CS0-003 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

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

https://www.passapply.com/cs0-003.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A digital forensics investigator works from duplicate images to preserve the integrity of the original evidence. Which of the following types of media are most volatile and should be preserved? (Select two).

A. Memory cache

B. Registry file

C. SSD storage

D. Temporary filesystems

E. Packet decoding

F. Swap volume

Correct Answer: AF

Memory cache and swap volume are types of media that are most volatile and should be preserved during a digital forensics investigation. Volatile media are those that store data temporarily and lose their contents when the power is turned off or interrupted. Memory cache is a small and fast memory that stores frequently used data or instructions for faster access by the processor. Swap volume is a part of the hard disk that is used as an extension of the memory when the memory is full or low . https://www.techopedia.com/definition39/memory-dump

QUESTION 2

A manufacturing company has joined the information sharing and analysis center for its sector. As a benefit, the company will receive structured IoC data contributed by other members. Which of the following best describes the utility of this data?

A. Other members will have visibility into instances of positive IoC identification within the manufacturing company\\'s corporate network.

B. The manufacturing company will have access to relevant malware samples from all other manufacturing sector members.

C. Other members will automatically adjust their security postures to defend the manufacturing company\\'s processes.

D. The manufacturing company can ingest the data and use tools to autogenerate security configurations for all of its infrastructure.

Correct Answer: B

QUESTION 3

A security engineer must deploy X 509 certificates to two web servers behind a load balancer. Each web server is configured identically. Which of the following should be done to ensure certificate name mismatch errors do not occur?

A. Create two certificates, each with the same fully qualified domain name, and associate each with the web servers\\' real IP addresses on the load balancer.

B. Create one certificate on the load balancer and associate the site with the web servers\\' real IP addresses.

C. Create two certificates, each with the same fully qualified domain name, and associate each with a corresponding web server behind the load balancer.

D. Create one certificate and export it to each web server behind the load balancer.

Correct Answer: C

QUESTION 4

A cybersecurity team has witnessed numerous vulnerability events recently that have affected operating systems. The team decides to implement host-based IPS, firewalls, and two-factor authentication.

Which of the following does this most likely describe?

A. System hardening

B. Hybrid network architecture

C. Continuous authorization

D. Secure access service edge

Correct Answer: A

System hardening is the process of securing a system by reducing its attack surface, applying patches and updates, configuring security settings, and implementing security controls. System hardening can help prevent or mitigate vulnerability events that may affect operating systems. Host-based IPS, firewalls, and two-factor authentication are examples of security controls that can be applied to harden a system. The other options are not the best descriptions of the scenario. A hybrid network architecture (B) is a network design that combines on-premises and cloud-based resources, which may or may not involve system hardening. Continuous authorization © is a security approach that monitors and validates the security posture of a system on an ongoing basis, which is different from system hardening. Secure access service edge (D) is a network architecture that delivers cloud-based security services to remote users and devices, which is also different from system hardening.

QUESTION 5

A security analyst wants to capture large amounts of network data that will be analyzed at a later time. The packet capture does not need to be in a format that is readable by humans, since it will be put into a binary file called "packetCapture." The capture must be as efficient as possible, and the analyst wants to minimize the likelihood that packets will be missed. Which of the following commands will best accomplish the analyst\\'s objectives?

A. tcpdump -w packetCapture

B. tcpdump -a packetCapture

C. tcpdump -n packetCapture

D. nmap -v > packetCapture

E. nmap -oA > packetCapture

Correct Answer: A

The tcpdump command is a network packet analyzer tool that can capture and display network traffic. The -w option specifies a file name to write the captured packets to, in a binary format that can be read by tcpdump or other tools later. This option is useful for capturing large amounts of network data that will be analyzed at a later time, as the question requires. The packet capture does not need to be in a format that is readable by humans, since it will be put into a binary file called " . The capture must be as efficient as possible, and the -w option minimizes the processing and output overhead of tcpdump, reducing the likelihood that packets will be missed.