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.pass2lead.com/210-255.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which regex matches on all lowercase letters only?

A. [a-z]+

B. a*z+

C. [a-z]+

D. a-z+

Correct Answer: C

QUESTION 2

Which description of a retrospective malware detection is true?

A. You use Wireshark to identify the malware source.

B. You use historical information from one or more sources to identify the affected host or file.

C. You use information from a network analyzer to identify the malware source.

D. You use Wireshark to identify the affected host or file.

Correct Answer: B

QUESTION 3

attacker using robots.txt is under which category?

A. Reconnaissance

B. Weaponization

C. Delivery

D. Exploitation

E. Installation

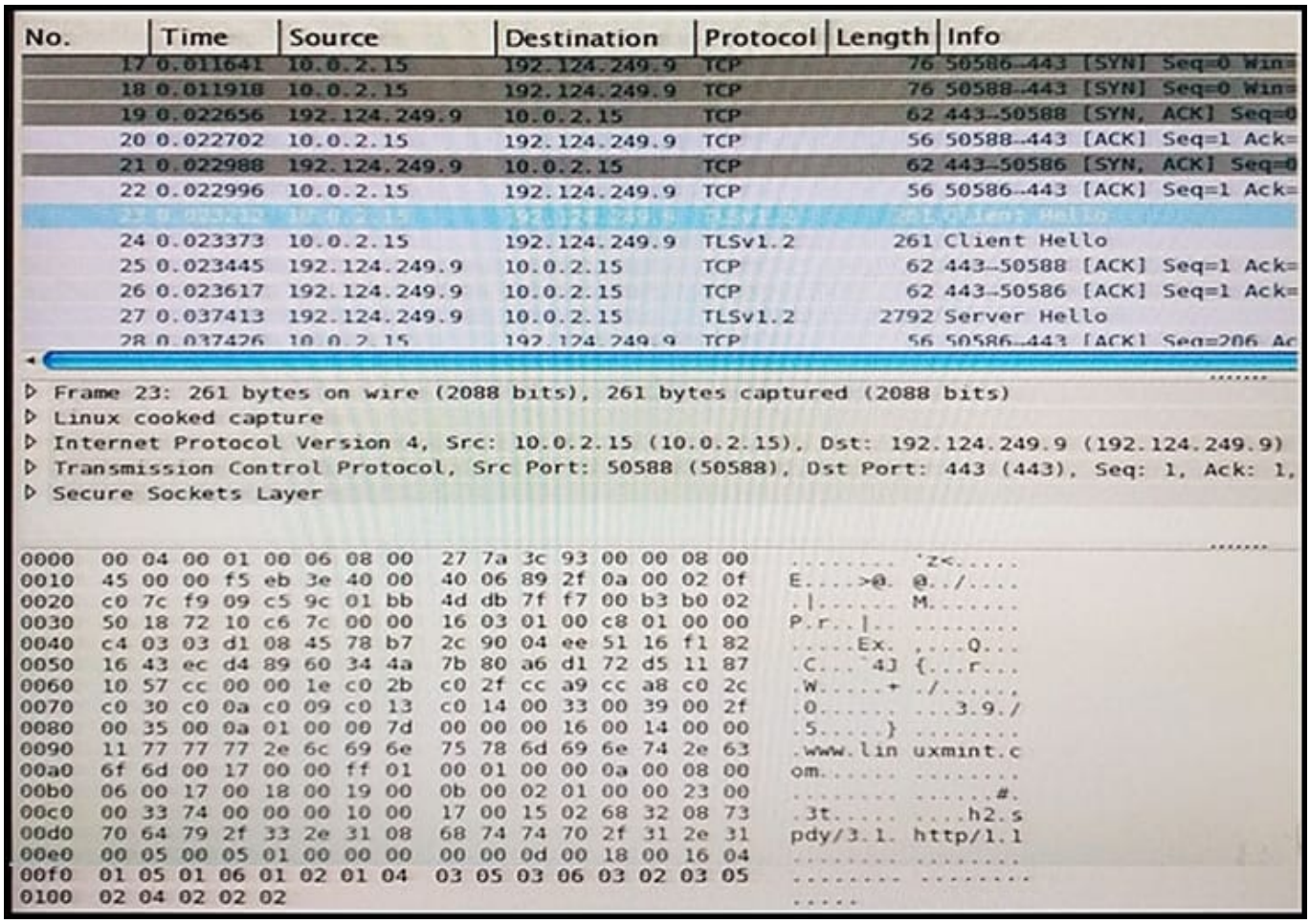
F. Command and control (C2)

G. Actions on objectives

Correct Answer: A

QUESTION 4

DRAG DROP

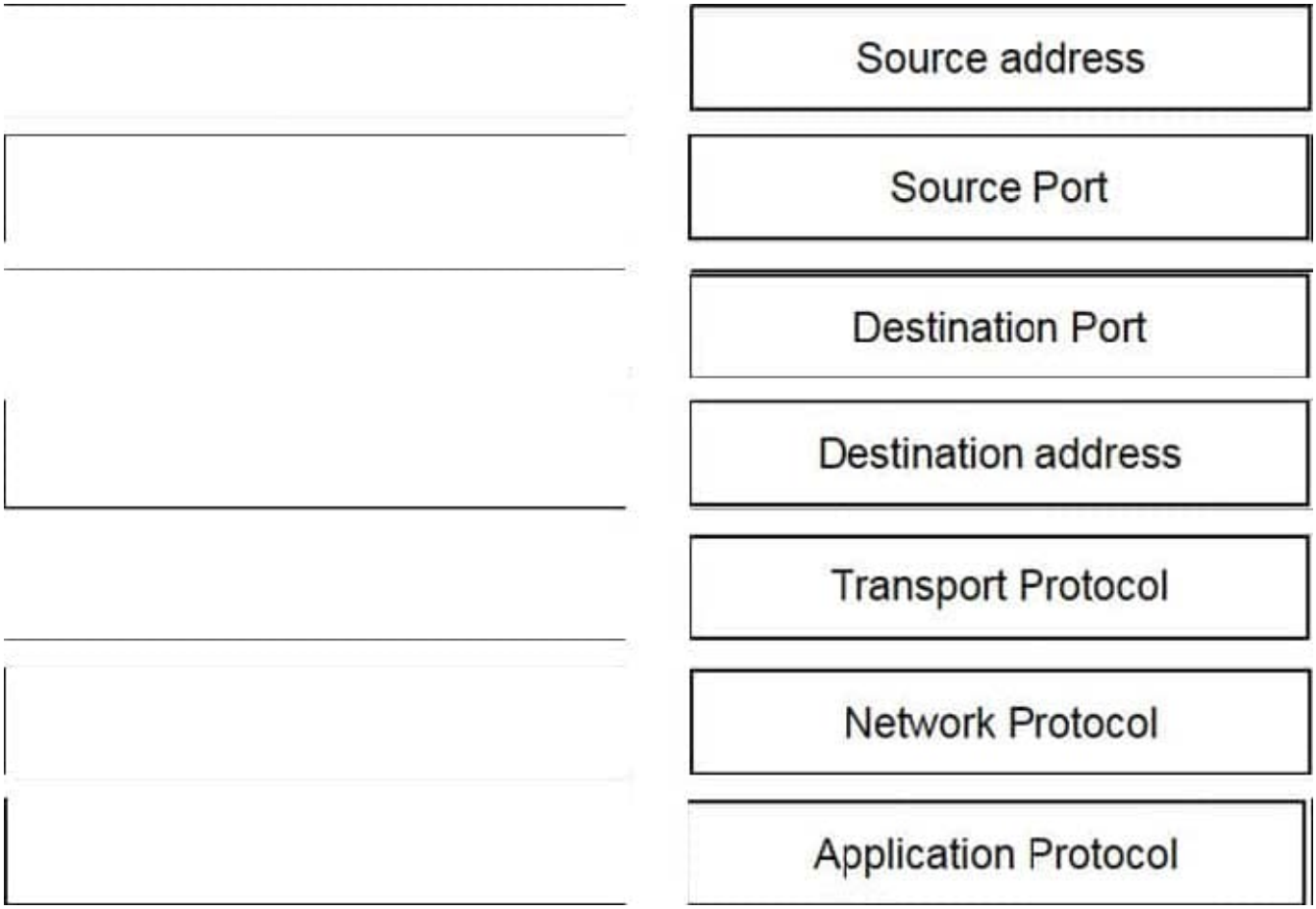


Refer to the exhibit. Drag and drop the element name from the left onto the correct piece of the PCAP file on the right.

Select and Place:

Source address	10.0.2.15
Destination address	50588
Source Port	443
Destination Port	192.124.249.9
Network Protocol	Transmission control protocol
Transport Protocol	Internet Protocol v4
Application Protocol	Transport Layer Security v1.2

Correct Answer:



QUESTION 5

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