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.pass4itsure.com/210-255.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

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 type verification typically consists of using tools to compute the message digest of the original and copies data, then comparing the digests to make sure that they are the same?

A. evidence collection order

B. data integrity

C. data preservation

D. volatile data collection

Correct Answer: B

QUESTION 3

Which incident handling is focused on minimizing the impact of an incident?

A. Scoping

B. Reporting

C. Containment

D. Eradication

Correct Answer: C

QUESTION 4

According to NIST-SP800-61R2, which option should be contained in the issue tracking system?

A. incidents related to the current incident

B. incident unrelated to the current incident

C. actions taken by nonincident handlers

D. latest public virus signatures

Correct Answer: A

QUESTION 5

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 6

Which of the following are examples of some of the responsibilities of a corporate CSIRT and the policies it helps create? (Select all that apply.)

A. Scanning vendor customer networks

B. Incident classification and handling

C. Information classification and protection

D. Information dissemination

E. Record retentions and destruction

Correct Answer: BCD

QUESTION 7

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

Correct Answer: B

QUESTION 8

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 9

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 10

Which type of analysis allows you to see how likely an exploit could affect your network?

A. descriptive

B. casual

C. probabilistic

D. inferential

Correct Answer: C

QUESTION 11

Which element can be used by a threat actor to discover a possible opening into a target network and can also be used by an analyst to determine the protocol of the malicious traffic?

A. TTLs

B. ports

C. SMTP replies

D. IP addresses

Correct Answer: B

QUESTION 12

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

210-255 PDF Dumps 210-255 VCE Dumps 210-255 Braindumps

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

Try our product !

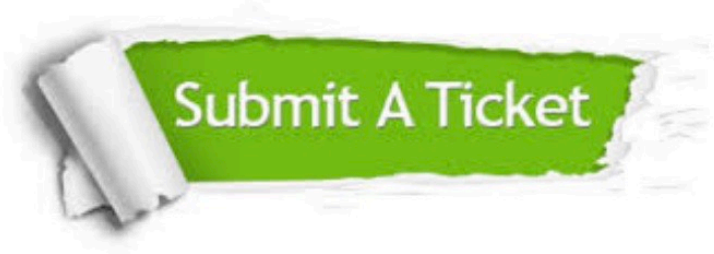
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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.pass4itsure.com/allproducts

Need Help

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



Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © pass4itsure, All Rights Reserved.