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.lead4pass.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

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 2

Which string matches the regular expression r(ege)+x?

A. rx

B. regeegex

C. r(ege)x

D. rege+x

Correct Answer: B

QUESTION 3

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 4

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 5

Which option allows a file to be extracted from a TCP stream within Wireshark?

A. File > Export Objects

B. Analyze > Extract

C. Tools > Export > TCP

D. View > Extract

Correct Answer: A

QUESTION 6

What is a common artifact used to uniquely identify a detected file?

A. file size

B. file extension

C. file timestamp

D. file hash

Correct Answer: D

QUESTION 7

What are the metric values for confidentiality impact in the CVSS v3.0 framework?

A. high, low

B. high, low, none

C. high, medium, none

D. open, closed, obsolete

Correct Answer: B

QUESTION 8

The united State CERT provides cybersecurity protection to Federal, civilian, and executive branch agencies through intrusion detection and prevention capabilities. Which type of incident response team is this an example of?

A. Federal PSIRT

B. National PSIRT

C. National CSIRT

D. Federal CSIRT

Correct Answer: C

QUESTION 9

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 10

What is the definition of integrity according to CVSSv3 framework?

A. This metric measures the impact to the confidentiality of the information resources that are managed by a software component due to a successfully exploited vulnerability.

B. This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information.

C. This metric measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability.

Correct Answer: B

QUESTION 11

Which analyzing technique describe the outcome as well as how likely each outcome is?

A. deterministic

B. exploratory

C. probabilistic

D. descriptive

Correct Answer: C

QUESTION 12

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 13

Which of the following has been used to evade IDS and IPS devices?

A. SNMP

B. HTTP

C. TNP

D. Fragmentation

Correct Answer: D

QUESTION 14

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 15

Refer to the exhibit. You notice that the email volume history has been abnormally high. Which potential result is true?

A. Email sent from your domain might be filtered by the recipient.

B. Messages sent to your domain may be queued up until traffic dies down.

C. Several hosts in your network may be compromised.

D. Packets may be dropped due to network congestion.

Correct Answer: C

QUESTION 16

Employees are allowed access to internal websites. An employee connects to an internal website and IDS reports it as malicious behavior. What is this example of?

A. true positive

B. false negative

C. false positive

D. true negative

Correct Answer: C

QUESTION 17

Which of the following is true about journaling?

A. The journal is the least used part of the disk, making the blocks that form part of it more prone to hardware failure.

B. The journal is the most used part of the disk, making the blocks that form part of it less prone to hardware failure.

C. The journal is the most used part of the disk, making the blocks that form part of it more prone to hardware failure.

D. The journal is the least used part of the disk, making the blocks that form part of it less prone to hardware failure.

Correct Answer: C

QUESTION 18

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 19

Which of the following is not an example of weaponization?

A. Connecting to a command and control server

B. Wrapping software with a RAT

C. Creating a backdoor in an application

D. Developing an automated script to inject commands on a USB device

Correct Answer: A

QUESTION 20

What is the process of remediation the system from attack so that responsible threat actor can be revealed?

A. Validating the Attacking Host\\'s IP Address

B. Researching the Attacking Host through Search Engines.

C. Using Incident Databases.

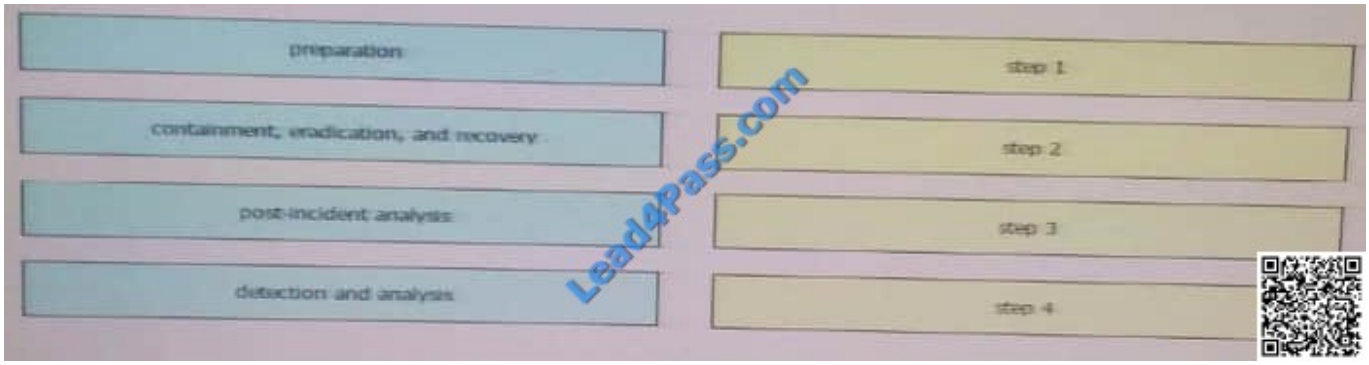
D. Monitoring Possible Attacker Communication Channels.

Correct Answer: A

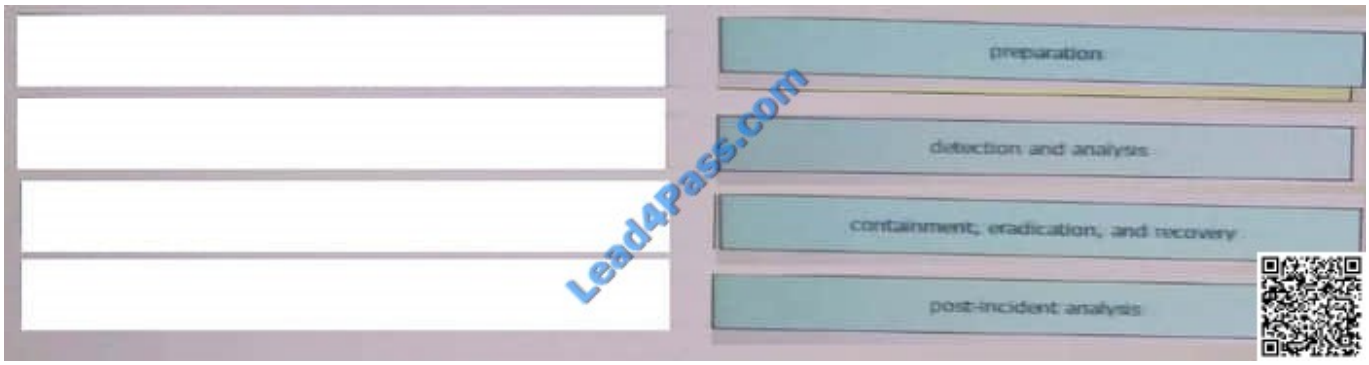
QUESTION 21

Drag and drop the elements of incident handling from the left into the correct order on the right.

Select and Place:



Correct Answer:



QUESTION 22

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 23

Which network device creates and sends the initial packet of a session?

A. source

B. origination

C. destination

D. network

Correct Answer: A

QUESTION 24

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

Correct Answer: A

QUESTION 25

According to NIST SP800-86, which action describes volatile data collection?

A. collection of data before a system reboot

B. collection of data that contains malware

C. collection of data during a system reboot

D. collection of data after a system reboot

Correct Answer: A

QUESTION 26

What attribute belonging VERIS schema?

A. confidentiality/possession

B. integrity/authenticity

C. availability/utility

Correct Answer: ABC

QUESTION 27

When performing threat hunting against a DNS server, which traffic toward the affected domain is considered a starting point?

A. HTTPS traffic

B. TCP traffic

C. HTTP traffic

D. UDP traffic

Correct Answer: D

QUESTION 28

Choose the option that best describes NIST data integrity

A. use only sha-1

B. use only md5

C. you must hash data and backup and compare hashes

D. no need to hash data and backup and compare hashes

Correct Answer: C

QUESTION 29

Which two statements correctly describe the victim demographics section of the VERIS schema? (Choose two.)

A. The victim demographics section describes but does not identify the organization that is affected by the incident.

B. The victim demographics section compares different types of organizations or departments within a single organization.

C. The victim demographics section captures general information about the incident.

D. The victim demographics section uses geolocation data to identify the organization name of the victim and the threat actor.

Correct Answer: AB

QUESTION 30

Which stakeholder group is responsible for containment, eradication, and recovery in incident handling?

A. facilitators

B. practitioners

C. leaders and managers

D. decision makers

Correct Answer: C

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.lead4pass.com/allproducts

Need Help

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