200-201 Q&As

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Pass Cisco 200-201 Exam with 100% Guarantee

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

https://www.leads4pass.com/200-201.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which system monitors local system operation and local network access for violations of a security policy?

A. host-based intrusion detection

B. systems-based sandboxing

C. host-based firewall

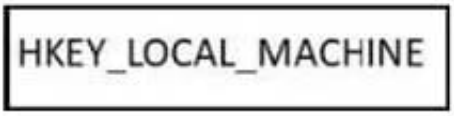
D. antivirus

Correct Answer: A

HIDS is capable of monitoring the internals of a computing system as well as the network packets on its network interfaces. Host-based firewall is a piece of software running on a single Host that can restrict incoming and outgoing Network activity for that host only.

QUESTION 2

Refer to the exhibit.



Which component is identifiable in this exhibit?

A. Trusted Root Certificate store on the local machine

B. Windows PowerShell verb

C. Windows Registry hive

D. local service in the Windows Services Manager

Correct Answer: C

https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry-hives https://ldapwiki.com/wiki/HKEY_LOCAL_MACHINE#:~:text=HKEY_LOCAL_MACHINE%20Windows%20registry%20hive%20contains,detected%20hardware%20and%20device%20d rivers.

QUESTION 3

What is the function of a command and control server?

A. It enumerates open ports on a network device

B. It drops secondary payload into malware

C. It is used to regain control of the network after a compromise

D. It sends instruction to a compromised system

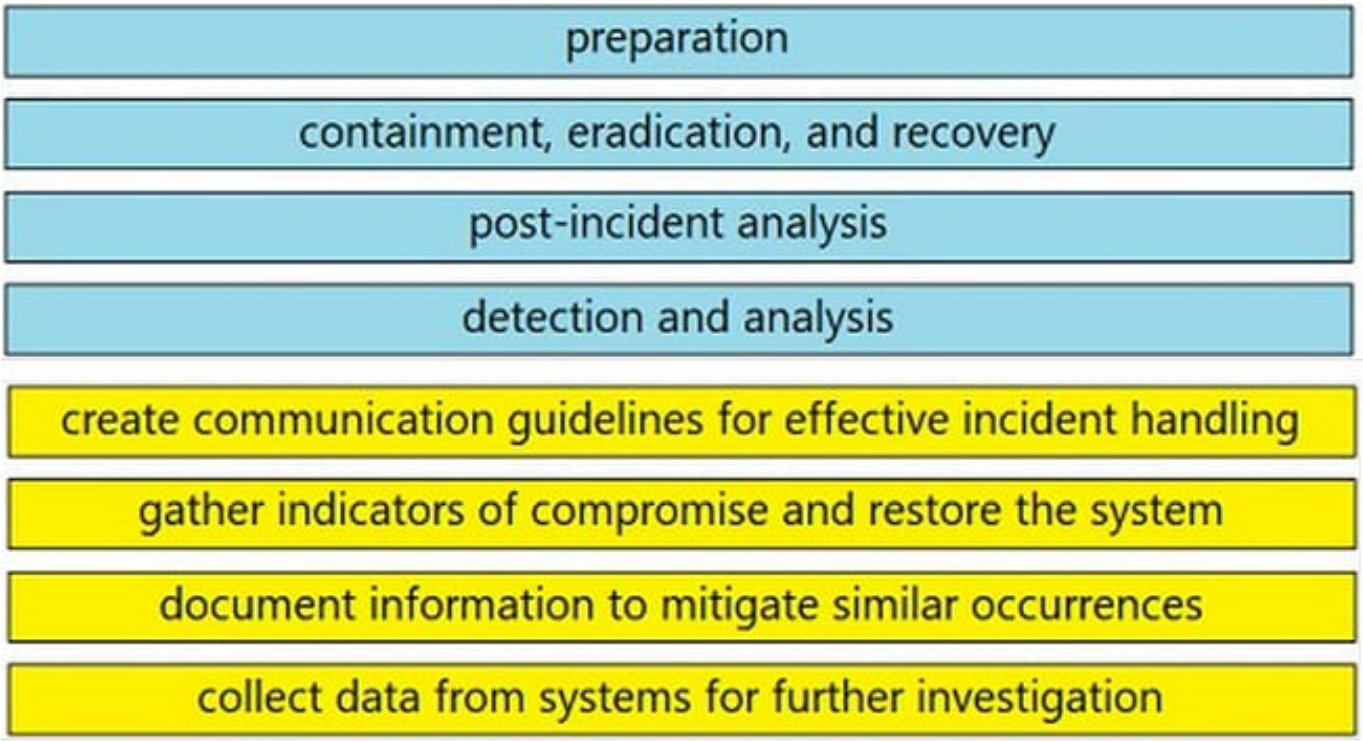
Correct Answer: D

QUESTION 4

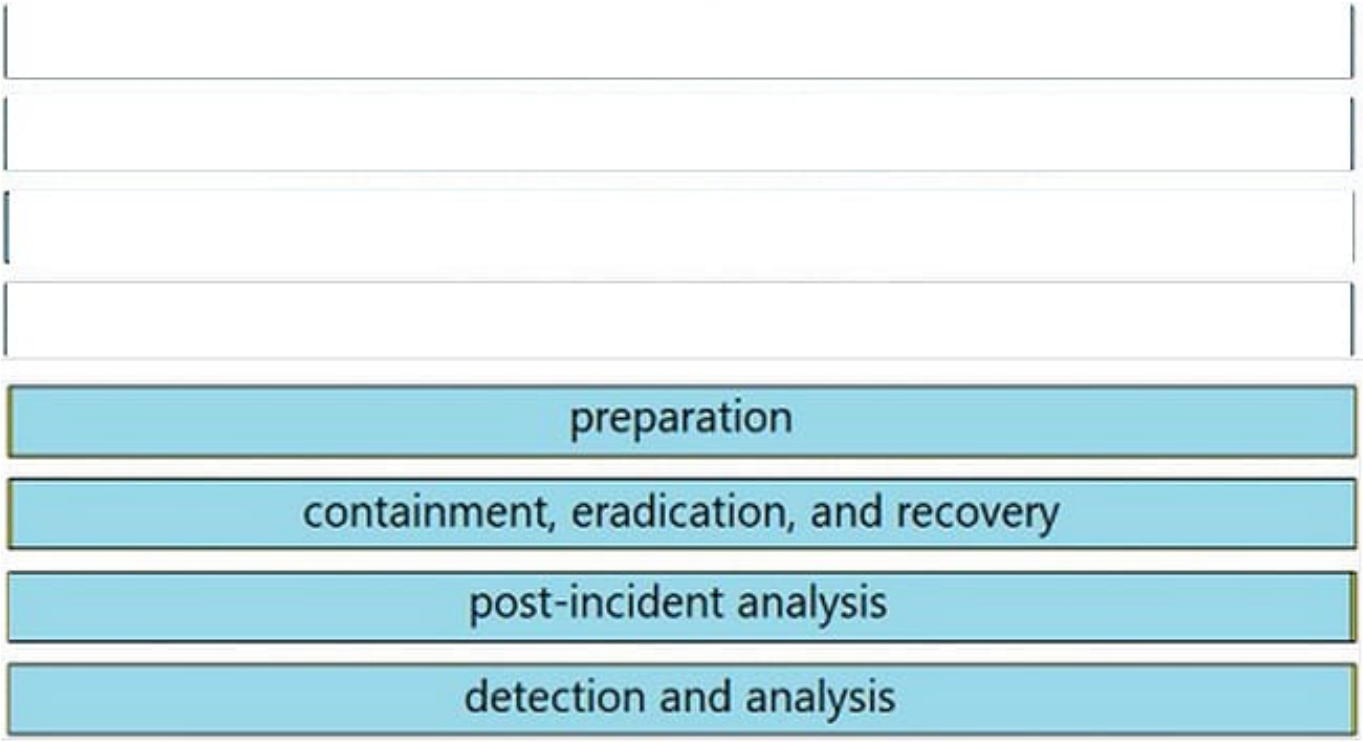
DRAG DROP

Drag and drop the elements from the left into the correct order for incident handling on the right.

Select and Place:



Correct Answer:



QUESTION 5

Which type of access control depends on the job function of the user?

A. discretionary access control

B. nondiscretionary access control

C. role-based access control

D. rule-based access control

Correct Answer: C

QUESTION 6

What are two denial-of-service (DoS) attacks? (Choose two)

A. port scan

B. SYN flood

C. man-in-the-middle

D. phishing

E. teardrop

Correct Answer: BE

Teardrop is a type of DoS attack where an attacker sends fragmented packets with overlapping offsets to a target system, causing it to crash or become unresponsive.

SYN flood is another type of DoS attack where an attacker sends a large number of SYN packets to a target system, overwhelming its ability to respond to legitimate connection requests and causing it to become unresponsive.

QUESTION 7

A user received an email attachment named "Hr405-report2609-empl094.exe" but did not run it. Which category of the cyber kill chain should be assigned to this type of event?

A. installation

B. reconnaissance

C. weaponization

D. delivery

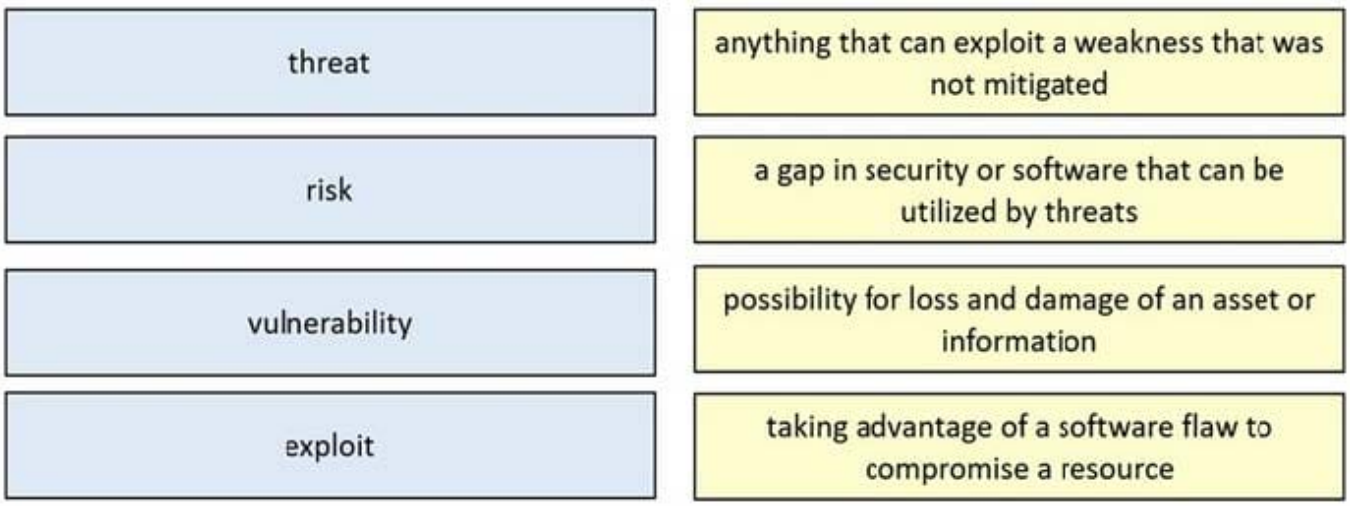
Correct Answer: A

QUESTION 8

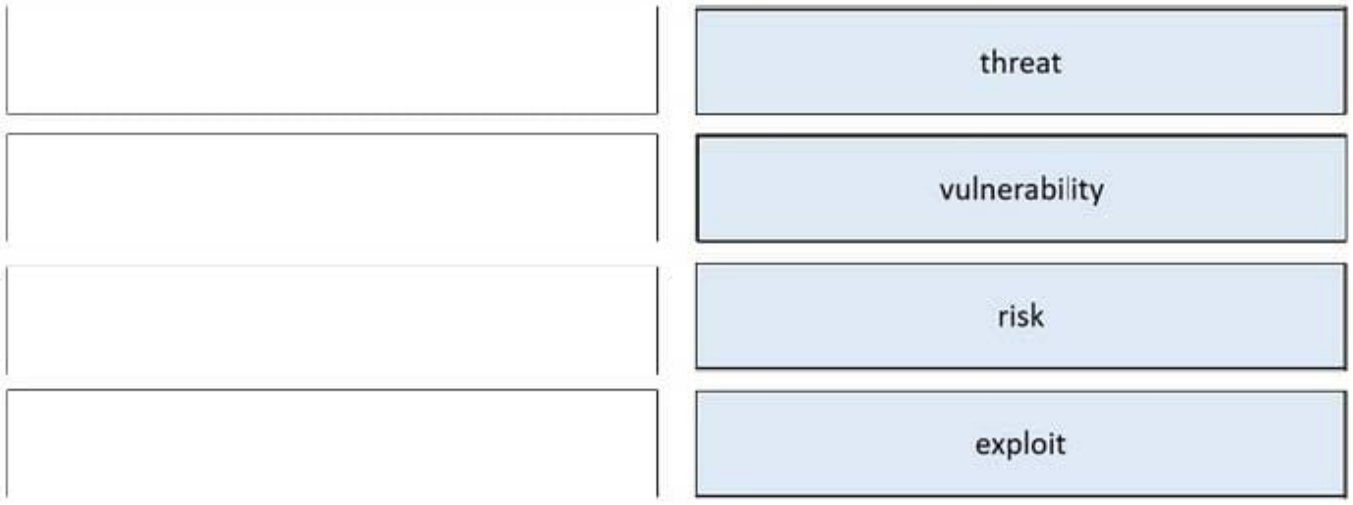
DRAG DROP

Drag and drop the security concept from the left onto the example of that concept on the right.

Select and Place:



Correct Answer:

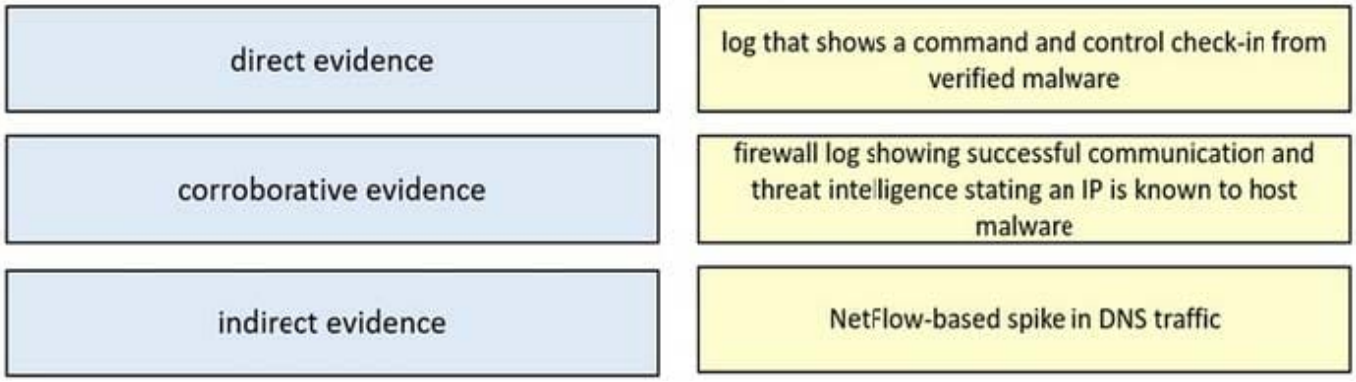


QUESTION 9

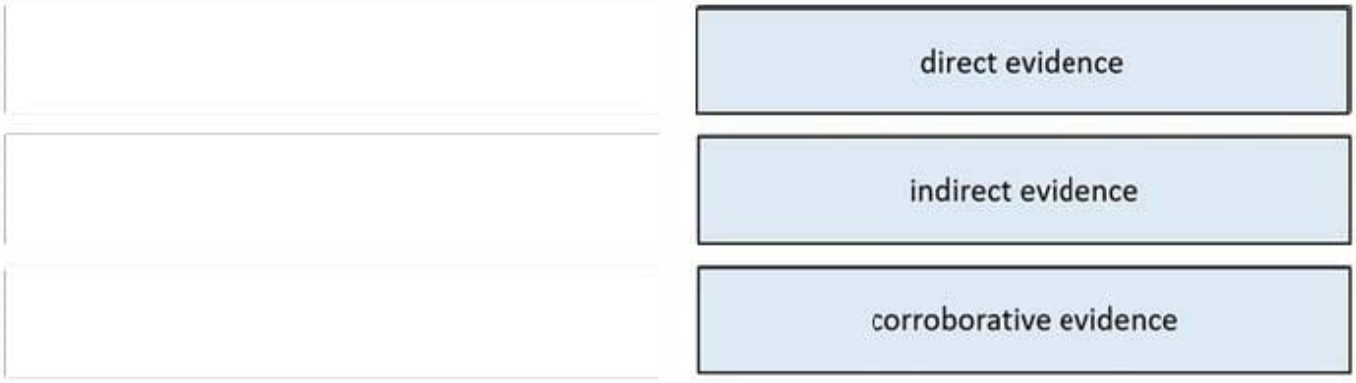
DRAG DROP

Drag and drop the type of evidence from the left onto the description of that evidence on the right.

Select and Place:



Correct Answer:



QUESTION 10

Which two elements of the incident response process are stated in NIST Special Publication 800-61 r2? (Choose two.)

A. detection and analysis

B. post-incident activity

C. vulnerability management

D. risk assessment

E. vulnerability scoring

Correct Answer: AB

Reference: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

QUESTION 11

Why is HTTPS traffic difficult to screen?

A. HTTPS is used internally and screening traffic (or external parties is hard due to isolation.

B. The communication is encrypted and the data in transit is secured.

C. Digital certificates secure the session, and the data is sent at random intervals.

D. Traffic is tunneled to a specific destination and is inaccessible to others except for the receiver.

Correct Answer: B

QUESTION 12

An engineer is analyzing a recent breach where confidential documents were altered and stolen by the receptionist Further analysis shows that the threat actor connected an externa USB device to bypass security restrictions and steal data The engineer could not find an external USB device Which piece of information must an engineer use for attribution in an investigation?

A. list of security restrictions and privileges boundaries bypassed

B. external USB device

C. receptionist and the actions performed

D. stolen data and its criticality assessment

Correct Answer: C

QUESTION 13

A security analyst notices a sudden surge of incoming traffic and detects unknown packets from unknown senders After further investigation, the analyst learns that customers claim that they cannot access company servers According to NIST SP800-61, in which phase of the incident response process is the analyst?

A. post-incident activity

B. detection and analysis

C. preparation

D. containment, eradication, and recovery

Correct Answer: B

QUESTION 14

What is obtained using NetFlow?

A. session data

B. application logs

C. network downtime report D. full packet capture

Correct Answer: A

QUESTION 15

What are two differences between tampered disk images and untampered disk images? (Choose two.)

A. The image is tampered if the stored hash and the computed hash are identical.

B. Tampered images are used as an element for the root cause analysis report.

C. Untampered images can be used as law enforcement evidence.

D. Tampered images are used in a security Investigation process.

E. The image is untampered if the existing stored hash matches the computed one.

Correct Answer: DE