20
Which of the following is MOST likely to result from misunderstanding the cloud service shared responsibility model?

- A. Misconfiguration of access controls for cloud services
- B. Improperly securing access to the cloud metastructure layer
- C. Falsely assuming that certain risks have been transferred to the vendor
- D. Being forced to remain with the cloud service provider due to vendor lock-In

Answer: C

Explanation:
Misunderstanding thecloud service shared responsibility modeloften leads to the false assumption that the cloud service provider (CSP) is responsible for securing all aspects of the cloud environment.
* What is the Shared Responsibility Model?It delineates the security responsibilities of the CSP and the customer.
* Typical Misconception:Customers may believe that the provider handles all security aspects, including data protection and application security, while in reality, the customer is usually responsible for securing data and application configurations.
* Impact:This misunderstanding can result in unpatched software, unsecured data, or weak access control.
Incorrect Options:
* B. Improperly securing access to the cloud metastructure layer:This is a specific security flaw but not directly caused by misunderstanding the shared responsibility model.
* C. Misconfiguration of access controls for cloud services:While common, this usually results from poor implementation rather than misunderstanding shared responsibility.
* D. Vendor lock-in:This issue arises from contractual or technical dependencies, not from misunderstanding the shared responsibility model.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 3, Section "Cloud Security Models," Subsection "Shared Responsibility Model" - Misunderstanding the shared responsibility model often leads to misplaced assumptions about who handles specific security tasks.

NEW QUESTION # 21
How can port security protect systems on a segmented network?

- A. By enforcing encryption of data on the network
- B. By establishing a Transport Layer Security (TLS) handshake
- C. By preventing unauthorized access to the network
- D. By requiring multi-factor authentication

Answer: C

Explanation:
Port security is a network control technique used primarily toprevent unauthorized accessto a network by:
* MAC Address Filtering:Restricts which devices can connect by allowing only known MAC addresses.
* Port Lockdown:Disables a port if an untrusted device attempts to connect.
* Mitigating MAC Flooding:Helps prevent attackers from overwhelming the switch with spoofed MAC addresses.
Incorrect Options:
* A. Enforcing encryption:Port security does not directly handle encryption.
* C. Establishing TLS handshake:TLS is related to secure communications, not port-level access control.
* D. Requiring multi-factor authentication:Port security works at the network level, not the authentication level.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 5, Section "Network Security," Subsection "Port Security" - Port security helps protect network segments by controlling device connections based on MAC address.

NEW QUESTION # 22
Which of the following is the PRIMARY benefit of compiled programming languages?

- A. Ability to change code in production
- B. Streamlined development
- C. Fasterapplication execution

- D. Flexibledeployment

Answer: C

Explanation:
Theprimary benefit of compiled programming languages(like C, C++, and Go) isfaster execution speed because:
* Direct Machine Code:Compiled code is converted to machine language before execution, eliminating interpretation overhead.
* Optimizations:The compiler optimizes code for performance during compilation.
* Performance-Intensive Applications:Ideal for system programming, game development, and high- performance computing.
Other options analysis:
* A. Streamlined development:Compiled languages often require more code and debugging compared to interpreted languages.
* C. Flexible deployment:Interpreted languages generally offer more flexibility.
* D. Changing code in production:Typically challenging without recompilation.
CCOA Official Review Manual, 1st Edition References:
* Chapter 10: Secure Coding Practices:Discusses the benefits and challenges of compiled languages.
* Chapter 8: Software Development Lifecycle (SDLC):Highlights the performance benefits of compiled code.

NEW QUESTION # 23
For this question you must log into GreenboneVulnerability Manager using Firefox. The URL is:https://10.
10.55.4:9392 and credentials are:
Username:admin
Password:Secure-gvm!
A colleague performed a vulnerability scan but did notreview prior to leaving for a family emergency. It hasbeen determined that a threat actor is using CVE-2021-22145 in the wild. What is the host IP of the machinethat is vulnerable to this CVE?

Answer:

Explanation:
See the solution in Explanation.
Explanation:
To determine the host IP of the machine vulnerable toCVE-2021-22145usingGreenbone Vulnerability Manager (GVM), follow these detailed steps:
Step 1: Access Greenbone Vulnerability Manager
* OpenFirefoxon your system.
* Go to the GVM login page:
URL: https://10.10.55.4:9392
* Enter the credentials:
Username: admin
Password: Secure-gvm!
* ClickLoginto access the dashboard.
Step 2: Navigate to Scan Reports
* Once logged in, locate the"Scans"menu on the left panel.
* Click on"Reports"under the"Scans"section to view the list of completed vulnerability scans.
Step 3: Identify the Most Recent Scan
* Check thedate and timeof the last completed scan, as your colleague likely used the latest one.
* Click on theReport NameorDateto open the detailed scan results.
Step 4: Filter for CVE-2021-22145
* In the report view, locate the"Search"or"Filter"box at the top.
* Enter the CVE identifier:
CVE-2021-22145
* PressEnterto filter the vulnerabilities.
Step 5: Analyze the Results
* The system will display any host(s) affected byCVE-2021-22145.
* The details will typically include:
* Host IP Address
* Vulnerability Name
* Severity Level
* Vulnerability Details
Example Display:
Host IP

Vulnerability ID
CVE
Severity
192.168.1.100
SomeVulnName
CVE-2021-22145
High
Step 6: Verify the Vulnerability
* Click on the host IP to see thedetailed vulnerability description.
* Check for the following:
* Exploitability: Proof that the vulnerability can be actively exploited.
* Description and Impact: Details about the vulnerability and its potential impact.
* Fixes/Recommendations: Suggested mitigations or patches.
Step 7: Note the Vulnerable Host IP
* The IP address that appears in the filtered list is thevulnerable machine.
Example Answer:
The host IP of the machine vulnerable to CVE-2021-22145 is: 192.168.1.100 Step 8: Take Immediate Actions
* Isolate the affected machineto prevent exploitation.
* Patch or updatethe software affected by CVE-2021-22145.
* Perform a quick re-scanto ensure that the vulnerability has been mitigated.
Step 9: Generate a Report for Documentation
* Export the filtered scan results as aPDForHTMLfrom the GVM.
* Include:
* Host IP
* CVE ID
* Severity and Risk Level
* Remediation Steps
Background on CVE-2021-22145:
* This CVE is related to a vulnerability in certain software, often associated withimproper access control orauthentication bypass.
* Attackers can exploit this to gain unauthorized access or escalate privileges.

NEW QUESTION # 24
.....

We can ensure you a pass rate as high as 99% of our CCOA exam questions. So with our CCOA study guide, you will pass the CCOA exam. And this is the right thing you can imagine. You surely desire the CCOA certification. So with a tool as good as our CCOA Exam Material, why not study and practice for just 20 to 30 hours and then pass the examination? It is more convenient for you to study and practice anytime, anywhere with our varied versions of CCOA exam braindumps.

- ISACA Certified Cybersecurity Operations Analyst pass guide: latest CCOA exam prep collection □ Search on ⇛ www.pdfvce.com ⇚ for ➥ CCOA □ to obtain exam materials for free download □Dumps CCOA PDF
- CCOA Brain Dumps □ CCOA Training Courses □ CCOA Latest Exam Simulator □ Search for □ CCOA □ and download it for free immediately on ☀ www.vce4dumps.com □☀□ □CCOA Pass4sure Dumps Pdf
- pct.edu.pk, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.alisuruniversity.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, academy.rankspro.io, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

BONUS!!! Download part of ActualCollection CCOA dumps for free: https://drive.google.com/open?id=1dr5LcVI0IPtAB-JlF3LjdsZFFYBl4ToD