Vendor: Cisco

Exam Code:210-255

Exam Name: Cisco Cybersecurity Operations

Version: Demo

QUESTION 1

Which two options can be used by a threat actor to determine the role of a server? (Choose two.)

A. PCAP

B. tracert

C. running processes

D. hard drive configuration

E. applications

Correct Answer: CE

QUESTION 2

Which two compliance frameworks require that data be encrypted when it is transmitted over a public network? (Choose two.)

A. PCI

B. GLBA

C. HIPAA

D. SOX

E. COBIT

Correct Answer: AC

QUESTION 3

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 4

Which data element must be protected with regards to PCI?

A. past health condition

B. geographic location

C. full name / full account number

D. recent payment amount

Correct Answer: C

QUESTION 5

When evidence is collected, what does NIST SP800-86 specify as a guideline to follow for the order of collection?

A. order of volatility

B. order of importance

C. most difficult to access first

D. least difficult to access first

Correct Answer: B

QUESTION 6

Which technology generates events utilizing proxy logs?

A. Firepower

B. Email Security Appliance

C. Stealthwatch

D. Web Security Appliance

Correct Answer: D

QUESTION 7

Which of the following is not an example of reconnaissance?

A. Searching the robots.txt file

B. Redirecting users to a source and scanning traffic to learn about the target

C. Scanning without completing the three-way handshake

D. Communicating over social media

Correct Answer: B

QUESTION 8

Which regex matches on all lowercase letters only?

A. [a-z]+

B. a*z+

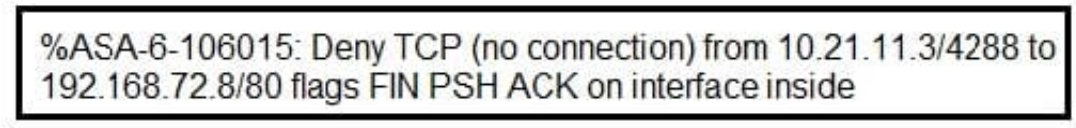
C. [a-z]+

D. a-z+

Correct Answer: C

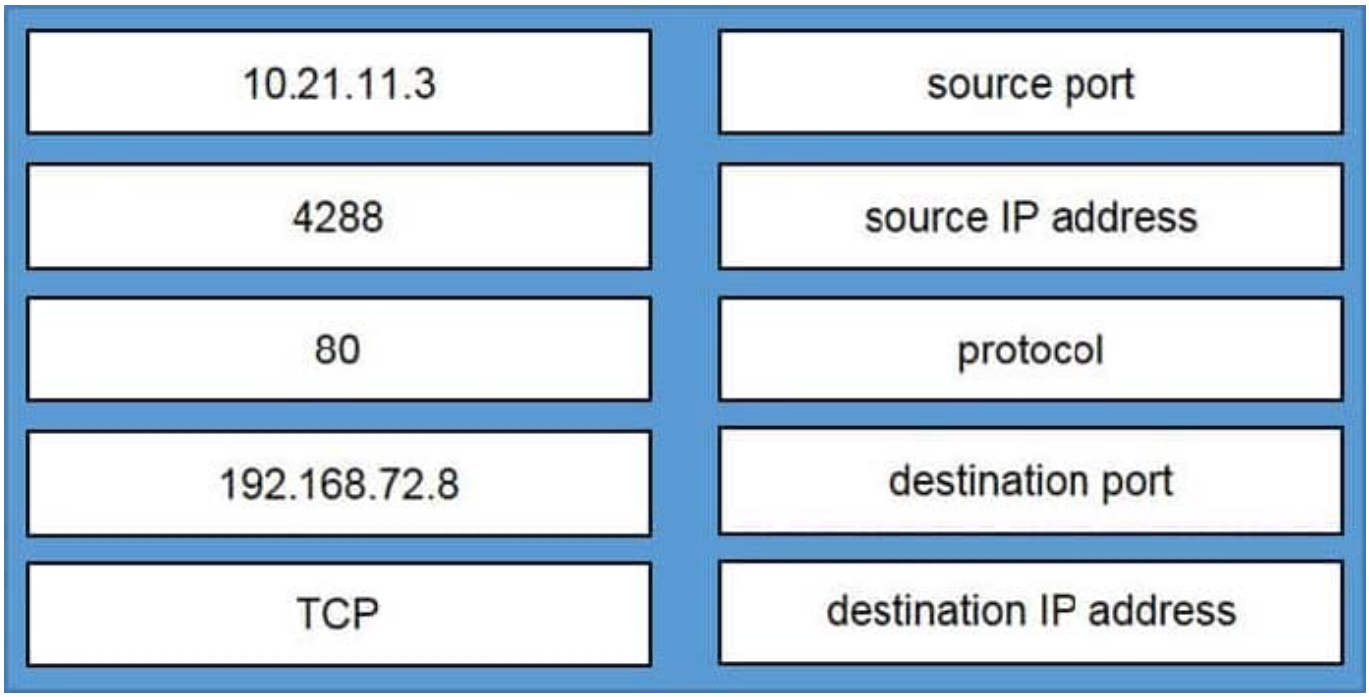
QUESTION 9

DRAG DROP

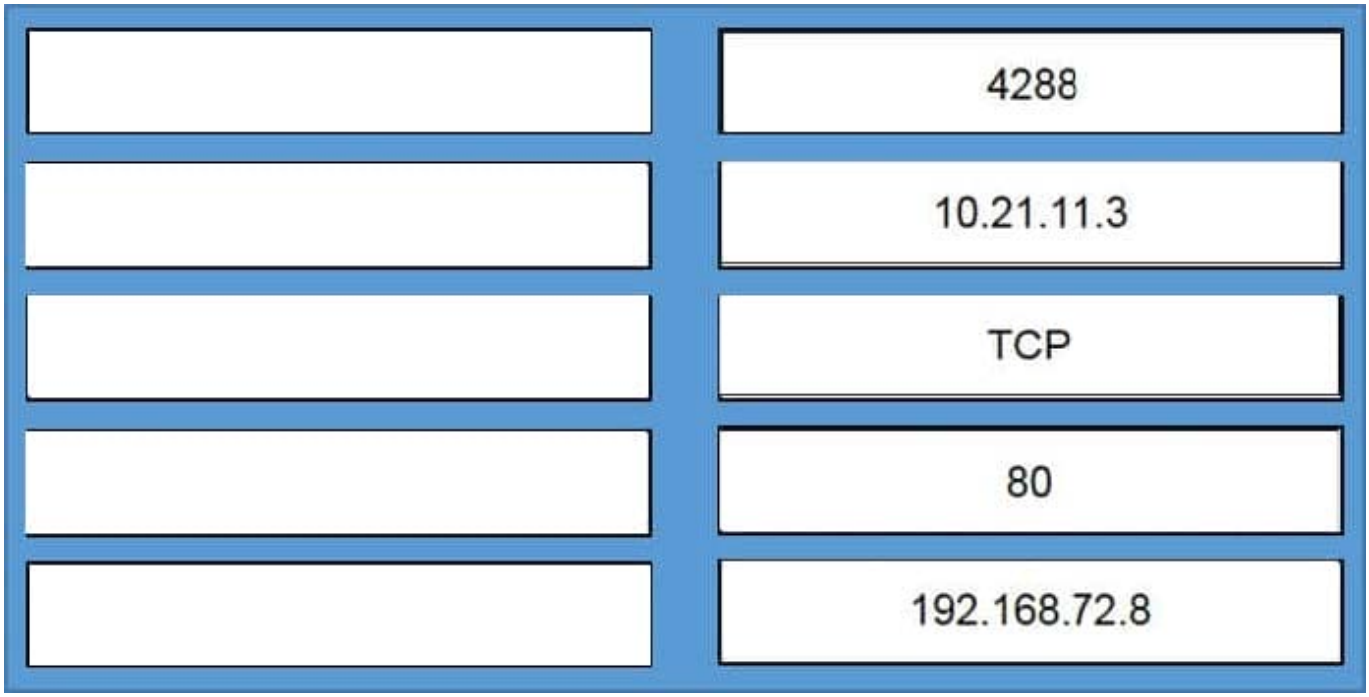


Refer to the exhibit. Drag and drop elements from the log onto the correct 5-tuple category on the right.

Select and Place:



Correct Answer:



QUESTION 10

Which description of deterministic 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: C

QUESTION 11

A user on your network receives an email in their mailbox that contains a malicious attachment. There is no indication that the file was run. Which category as defined in the Diamond Model of Intrusion does this activity fall under?

A. reconnaissance

B. weaponization

C. delivery

D. installation

Correct Answer: C

QUESTION 12

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