210-255 Q&As

Cisco Cybersecurity Operations

Pass Cisco 210-255 Exam with 100% Guarantee

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

https://www.leads4pass.com/210-255.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

Which description of probabilistic analysis is true?

A. probable proof of a user\\'s identity

B. lack of proof of a user\\'s identity

C. definitive proof of a user\\'s identity

D. false proof of a user\\'s identity

Correct Answer: A

QUESTION 2

Refer to the exhibit.

Threat Intelligence:

IP Address	Reputation (-100 to 100 higher is safer)
ABC.example.com	25
DEF.example.com	-75
FGH.example.com	0
XYZ.example.com	75

DNS Information:

Domain Name	IP Address
ABC.example.com	209.165.201.10
DEF.example.com	209.165.201.130
FGH.example.com	209.165.200.230
XYZ.example.com	209.165.202.25

Session Logs:

Source	Destination	Protocol
10.0.1.1/5567	209.165.201.130/443	TCP
10.0.1.2/8012	209.165.201.10/80	TCP
10.0.1.10/8125	209.165.200.230/80	TCP
10.0.1.20/9765	209.165.202.25/443	TCP

Which host is likely connecting to a malicious site?

A. 10.0.1.10

B. 10.0.1.1

C. 10.0.1.2

D. 10.0.1.20

Correct Answer: B

QUESTION 3

What can be addressed when using retrospective security techniques?

A. why the malware is still in our network

B. if the affected host needs a software update

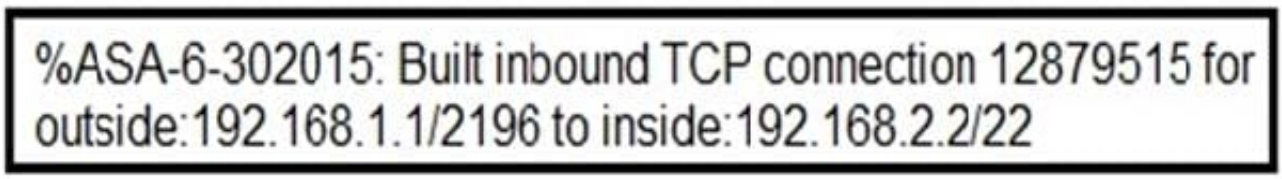
C. origin of the malware

D. if the affected system needs replacement

Correct Answer: A

QUESTION 4

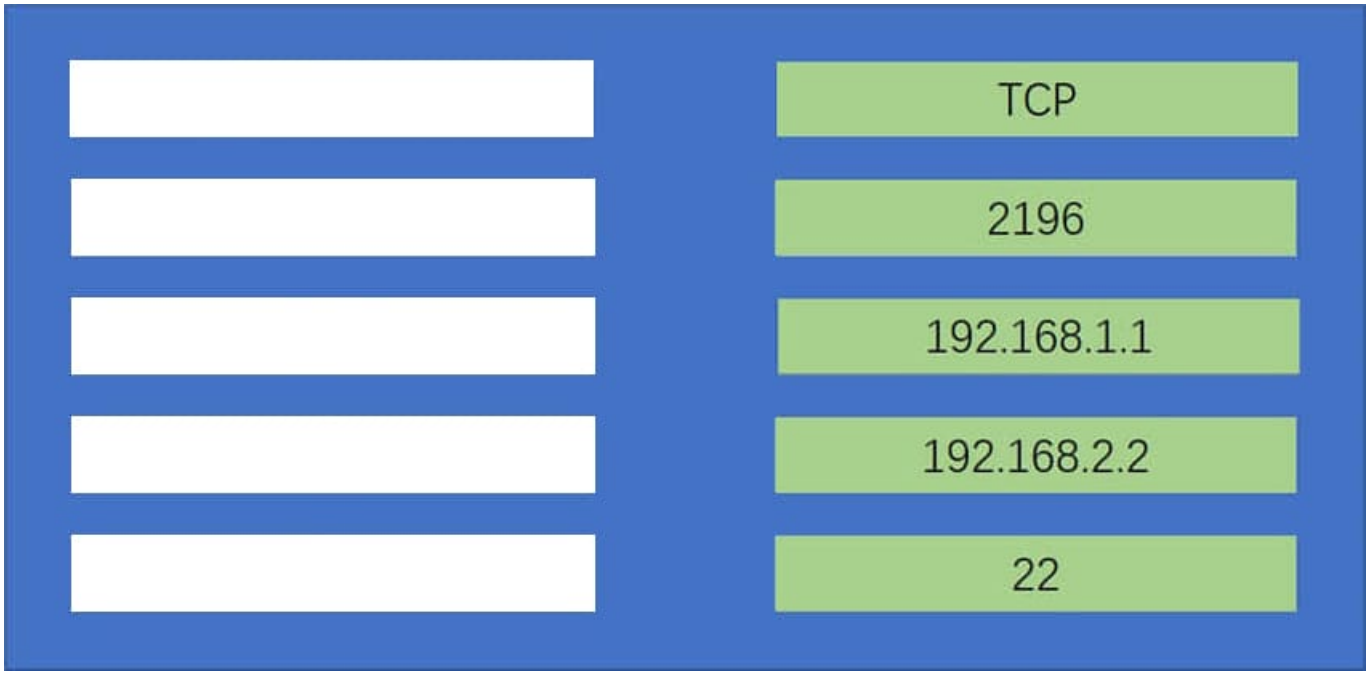
DRAG DROP



Refer to the exhibit. Drag and drop the items from the left onto the correct 5-tuple on the right.

Select and Place:

Correct Answer:



QUESTION 5

According to NIST 86, which action describes the volatile data collection?

A. Collect data before rebooting

B. Collect data while rebooting

C. Collect data after rebooting

D. Collect data that contains malware

Correct Answer: A