DUMPSARENA

Understanding Cisco Cybersecurity Operations Fundamentals

Cisco 200-201

Version Demo

Total Demo Questions: 15

Total Premium Questions: 263

Buy Premium PDF

https://dumpsarena.com

sales@dumpsarena.com

QUESTION NO: 1

What is the difference between the ACK flag and the RST flag in the NetFlow log session?

A. The RST flag confirms the beginning of the TCP connection, and the ACK flag responds when the data for the payload is complete

B. The ACK flag confirms the beginning of the TCP connection, and the RST flag responds when the data for the payload is complete

C. The RST flag confirms the receipt of the prior segment, and the ACK flag allows for the spontaneous termination of a connection

D. The ACK flag confirms the receipt of the prior segment, and the RST flag allows for the spontaneous termination of a connection

ANSWER: D

QUESTION NO: 2

A security expert is working on a copy of the evidence, an ISO file that is saved in CDFS format. Which type of evidence is this file?

A. CD data copy prepared in Windows

B. CD data copy prepared in Mac-based system

C. CD data copy prepared in Linux system

D. CD data copy prepared in Android-based system

ANSWER: A

QUESTION NO: 3

What is the impact of encryption?

A. Confidentiality of the data is kept secure and permissions are validated

B. Data is accessible and available to permitted individuals

C. Data is unaltered and its integrity is preserved

D. Data is secure and unreadable without decrypting it

ANSWER: A

QUESTION NO: 4

Which piece of information is needed for attribution in an investigation?

A. proxy logs showing the source RFC 1918 IP addresses

B. RDP allowed from the Internet

C. known threat actor behavior

D. 802.1x RADIUS authentication pass arid fail logs

ANSWER: C

QUESTION NO: 5

Refer to the exhibit.

Which type of attack is being executed?

A. SQL injection

B. cross-site scripting

C. cross-site request forgery

D. command injection

ANSWER: A

QUESTION NO: 6

Refer to the exhibit.

Which two elements in the table are parts of the 5-tuple? (Choose two.)

A. First Packet

B. Initiator User

C. Ingress Security Zone

D. Source Port

E. Initiator IP

ANSWER: D E

QUESTION NO: 7

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.

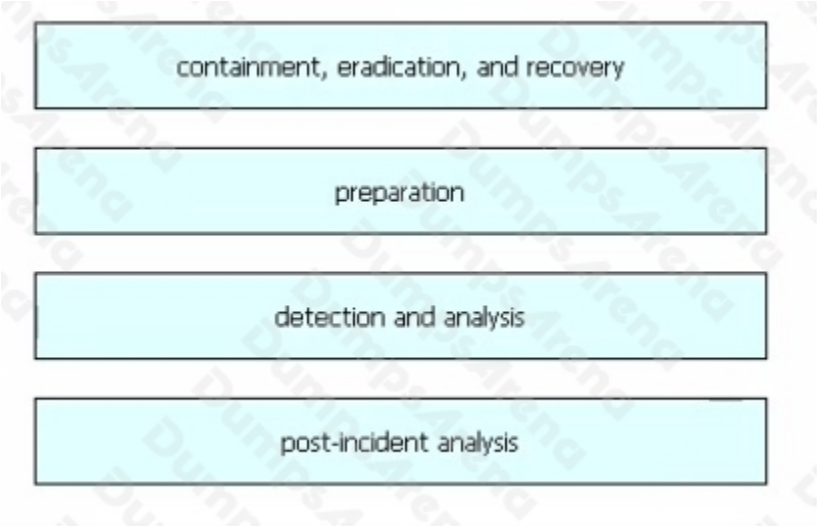
ANSWER: B

QUESTION NO: 8 - (DRAG DROP)

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

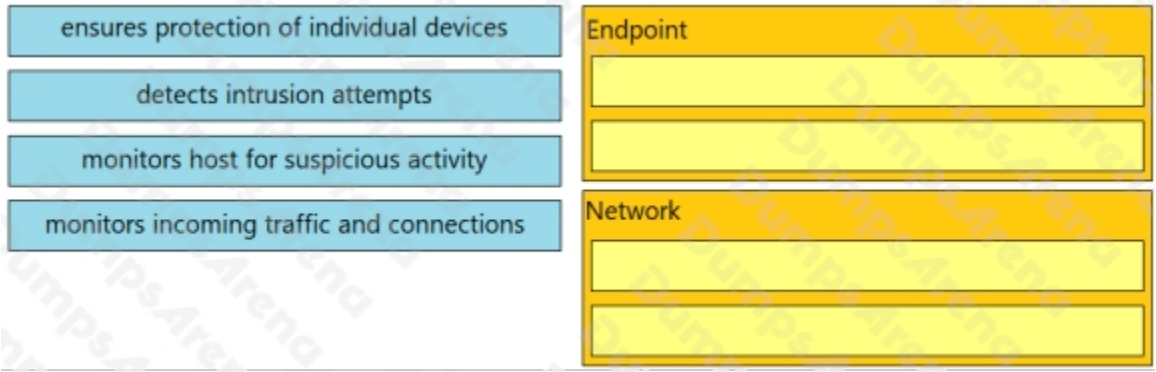
preparation	create communication guidelines for effective incident handling
containment, eradication, and recovery	gather indicators of compromise and restore the system
post-incident analysis	document information to mitigate similar occurrences
detection and analysis	collect data from systems for further investigation

ANSWER:

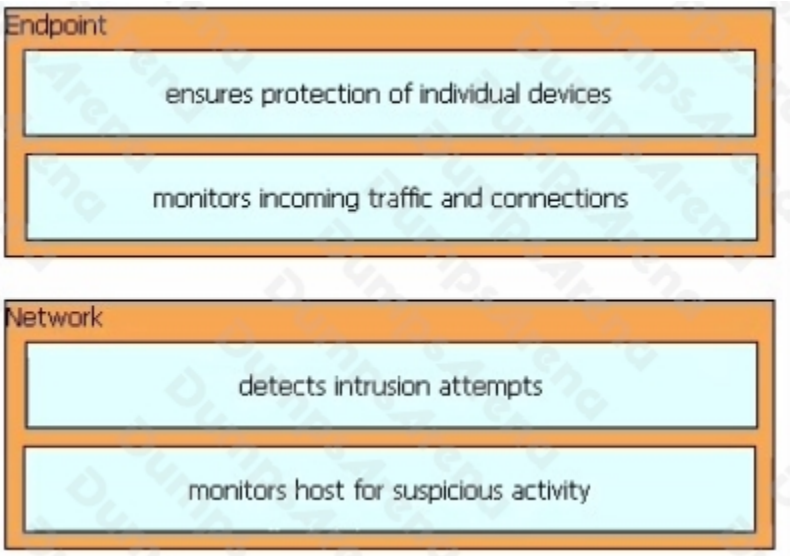


QUESTION NO: 9 - (DRAG DROP)

Drag and drop the uses on the left onto the type of security system on the right.



ANSWER:



QUESTION NO: 10

Which two elements are used for profiling a network? (Choose two.)

A. session duration

B. total throughput

C. running processes

D. listening ports

E. OS fingerprint

ANSWER: A B

QUESTION NO: 11

What describes the concept of data consistently and readily being accessible for legitimate users?

A. integrity

B. availability

C. accessibility

D. confidentiality

ANSWER: B

QUESTION NO: 12

Which two elements are assets in the role of attribution in an investigation? (Choose two.)

A. context

B. session

C. laptop

D. firewall logs

E. threat actor

ANSWER: C D

QUESTION NO: 13

An engineer must compare NIST vs ISO frameworks The engineer deeded to compare as readable documentation and also to watch a comparison video review. Using Windows 10 OS. the engineer started a browser and searched for a NIST document and then opened a new tab in the same browser and searched for an ISO document for comparison

The engineer tried to watch the video, but there 'was an audio problem with OS so the engineer had to troubleshoot it At first the engineer started CMD and looked fee a driver path then locked for a corresponding registry in the registry editor The engineer enabled "Audiosrv" in task manager and put it on auto start and the problem was solved Which two components of the OS did the engineer touch? (Choose two)

A. permissions

B. PowerShell logs

C. service

D. MBR

E. process and thread

ANSWER: A C

QUESTION NO: 14

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

A. detection and analysis

B. post-incident activity

C. vulnerability scoring

D. vulnerability management

E. risk assessment

ANSWER: A B

QUESTION NO: 15

What are two denial of service attacks? (Choose two.)

A. MITM

B. TCP connections

C. ping of death

D. UDP flooding

E. code red

ANSWER: C D