210-255 Q&As

Implementing Cisco Cybersecurity Operations

Pass Cisco 210-255 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.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

You receive an alert for malicious code that exploits Internet Explorer and runs arbitrary code on the site visitor machine. The malicous code is on an external site that is being visited by hosts on your network. Which user agent in the HTTP headers in the requests from your internal hosts warrants further investigation?

A. Mozilla/5.0 (compatible, MSIE 10.0, Windows NT 6.2, Trident 6.0)

B. Mozilla/5.0 (XII; Linux i686; rv: 1.9.2.20) Gecko/20110805

C. Mozilla/5.0 (Windows NT 6.1; WOW64; rv: 4O0) Gecko/20100101

D. Opera/9.80 (XII; Linux i686; Ubuntu/14.10) Presto/2.12.388 Version/12.16

Correct Answer: A

QUESTION 2

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 3

Which two potions are the primary 5-tuple components? (Choose two)

A. destination IP address

B. header length

C. sequence number

D. checksum

E. source IP address

Correct Answer: AE

QUESTION 4

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.

Correct Answer: A

QUESTION 5

You have a video of a suspect entering a data center that was captured on the same day that files in the same data center were transferred to a competitor. Which type of evidence is this?

A. indirect evidence

B. prima facie evidence

C. best evidence

D. physical evidence

Correct Answer: A

QUESTION 6

Refer to the exhibit. Which type of log is this an example of?

A. IDS log

B. proxy log

C. NetFlow log

D. syslog

Correct Answer: C

A typical output of a NetFlow command line tool (nfdump in this case) when printing the stored flows may look as follows:

Date flow start Duration Proto Src IP Addr:Port Dst IP Addr:Port Packets Bytes Flows 2010-09-01 00:00:00.459 0.000 UDP 127.0.0.1:24920 -> 192.168.0.1:22126 1 46 1 2010-09-01 00:00:00.363 0.000 UDP 192.168.0.1:22126 -> 127.0.0.1:24920 1 80 1

Reference: http://nfdump.sourceforge.net/

QUESTION 7

Which kind of evidence can be considered most reliable to arrive at an analytical assertion?

A. direct

B. corroborative

C. indirect

D. circumstantial

E. textual

Correct Answer: A

QUESTION 8

Which CVSSv3 metric value increases when attacks consume network bandwidth, processor cycles, or disk space?

A. confidentiality

B. integrity

C. availability

D. complexity

Correct Answer: C

QUESTION 9

Which of the following is not a metadata feature of the Diamond Model?

A. Direction

B. Result

C. Devices

D. Resources

Correct Answer: C

QUESTION 10

Which example of a precursor is true?

A. A notification that a host is infected with malware.

B. An admin finds their password has been changed.

C. A log indicating a port scan was run against a host

D. A device configuration changed from the baseline without an audit log entry.

Correct Answer: C

QUESTION 11

You have a video of suspect entering your office the day your data has being stolen?

A. Direct evidence

B. Indirect

C. Circumstantial

Correct Answer: B

QUESTION 12

Which regular expression matches andquot;colorandquot; and andquot;colourandquot;?

A. col[0-9]+our

B. colo?ur

C. colou?r

D.]a-z]{7}

Correct Answer: C

QUESTION 13

When incident data is collected, it is important that evidentiary cross-contamination is prevented. How is this accomplished?

A. by allowing unrestricted access to impacted devices

B. by not allowing items of evidence to physically touch

C. by ensuring power is removed to all devices involved

D. by not permitting a device to store evidence if it is the evidence itself.

Correct Answer: D

QUESTION 14

Refer to the following packet capture. Which of the following statements is true about this packet capture?

00:00:04.549138 IP omar.cisco.com.34548 > 93.184.216.34.telnet: Flags [S], seq 3152949738, win 29200,

options [mss 1460,sackOK,TS val 1193148797 ecr 0,nop,wscale 7], length 0 00:00:05.547084 IP omar.cisco.com.34548 > 93.184.216.34.telnet: Flags [S], seq 3152949738, win 29200,

options [mss 1460,sackOK,TS val 1193149047 ecr 0,nop,wscale 7], length 0 00:00:07.551078 IP omar.cisco.com.34548 > 93.184.216.34.telnet: Flags [S], seq 3152949738, win 29200,

options [mss 1460,sackOK,TS val 1193149548 ecr 0,nop,wscale 7], length 0 00:00:11.559081 IP omar.cisco.com.34548 > 93.184.216.34.telnet: Flags [S], seq 3152949738, win 29200,

options [mss 1460,sackOK,TS val 1193150550 ecr 0,nop,wscale 7], length 0

A. The host with the IP address 93.184.216.34 is the source.

B. The host omar.cisco.com is the destination.

C. This is a Telnet transaction that is timing out and the server is not responding.

D. The server omar.cisco.com is responding to 93.184.216.34 with four data packets.

Correct Answer: C

QUESTION 15

Which of the following is not true regarding the use of digital evidence?

A. Digital forensics evidence provides implications and extrapolations that may assist in proving some key fact of the case.

B. Digital evidence helps legal teams and the court develop reliable hypotheses or theories as to the committer of the crime or threat actor.

C. The reliability of the digital evidence is vital to supporting or refuting any hypothesis put forward, including the attribution of threat actors.

D. The reliability of the digital evidence is not as important as someone\\'s testimony to supporting or refuting any hypothesis put forward, including the attribution of threat actors.

Correct Answer: D

QUESTION 16

Refer to the exhibit. Which type of log is this an example of?

A. syslog

B. NetFlow log

C. proxy log

D. IDS log

Correct Answer: D

QUESTION 17

Which type of intrusion event is an attacker retrieving the robots. txt file from target site?

A. exploitation

B. weaponization

C. scanning

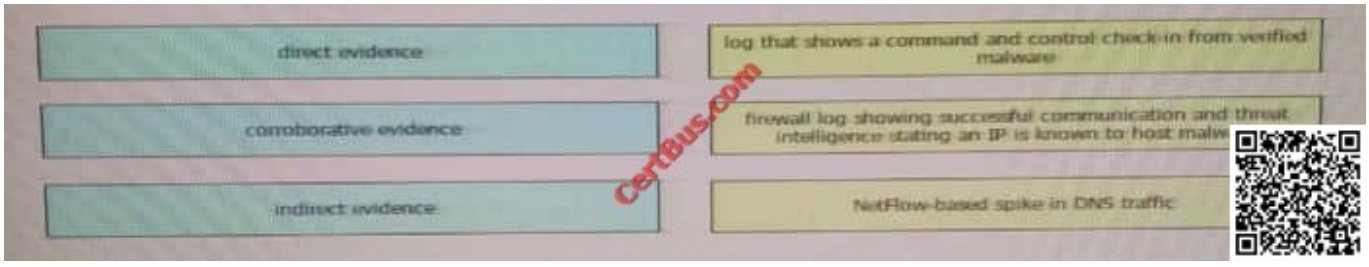
D. reconnaissance

Correct Answer: D

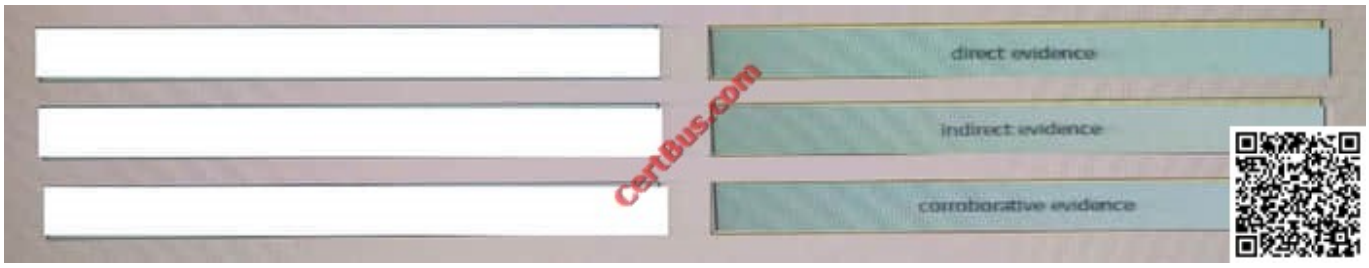
QUESTION 18

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 19

Which option has a drastic impact on network traffic because it can cause legitimate traffic to be blocked?

A. true positive

B. true negative

C. false positive

D. false negative

Correct Answer: C

QUESTION 20

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 21

Which of the following are examples of Linux boot loaders?

A. GRUB

B. ILOS

C. LILO

D. Ubuntu BootPro

Correct Answer: C

QUESTION 22

During which phase of the forensic process are tools and techniques used to extract the relevant information from the collective data?

A. examination

B. reporting

C. collection

D. investigation

Correct Answer: A

Examinations involve forensically processing large amounts of collected data using a combination of automated and manual methods to assess and extract data of particular interest, while preserving the integrity of the data. Forensic tools and techniques appropriate to the types of data that were collected are executed to identify and extract the relevant information from the collected data while protecting its integrity. Examination may use a combination of automated tools and manual processes.

QUESTION 23

From a security perspective, why is it important to employ a clock synchronization protocol on a network?

A. so that everyone knows the local time

B. to ensure employees adhere to work schedule

C. to construct an accurate timeline of events when responding to an incident

D. to guarantee that updates are pushed out according to schedule

Correct Answer: C

QUESTION 24

What are the metric values of the confidentiality based on the CVSS framework?

A. Low-high

B. Low -Medium-high

C. High-Low-none

Correct Answer: C

QUESTION 25

Which HTTP header field is usually used in forensics to identify the type of browser used?

A. User agent

B. Referrer

C. Host

D. Accept-language

Correct Answer: A

QUESTION 26

Which option is the process of remediating the network and systems and/or reconstructing the attack so that the responsible threat actor can be revealed?

A. data analytics

B. asset attribution

C. threat actor attribution

D. evidence collection

Correct Answer: A

QUESTION 27

Which event artifact can be used to identify HTTP GET requests for a specific file?

A. HTTP status code

B. TCP ACK

C. destination IP

D. URI

Correct Answer: D

QUESTION 28

Which of the following is an example of a managed security offering where incident response experts monitor and respond to security alerts in a security operations center (SOC)?

A. Cisco CloudLock

B. Cisco\\'s Active Threat Analytics (ATA)

C. Cisco Managed Firepower Service

D. Cisco Jasper

Correct Answer: B

QUESTION 29

According to NIST 86, which action describes the volatile data collection?

A. Collect data before rebooting

B. Collect data while rebooting

C. Collect data after rebooting

D. Collect data that contains malware

Correct Answer: A

QUESTION 30

You have run a suspicious file in a sandbox analysis tool to see what the file does. The analysis report shows that outbound callouts were made post infection. Which two pieces of information from the analysis report are needed or required to investigate the callouts? (Choose two.)

A. file size

B. domain names

C. dropped files

D. signatures

E. host IP addresses

Correct Answer: BE

To Read the Whole Q&As, please purchase the Complete Version from Our website.

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

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.certbus.com/allproducts

Need Help

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