



CS0-001^{Q&As}

CompTIA Cybersecurity Analyst

Pass CompTIA CS0-001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/cs0-001.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

A security analyst's daily review of system logs and SIEM showed fluctuating patterns of latency. During the analysis, the analyst discovered recent attempts of intrusion related to malware that overwrites the MBR. The facilities manager informed the analyst that a nearby construction project damaged the primary power lines, impacting the analyst's support systems. The electric company has temporarily restored power, but the area may experience temporary outages.

Which of the following issues the analyst focus on to continue operations?

- A. Updating the ACL
- B. Conducting backups
- C. Virus scanning
- D. Additional log analysis

Correct Answer: C

QUESTION 2

A cybersecurity analyst has received an alert that well-known "call home" messages are continuously observed by network sensors at the network boundary. The proxy firewall successfully drops the messages. After determining the alert was a true positive, which of the following represents the MOST likely cause?

- A. Attackers are running reconnaissance on company resources.
- B. An outside command and control system is attempting to reach an infected system.
- C. An insider is trying to exfiltrate information to a remote network.
- D. Malware is running on a company system.

Correct Answer: B

QUESTION 3

An organization is requesting the development of a disaster recovery plan. The organization has grown and so has its infrastructure. Documentation, policies, and procedures do not exist. Which of the following steps should be taken to assist in the development of the disaster recovery plan?

- A. Conduct a risk assessment.
- B. Develop a data retention policy.
- C. Execute vulnerability scanning.
- D. Identify assets.

Correct Answer: D



QUESTION 4

A security analyst, who is working for a company that utilizes Linux servers, receives the following results from a vulnerability scan:

CVE ID	CVSS Base	Name
CVE-1999-0524	None	ICMP timestamp request remote date disclosure
CVE-1999-0497	5.0	Anonymous FTP enabled
None	7.5	Unsupported web server detection
CVE-2005-2150	5.0	Windows SMB service enumeration via \srvsvc

Which of the following is MOST likely a false positive?

- A. ICMP timestamp request remote date disclosure
- B. Windows SMB service enumeration via \srvsvc
- C. Anonymous FTP enabled
- D. Unsupported web server detection

Correct Answer: B

QUESTION 5

A recent audit has uncovered several coding errors and a lack of input validation being used on a public portal. Due to the nature of the portal and the severity of the errors, the portal is unable to be patched. Which of the following tools could be used to reduce the risk of being compromised?

- A. Web application firewall
- B. Network firewall
- C. Web proxy
- D. Intrusion prevention system

Correct Answer: A



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

- 100% Guaranteed Success
- 100% Money Back Guarantee
- 365 Days Free Update
- Instant Download After Purchase
- 24x7 Customer Support
- Average 99.9% Success Rate
- More than 800,000 Satisfied Customers Worldwide
- Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.geekcert.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



 One Year Free Update <p>Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 Money Back Guarantee <p>To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 Security & Privacy <p>We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © geekcert, All Rights Reserved.