Cisco

210-255 Exam

Cisco Cybersecurity Operations Exam

Questions & Answers
Demo

Version: 16.0

Question: 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 0 checks.

Answer: A

Explanation:
https://www.virustotal.com/en/url/df05d8e27bd760c33dc709951a5840cc6578d78d544d869890b7b94ea21e46b0/analysis/1368183553/

Question: 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: 3

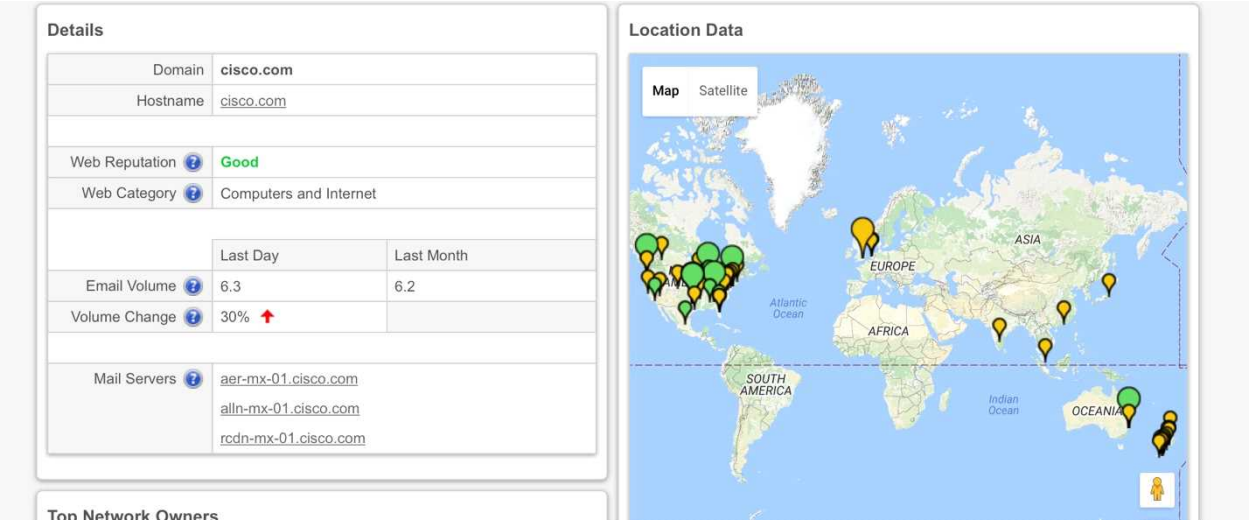
Refer to the Exhibit.

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: D

Explanation:
Every firewall has its own database where it maintains the website reputation on terms of security, ease of access, performance etc and below certain score (generally 7 in case of Cisco), firewalls block access to the sites. For example, you can visit www.senderbase.org and enter name of any website and you will see the reputation of that website.



Question: 4

You see 100 HTTP GET and POST requests for various pages on one of your web servers. 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: A

Question: 5

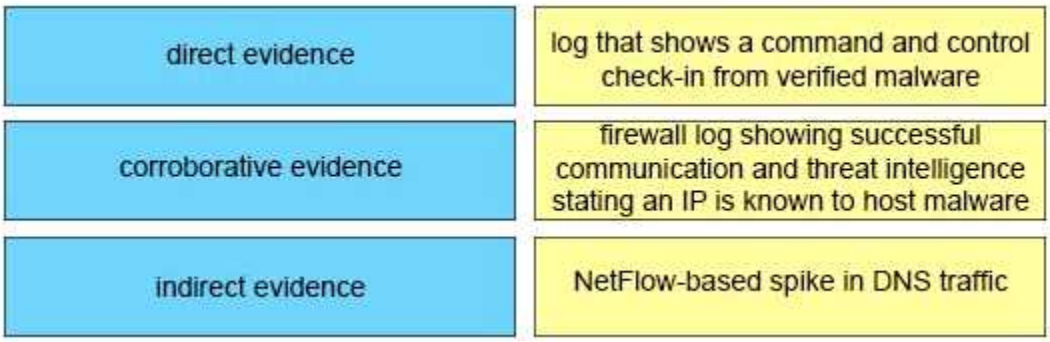
Which two options can be used by a threat actor to determine the role of a server? (Choose two.)

A. PCAP
B. tracert
C. running processes
D. hard drive configuration
E. applications

Answer: C, E

Question: 6

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



Answer:

Question: 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: A

Explanation:
Data normalization is the process of intercepting and storing incoming data so it exists in one form only. This eliminates redundant data and protects the data's integrity.
Link: https://www.helpnetsecurity.com/2013/01/07/the-importance-of-data-normalization-in-ips/

Question: 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: B

Explanation:
Free (unallocated) space fragmentation occurs when there are several unused areas of the file system where new files or meta data can be written to. Unwanted free space fragmentation is generally caused by deletion or truncation of files, but file systems may also intentionally insert fragments ("bubbles") of free space in order to facilitate extending nearby files
Reference: https://en.wikipedia.org/wiki/FileHYPERLINK "https://en.wikipedia.org/wiki/File_system_fragmentation"_system_fragmentation

Question: 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: A, B

Explanation:
The source and destination addresses are primary 5-tuple components. The source address is the IP address of the network that creates and sends a data packet, and the destination address is the recipient.

Question: 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: B

Explanation:
Consider a vulnerability in an Internet service such as web, email, or DNS that allows an attacker to modify or delete all web files in a directory would incur an impact to Integrity only, rather than Availability. The reason is that the web service is still performing properly – it just happens to be serving back altered content.

Question: 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: B

Question: 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: 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
B. victim demographics, incident details, indicators of compromise, impact assessment
C. actors, attributes, impact, remediation
D. actors, actions, assets, attributes

Answer: D

Question: 14

Which statement about threat actors is true?

A. They are any company assets that are threatened.
B. They are any assets that are threatened.
C. They are perpetrators of attacks.
D. They are victims of attacks.

Answer: C

Explanation:
A threat actor is an individual or a group of individuals who are responsible for a malicious incident that negatively impacts the security posture of an organization. Threat actors can be further categorized by a combination of skill level, type of activity within the network, and their pursuing motivations.

Question: 15

Which Security Operations Center's goal is to provide incident handling to a country?

A. Coordination Center
B. Internal CSIRT
C. National CSIRT
D. Analysis Center

Answer: C

Question: 16

Which element is part of an incident response plan?

A. organizational approach to incident response
B. organizational approach to security
C. disaster recovery
D. backups

Answer: A

Question: 17

What mechanism does the Linux operating system provide to control access to files?

A. privileges required
B. user interaction
C. file permissions
D. access complexity

Answer: C

Question: 18

Which component of the NIST SP800-61 r2 incident handling strategy reviews data?

A. preparation
B. detection and analysis
C. containment, eradication, and recovery
D. post-incident analysis

Answer: D

Explanation:
3.4.2 Using Collected Incident Data (which falls under post incident analysis in the aforementioned document)
Lessons learned activities should produce a set of objective and subjective data regarding each incident.
Over time, the collected incident data should be useful in several capacities. The data, particularly the total hours of involvement and the cost, may be used to justify additional funding of the incident response team. A study of incident characteristics may indicate systemic security weaknesses and threats, as well as changes in incident trends. This data can be put back into the risk assessment process, ultimately leading to the selection and implementation of additional controls. Another good use of the data is measuring the success of the incident response team. If incident data is collected and stored properly, it should provide several measures of the success (or at least the activities) of the incident response team.
Incident data can also be collected to determine if a change to incident response capabilities causes a corresponding change in the team's performance (e.g., improvements in efficiency, reductions in costs).