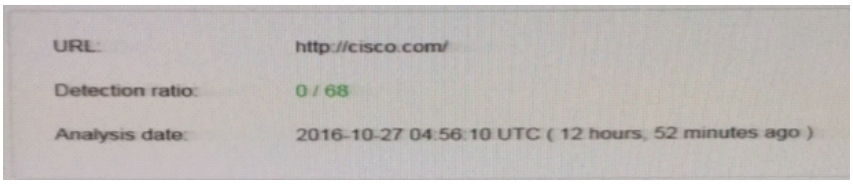
Cisco 210-255 Exam

Volume: 65 Questions

Question No: 1
Refer to the exhibit.



We have performed a malware detection on the Cisco website. Which statement about the result is true?

A. The website has been marked benign on all 68 checks.

B. The threat detection needs to run again.

C. The website has 68 open threats.

D. The website has been marked benign on O checks.

Answer: A

Question No: 2
During which phase of the forensic process is data that is related to a specific event labeled and recorded to preserve its integrity?

A. collection

B. examination

C. reporting

D. investigation

Answer: A

Question No: 3
Refer to the Exhibit.

A customer reports that they cannot access your organization's website. Which option is a possible reason that the customer cannot access the website?

A. The server at 10.33.1.5 is using up too much bandwidth causing a denial- of-service.

B. The server at 10.67.10.5 has a virus.

C. A vulnerability scanner has shown that 10.67.10.5 has been compromised.

D. Web traffic sent from 10.67.10.5 has been identified as malicious by Internet sensors.

Answer: C

Question No: 4
You see 100 HTTP GET and POST requests for various pages on one of your webservers. The user agent in the requests contain php code that, if executed, creates and writes to a new php file on the webserver. Which category does this event fall under as defined in the Diamond Model of Intrusion?

A. delivery

B. reconnaissance

C. action on objectives

D. installation

E. exploitation

Answer: D

Question No: 5
Which two options can be used by a threat actor to determine the role of a server? (Choose two.)

A. PCAP

B. tracert

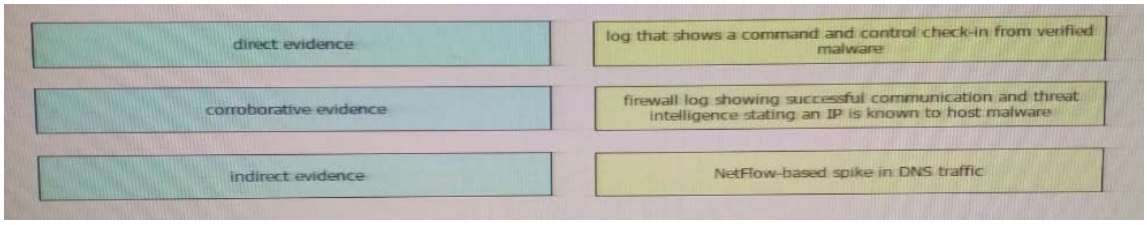
C. running processes

D. hard drive configuration

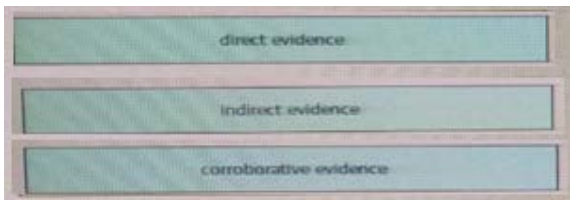
E. applications

Answer: CD

Question No: 6 DRAG DROP
Drag and drop the type of evidence from the left onto the correct description(s) of that evidence on the right.



Answer:



Question No: 7
Which process is being utilized when IPS events are removed to improve data integrity?

A. data normalization

B. data availability

C. data protection

D. data signature

Answer: B

Question No: 8
In Microsoft Windows, as files are deleted the space they were allocated eventually is considered available for use by other files. This creates alternating used and unused areas of various sizes. What is this called?

A. network file storing

B. free space fragmentation

C. alternate data streaming

D. defragmentation

Answer: A

Question No: 9
Which two components are included in a 5-tuple? (Choose two.)

A. port number

B. destination IP address

C. data packet

D. user name

E. host logs

Answer: BC

Question No: 10
Which CVSSv3 metric value increases when the attacker is able to modify all files protected by the vulnerable component?

A. confidentiality

B. integrity

C. availability

D. complexity

Answer: A

Question No: 11
Which option is generated when a file is run through an algorithm and generates a string specific to the contents of that file?

A. URL

B. hash

C. IP address

D. destination port

Answer: C

Question No: 12
Which regular expression matches "color" and "colour"?

A. col[0-9]+our

B. colo?ur

C. colou?r

D.]a-z]{7}

Answer: C

Question No: 13
In VERIS, an incident is viewed as a series of events that adversely affects the information assets of an organization. Which option contains the elements that every event is comprised of according to VERIS incident model'?

A. victim demographics, incident description, incident details, discovery & response