350-201$^{\text{Q\&As}}$

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.geekcert.com/350-201.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An engineer notices that every Sunday night, there is a two-hour period with a large load of network activity. Upon further investigation, the engineer finds that the activity is from locations around the globe outside the organization\\'s service area. What are the next steps the engineer must take?

A. Assign the issue to the incident handling provider because no suspicious activity has been observed during business hours.

B. Review the SIEM and FirePower logs, block all traffic, and document the results of calling the call center.

C. Define the access points using StealthWatch or SIEM logs, understand services being offered during the hours in question, and cross-correlate other source events.

D. Treat it as a false positive, and accept the SIEM issue as valid to avoid alerts from triggering on weekends.

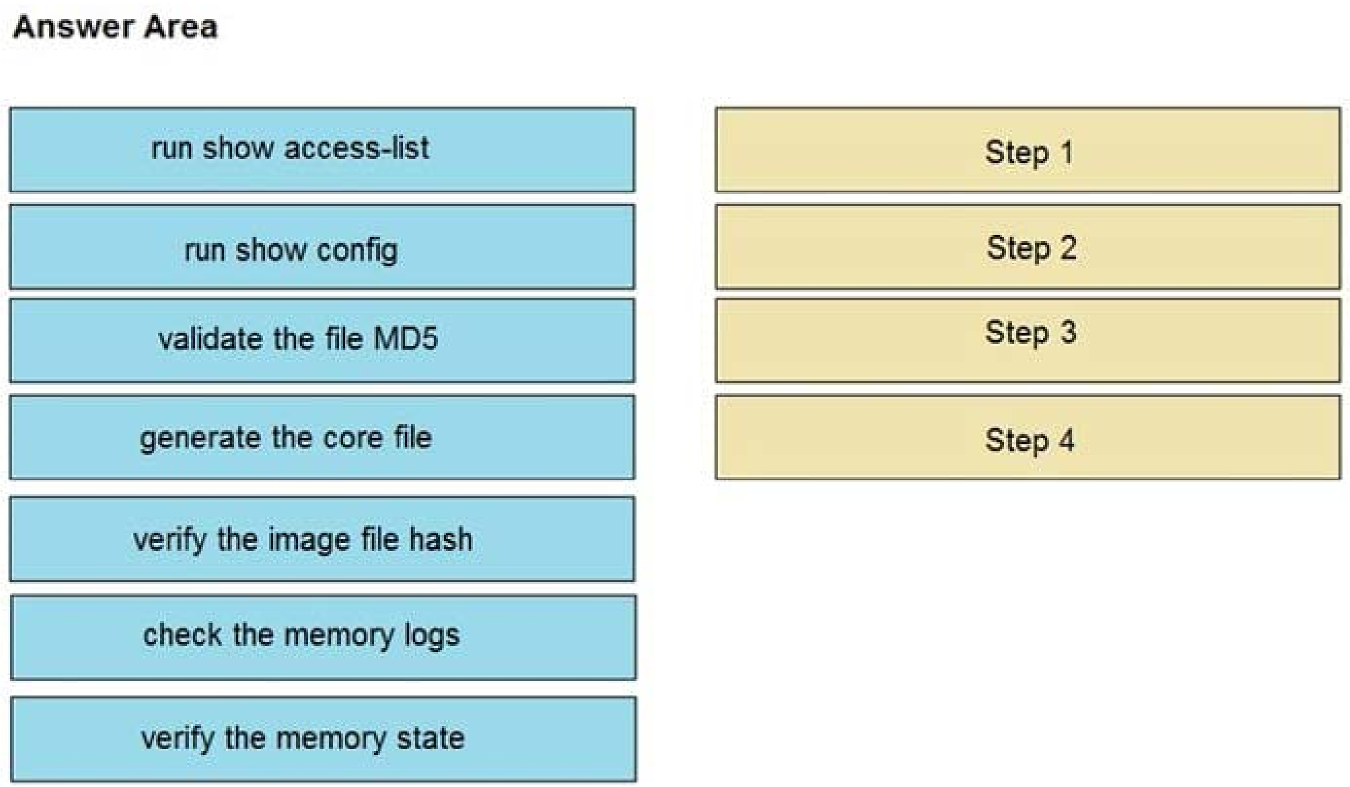
Correct Answer: A

QUESTION 2

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:



Answer Area

run show access-list

run show config

validate the file MD5

generate the core file

verify the image file hash

check the memory logs

verify the memory state

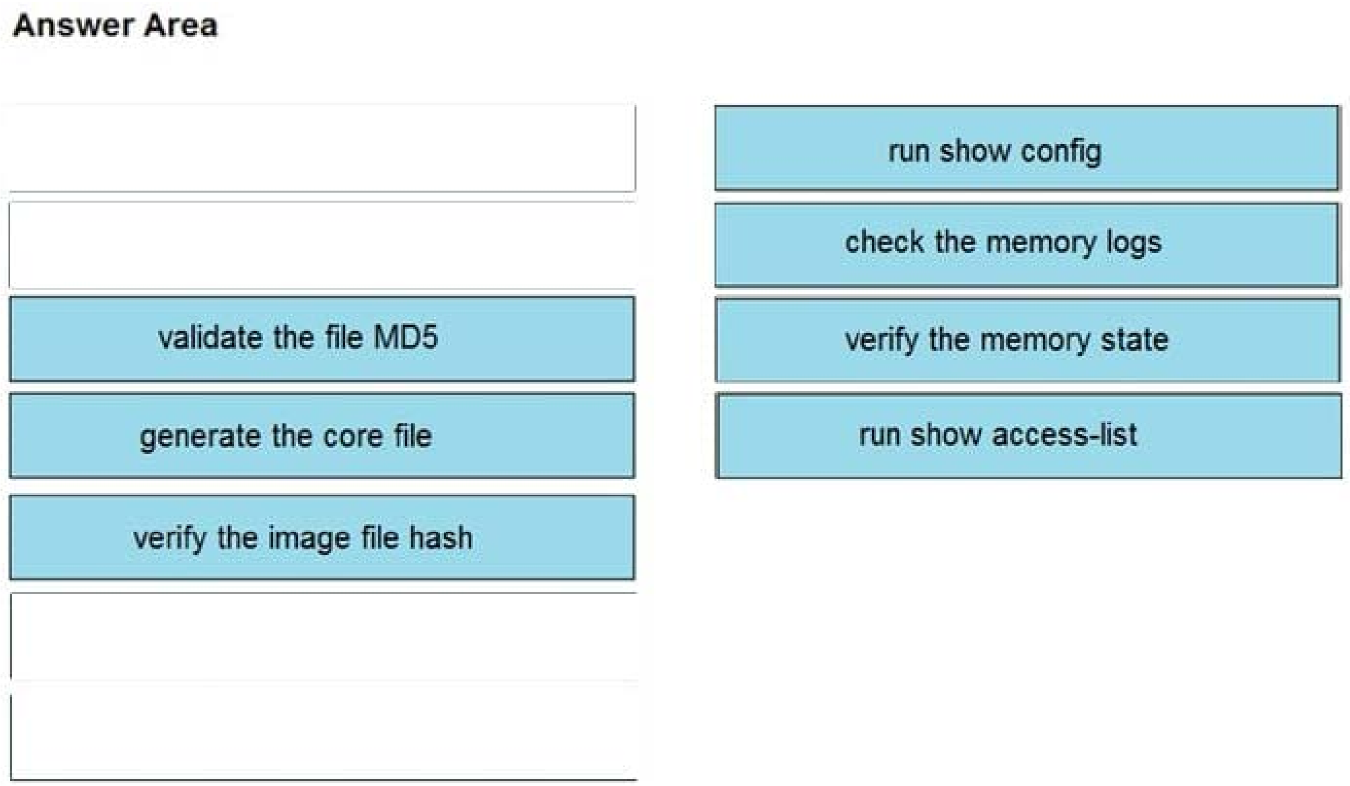
Step 1

Step 2

Step 3

Step 4

Correct Answer:



Answer Area

validate the file MD5

generate the core file

verify the image file hash

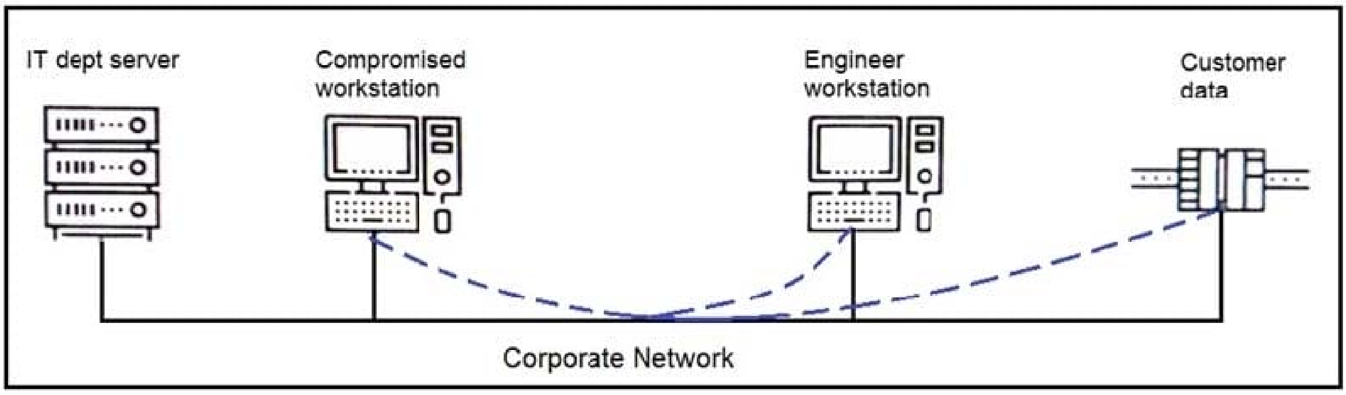
run show config

check the memory logs

verify the memory state

run show access-list

QUESTION 3



Refer to the exhibit. An engineer received a report that an attacker has compromised a workstation and gained access to sensitive customer data from the network using insecure protocols. Which action prevents this type of attack in the future?

A. Use VLANs to segregate zones and the firewall to allow only required services and secured protocols

B. Deploy a SOAR solution and correlate log alerts from customer zones

C. Deploy IDS within sensitive areas and continuously update signatures

D. Use syslog to gather data from multiple sources and detect intrusion logs for timely responses

Correct Answer: A

QUESTION 4

A company recently started accepting credit card payments in their local warehouses and is undergoing a PCI audit. Based on business requirements, the company needs to store sensitive authentication data for 45 days. How must data be stored for compliance?

A. post-authorization by non-issuing entities if there is a documented business justification

B. by entities that issue the payment cards or that perform support issuing services

C. post-authorization by non-issuing entities if the data is encrypted and securely stored

D. by issuers and issuer processors if there is a legitimate reason

Correct Answer: C

QUESTION 5

A malware outbreak is detected by the SIEM and is confirmed as a true positive. The incident response team follows the playbook to mitigate the threat. What is the first action for the incident response team?

A. Assess the network for unexpected behavior

B. Isolate critical hosts from the network

C. Patch detected vulnerabilities from critical hosts

D. Perform analysis based on the established risk factors

Correct Answer: B