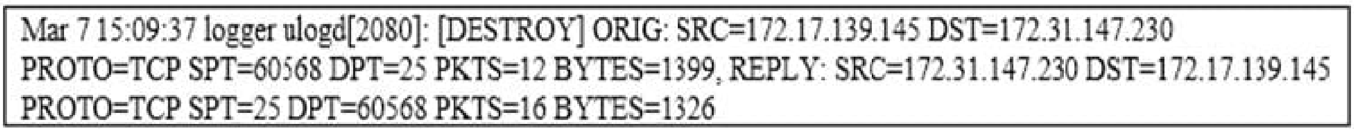
210-255Q&As

Cisco Cybersecurity Operations

QUESTION 1

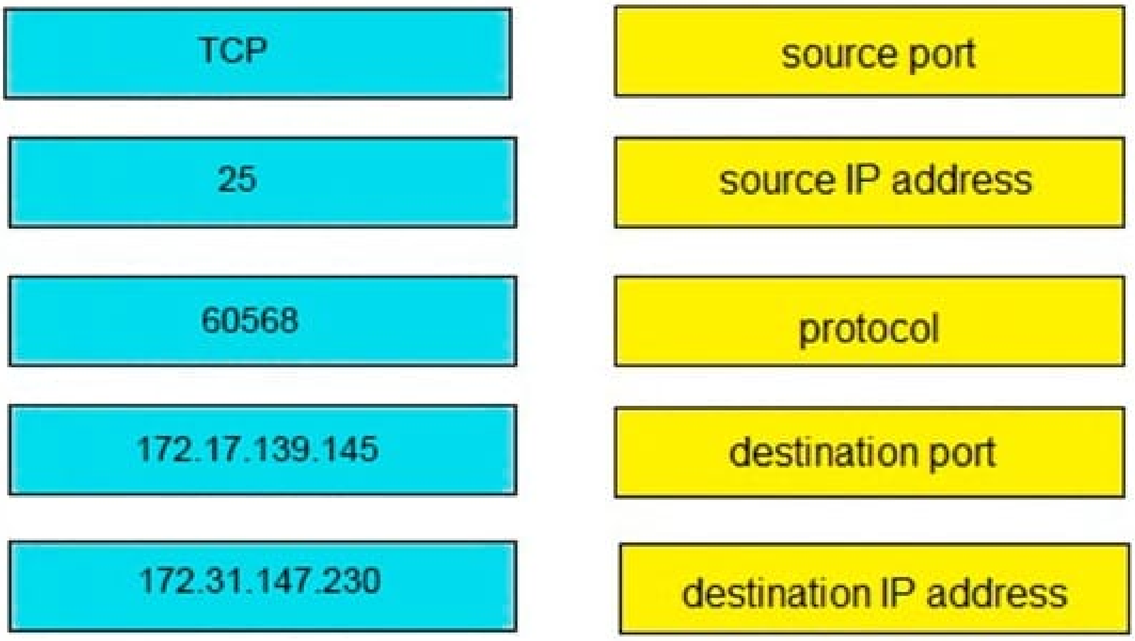
DRAG DROP

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



```
Mar 7 15:09:37 logger ulogd[2080]: [DESTROY] ORIG: SRC=172.17.139.145 DST=172.31.147.230
PROTO=TCP SPT=60568 DPT=25 PKTS=12 BYTES=1399, REPLY: SRC=172.31.147.230 DST=172.17.139.145
PROTO=TCP SPT=25 DPT=60568 PKTS=16 BYTES=1326
```

Select and Place:



TCP

25

60568

172.17.139.145

172.31.147.230

source port

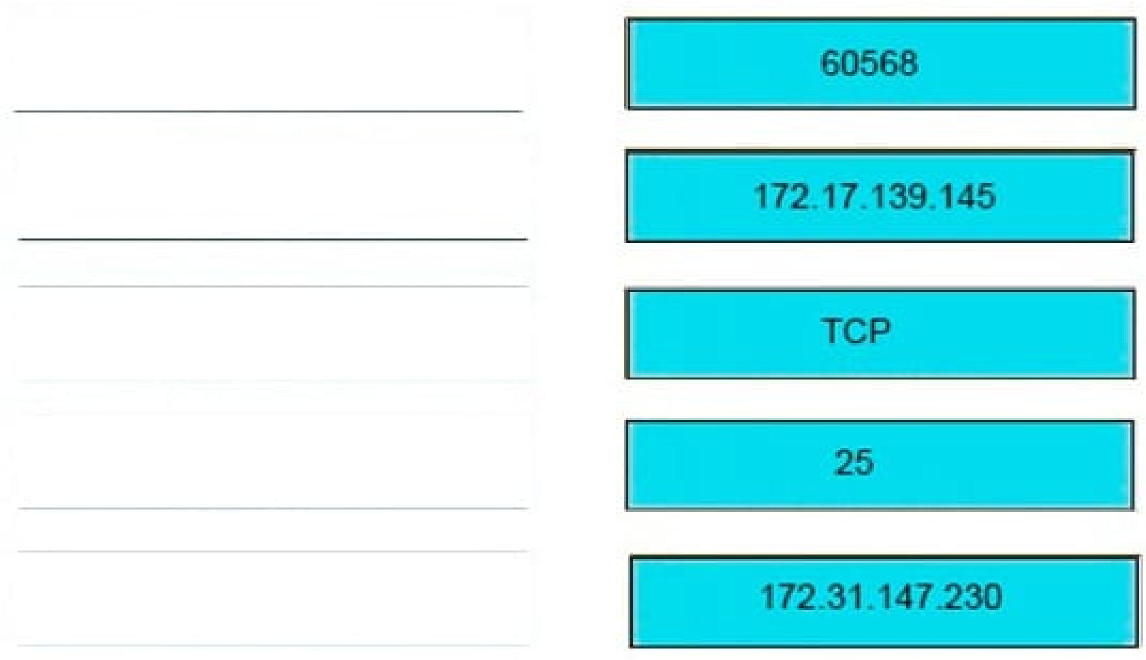
source IP address

protocol

destination port

destination IP address

Correct Answer:



QUESTION 2

Which of the following is not a metadata feature of the Diamond Model?

A. Direction

B. Result

C. Devices

D. Resources

Correct Answer: C

QUESTION 3

Which technology is the leading industry approach used to automatically enforce NAC?

A. IGMP

B. SNMP

C. 802.1X

D. Port Security

Correct Answer: C

QUESTION 4

Which file is allocated with 32 bits?

A. NTFS

B. FAT32

C. FAT

D. EXT4

Correct Answer: B

QUESTION 5

Which of the following is typically a responsibility of a PSIRT?

A. Configure the organization\\'s firewall

B. Monitor security logs

C. Investigate security incidents in a security operations center (SOC)

D. Disclose vulnerabilities in the organization\\'s products and services

Correct Answer: D

QUESTION 6

Which type of intrusion event is an attacker retrieving the robots. txt file from target site?

A. exploitation

B. weaponization

C. scanning

D. reconnaissance

Correct Answer: D

QUESTION 7

Based on nistsp800-61R2 what are the recommended protections against malware?

A. install software to detect malware

B. update antivirus signature

C. Other options

Correct Answer: AB

QUESTION 8

In which type of analysis is all data used for the analysis known beforehand?

A. dynamic

B. statistical

C. probabilistic

D. deterministic

Correct Answer: D

QUESTION 9

Which netstat command show ports? (Choose two)

A. netstat a

B. netstat -l

C. netstat -v

D. netstat -g

Correct Answer: AB

QUESTION 10

Which of the following is the team that handles the investigation, resolution, and disclosure of security vulnerabilities in vendor products and services?

A. CSIRT

B. ICASI

C. USIRP

D. PSIRT

Correct Answer: D

QUESTION 11

Which option is unnecessary for determining the appropriate containment strategy according to NIST.SP800-61 r2?

A. effectiveness of the strategy

B. time and resource needed to implement the strategy

C. need for evidence preservation

D. attack vector used to compromise the system

Correct Answer: D

QUESTION 12

Which Cyber Kill Chain Model category does attacking a vulnerability belong to?

A. Exploitation

B. Action on Objectives

C. Installation

D. Delivery

Correct Answer: A

QUESTION 13

Which option is a misuse variety per VERIS enumerations?

A. snooping

B. hacking

C. theft

D. assault

Correct Answer: B

QUESTION 14

Which of the following is an example of a coordination center?

A. Cisco PSIRT

B. Microsoft MSRC

C. CERT division of the Software Engineering Institute (SEI)

D. FIRST

Correct Answer: C

QUESTION 15

Which two statements correctly describe the victim demographics section of the VERIS schema? (Choose two.)

A. The victim demographics section describes but does not identify the organization that is affected by the incident.

B. The victim demographics section compares different types of organizations or departments within a single organization.

C. The victim demographics section captures general information about the incident.

D. The victim demographics section uses geolocation data to identify the organization name of the victim and the threat actor.

Correct Answer: AB