SY0-501 Q&As

CompTIA Security+ Certification Exam

Pass CompTIA SY0-501 Exam with 100% Guarantee

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

https://www.geekcert.com/sy0-501.html

100% Passing Guarantee
100% Money Back Assurance

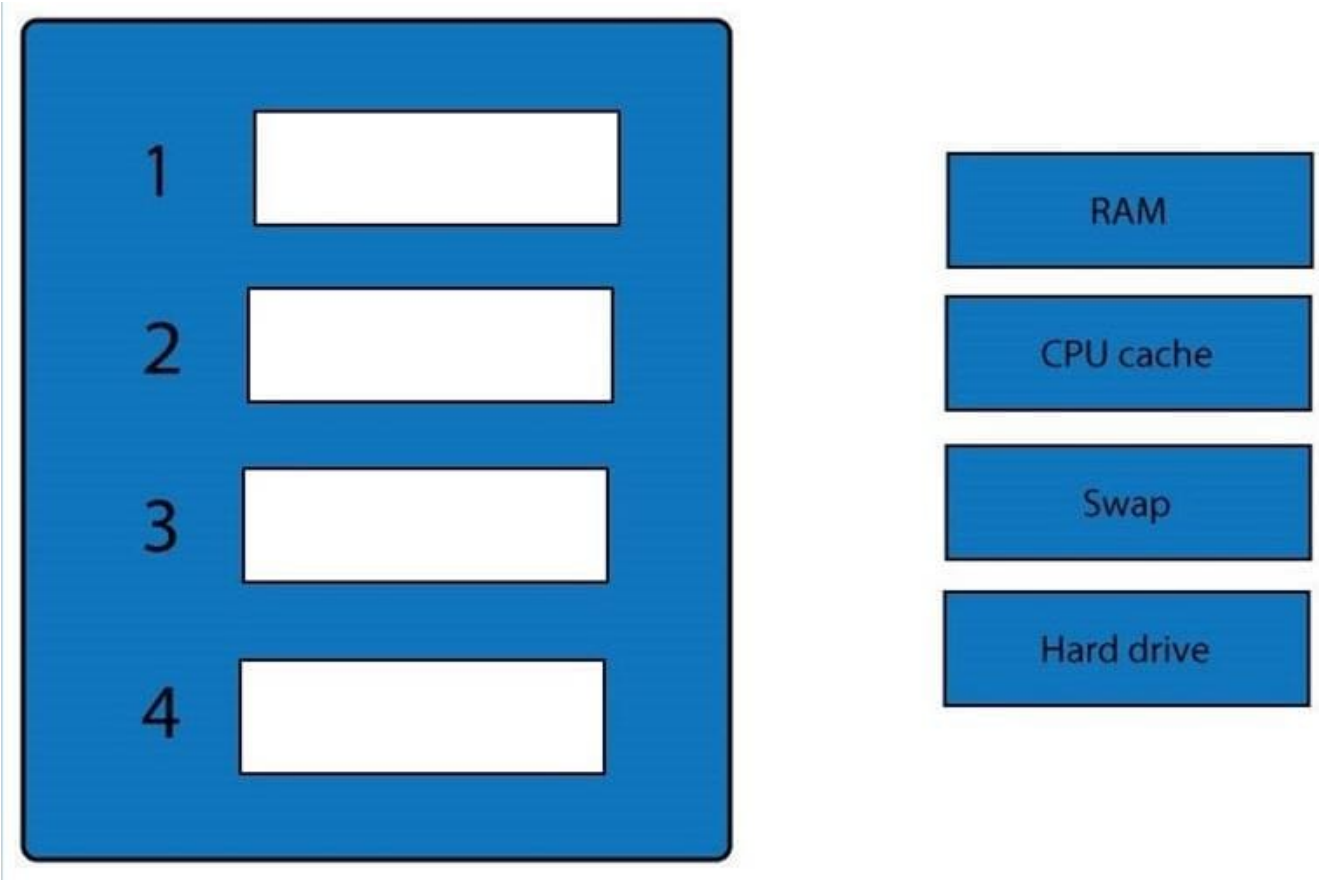
Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

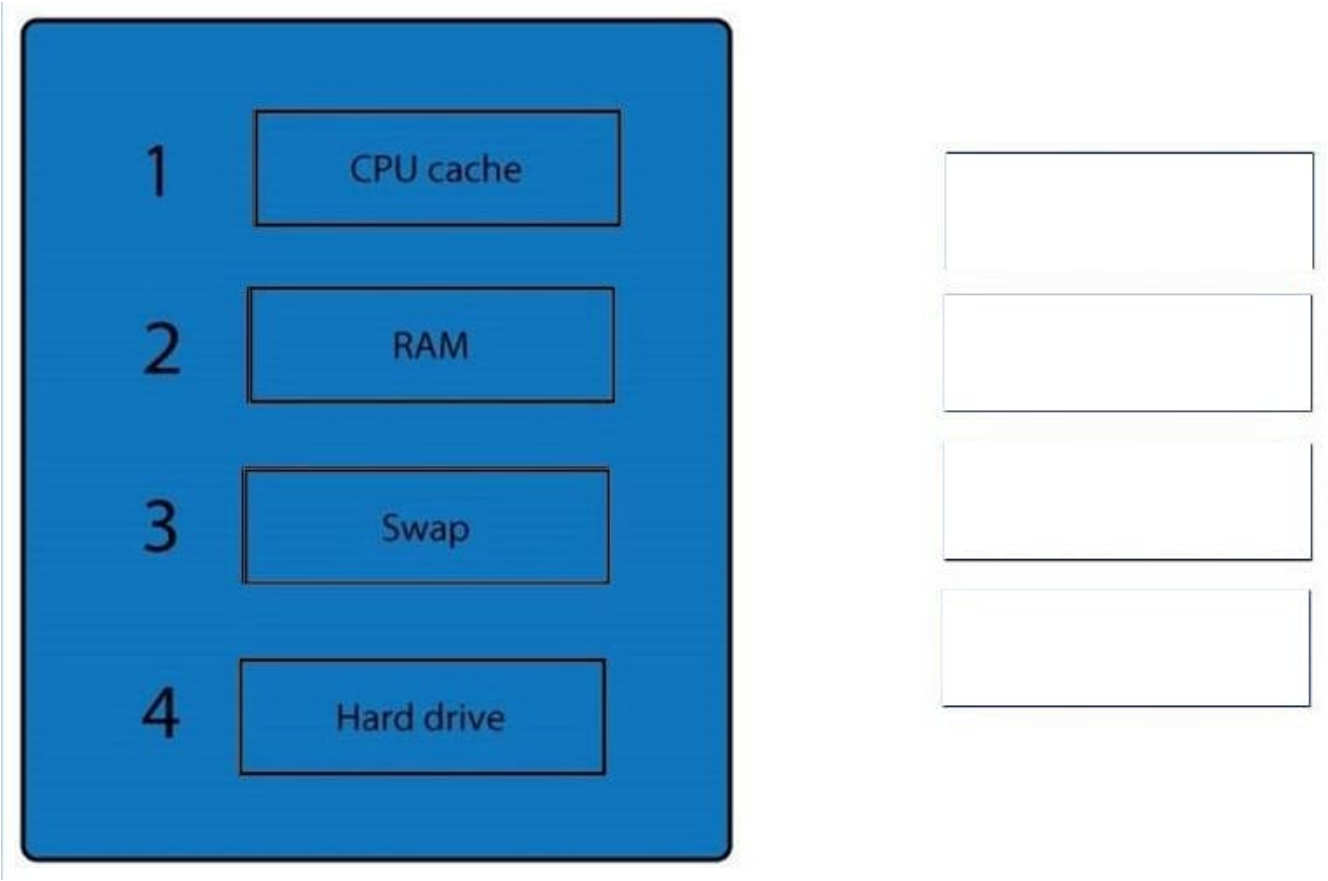
QUESTION 1

A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the correct order in which the forensic analyst should preserve them.

Select and Place:



Correct Answer:



When dealing with multiple issues, address them in order of volatility (OOV); always deal with the most volatile first. Volatility can be thought of as the amount of time that you have to collect certain data before a window of opportunity is gone.

Naturally, in an investigation you want to collect everything, but some data will exist longer than others, and you cannot possibly collect all of it once. As an example, the OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and

printouts.

Order of volatility: Capture system images as a snapshot of what exists, look at network traffic and logs, capture any relevant video/screenshots/hashes, record time offset on the systems, talk to witnesses, and track total man-hours and

expenses associated with the investigation.

QUESTION 2

Which of the following would meet the requirements for multifactor authentication?

A. Username, PIN, and employee ID number

B. Fingerprint and password

C. Smart card and hardware token

D. Voice recognition and retina scan

Correct Answer: B

QUESTION 3

Which of the following types of attack is being used when an attacker responds by sending the MAC address of the attacking machine to resolve the MAC to IP address of a valid server?

A. Session hijacking

B. IP spoofing

C. Evil twin

D. ARP poisoning

Correct Answer: D

An ARP spoofing, also known as ARP poisoning, is a Man in the Middle (MitM) attack that allows attackers to intercept communication between network devices. The attack works as follows: The attacker must have access to the network.

QUESTION 4

The administrator installs database software to encrypt each field as it is written to disk. Which of the following describes the encrypted data?

A. In-transit

B. In-use

C. Embedded

D. At-rest

Correct Answer: B

QUESTION 5

An application was recently compromised after some malformed data came in via web form. Which of the following would MOST likely have prevented this?

A. Input validation

B. Proxy server

C. Stress testing

D. Encoding

Correct Answer: A

Latest SY0-501 Dumps SY0-501 PDF Dumps SY0-501 Exam Questions