CS0-002 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-002 Exam with 100% Guarantee

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

https://www.passapply.com/cs0-002.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An analyst needs to forensically examine a Windows machine that was compromised by a threat actor. Intelligence reports state this specific threat actor is characterized by hiding malicious artifacts, especially with alternate data streams. Based on this intelligence, which of the following BEST explains alternate data streams?

A. A different way data can be streamlined if the user wants to use less memory on a Windows system for forking resources.

B. A way to store data on an external drive attached to a Windows machine that is not readily accessible to users.

C. A Windows attribute that provides for forking resources and is potentially used to hide the presence of secret or malicious files inside the file records of a benign file.

D. A Windows attribute that can be used by attackers to hide malicious files within system memory.

Correct Answer: C

QUESTION 2

An audit has revealed an organization is utilizing a large number of servers that are running unsupported operating systems.

As part of the management response phase of the audit, which of the following would BEST demonstrate senior management is appropriately aware of and addressing the issue?

A. Copies of prior audits that did not identify the servers as an issue

B. Project plans relating to the replacement of the servers that were approved by management

C. Minutes from meetings in which risk assessment activities addressing the servers were discussed

D. ACLs from perimeter firewalls showing blocked access to the servers

E. Copies of change orders relating to the vulnerable servers

Correct Answer: B

QUESTION 3

A company has decided to process credit card transactions directly. Which of the following would meet the requirements for scanning this type of data?

A. Quarterly

B. Yearly

C. Bi-annually

D. Monthly

Correct Answer: A

QUESTION 4

A large amount of confidential data was leaked during a recent security breach. As part of a forensic investigation, the security team needs to identify the various types of traffic that were captured between two

compromised devices.

Which of the following should be used to identify the traffic?

A. Carving

B. Disk imaging

C. Packet analysis

D. Memory dump

E. Hashing

Correct Answer: C

QUESTION 5

An organization has the following policies:

1.

Services must run on standard ports.

2.

Unneeded services must be disabled.

The organization has the following servers:

192.168.10.1 - web server

192.168.10.2 - database server

A security analyst runs a scan on the servers and sees the following output:

```
Host 192.168.10.1
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
443/tcp   open     https
1027/tcp  open     IIS

Host 192.168.10.2
PORT      STATE    SERVICE
22/tcp    open     ssh
53/tcp    open     dns
1434/tcp  open     mssql
```

Which of the following actions should the analyst take?

A. Disable HTTPS on 192.168.10.1.

B. Disable IIS on 192.168.10.1.

C. Disable DNS on 192.168.10.2.

D. Disable MSSQL on 192.168.10.2.

E. Disable SSH on both servers.

Correct Answer: C