



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.pass4itsure.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**

After implementing and running an automated patching tool, a security administrator ran a vulnerability scan that reported no missing patches found. Which of the following BEST describes why this tool was used?

- A. To create a chain of evidence to demonstrate when the servers were patched.
- B. To harden the servers against new attacks.
- C. To provide validation that the remediation was active.
- D. To generate log data for unreleased patches.

Correct Answer: B

QUESTION 2

A company discovers an unauthorized device accessing network resources through one of many network drops in a common area used by visitors. The company decides that it wants to quickly prevent unauthorized devices from accessing

the network but policy prevents the company from making changes on every connecting client.

Which of the following should the company implement?

- A. Port security
- B. WPA2
- C. Mandatory Access Control
- D. Network Intrusion Prevention

Correct Answer: A

QUESTION 3

An analyst is reviewing the following log from the company web server:

```
15.34.24 GET /directory/listening.php?user=admin&pass=admin1
15.34.27 GET /directory/listening.php?user=admin&pass=admin2
15.34.29 GET /directory/listening.php?user=admin&pass=1admin
15.34.35 GET /directory/listening.php?user=admin&pass=2admin
```

Which of the following is this an example of?

- A. Online rainbow table attack
- B. Offline brute force attack



C. Offline dictionary attack

D. Online hybrid attack

Correct Answer: B

QUESTION 4

A company office was broken into over the weekend. The office manager contacts the IT security group to provide details on which servers were stolen. The security analyst determines one of the stolen servers contained a list of customer PII information, and another server contained a copy of the credit card transactions processed on the Friday before the break-in. In addition to potential security implications of information that could be gleaned from those servers and the rebuilding/restoring of the data on the stolen systems, the analyst needs to determine any communication or notification requirements with respect to the incident. Which of the following items is MOST important when determining what information needs to be provided, who should be contacted, and when the communication needs to occur.

A. Total number of records stolen

B. Government and industry regulations

C. Impact on the reputation of the company's name/brand

D. Monetary value of data stolen

Correct Answer: B

QUESTION 5

A production web server is experiencing performance issues. Upon investigation, new unauthorized applications have been installed and suspicious traffic was sent through an unused port. Endpoint security is not detecting any malware or virus. Which of the following types of threats would this MOST likely be classified as?

A. Advanced persistent threat

B. Buffer overflow vulnerability

C. Zero day

D. Botnet

Correct Answer: A

[Latest CS0-001 Dumps](#)

[CS0-001 PDF Dumps](#)

[CS0-001 Braindumps](#)



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.pass4itsure.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 © pass4itsure, All Rights Reserved.