ISACA CCOA Exam Topic | CCOA Cert Exam

BTW, DOWNLOAD part of PracticeVCE CCOA dumps from Cloud Storage: https://drive.google.com/open?id=1OLLW3GBUPxsKz7GP9IOFcSnhfMq9HgL9

The main objective of PracticeVCE CCOA practice test questions features to assist the CCOA exam candidates with quick and complete CCOA exam preparation. The ISACA CCOA exam dumps features are a free demo download facility, real, updated, and error-free ISACA CCOA Test Questions, 12 months free updated ISACA CCOA exam questions and availability of CCOA real questions in three different formats.

Having more competitive advantage means that you will have more opportunities and have a job that will satisfy you. This is why more and more people have long been eager for the certification of CCOA. Our CCOA test material can help you focus and learn effectively. You don't have to worry about not having a dedicated time to learn every day. You can learn our CCOA exam torrent in a piecemeal time, and you don't have to worry about the tedious and cumbersome learning content. We will simplify the complex concepts by adding diagrams and examples during your study. By choosing our CCOA test material, you will be able to use time more effectively than others and have the content of important information in the shortest time.

>> ISACA CCOA Exam Topic <<

CCOA Cert Exam | CCOA Lead2pass Review

There is no doubt that the CCOA certification can help us prove our strength and increase social competitiveness. Although it is not an easy thing for some candidates to pass the exam, but our CCOA question torrent can help aggressive people to achieve their goals. This is the reason why we need to recognize the importance of getting the test CCOA Certification. Now give me a chance to know our CCOA study tool before your payment, you can just free download the demo of our CCOA exam questions on the web.

ISACA Certified Cybersecurity Operations Analyst Sample Questions (Q92-Q97):

NEW QUESTION # 92
The network team has provided a PCAP file withsuspicious activity located in the Investigations folderon the Desktop titled, investigation22.pcap.
What date was the webshell accessed? Enter the formatas YYYY-MM-DD.

Answer:

Explanation:
See the solution in Explanation.
Explanation:
To determine thedate the webshell was accessedfrom theinvestigation22.pcapfile, follow these detailed steps:
Step 1: Access the PCAP File
* Log into the Analyst Desktop.
* Navigate to theInvestigationsfolder on the desktop.
* Locate the file:

investigation22.pcap
Step 2: Open the PCAP File in Wireshark
* LaunchWireshark.
* Open the PCAP file:
mathematica
File > Open > Desktop > Investigations > investigation22.pcap
* ClickOpento load the file.
Step 3: Filter for Webshell Traffic
* Since webshells typically useHTTP/Sto communicate, apply a filter:
http.request or http.response
* Alternatively, if you know the IP of the compromised host (e.g.,10.10.44.200), use:
nginx
http and ip.addr == 10.10.44.200
* PressEnterto apply the filter.
Step 4: Identify Webshell Activity
* Look for HTTP requests that include:
* Common Webshell Filenames:shell.jsp, cmd.php, backdoor.aspx, etc.
* Suspicious HTTP Methods:MainlyPOSTorGET.
* Right-click a suspicious packet and choose:
arduino
Follow > HTTP Stream
* Inspect the HTTP headers and content to confirm the presence of a webshell.
Step 5: Extract the Access Date
* Look at theHTTP request/response header.
* Find theDatefield orTimestampof the packet:
* Wireshark displays timestamps on the left by default.
* Confirm theHTTP streamincludes commands or uploads to the webshell.
Example HTTP Stream:
POST /uploads/shell.jsp HTTP/1.1
Host: 10.10.44.200
User-Agent: Mozilla/5.0
Date: Mon, 2024-03-18 14:35:22 GMT
Step 6: Verify the Correct Date
* Double-check other HTTP requests or responses related to the webshell.
* Make sure thedate fieldis consistent across multiple requests to the same file.
2024-03-18
Step 7: Document the Finding
* Date of Access:2024-03-18
* Filename:shell.jsp (as identified earlier)
* Compromised Host:10.10.44.200
* Method of Access:HTTP POST
Step 8: Next Steps
* Isolate the Affected Host:
* Remove the compromised server from the network.
* Remove the Webshell:
rm /path/to/webshell/shell.jsp
* Analyze Web Server Logs:
* Correlate timestamps with access logs to identify the initial compromise.
* Implement WAF Rules:
* Block suspicious patterns related to file uploads and webshell execution.

NEW QUESTION # 93
Question 1 and 2
You have been provided with authentication logs toinvestigate a potential incident. The file is titledwebserver- auth-logs.txt and located in theInvestigations folder on the Desktop.
Which IP address is performing a brute force attack?
What is the total number of successful authenticationsby the IP address performing the brute force attack?

Answer:

Explanation:
See the solution in Explanation:
Explanation:
Step 1: Define the Problem and Objective
Objective:
We need to identify the following from the webserver-auth-logs.txt file:
* TheIP address performing a brute force attack.
* Thetotal number of successful authenticationsmade by that IP.
Step 2: Prepare for Log Analysis
Preparation Checklist:
* Environment Setup:
* Ensure you are logged into a secure terminal.
* Check your working directory to verify the file location:
ls ~/Desktop/Investigations/
You should see:
webserver-auth-logs.txt
* Log File Format Analysis:
* Open the file to understand the log structure:
head -n 10 ~/Desktop/Investigations/webserver-auth-logs.txt
* Look for patterns such as:
pg
2025-04-07 12:34:56 login attempt from 192.168.1.1 - SUCCESS
2025-04-07 12:35:00 login attempt from 192.168.1.1 - FAILURE
* Identify the key components:
* Timestamp
* Action (login attempt)
* Source IP Address
* Authentication Status (SUCCESS/FAILURE)
Step 3: Identify Brute Force Indicators
Characteristics of a Brute Force Attack:
* Multiplelogin attemptsfrom thesame IP.
* Combination ofFAILUREandSUCCESSmessages.
* High volumeof attempts compared to other IPs.
Step 3.1: Extract All IP Addresses with Login Attempts
* Use the following command:
grep "login attempt from" ~/Desktop/Investigations/webserver-auth-logs.txt | awk '{print $6}' | sort | uniq -c | sort -nr > brute-force-ips.txt
* Explanation:
* grep "login attempt from": Finds all login attempt lines.
* awk '{print $6}': Extracts IP addresses.
* sort | uniq -c: Groups and counts IP occurrences.
* sort -nr: Sorts counts in descending order.
* > brute-force-ips.txt: Saves the output to a file for documentation.
Step 3.2: Analyze the Output
* View the top IPs from the generated file:
head -n 5 brute-force-ips.txt
* Expected Output:
1500 192.168.1.1
45 192.168.1.2
30 192.168.1.3
* Interpretation:
* The first line shows 192.168.1.1 with 1500 attempts, indicating brute force.
Step 4: Count Successful Authentications
Why Count Successful Logins?
* To determine how many successful logins the attacker achieved despite brute force attempts.
Step 4.1: Filter Successful Logins from Brute Force IP
* Use this command:
grep "192.168.1.1" ~/Desktop/Investigations/webserver-auth-logs.txt | grep "SUCCESS" | wc -l
* Explanation:
* grep "192.168.1.1": Filters lines containing the brute force IP.
* grep "SUCCESS": Further filters successful attempts.

* wc -l: Counts the resulting lines.
Step 4.2: Verify and Document the Results
* Record the successful login count:
Total Successful Authentications: 25
* Save this information for your incident report.
Step 5: Incident Documentation and Reporting
5.1: Summary of Findings
* IP Performing Brute Force Attack:192.168.1.1
* Total Number of Successful Authentications:25
5.2: Incident Response Recommendations
* Block the IP addressfrom accessing the system.
* Implementrate-limiting and account lockout policies.
* Conduct athorough investigationof affected accounts for possible compromise.
Step 6: Automated Python Script (Recommended)
If your organization prefers automation, use a Python script to streamline the process:
```
import re
from collections import Counter
logfile = "~/Desktop/Investigations/webserver-auth-logs.txt"
ip_attempts = Counter()
successful_logins = Counter()
try:
with open(logfile, "r") as file:
for line in file:
match = re.search(r"from (\d+\.\d+\.\d+\.\d+)", line)
if match:
ip = match.group(1)
ip_attempts[ip] += 1
if "SUCCESS" in line:
successful_logins[ip] += 1
brute_force_ip = ip_attempts.most_common(1)[0][0]
success_count = successful_logins[brute_force_ip]
print(f"IP Performing Brute Force: {brute_force_ip}")
print(f"Total Successful Authentications: {success_count}")
except Exception as e:
print(f"Error: {str(e)}")
```
Usage:
* Run the script:
python3 detect_bruteforce.py
* Output:
IP Performing Brute Force: 192.168.1.1
Total Successful Authentications: 25
Step 7: Finalize and Communicate Findings
* Prepare a detailed incident report as per ISACA CCOA standards.
* Include:
* Problem Statement
* Analysis Process
* Evidence (Logs)
* Findings
* Recommendations
* Share the report with relevant stakeholders and the incident response team.
Final Answer:
* Brute Force IP:192.168.1.1
* Total Successful Authentications:25

NEW QUESTION # 94
Which of the following Is the MOST effective way to ensure an organization's management of supply chain risk remains consistent?

- A. Periodically counting the number of incident tickets associated with supplier services
- B. Regularly seeking feedback from the procurement team regarding supplier responsiveness

- C. Periodically confirming suppliers' contractual obligations are met
- D. Regularly meeting with suppliers to informally discuss Issues

Answer: C

Explanation:
To maintain consistent management ofsupply chain risk, it is essential toperiodically confirm that suppliers meet their contractual obligations.
* Risk Assurance:Verifies that suppliers adhere to security standards and commitments.
* Compliance Monitoring:Ensures that the agreed-upon controls and service levels are maintained.
* Consistency:Regular checks prevent lapses in compliance and identify potential risks early.
* Supplier Audits:Include reviewing security controls, data protection measures, and compliance with regulations.
Incorrect Options:
* A. Seeking feedback from procurement:Useful but not directly related to risk management.
* C. Counting incident tickets:Measures service performance, not risk consistency.
* D. Informal meetings:Lacks formal assessment and verification of obligations.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 9, Section "Supply Chain Risk Management," Subsection "Monitoring and Compliance" - Periodic verification of contractual compliance ensures continuous risk management.

NEW QUESTION # 95
Which type of cloud deployment model is intended to be leveraged over the Internet by many organizations with varying needs and requirements?

- A. Hybrid cloud
- B. Private cloud
- C. Community cloud
- D. Public cloud

Answer: D

Explanation:
Apublic cloudis intended to be accessible over theInternetby multiple organizations with varying needs and requirements:
* Multi-Tenancy:The same infrastructure serves numerous clients.
* Accessibility:Users can access resources from anywhere via the Internet.
* Scalability:Provides flexible and on-demand resource allocation.
* Common Providers:AWS, Azure, and Google Cloud offer public cloud services.
Incorrect Options:
* A. Hybrid cloud:Combines private and public cloud, not primarily public.
* B. Community cloud:Shared by organizations with common concerns, not broadly public.
* D. Private cloud:Exclusive to a single organization, not accessible by many.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 3, Section "Cloud Deployment Models," Subsection "Public Cloud Characteristics" - Public clouds are designed for use by multiple organizations via the Internet.

NEW QUESTION # 96
A nation-state that is employed to cause financial damage on an organization is BEST categorized as:

- A. an attach vector.
- B. a threat actor.
- C. a vulnerability.
- D. a risk.

Answer: B

Explanation:
Anation-stateemployed to cause financial damage to an organization is considered athreat actor.
* Definition:Threat actors are individuals or groups that aim to harm an organization's security, typically through cyberattacks or data breaches.

* Characteristics:Nation-state actors are often highly skilled, well-funded, and operate with strategic geopolitical objectives.
* Typical Activities:Espionage, disruption of critical infrastructure, financial damage through cyberattacks (like ransomware or supply chain compromise).
Incorrect Options:
* A. A vulnerability:Vulnerabilities are weaknesses that can be exploited, not the actor itself.
* B. A risk:A risk represents the potential for loss or damage, but it is not the entity causing harm.
* C. An attack vector:This represents the method or pathway used to exploit a vulnerability, not the actor.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 2, Section "Threat Landscape," Subsection "Types of Threat Actors" - Nation-states are considered advanced threat actors that may target financial systems for political or economic disruption.

NEW QUESTION # 97
.....

It is convenient for our consumers to check ISACA CCOA exam questions free of charge before purchasing the ISACA Certified Cybersecurity Operations Analyst CCOA practice exam. To make the ISACA CCOA exam questions content up-to-date for free of cost up to 365 days after buying them, our certified trainers work strenuously to formulate the exam questions in compliance with the ISACA Certified Cybersecurity Operations Analyst CCOA Dumps.

CCOA Cert Exam: https://www.practicevce.com/ISACA/CCOA-practice-exam-dumps.html

Nowadays, we heard that CCOA certification is becoming an important index in related IT incorporation, If you buy the CCOA learning dumps from our company, we are glad to provide you with the high quality CCOA study question and the best service, In the past few years, CCOA Cert Exam - ISACA Certified Cybersecurity Operations Analyst certification has become an influenced IT technology skill, ISACA CCOA Exam Topic Besides, we give discounts to our customers from time to time.

You will learn about concepts such as a ghost CCOA market and the DarkWeb, and how cyber criminals leverage their capabilities, Be aware of which icon appeared on the screen just CCOA Valid Dumps Pdf before the freeze occurred-you may need to restart again and write down what you see.

Pass Guaranteed 2026 ISACA CCOA: High Pass-Rate ISACA Certified Cybersecurity Operations Analyst Exam Topic

Nowadays, we heard that CCOA Certification is becoming an important index in related IT incorporation, If you buy the CCOA learning dumps from our company, we are glad to provide you with the high quality CCOA study question and the best service.

In the past few years, ISACA Certified Cybersecurity Operations Analyst certification has CCOA Cert Exam become an influenced IT technology skill, Besides, we give discounts to our customers from time to time, In order to help most candidates who want to pass CCOA exam, so we compiled such a study materials to make CCOA exam simply.

- ISACA Certified Cybersecurity Operations Analyst dumps torrent - valid free CCOA vce dumps □ The page for free download of ▸ CCOA ◂ on 「 www.vce4dumps.com 」 will open immediately □CCOA Training Material
- ISACA Certified Cybersecurity Operations Analyst dumps torrent - valid free CCOA vce dumps □ Go to website ⇛ www.pdfvce.com ⇚ open and search for □ CCOA □ to download for free □CCOA Valid Braindumps Ppt
- 100% Pass 2026 ISACA CCOA: ISACA Certified Cybersecurity Operations Analyst –Professional Exam Topic □ Search for ✔ CCOA □✔□ on { www.verifieddumps.com } immediately to obtain a free download □CCOA Exam Materials
- New CCOA Dumps Sheet □ CCOA Training Material □ CCOA Valid Exam Notes □ Download ➡ CCOA □□□ for free by simply searching on □ www.pdfvce.com □ □CCOA Training Material
- 100% Pass 2026 ISACA CCOA: ISACA Certified Cybersecurity Operations Analyst –Professional Exam Topic □ Search on 《 www.pdfdumps.com 》 for 「 CCOA 」 to obtain exam materials for free download □CCOA Valid Braindumps Ppt
- CCOA Reliable Test Vce □ Exam CCOA Questions □ CCOA Valid Exam Notes □ Open ➽ www.pdfvce.com □ enter ⇛ CCOA ⇚ and obtain a free download □CCOA Free Updates
- CCOA Download □ CCOA Practice Engine □ Valid CCOA Exam Questions □ Search on ✔ www.pdfdumps.com □✔□ for ➥ CCOA □ to obtain exam materials for free download □Pdf CCOA Files
- CCOA Training Material □ CCOA Training Material □ CCOA Valid Braindumps Ppt □ Search for ⇛ CCOA ⇚ and download exam materials for free through □ www.pdfvce.com □ □New CCOA Dumps Sheet
- 100% Pass ISACA - Useful CCOA Exam Topic □ Search for 《 CCOA 》 and download exam materials for free through ➽ www.pass4test.com □ □CCOA Training Material

- Top Features of Pdfvce ISACA CCOA Dumps PDF file □ Open ☀ www.pdfvce.com □☀□ and search for （ CCOA ） to download exam materials for free □New CCOA Exam Prep
- ISACA Certified Cybersecurity Operations Analyst dumps torrent - valid free CCOA vce dumps □ Search on 《 www.exam4labs.com 》 for ✔ CCOA □✔□ to obtain exam materials for free download □New CCOA Dumps Sheet
- www.askmap.net, 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, 112.124.44.60, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, 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

BONUS!!! Download part of PracticeVCE CCOA dumps for free: https://drive.google.com/open?id=1OLLW3GBUPxsKz7GP9IOFcSnhfMq9HgL9