Vendor: Cisco

Exam Code:350-201

Exam Name: Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Version: Demo

QUESTION 1

An engineer is analyzing a possible compromise that happened a week ago when the company? (Choose two.)

A. firewall

B. Wireshark

C. autopsy

D. SHA512

E. IPS

Correct Answer: AB

QUESTION 2

What is idempotence?

A. the assurance of system uniformity throughout the whole delivery process

B. the ability to recover from failures while keeping critical services running

C. the necessity of setting maintenance of individual deployment environments

D. the ability to set the target environment configuration regardless of the starting state

Correct Answer: A

QUESTION 3

A threat actor has crafted and sent a spear-phishing email with what appears to be a trustworthy link to the site of a conference that an employee recently attended. The employee clicked the link and was redirected to a malicious site through which the employee downloaded a PDF attachment infected with ransomware. The employee opened the attachment, which exploited vulnerabilities on the desktop. The ransomware is now installed and is calling back to its command and control server.

Which security solution is needed at this stage to mitigate the attack?

A. web security solution

B. email security solution

C. endpoint security solution

D. network security solution

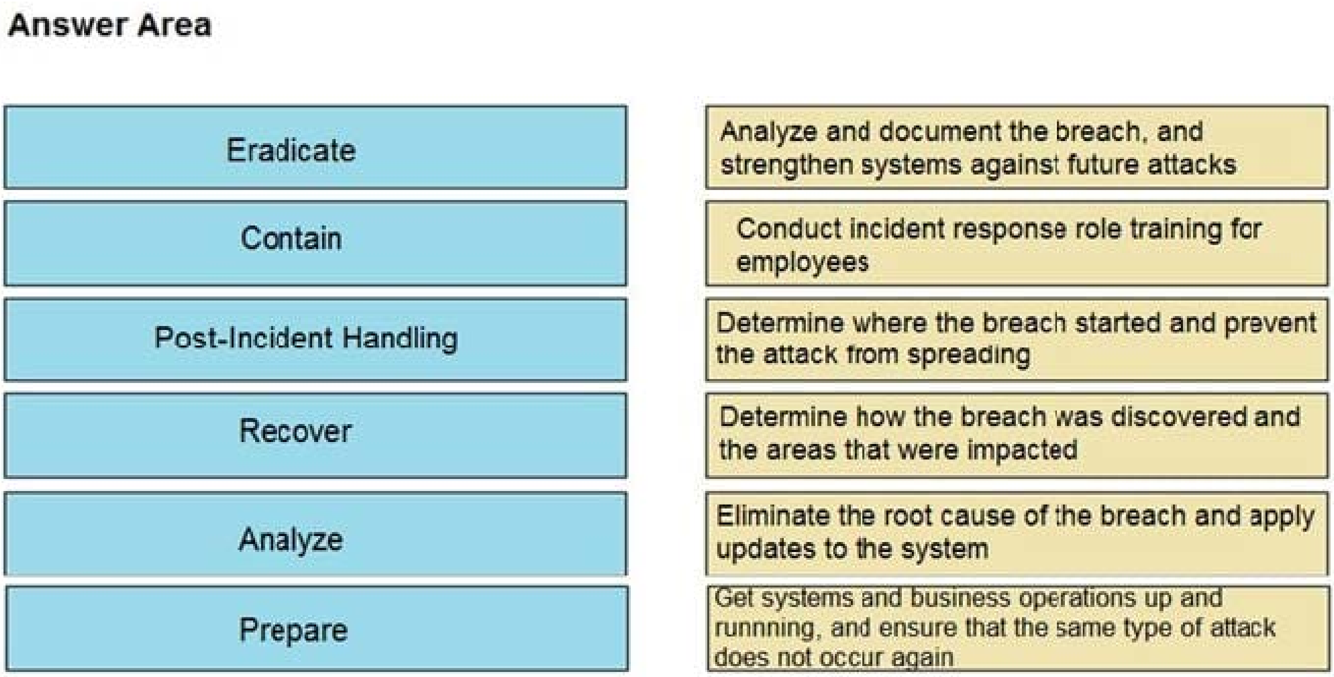
Correct Answer: D

QUESTION 4

DRAG DROP

Drag and drop the NIST incident response process steps from the left onto the actions that occur in the steps on the right.

Select and Place:



Answer Area

Eradicate

Contain

Post-Incident Handling

Recover

Analyze

Prepare

Analyze and document the breach, and strengthen systems against future attacks

Conduct incident response role training for employees

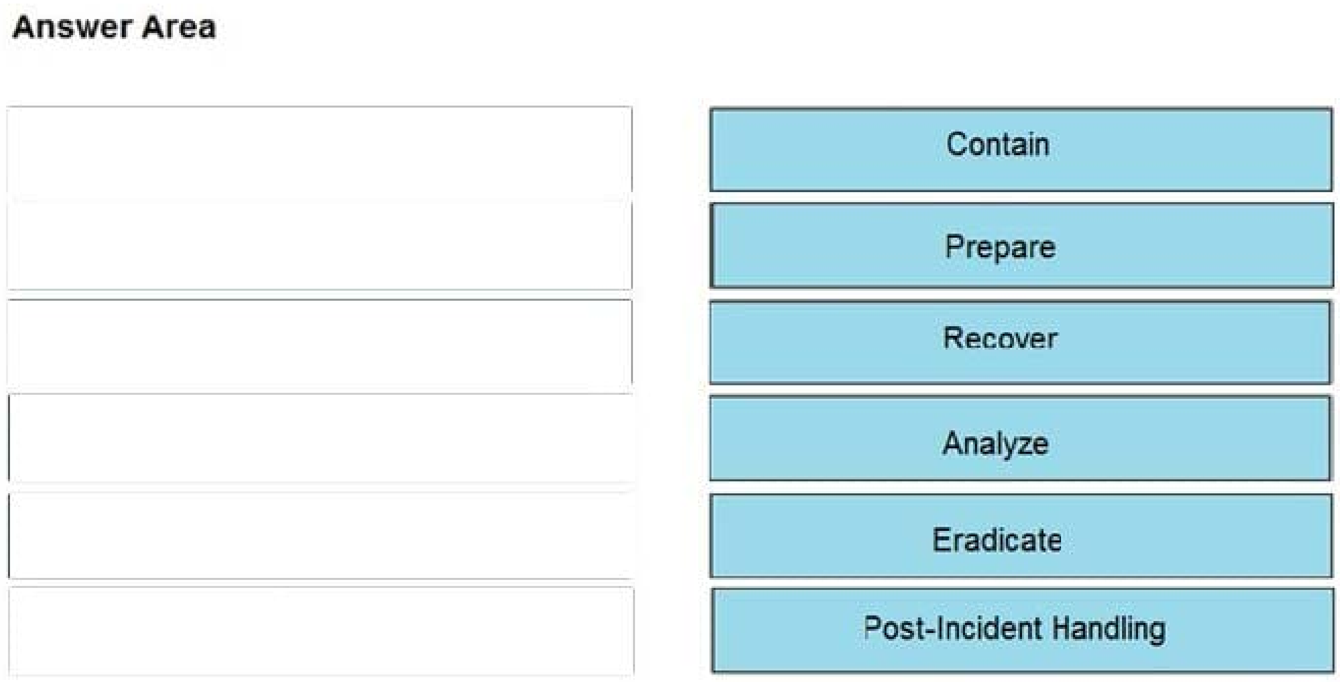
Determine where the breach started and prevent the attack from spreading

Determine how the breach was discovered and the areas that were impacted

Eliminate the root cause of the breach and apply updates to the system

Get systems and business operations up and runnning, and ensure that the same type of attack does not occur again

Correct Answer:



Reference: https://www.securitymetrics.com/blog/6-phases-incident-response-plan

---

QUESTION 5

What is needed to assess risk mitigation effectiveness in an organization?

A. analysis of key performance indicators

B. compliance with security standards

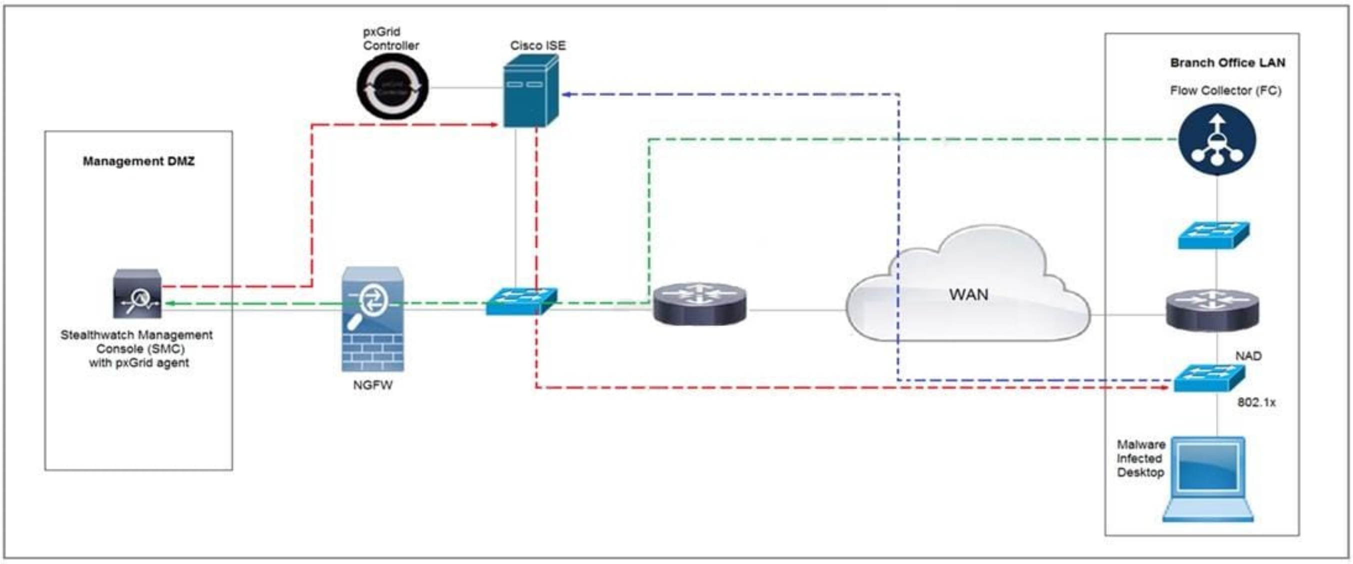
C. cost-effectiveness of control measures

D. updated list of vulnerable systems

Correct Answer: C

QUESTION 6

Refer to the exhibit. Rapid Threat Containment using Cisco Secure Network Analytics (Stealthwatch) and ISE detects the threat of malware-infected 802.1x authenticated endpoints and places that endpoint into a quarantine VLAN using Adaptive Network Control policy. Which method was used to signal ISE to quarantine the endpoints?



A. SNMP

B. syslog

C. REST API

D. pxGrid

Correct Answer: C

QUESTION 7

A Mac laptop user notices that several files have disappeared from their laptop documents folder. While looking for the files, the user notices that the browser history was recently cleared. The user raises a case, and an analyst reviews the network usage and discovers that it is abnormally high.

Which step should be taken to continue the investigation?

A. Run the sudo sysdiagnose command

B. Run the sh command

C. Run the w command

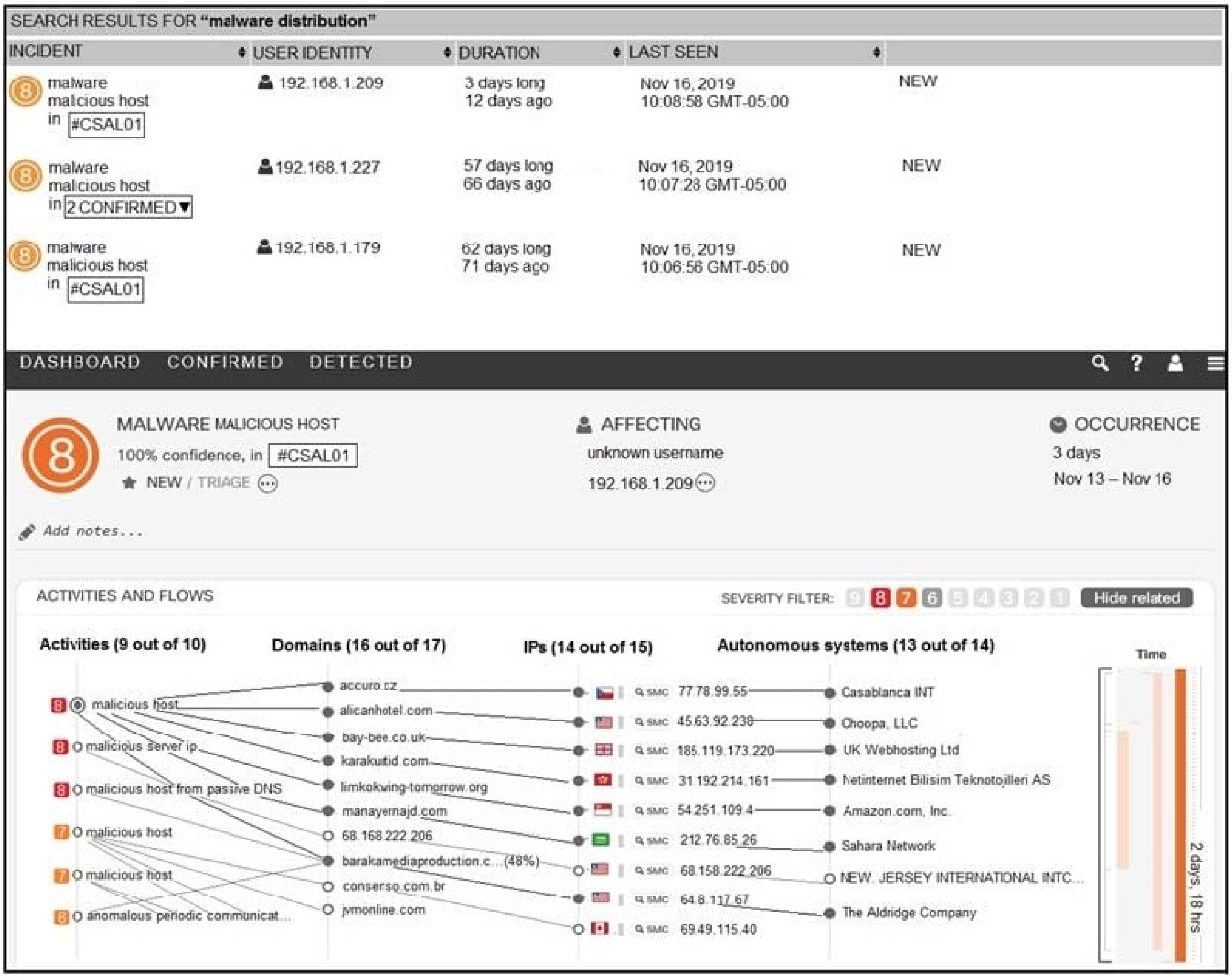
D. Run the who command

Correct Answer: A

Reference: https://eclecticlight.co/2016/02/06/the-ultimate-diagnostic-tool-sysdiagnose/

QUESTION 8

Refer to the exhibit. For IP 192.168.1.209, what are the risk level, activity, and next step?



SEARCH RESULTS FOR **"malware distribution"**

INCIDENT	USER IDENTITY	DURATION	LAST SEEN	
8 malware malcious host in #CSAL01	192.168.1.209	3 days long 12 days ago	Nov 16, 2019 10:08:58 GMT-05:00	NEW
8 malware malcious host in 2 CONFIRMED ▾	192.168.1.227	57 days long 66 days ago	Nov 16, 2019 10:07:23 GMT-05:00	NEW
8 malware malicious host in #CSAL01	192.168.1.179	62 days long 71 days ago	Nov 16, 2019 10:06:58 GMT-05:00	NEW

DASHBOARD CONFIRMED DETECTED

8 MALWARE MALICIOUS HOST
100% confidence, in #CSAL01
★ NEW / TRIAGE

AFFECTING
unknown username
192.168.1.209

OCCURRENCE
3 days
Nov 13 – Nov 16

Add notes...

ACTIVITIES AND FLOWS

SEVERITY FILTER: 9 8 7 6 5 4 3 2 1 Hide related

A. high risk level, anomalous periodic communication, quarantine with antivirus

B. critical risk level, malicious server IP, run in a sandboxed environment

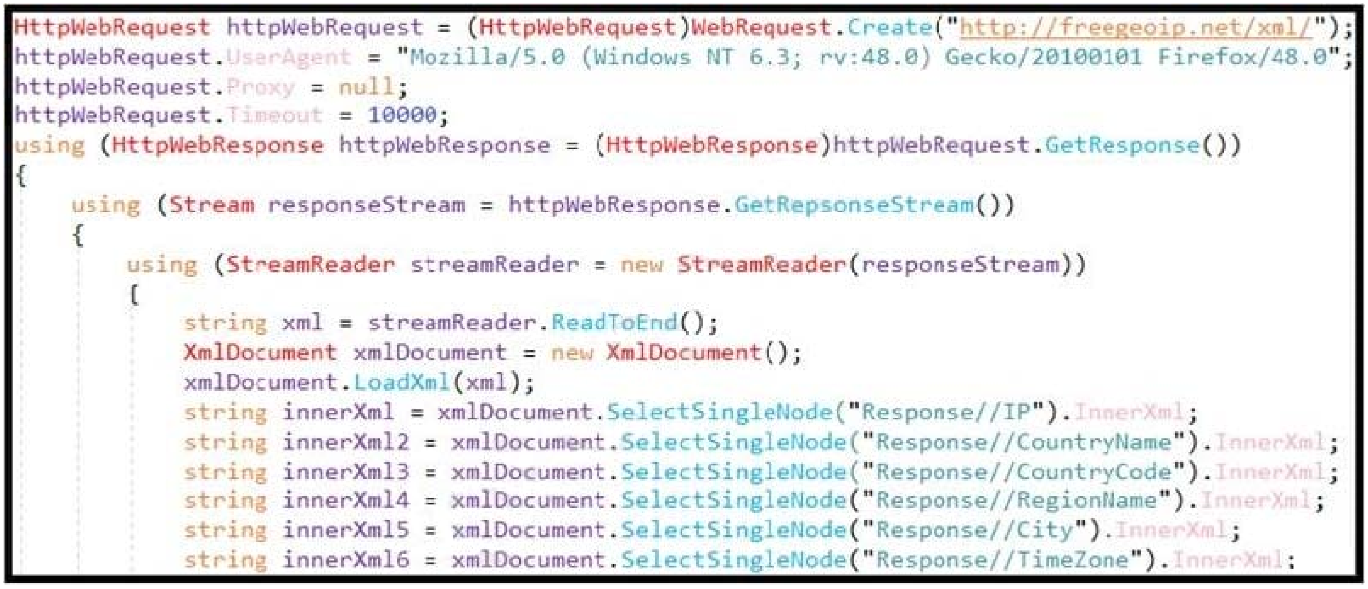
C. critical risk level, data exfiltration, isolate the device

D. high risk level, malicious host, investigate further

Correct Answer: A

QUESTION 9

Refer to the exhibit. An engineer is performing static analysis of a file received and reported by a user. Which risk is indicated in this STIX?



```
HttpWebRequest httpWebRequest = (HttpWebRequest)WebRequest.Create("http://freegeoip.net/xml/");
httpWebRequest.UserAgent = "Mozilla/5.0 (Windows NT 6.3; rv:48.0) Gecko/20100101 Firefox/48.0";
httpWebRequest.Proxy = null;
httpWebRequest.Timeout = 10000;
using (HttpWebResponse httpWebResponse = (HttpWebResponse)httpWebRequest.GetResponse())
{
    using (Stream responseStream = httpWebResponse.GetRepsonseStream())
    {
        using (StreamReader streamReader = new StreamReader(responseStream))
        {
            string xml = streamReader.ReadToEnd();
            XmlDocument xmlDocument = new XmlDocument();
            xmlDocument.LoadXml(xml);
            string innerXml = xmlDocument.SelectSingleNode("Response//IP").InnerXml;
            string innerXml2 = xmlDocument.SelectSingleNode("Response//CountryName").InnerXml;
            string innerXml3 = xmlDocument.SelectSingleNode("Response//CountryCode").InnerXml;
            string innerXml4 = xmlDocument.SelectSingleNode("Response//RegionName").InnerXml;
            string innerXml5 = xmlDocument.SelectSingleNode("Response//City").InnerXml;
            string innerXml6 = xmlDocument.SelectSingleNode("Response//TimeZone").InnerXml;
```

A. The file is redirecting users to a website that requests privilege escalations from the user.

B. The file is redirecting users to the website that is downloading ransomware to encrypt files.

C. The file is redirecting users to a website that harvests cookies and stored account information.

D. The file is redirecting users to a website that is determining users' geographic location.

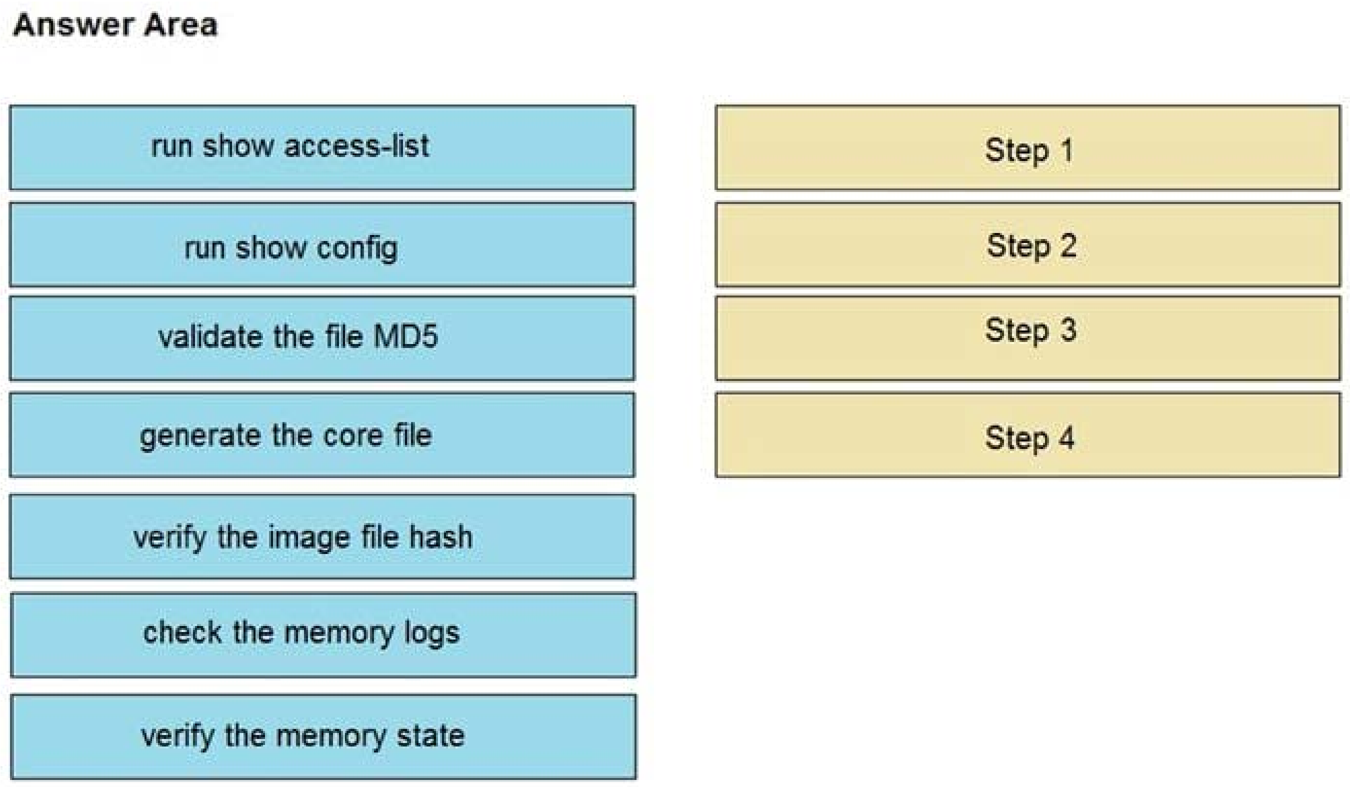
Correct Answer: D

QUESTION 10

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.

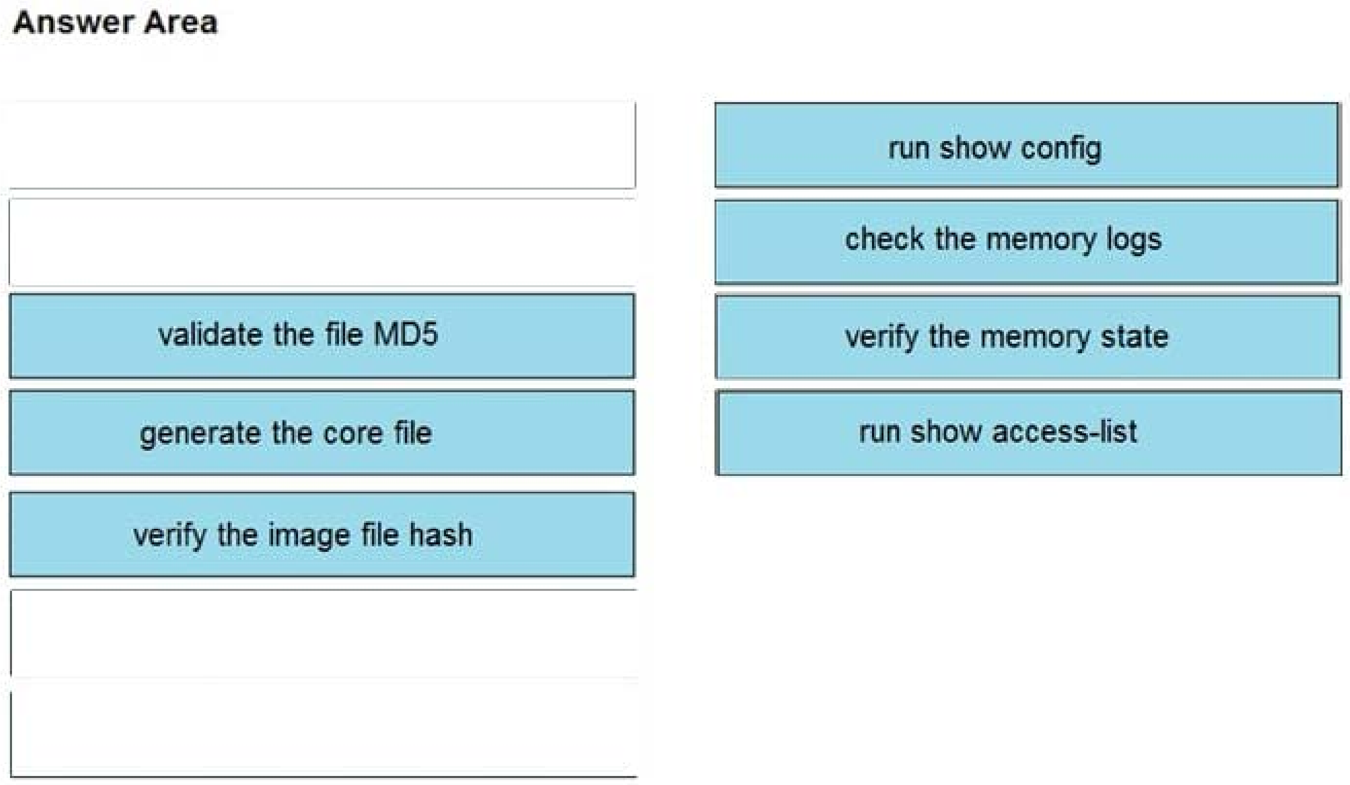
Select and Place:



Answer Area

run show access-list	Step 1
run show config	Step 2
validate the file MD5	Step 3
generate the core file	Step 4
verify the image file hash	
check the memory logs	
verify the memory state	

Correct Answer:



Answer Area

	run show config
	check the memory logs
validate the file MD5	verify the memory state
generate the core file	run show access-list
verify the image file hash	

QUESTION 11

An engineer has created a bash script to automate a complicated process. During script execution, this error occurs: permission denied. Which command must be added to execute this script?

A. chmod +x ex.sh

B. source ex.sh

C. chroot ex.sh

D. sh ex.sh

Correct Answer: A

Reference: https://www.redhat.com/sysadmin/exit-codes-demystified

---

QUESTION 12

What is a benefit of key risk indicators?

A. clear perspective into the risk position of an organization

B. improved visibility on quantifiable information

C. improved mitigation techniques for unknown threats

D. clear procedures and processes for organizational risk

Correct Answer: C

Reference: https://www.metricstream.com/insights/Key-Risk-indicators-ERM.htm#:~:text=Risk%20Management%20(ERM)-,Overview,and%20mitigate%20them%20in%20time.