350-201 Q&As

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Pass Cisco 350-201 Exam with 100% Guarantee

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

https://www.pass2lead.com/350-201.html

100% Passing Guarantee
100% Money Back Assurance

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

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

QUESTION 1

An engineer detects an intrusion event inside an organization\\'s network and becomes aware that files that contain personal data have been accessed. Which action must be taken to contain this attack?

A. Disconnect the affected server from the network.

B. Analyze the source.

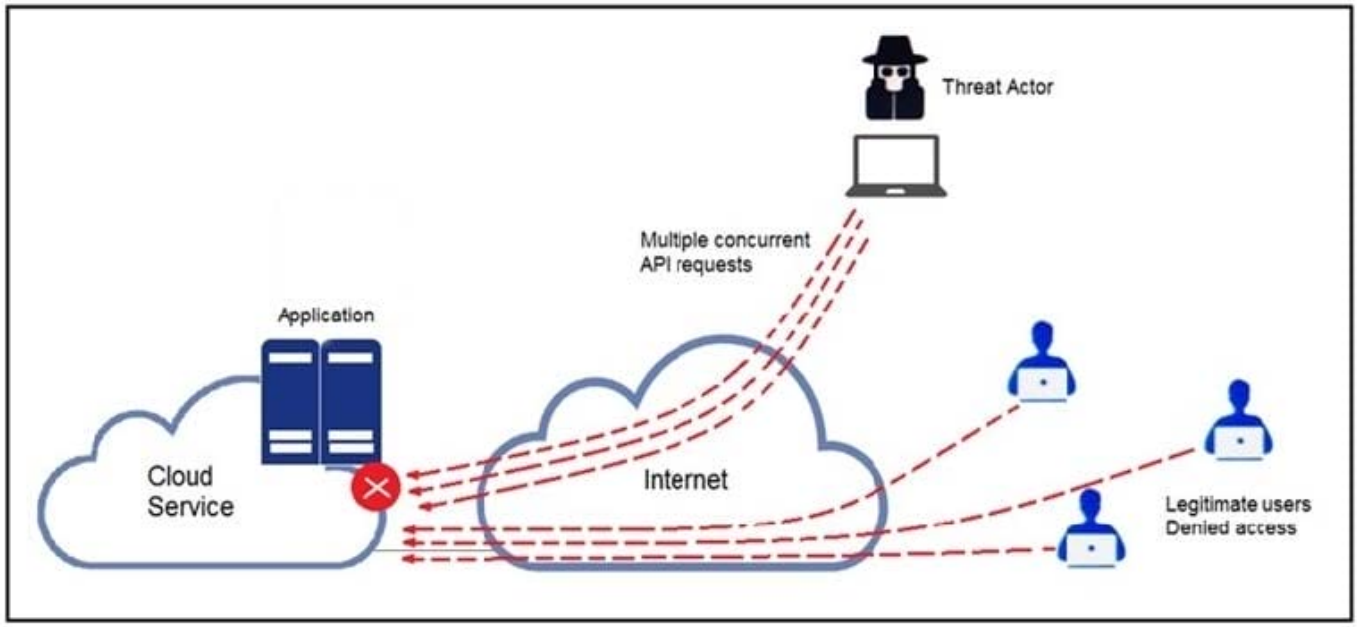
C. Access the affected server to confirm compromised files are encrypted.

D. Determine the attack surface.

Correct Answer: C

QUESTION 2

Refer to the exhibit. A threat actor behind a single computer exploited a cloud-based application by sending multiple concurrent API requests. These requests made the application unresponsive. Which solution protects the application from being overloaded and ensures more equitable application access across the end-user community?



A. Limit the number of API calls that a single client is allowed to make

B. Add restrictions on the edge router on how often a single client can access the API

C. Reduce the amount of data that can be fetched from the total pool of active clients that call the API

D. Increase the application cache of the total pool of active clients that call the API

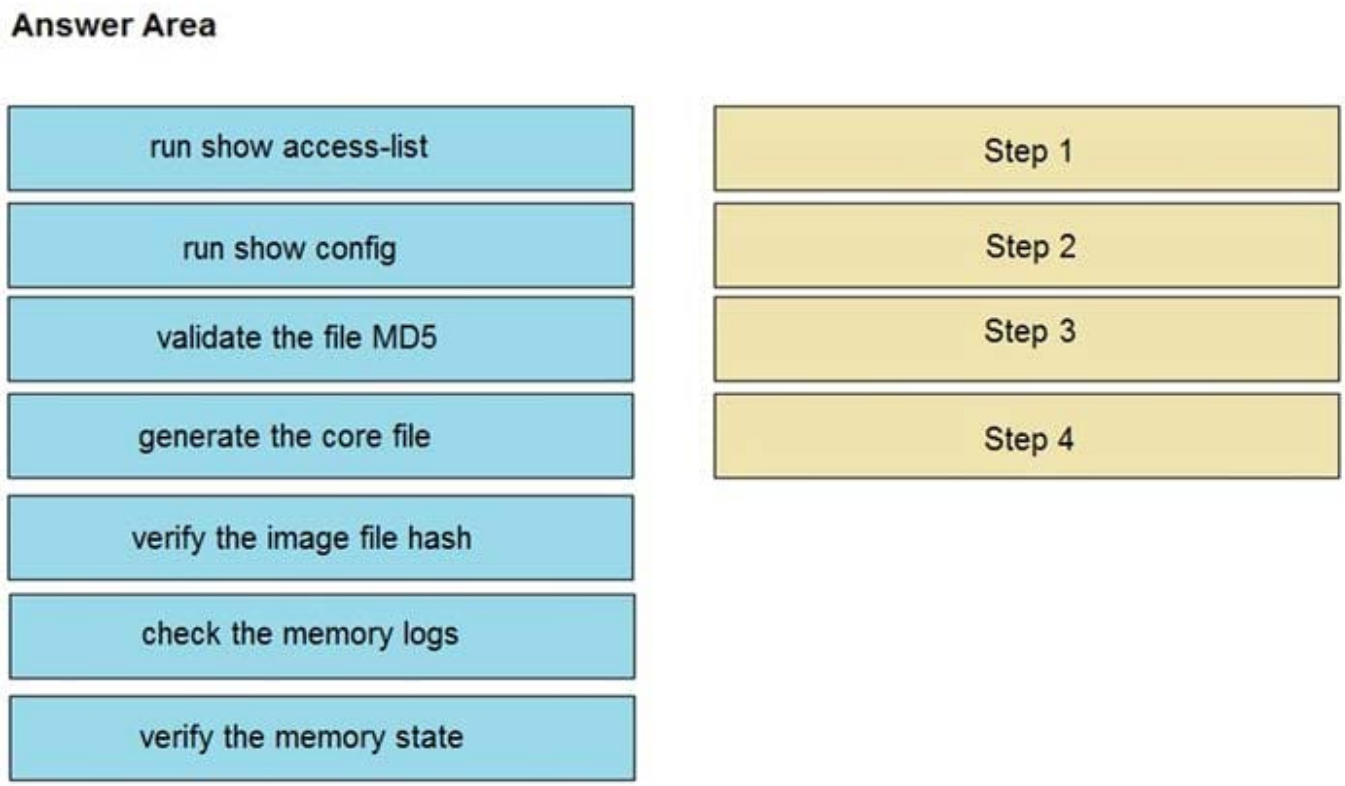
Correct Answer: A

QUESTION 3

DRAG DROP

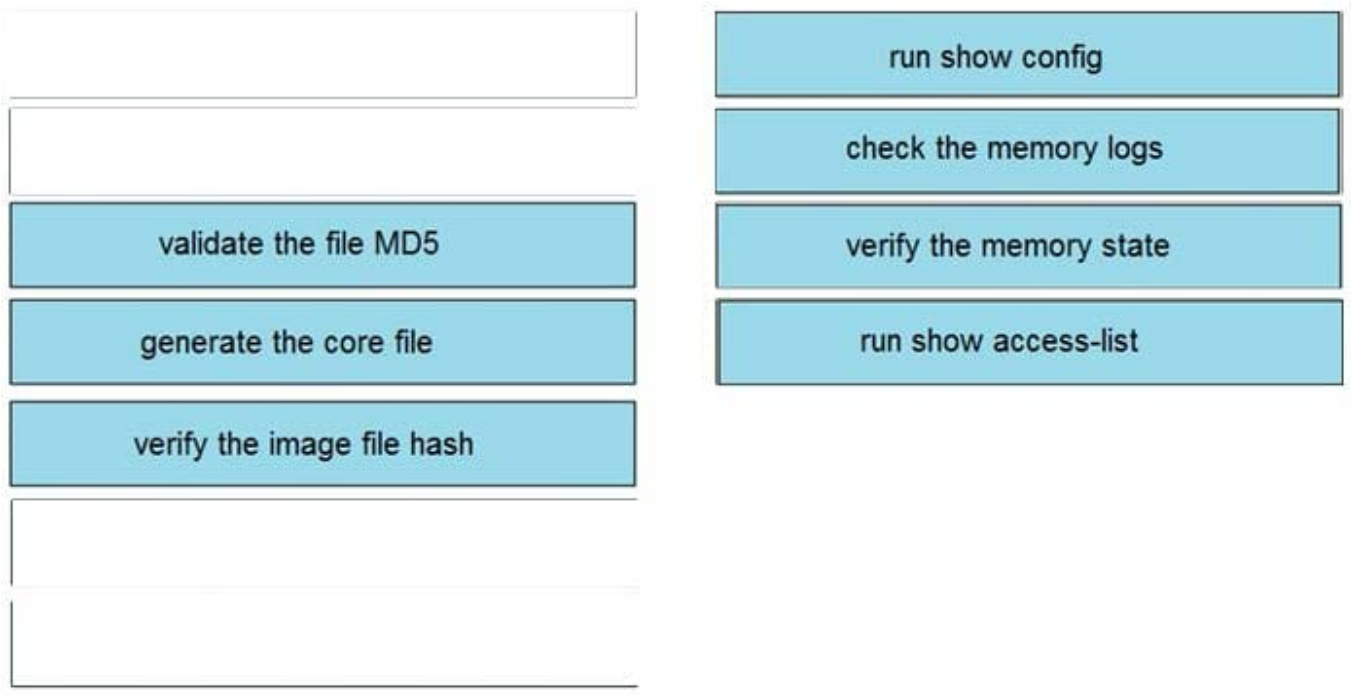
An organization lost connectivity to critical servers, and users cannot access business applications and internal websites. An engineer checks the network devices to investigate the outage and determines that all devices are functioning. Drag and drop the steps from the left into the sequence on the right to continue investigating this issue. Not all options are used.

Select and Place:



Correct Answer:

Answer Area



QUESTION 4

A security manager received an email from an anomaly detection service, that one of their contractors has downloaded 50 documents from the company\\'s confidential document management folder using a company-owned asset al039-ice4ce687TL0500. A security manager reviewed the content of downloaded documents and noticed that the data affected is from different departments. What are the actions a security manager should take?

A. Measure confidentiality level of downloaded documents.

B. Report to the incident response team.

C. Escalate to contractor\\'s manager.

D. Communicate with the contractor to identify the motives.

Correct Answer: B

QUESTION 5

An organization had a breach due to a phishing attack. An engineer leads a team through the recovery phase of the incident response process. Which action should be taken during this phase?

A. Host a discovery meeting and define configuration and policy updates

B. Update the IDS/IPS signatures and reimage the affected hosts

C. Identify the systems that have been affected and tools used to detect the attack

D. Identify the traffic with data capture using Wireshark and review email filters

Correct Answer: C

Latest 350-201 Dumps 350-201 Study Guide 350-201 Exam Questions