Vendor: Cisco

Exam Code:210-255

Exam Name: Cisco Cybersecurity Operations

Version: Demo

QUESTION 1

Which incident handling phase is focused on minimizing the impact of the incident?

A. reporting

B. remediation

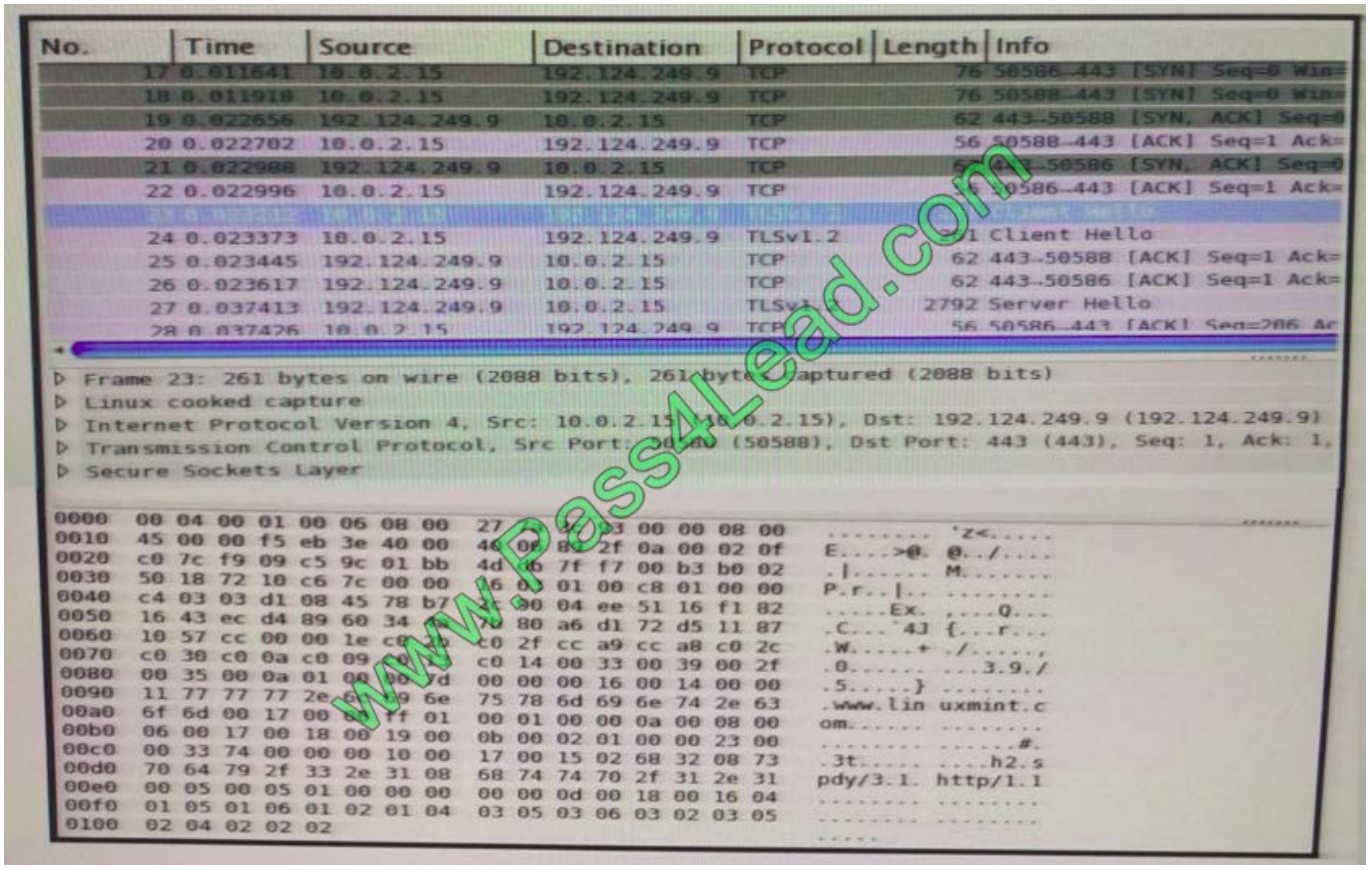
C. containment

D. scoping

Correct Answer: C

QUESTION 2

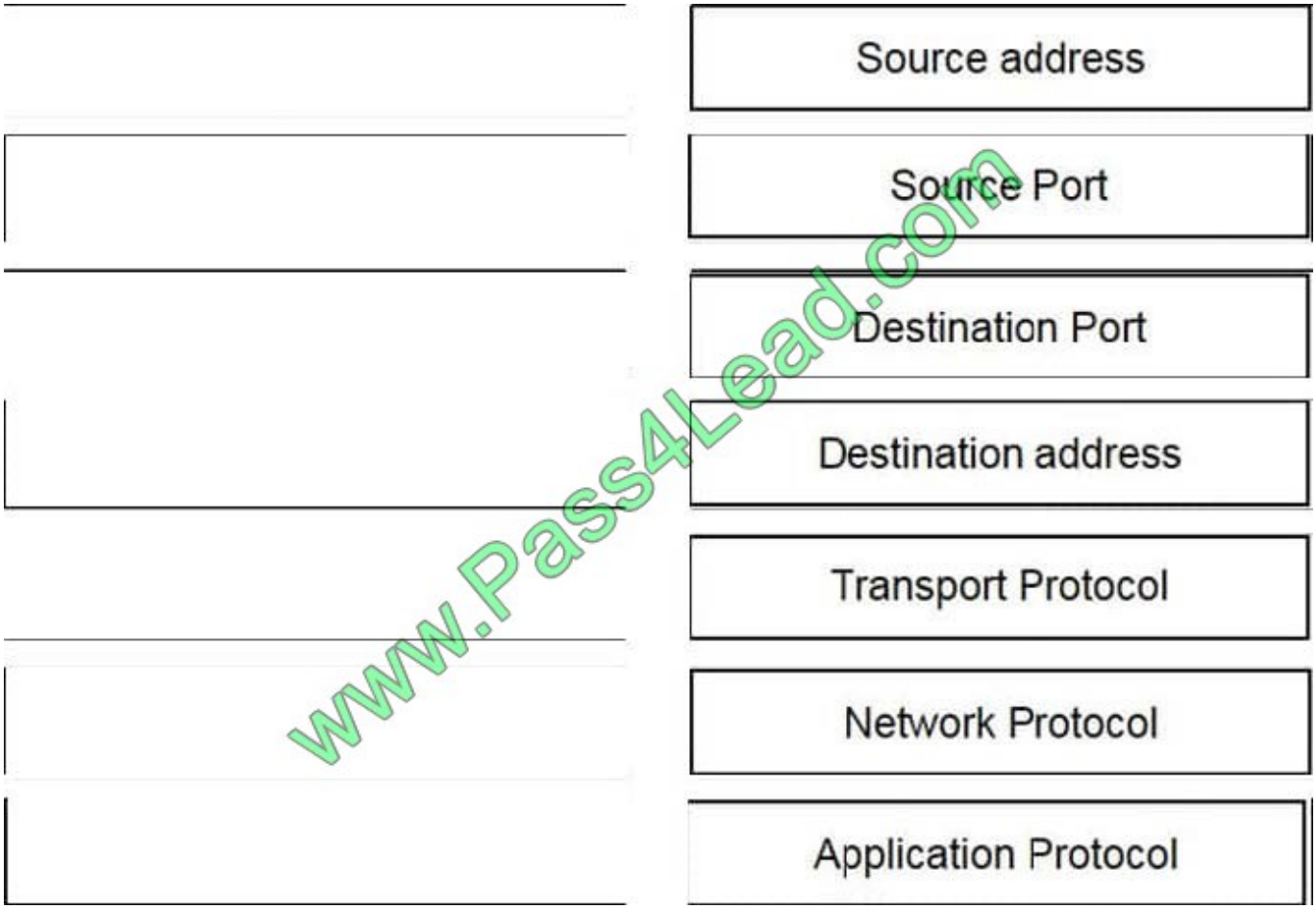
Refer to the exhibit. Drag and drop the element name from the left onto the correct piece of the PCAP file on the right.



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 3

Which file is allocated with 32 bits?

A. NTFS

B. FAT32

C. FAT

D. EXT4

Correct Answer: B

QUESTION 4

Which CVSSv3 metric captures the level of access that is required for a successful attack?

A. attack vector

B. attack complexity

C. privileges required

D. user interaction

Correct Answer: C

Privileges Required The new metric, Privileges Required, replaces the Authentication metric of v2.0. Instead of measuring the number of times an attacker must separately authenticate to a system, Privileges Required captures the level of access required for a successful attack. Specifically, the metric values High, Low, and None refilect the privileges required by an attacker in order to explogt the vulnerability.

QUESTION 5

Which signature type results in a legitime alert been dismissed?

A. True negative

B. False negative

C. True Positive

D. False Positive

Correct Answer: B

QUESTION 6

Which two HTTP header fields relate to intrusion analysis? (Choose two).

A. user-agent

B. host

C. connection

D. language

E. handshake type

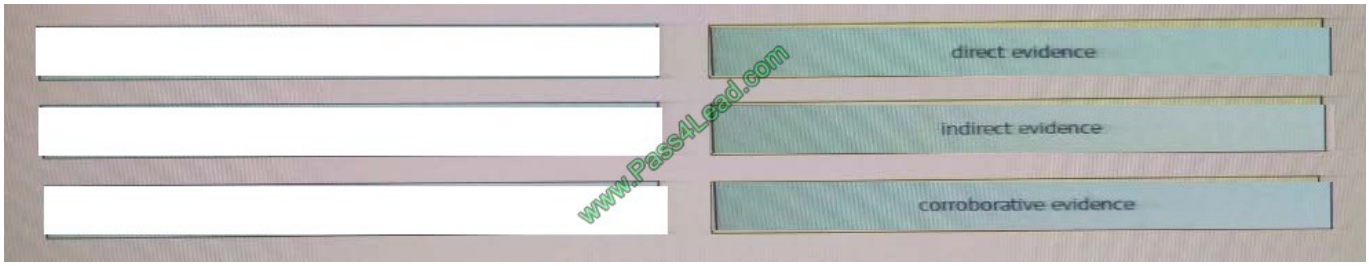
Correct Answer: AB

QUESTION 7

Drag and drop the type of evidence from the left onto the correct descnption(s) of that evidence on the right.

Select and Place:

Correct Answer:



QUESTION 8

Which option is a misuse variety per VERIS enumerations?

A. snooping

B. hacking

C. theft

D. assault

Correct Answer: B

QUESTION 9

Which of the following Linux file systems not only supports journaling but also modifies important data structures of the file system, such as the ones destined to store the file data for better performance and reliability?

A. GRUB

B. LILO

C. Ext4

D. FAT32

Correct Answer: C

QUESTION 10

In addition to cybercrime and attacks, evidence found on a system or network may be presented in a court of law to support accusations of crime or civil action, including which of the following?

A. Fraud, money laundering, and theft

B. Drug-related crime

C. Murder and acts of violence

D. All of the above

Correct Answer: D

QUESTION 11

What does the CSIRT incident response provider usually do?

A. provide incident handling services to their parent organization.

B. provide incident handling services to a country

C. coordinate and facilitate the handling of incidents across various CSIRTs

D. focus on synthesizing data from various sources to determine trends and patterns in incident activity

E. handle reports of vulnerabilities in their software or hardware products

F. offer incident handling services as a for-fee service to other organizations

Correct Answer: D

QUESTION 12

Which CVSSv3 Attack Vector metric value requires the attacker to physically touch or manipulate the vulnerable component?

A. local

B. physical

C. network

D. adjacent

Correct Answer: B

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: