210-255$^{\text{Q\&As}}$

Cisco Cybersecurity Operations

Pass Cisco 210-255 Exam with 100% Guarantee

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

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

Correct Answer: A

QUESTION 3

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 4

What does 5-typle refer to?

A. set of five different values that comprise a SSL connection

B. set of five different values that comprise a HTTPS connection

C. set of five different values that comprise a UDP connection

D. set of five different values that comprise a TCP/IP connection

Correct Answer: D

QUESTION 5

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

A. SNMP

B. HTTP

C. TNP

D. Fragmentation

Correct Answer: D