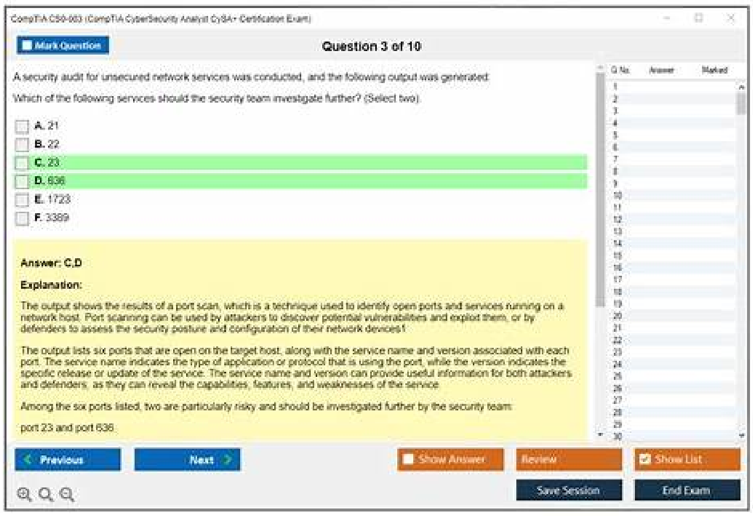
CS0-003 Vce Test Simulator - Test CS0-003 Dumps.zip



Question 3 of 10

A security audit for unsecured network services was conducted, and the following output was generated:

Which of the following services should the security team investigate further? (Select two).

- □ A. 21
- □ B. 22
- □ C. 23
- □ D. 636
- □ E. 1723
- □ F. 3389

Answer: C,D

Explanation:

The output shows the results of a port scan, which is a technique used to identify open ports and services running on a network host. Port scanning can be used by attackers to discover potential vulnerabilities and exploit them, or by defenders to assess the security posture and configuration of their network devices1

The output lists six ports that are open on the target host, along with the service name and version associated with each port. The service name indicates the type of application or protocol that is using the port, while the version indicates the specific release or update of the service. The service name and version can provide useful information for both attackers and defenders, as they can reveal the capabilities, features, and weaknesses of the service.

Among the six ports listed, two are particularly risky and should be investigated further by the security team:

port 23 and port 636

DOWNLOAD the newest ActualCollection CS0-003 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1cDVgzQEiOSDsqtIT4x1I8Zv5qakfd6NI

We offer three different formats for preparing for the CompTIA Cybersecurity Analyst (CySA+) Certification Exam (CS0-003) exam questions, all of which will ensure your definite success on your CompTIA Cybersecurity Analyst (CySA+) Certification Exam (CS0-003) exam dumps. ActualCollection is there with updated CS0-003 Questions so you can pass the CompTIA Cybersecurity Analyst (CySA+) Certification Exam (CS0-003) exam and move toward the new era of technology with full ease and confidence.

Our company offers valid CompTIA CS0-003 Exam Cram materials; you can purchase our products any time as we are 7*24 on duty throughout the whole year. We can guarantee you that if you purchase our CS0-003 exam cram materials you can pass test at first attempt without large time and energy. If the test questions change, candidates share one year updates materials and service warranty, or if you fail exam we will full refund directly.

>> CS0-003 Vce Test Simulator <<

Test CS0-003 Dumps.zip - CS0-003 Latest Test Questions

With the development of science and technology the internet in our daily life is playing a more and more important role! IT workers become high-salary people. CompTIA certifications become hot vocational qualification certificate. ActualCollection offers the best CS0-003 Guide Torrent files to help people clear exams and realize their idea better. We are engaged in this field more than 8 years. If you have dream in this field, our valid CS0-003 guide torrent files will be a good chance for you.

The cyber incident response domain covers the identification, analysis, and response to cybersecurity incidents, while the compliance and assessment domain involves understanding and implementing the various laws, regulations, and compliance requirements. Passing the CompTIA CySA+ certification exam can boost your career prospects in the cybersecurity field, as it validates your knowledge and skills in cybersecurity analysis, helping you stand out from the rest of the competition.

CompTIA Cybersecurity Analyst (CySA+) Certification Exam Sample Questions (Q406-Q411):

NEW QUESTION # 406
A security analyst is trying to identify anomalies on the network routing. Which of the following functions can the analyst use on a shell script to achieve the objective most accurately?

- A. function x() { info=$(dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1} ').origin.asn.cymru.com TXT +short) && echo "$1 | $info" }
- B. function x() { info=$(geoiplookup $1) && echo "$1 | $info" }
- C. function x() { info=$(ping -c 1 $1 | awk -F "/" 'END{print $5}') && echo "$1 | $info" }
- D. function x() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $info" }

Answer: A

Explanation:
The function that can be used on a shell script to identify anomalies on the network routing most accurately is:
function x() { info=(dig(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1} ').origin.asn.cymru.com TXT +short) && echo "$1 | $info" }
This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address. The function then prints the IP address and the ASN information, which can help identify any routing anomalies or inconsistencies

NEW QUESTION # 407
A company is concerned with finding sensitive file storage locations that are open to the public.
The current internal cloud network is flat. Which of the following is the best solution to secure the network?

- A. Implement segmentation with ACLs.
- B. Roll out an IDS.
- C. Configure logging and monitoring to the SIEM.
- D. Deploy MFA to cloud storage locations.

Answer: A

Explanation:
Implementing segmentation with ACLs is the best solution to secure the network. Segmentation is the process of dividing a network into smaller subnetworks, or segments, based on criteria such as function, location, or security level. Segmentation can help improve the network performance, scalability, and manageability, as well as enhance the network security by isolating the sensitive or critical data and systems from the rest of the network. ACLs are Access Control Lists, which are rules or policies that specify which users, devices, or applications can access a network segment or resource, and which actions they can perform. ACLs can help enforce the principle of least privilege, and prevent unauthorized or malicious access to the network segments or resources.

NEW QUESTION # 408
Which of the following stakeholders are most likely to receive a vulnerability scan report? (Select two).

- A. Systems admininstration
- B. Marketing
- C. Product owner
- D. Law enforcement
- E. Legal
- F. Executive management

Answer: A,F

Explanation:
Executive management and systems administration are the most likely stakeholders to receive a vulnerability scan report because they are responsible for overseeing the security posture and remediation efforts of the organization. Law enforcement, marketing, legal, and product owner are less likely to be involved in the vulnerability management process or need access to the scan results.
Reference: Cybersecurity Analyst+ - CompTIA, How To Write a Vulnerability Assessment Report | EC-Council, Driving Stakeholder Alignment in Vulnerability Management - LogicGate

NEW QUESTION # 409
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? (Choose two.)

- A. SIEM
- B. NGFW
- C. SOAR
- D. MSP

- E. XDR
- F. DLP

Answer: A,C

NEW QUESTION # 410
An incident response team receives an alert to start an investigation of an internet outage. The outage is preventing all users in multiple locations from accessing external SaaS resources. The team determines the organization was impacted by a DDoS attack.
Which of the following logs should the team review first?

- A. DNS
- B. CDN
- C. Vulnerability scanner
- D. Web server

Answer: A

Explanation:
A DDoS attack is a type of attack that floods a target with more traffic than it can handle. This can cause the target to become unavailable to legitimate users.
The DNS logs will show the IP addresses of the devices that were sending the traffic to the target.
This information can be used to identify the attackers.
The other logs may also be helpful in investigating a DDoS attack, but they are less likely to provide the same level of detail as the DNS logs.

NEW QUESTION # 411
......

As we all know, Selecting high quality, respected study material will help develop the required skills to pass your CS0-003 exam test. While, where to find the best valid CS0-003 practice dumps is an important question. CompTIA CS0-003 study material will be your good guide. CS0-003 Questions cover almost all the main topic, which can make you clear about the actual test. I believe, with the confident and our CS0-003 valid dumps, you will get your CS0-003 certification with ease.

Test CS0-003 Dumps.zip: https://www.actualcollection.com/CS0-003-exam-questions.html

- CS0-003 Tesking Torrent - CS0-003 Pdf Questions - CS0-003 Practice Training □ Search for （ CS0-003 ） and download it for free on □ www.verifieddumps.com □ website □Exam CS0-003 Duration
- CS0-003 Dump Ready - Exam Questions and Answers □ Easily obtain ➡ CS0-003 □□□ for free download through □ www.pdfvce.com □ □Clear CS0-003 Exam
- CS0-003 Tesking Torrent - CS0-003 Pdf Questions - CS0-003 Practice Training □ Enter □ www.examcollectionpass.com □ and search for ☀ CS0-003 □☀□ to download for free □CS0-003 New Braindumps Files
- Current CS0-003 Exam Content !! Reliable CS0-003 Test Materials □ CS0-003 Reliable Exam Topics □ Search on ➥ www.pdfvce.com □ for □ CS0-003 □ to obtain exam materials for free download □Valid Dumps CS0-003 Pdf
- CS0-003 Hottest Certification □ CS0-003 Reliable Exam Topics □ Valid Dumps CS0-003 Pdf □ Search for ➡ CS0-003 □□□ on 【 www.exam4labs.com 】 immediately to obtain a free download □CS0-003 New Braindumps Files
- CS0-003 Exam Simulator Fee □ Latest CS0-003 Test Materials □ Reliable CS0-003 Test Simulator □ Download 「 CS0-003 」 for free by simply searching on ✔ www.pdfvce.com □✔□ □Reliable CS0-003 Braindumps
- Quiz CompTIA - CS0-003 - Authoritative CompTIA Cybersecurity Analyst (CySA+) Certification Exam Vce Test Simulator □ Download ➤ CS0-003 □ for free by simply entering 《 www.easy4engine.com 》 website □Clear CS0-003 Exam
- Latest CS0-003 Test Materials □ Exam CS0-003 Duration □ Valid Dumps CS0-003 Pdf □ Search for （ CS0-003 ） on [www.pdfvce.com] immediately to obtain a free download □CS0-003 Technical Training
- Ace the CompTIA CS0-003 Exam preparation material with Three Formats □ Search for “ CS0-003 ” and download exam materials for free through 《 www.examcollectionpass.com 》 □Current CS0-003 Exam Content
- CS0-003 Dump Ready - Exam Questions and Answers □ Search for □ CS0-003 □ and download it for free on ➠ www.pdfvce.com □ website □CS0-003 Exam Simulator Fee
- CS0-003 Tesking Torrent - CS0-003 Pdf Questions - CS0-003 Practice Training □ Easily obtain free download of ⇒ CS0-003 ⇐ by searching on □ www.exam4labs.com □ □Reliable CS0-003 Braindumps

- courses.sspcphysics.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, ncon.edu.sa, 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, ncon.edu.sa, myportal.utt.edu.tt, Disposable vapes

BONUS!!! Download part of ActualCollection CS0-003 dumps for free: https://drive.google.com/open?id=1cDVgzQEiOSDsqtIT4x1I8Zv5qakfd6NI