



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.pass4lead.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 red team actor observes it is common practice to allow cell phones to charge on company computers, but access to the memory storage is blocked. Which of the following are common attack techniques that take advantage of this practice? (Choose two.)

- A. A USB attack that tricks the computer into thinking the connected device is a keyboard, and then sends characters one at a time as a keyboard to launch the attack (a prerecorded series of keystrokes)
- B. A USB attack that turns the connected device into a rogue access point that spoofs the configured wireless SSIDs
- C. A Bluetooth attack that modifies the device registry (Windows PCs only) to allow the flash drive to mount, and then launches a Java applet attack
- D. A Bluetooth peering attack called "Snarfing" that allows Bluetooth connections on blocked device types if physically connected to a USB port
- E. A USB attack that tricks the system into thinking it is a network adapter, then runs a user password hash gathering utility for offline password cracking

Correct Answer: CD

QUESTION 2

A cybersecurity analyst develops a regular expression to find data within traffic that will alarm on a hit.

```
^(?:4[0-9]{12}(?:[0-9]{3})?:5[1-5][0-9]{2})$
```

The SIEM alarms on seeing this data in cleartext between the web server and the database server.

```
'4554-8795-1596-7948'  
'3723-159786-57984'
```

Which of the following types of data would the analyst MOST likely be concerned with, and to which type of data classification does it belong?

- A. Credit card numbers that are PCI
- B. Social security numbers that are PHI
- C. Credit card numbers that are PII
- D. Social security numbers that are PII

Correct Answer: A

QUESTION 3

Company A suspects an employee has been exfiltrating PII via a USB thumb drive. An analyst is tasked with attempting



to locate the information on the drive. The PII in question includes the following:

| | |
|----------------|-------------|
| comp@mail.com | 564-23-4765 |
| tia@mail.com | 754-09-3276 |
| puter@mail.com | 143-32-2323 |
| sam@mail.com | 545-11-0192 |
| jim@mail.com | 093-45-3748 |

Which of the following would BEST accomplish the task assigned to the analyst?

- A. 3 [0-9]\d-2[0-9]\d-4[0-9]\d
- B. \d(3)-d(2)-\d(4)
- C. ?[3]-?[2]-?[3]
- D. \d[9] `XXX-XX-XX\`

Correct Answer: B

QUESTION 4

A Chief Information Security Officer (CISO) wants to standardize the company's security program so it can be objectively assessed as part of an upcoming audit requested by management.

Which of the following would holistically assist in this effort?

- A. ITIL
- B. NIST
- C. Scrum
- D. AUP
- E. Nessus

Correct Answer: B

QUESTION 5

A company that is hiring a penetration tester wants to exclude social engineering from the list of authorized activities. Which of the following documents should include these details?

- A. Acceptable use policy
- B. Service level agreement



C. Rules of engagement

D. Memorandum of understanding

E. Master service agreement

Correct Answer: C

[CS0-001 Practice Test](#)

[CS0-001 Study Guide](#)

[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.pass4lead.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



| | | |
|---|---|--|
|  <p>One Year Free Update 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> |  <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p> |  <p>Security & Privacy 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 © pass4lead, All Rights Reserved.