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.lead4pass.com/cs0-001.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An ATM in a building lobby has been compromised. A security technician has been advised that the ATM must be forensically analyzed by multiple technicians. Which of the following items in a forensic tool kit would likely be used FIRST? (Select TWO).

A. Drive adapters

B. Chain of custody form

C. Write blockers

D. Crime tape

E. Hashing utilities

F. Drive imager

Correct Answer: BC

QUESTION 2

The new Chief Technology Officer (CTO) is seeking recommendations for network monitoring services for the local intranet. The CTO would like the capability to monitor all traffic to and from the gateway, as well as the capability to block certain content. Which of the following recommendations would meet the needs of the organization?

A. Recommend setup of IP filtering on both the internal and external interfaces of the gateway router.

B. Recommend installation of an IDS on the internal interface and a firewall on the external interface of the gateway router.

C. Recommend installation of a firewall on the internal interface and a NIDS on the external interface of the gateway router.

D. Recommend installation of an IPS on both the internal and external interfaces of the gateway router.

Correct Answer: C

QUESTION 3

An investigation showed a worm was introduced from an engineer\\'s laptop. It was determined the company does not provide engineers with company-owned laptops, which would be subject to company policy and technical controls.

Which of the following would be the MOST secure control implement?

A. Deploy HIDS on all engineer-provided laptops, and put a new router in the management network.

B. Implement role-based group policies on the management network for client access.

C. Utilize a jump box that is only allowed to connect to clients from the management network.

D. Deploy a company-wide approved engineering workstation for management access.

Correct Answer: D

QUESTION 4

An organization is performing vendor selection activities for penetration testing, and a security analyst is reviewing the MOA and rules of engagement, which were supplied with proposals. Which of the following should the analyst expect will be included in the documents and why?

A. The scope of the penetration test should be included in the MOA to ensure penetration testing is conducted against only specifically authorized network resources.

B. The MOA should address the client SLA in relation to reporting results to regulatory authorities, including issuing banks for organizations that process cardholder data.

C. The rules of engagement should include detailed results of the penetration scan, including all findings, as well as designation of whether vulnerabilities identified during the scanning phases are found to be exploitable during the penetration test.

D. The exploitation standards should be addressed in the rules of engagement to ensure both parties are aware of the depth of exploitation that will be attempted by penetration testers.

Correct Answer: C

QUESTION 5

A cybersecurity analyst has been asked to follow a corporate process that will be used to manage vulnerabilities for an organization. The analyst notices the policy has not been updated in three years. Which of the following should the analyst check to ensure the policy is still accurate?

A. Threat intelligence reports

B. Technical constraints

C. Corporate minutes

D. Governing regulations

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.lead4pass.com/allproducts

Need Help

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