DUMPSARENA

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Cisco 200-201

Version Demo

Total Demo Questions: 15

Total Premium Questions: 263

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which two components reduce the attack surface on an endpoint? (Choose two.)

A. secure boot

B. load balancing

C. increased audit log levels

D. restricting USB ports

E. full packet captures at the endpoint

ANSWER: A D

QUESTION NO: 2

Which vulnerability type is used to read, write, or erase information from a database?

A. cross-site scripting

B. cross-site request forgery

C. buffer overflow

D. SQL injection

ANSWER: D

QUESTION NO: 3

What describes a buffer overflow attack?

A. injecting new commands into existing buffers

B. fetching data from memory buffer registers

C. overloading a predefined amount of memory

D. suppressing the buffers in a process

ANSWER: C

QUESTION NO: 4

What are the two differences between stateful and deep packet inspection? (Choose two)

A. Stateful inspection is capable of TCP state tracking, and deep packet filtering checks only TCP source and destination ports

B. Deep packet inspection is capable of malware blocking, and stateful inspection is not

C. Deep packet inspection operates on Layer 3 and 4. and stateful inspection operates on Layer 3 of the OSI model

D. Deep packet inspection is capable of TCP state monitoring only, and stateful inspection can inspect TCP and UDP.

E. Stateful inspection is capable of packet data inspections, and deep packet inspection is not

ANSWER: A B

QUESTION NO: 5

What are two social engineering techniques? (Choose two.)

A. privilege escalation

B. DDoS attack

C. phishing

D. man-in-the-middle

E. pharming

ANSWER: C E

QUESTION NO: 6

Which metric is used to capture the level of access needed to launch a successful attack?

A. privileges required

B. user interaction

C. attack complexity

D. attack vector

ANSWER: D

QUESTION NO: 7

An analyst is exploring the functionality of different operating systems.

What is a feature of Windows Management Instrumentation that must be considered when deciding on an operating system?

A. queries Linux devices that have Microsoft Services for Linux installed

B. deploys Windows Operating Systems in an automated fashion

C. is an efficient tool for working with Active Directory

D. has a Common Information Model, which describes installed hardware and software

ANSWER: D

QUESTION NO: 8

Which two elements are assets in the role of attribution in an investigation? (Choose two.)

A. context

B. session

C. laptop

D. firewall logs

E. threat actor

ANSWER: C D

QUESTION NO: 9

Refer to the exhibit.

An engineer is reviewing a Cuckoo report of a file. What must the engineer interpret from the report?

A. The file will appear legitimate by evading signature-based detection.

B. The file will not execute its behavior in a sandbox environment to avoid detection.

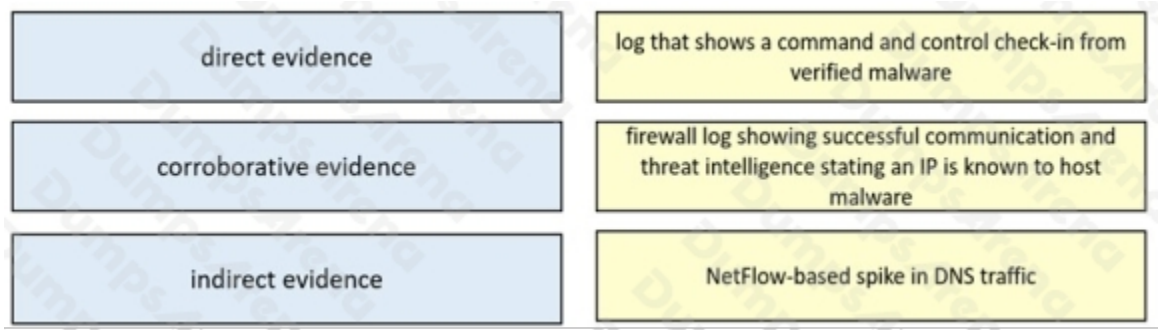
C. The file will insert itself into an application and execute when the application is run.

D. The file will monitor user activity and send the information to an outside source.

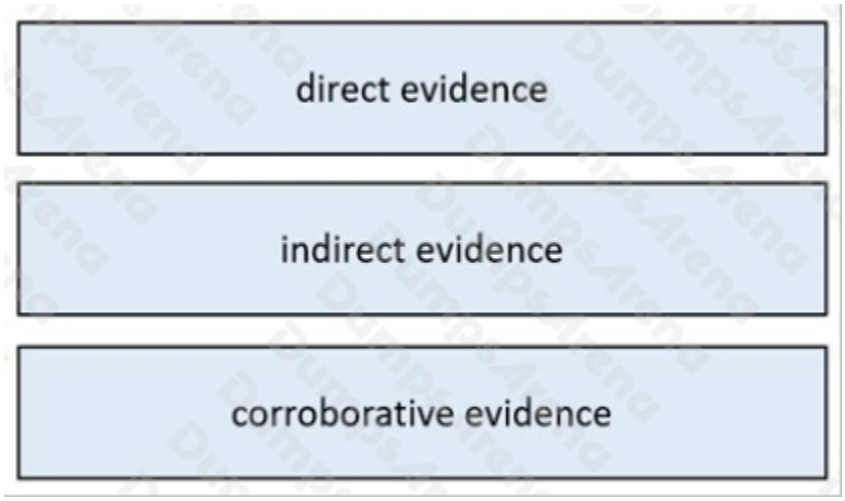
ANSWER: B

QUESTION NO: 10 - (DRAG DROP)

Drag and drop the type of evidence from the left onto the description of that evidence on the right.



ANSWER:



QUESTION NO: 11

Which are two denial-of-service attacks? (Choose two.)

A. TCP connections

B. ping of death

C. man-in-the-middle

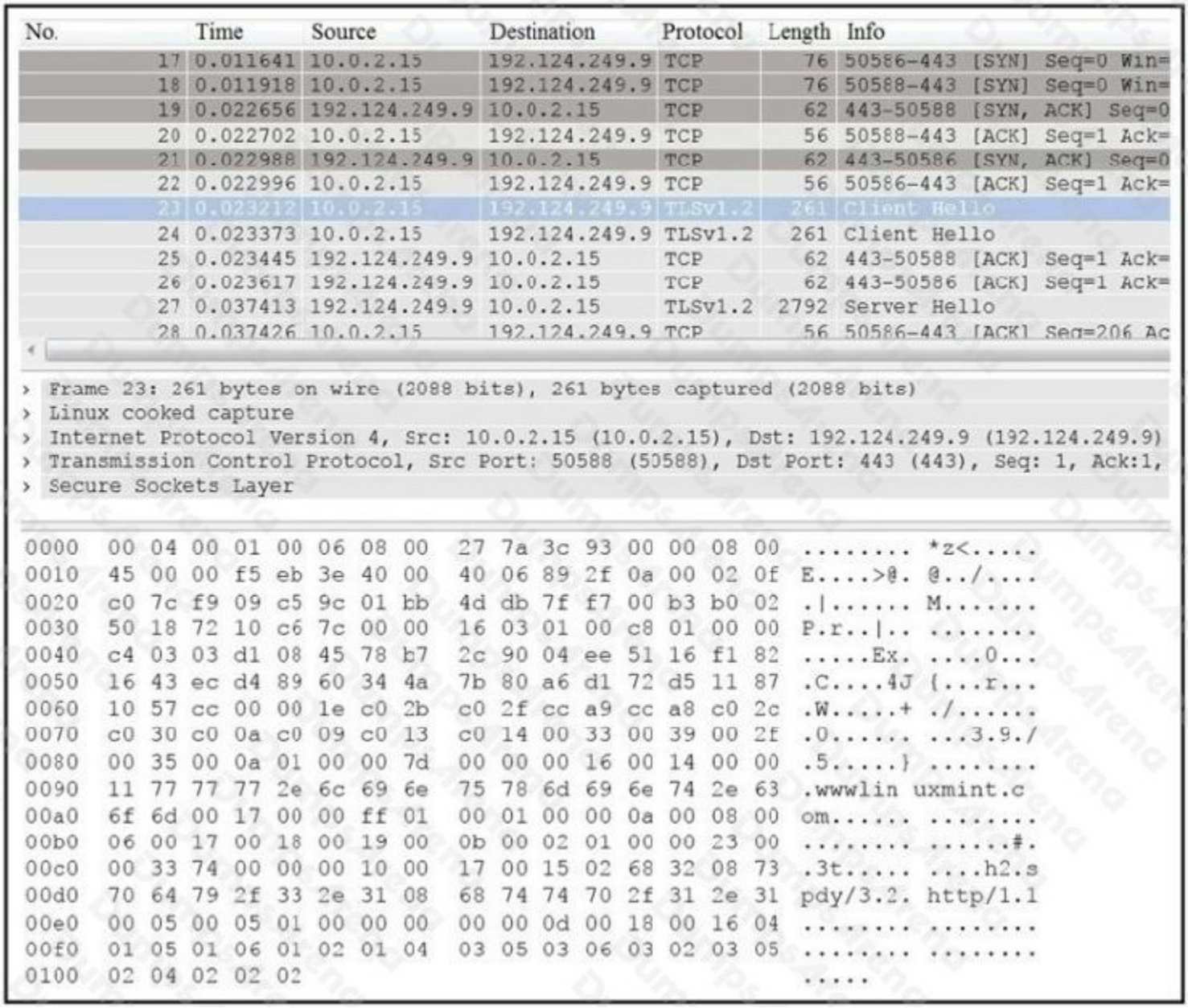
D. code-red

E. UDP flooding

ANSWER: B E

QUESTION NO: 12 - (DRAG DROP)

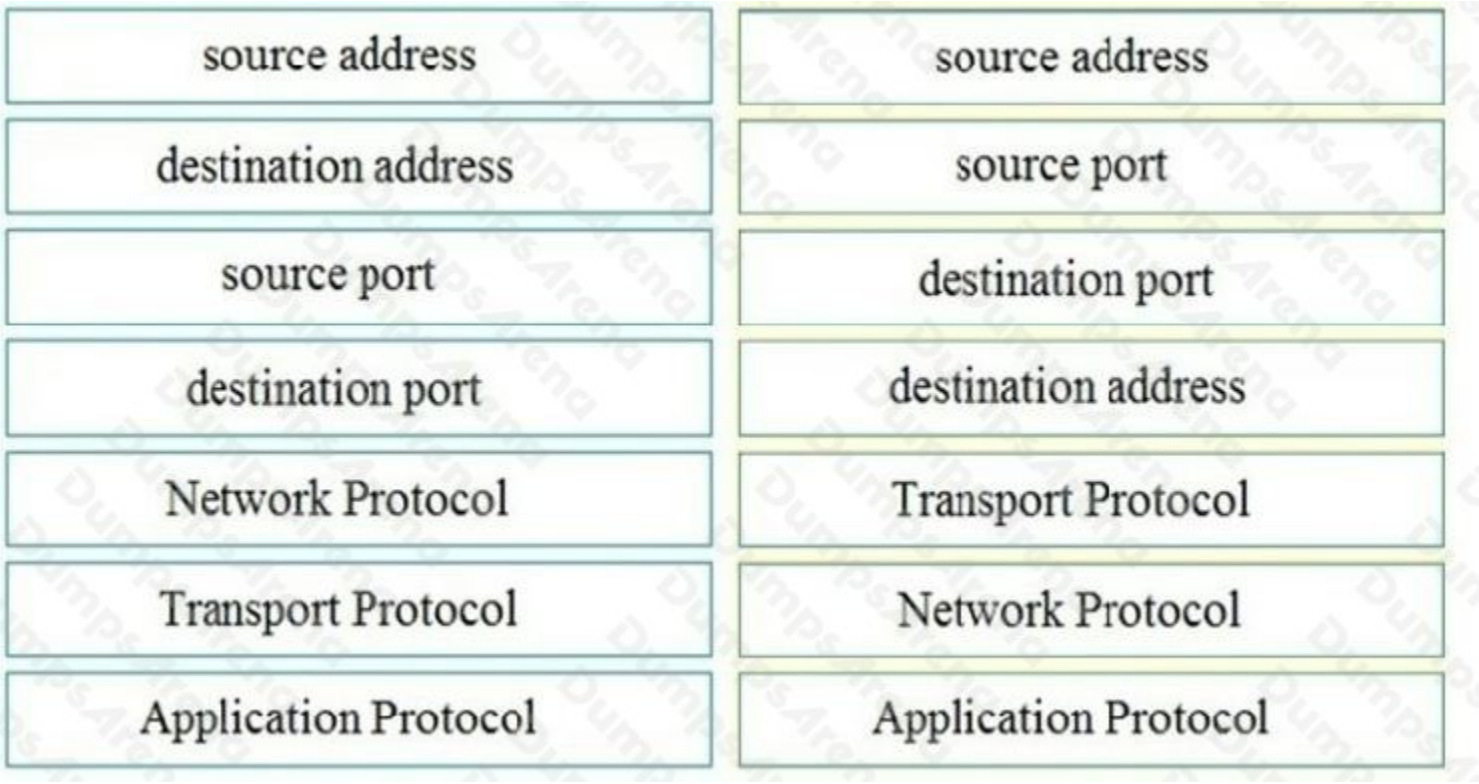
DRAG DROP



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:

ANSWER:



Explanation:

QUESTION NO: 13

What is a description of a social engineering attack?

A. fake offer for free music download to trick the user into providing sensitive data

B. package deliberately sent to the wrong receiver to advertise a new product

C. mistakenly received valuable order destined for another person and hidden on purpose

D. email offering last-minute deals on various vacations around the world with a due date and a counter

ANSWER: D

QUESTION NO: 14

Which technology prevents end-device to end-device IP traceability?

A. encryption

B. load balancing

C. NAT/PAT

D. tunneling

ANSWER: C

QUESTION NO: 15

What ate two categories of DDoS attacks? (Choose two.)

A. split brain

B. scanning

C. phishing

D. reflected

E. direct

ANSWER: D E