210-255 Q&As

Cisco Cybersecurity Operations

Pass Cisco 210-255 Exam with 100% Guarantee

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

https://www.leads4pass.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

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 2

Which technology generates events utilizing proxy logs?

A. Firepower

B. Email Security Appliance

C. Stealthwatch

D. Web Security Appliance

Correct Answer: D

QUESTION 3

Which of the following is not true about listening ports?

A. A listening port is a port held open by a running application in order to accept inbound connections.

B. Seeing traffic from a known port will identify the associated service.

C. Listening ports use values that can range between 1 and 65535.

D. TCP port 80 is commonly known for Internet traffic.

Correct Answer: B

QUESTION 4

Which two compliance frameworks require that data be encrypted when it is transmitted over a public network? (Choose two.)

A. PCI

B. GLBA

C. HIPAA

D. SOX

E. COBIT

Correct Answer: AC

QUESTION 5

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

Correct Answer: B

QUESTION 6

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 7

Which of the following statements is true about processes and threads?

A. Each thread starts with a single process, known as the primary process, but can also create additional processes from any of itsservices.

B. Each service starts with a single hive, known as the primary hive, but can also create additional threads from any of its hives.

C. Each process starts with a single thread, known as the primary thread, but can also create additional threads from any of its threads.

D. Each hive starts with a single thread, known as the primary thread, but can also create additional threads from any of its threads.

Correct Answer: C

QUESTION 8

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 9

Which two potions about deterministic and probabilistic analysis are true? (Choose two.)

A. probabilistic analysis uses data known beforehand and deterministic analysis is based off assumptions.

B. Deterministic analysis uses data known beforehand and probabilistic analysis based off of assumptions.

C. Deterministic analysis is based off of assumptions

D. Probabilistic analysis result in a result that is definitive.

E. probabilistic analysis results in a result that is not definitive.

Correct Answer: BE

QUESTION 10

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 11

Which Cyber Kill Chain Model category does attacking a vulnerability belong to?

A. Exploitation

B. Action on Objectives

C. Installation

D. Delivery

Correct Answer: A

QUESTION 12

Which two HTTP header fields relate to intrusion analysis? (Choose two).

A. user-agent

B. host

C. connection

D. language

E. handshake type

Correct Answer: AB

QUESTION 13

Which of the following is an example of a coordination center?

A. Cisco PSIRT

B. Microsoft MSRC

C. CERT division of the Software Engineering Institute (SEI)

D. FIRST

Correct Answer: C

QUESTION 14

Refer to the exhibit. Which packet contains a file that is extractable within Wireshark?

No.	Time	Source	Destination	Protocol	Length	Info
1878	6.473353	173.37.145.84	10.0.2.15	TCP	62	80-49522 [ACK] Seq=14404 ACK=2987 Win=65535 Len=0
1986	6.736855	173.37.145.84	10.0.2.15	HTTP	245	HTTP/1.1 304 Not Modified
1987	6.736873	10.0.2.15	173.37.145.84	TCP	56	49522-80 [ACK] Seq=2987 ACK=14593 Win=59640 Len=0
2317	7.245088	10.0.2.15	173.37.145.84	TCP	2976	[TCP segment of a reassembled PDU]
2318	7.245192	10.0.2.15	173.37.145.84	HTTP	1020	GET /web/fw/1/ntpagetag.gif?js=14ts=1476292607552.2866tc
2321	7.246633	173.37.145.84	10.0.2.15	TCP	62	80-49522 [ACK] Seq=14593 ACK=4447 Win=65535 Len=0
2322	7.246640	173.37.145.84	10.0.2.15	TCP	62	80-49522 [ACK] Seq=14593 ACK=5907 Win=65535 Len=0
2323	7.246642	173.37.145.84	10.0.2.15	TCP	62	80-49522 [ACK] Seq=14593 ACK=6871 Win=65535 Len=0
2542	7.512750	173.37.145.84	10.0.2.15	HTTP	442	HTTP/1.1 200 OK (GIF89a)
2543	7.512781	10.0.2.15	173.37.145.84	TCP	56	49522-80 [ACK] Seq=6871 ACK=14979 Win=62480 Len=0

A. 1986

B. 2318

C. 2542

D. 2317

Correct Answer: B

QUESTION 15

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