

Free PDF Quiz Professional CS0-003 - CompTIA Cybersecurity Analyst (CySA+) Certification Exam Valid Test Testking

CompTIA

CYSA+

CS0-003

227 Practice Test Questions

in PDF Format with Verified Answers

BTW, DOWNLOAD part of BraindumpsPass CS0-003 dumps from Cloud Storage: <https://drive.google.com/open?id=1epXLgjR0YAcFX2pEXv8hivgjs8mJzJ9>

Do you want to find a fast way to step towards your dreams? We can help you by providing the latest and best useful CS0-003 pdf torrent to guarantee your success in CompTIA CS0-003 test certification. We keep our CS0-003 vce torrent the latest by checking the newest information about the updated version every day. Add the latest topics into the CS0-003 Dumps, and remove the useless questions, so that your time will be saved and study efficiency will be improved.

Three versions of CS0-003 exam torrent are available. Each version has its own feature, and you can choose the suitable one according your needs. CS0-003 PDF version is printable, and you can print it into the hard one, and if you prefer the paper one. CS0-003 Online test I engine is convenient and easy to learn, and it supports all web browsers, and can record the process of your training, you can have a general review of what you have learnt. CS0-003 Soft test engine can stimulate the real exam environment, and you can know how the real exam look like if you buy this version.

>> CS0-003 Valid Test Testking <<

New CS0-003 Exam Prep & Test CS0-003 Dumps Demo

Passing the CompTIA Cybersecurity Analyst (CySA+) Certification Exam certification test is an important step in professional development, and preparing with actual CompTIA Cybersecurity Analyst (CySA+) Certification Exam exam questions can help applicants achieve this certification. The CS0-003 Study Material promotes an organized approach to studying, aid applicants in identifying areas for development, build confidence and reduces exam anxiety. BraindumpsPass has created three formats for applicants to pass the CompTIA Cybersecurity Analyst (CySA+) Certification Exam test on the first try.

The CS0-003 Exam is designed to test the candidate's ability to identify and analyze cybersecurity threats, assess the impact of those threats, and implement effective strategies to mitigate them. CS0-003 exam covers a wide range of topics including threat management, vulnerability management, incident response, security architecture and toolsets. It is a comprehensive exam that requires a thorough understanding of cybersecurity principles and practices.

CompTIA Cybersecurity Analyst (CySA+) Certification Exam Sample Questions (Q609-Q614):

NEW QUESTION # 609

A security analyst recently joined the team and is trying to determine which scripting language is being used in a production script to determine if it is malicious. Given the following script:

```
foreach ($user in Get-Content .\this.txt)
{
    Get-ADUser $user -Properties primaryGroupID |select-object primaryGroupID
    Add-ADGroupMember "Domain Users" -Members $user
    Set-ADUser $user -Replace @{primaryGroupID=518}
}
```

Which of the following scripting languages was used in the script?

- A. Shell script
- **B. PowerShell**
- C. Python
- D. Ruby

Answer: B

Explanation:

The script uses PowerShell syntax, such as cmdlets, parameters, variables, and comments. PowerShell is a scripting language that can be used to automate tasks and manage systems.

NEW QUESTION # 610

After an upgrade to a new EDR, a security analyst received reports that several endpoints were not communicating with the SaaS provider to receive critical threat signatures. To comply with the incident response playbook, the security analyst was required to validate connectivity to ensure communications. The security analyst ran a command that provided the following output:

* ComputerName: comptia007

* RemotePort: 443

* InterfaceAlias: Ethernet 3

* TcpTestSucceeded: False

Which of the following did the analyst use to ensure connectivity?

- A. ping
- **B. tnc**
- C. tracert
- D. nmap

Answer: B

Explanation:

Comprehensive Detailed Explanation: The command output shown indicates that the analyst used a TCP connection test to check if communication on port 443 (usually HTTPS) succeeded. Here's why each option was or was not suitable:

- * A. nmap: While nmap can scan ports, it does not provide direct feedback on connection success or failure in the manner shown.
- * B. tnc (Test-NetConnection in PowerShell): This command in PowerShell is specifically designed to test connectivity to a specified port and IP address. The output (TcpTestSucceeded: False) is characteristic of the tnc command.
- * C. ping: The ping command only tests ICMP echo replies and does not indicate success or failure on specific ports.
- * D. tracert: tracert traces the path packets take to reach a host but does not provide a direct indication of port availability or success.

NEW QUESTION # 611

Which of the following is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence?

- A. Vulnerability assessment
- B. Penetration test

- C. Risk register
- D. Compliance report

Answer: C

Explanation:

A risk register is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence. A risk register is a document that records the details of all the risks identified in a project or an organization, such as their sources, causes, consequences, probabilities, impacts, and mitigation strategies. A risk register can help the security team to prioritize the risks based on their severity and urgency, and to monitor and control them throughout the project or the organization's lifecycle. A vulnerability assessment, a penetration test, and a compliance report are all methods or outputs of identifying and evaluating the threats and vulnerabilities, but they are not tools for mapping, tracking, and mitigating them.

NEW QUESTION # 612

A security analyst has found the following suspicious DNS traffic while analyzing a packet capture:

- * DNS traffic while a tunneling session is active.
- * The mean time between queries is less than one second.
- * The average query length exceeds 100 characters.

Which of the following attacks most likely occurred?

- A. DNS poisoning
- B. DNS spoofing
- C. DNS exfiltration
- D. DNS zone transfer

Answer: C

Explanation:

DNS exfiltration is a technique that uses the DNS protocol to transfer data from a compromised network or device to an attacker-controlled server. DNS exfiltration can bypass firewall rules and security products that do not inspect DNS traffic. The characteristics of the suspicious DNS traffic in the question match the indicators of DNS exfiltration, such as:

DNS traffic while a tunneling session is active: This implies that the DNS protocol is being used to create a covert channel for data transfer.

The mean time between queries is less than one second: This implies that the DNS queries are being sent at a high frequency to maximize the amount of data transferred.

The average query length exceeds 100 characters: This implies that the DNS queries are encoding large amounts of data in the subdomains or other fields of the DNS packets.

Official Reference:

<https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>

<https://resources.infosecinstitute.com/topic/bypassing-security-products-via-dns-data-exfiltration/>

https://www.reddit.com/r/CompTIA/comments/nvjuzt/dns_exfiltration_explanation/

NEW QUESTION # 613

Which of the following best explains the importance of utilizing an incident response playbook?

- A. It defines how many disaster recovery sites should be staged.
- B. It prioritizes the business-critical assets for data recovery.
- C. It establishes actions to execute when inputs trigger an event.
- D. It documents the organization asset management and configuration.

Answer: C

Explanation:

Incident response playbooks provide a structured step-by-step guide for handling security incidents. They define actions to take when specific threat indicators or events occur, ensuring a coordinated and consistent response.

* Option A (Prioritizing business-critical assets) relates more to disaster recovery (DR) than incident response.

* Option C (Documenting asset management) is part of IT governance, not incident response.

* Option D (Defining DR sites) falls under business continuity planning, not real-time incident handling.

Thus, B is the best answer, as playbooks are designed to trigger appropriate responses to incidents.

• • • • •

New CS0-003 Exam Prep: <https://www.braindumps.com/CompTIA/CS0-003-practice-exam-dumps.html>

- What's more, part of that BraindumpsPass CS0-003 dumps now are free: <https://drive.google.com/open?id=1epXLgR0YAcFX2pEXv8hivgis8mJzJ9>

id=1epXLgljR0YAcFX2pEXv8hivgjs8mJzJ9