CV0-004 Q&As

CompTIA Cloud+ (2024)

Pass CompTIA CV0-004 Exam with 100% Guarantee

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

https://www.leads4pass.com/cv0-004.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 system surpasses 75% to 80% of resource consumption. Which of the following scaling approaches is the most appropriate?

A. Trending

B. Manual

C. Load

D. Scheduled

Correct Answer: C

Load scaling is the most appropriate approach when a system surpasses 75% to 80% of resource consumption. This method involves adjusting resources dynamically in response to the current load, ensuring the system can handle increased demand without performance degradation. Load scaling can be automatic, allowing systems to scale up or down based on predefined metrics like CPU usage, memory, or network traffic, providing an efficient way to manage resources and maintain optimal performance. References: The CompTIA Cloud+ exam objectives include understanding cloud management and technical operations, which encompass knowledge of various scaling approaches, including load scaling, to ensure efficient resource utilization in cloud environments.

QUESTION 2

A cloud infrastructure administrator updated the IP tables to block incoming connections and outgoing responses to 104.225.110.203. Which of the following vulnerability management steps is this an example of?

A. Scanning scope

B. Remediation

C. Identification

D. Assessment

Correct Answer: B

Updating the IP tables to block connections to a specific IP address as a response to vulnerabilities is an example of remediation. Remediation involves taking direct action to fixvulnerabilities, such as by applying patches, changing configurations, or, in this case, updating firewall rules to block potentially harmful traffic. References: CompTIA Cloud+ resources and vulnerability management processes

QUESTION 3

A cloud engineer is deploying a server in a cloud platform. The engineer reviews a security scan report. Which of the following recommended services should be disabled? (Select two).

A. Telnet

B. FTP

C. Remote log-in

D. DNS

E. DHCP

F. LDAP

Correct Answer: AB

Telnet and FTP are recommended services to be disabled when deploying a server in a cloud platform, as they are insecure protocols that transmit data in plain text and expose credentials and sensitive information to potential attackers12.

Remote log-in, DNS, DHCP, and LDAP are not necessarily recommended to be disabled, as they may provide useful functionality for the server and the cloud environment. However, they should be configured properly and secured with

encryption, authentication, and authorization mechanisms34.

References: CompTIA Cloud+ CV0-003 Exam Objectives, Objective 4.2: Given a scenario, apply security configurations and compliance controls ; CompTIA Quick Start Guide to Tackling Cloud Security Concerns3

QUESTION 4

A technician receives an email from a vendor who is requesting payment of an invoice for human resources services. The email contains a request for bank account numbers. Which of the following types of attacks does this behavior most likely indicate?

A. Malware

B. Cryptojacking

C. Ransomware

D. Phishing

Correct Answer: D

The behavior described in the question indicates a phishing attack. Phishing typically involves an attacker masquerading as a legitimate entity to trick individuals into providing sensitive information, such as bank account numbers, through seemingly trustworthy communication channels like email.References: Understanding security concerns and measures is part of the Governance, Risk, Compliance, and Security domain of the CompTIA Cloud+ objectives.

QUESTION 5

A developer at a small startup company deployed some code for a new feature to its public repository. A few days later, a data breach occurred. A security team investigated the incident and found that the database was hacked.

Which of the following is the most likely cause of this breach?

A. Database core dump

B. Hard-coded credentials

C. Compromised deployment agent

D. Unpatched web servers

Correct Answer: B

Hard-coded credentials within code, especially when deployed in a public repository, are a common security vulnerability. If credentials such as passwords or API keys are embedded in the code, anyone with access to the repository can

potentially use them to gain unauthorized access to databases or other sensitive resources. This is a likely cause of the data breach in the scenario described.

References: CompTIA Security+ Guide to Network Security Fundamentals by Mark Ciampa.

CV0-004 PDF Dumps CV0-004 VCE Dumps CV0-004 Practice Test