200-201 Q&As

Threat Hunting and Defending using Cisco Technologies for CyberOps (CBROPS)

Pass Cisco 200-201 Exam with 100% Guarantee

QUESTION 1

What is a purpose of a vulnerability management framework?

A. identifies, removes, and mitigates system vulnerabilities

B. detects and removes vulnerabilities in source code

C. conducts vulnerability scans on the network

D. manages a list of reported vulnerabilities

Correct Answer: A

QUESTION 2

What is the difference between statistical detection and rule-based detection models?

A. Rule-based detection involves the collection of data in relation to the behavior of legitimate users over a period of time

B. Statistical detection defines legitimate data of users over a period of time and rule-based detection defines it on an IF/THEN basis

C. Statistical detection involves the evaluation of an object on its intended actions before it executes that behavior

D. Rule-based detection defines legitimate data of users over a period of time and statistical detection defines it on an IF/THEN basis

Correct Answer: B

QUESTION 3

Which NIST IR category stakeholder is responsible for coordinating incident response among various business units, minimizing damage, and reporting to regulatory agencies?

A. CSIRT

B. PSIRT

C. public affairs

D. management

Correct Answer: D

QUESTION 4

An organization has recently adjusted its security stance in response to online threats made by a known hacktivist group.

What is the initial event called in the NIST SP800-61?

A. online assault

B. precursor

C. trigger

D. instigator

Correct Answer: B

QUESTION 5

Which incidence response step includes identifying all hosts affected by an attack?

A. detection and analysis

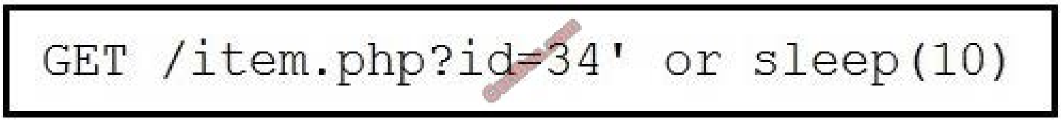
B. post-incident activity

C. preparation

D. containment, eradication, and recovery

Correct Answer: D

QUESTION 6



```
GET /item.php?id=34' or sleep(10)
```

Refer to the exhibit. This request was sent to a web application server driven by a database.

Which type of web server attack is represented?

A. parameter manipulation

B. heap memory corruption

C. command injection

D. blind SQL injection

Correct Answer: D

QUESTION 7

What is the difference between deep packet inspection and stateful inspection?

A. Deep packet inspection is more secure than stateful inspection on Layer 4

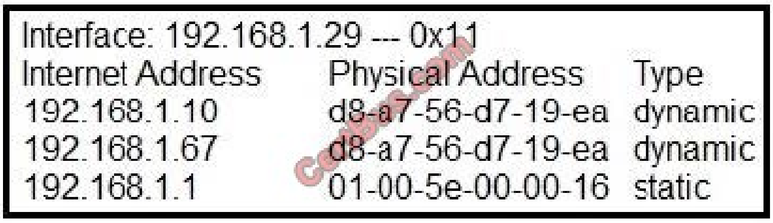
B. Stateful inspection verifies contents at Layer 4 and deep packet inspection verifies connection at Layer 7

C. Stateful inspection is more secure than deep packet inspection on Layer 7

D. Deep packet inspection allows visibility on Layer 7 and stateful inspection allows visibility on Layer 4

Correct Answer: D

QUESTION 8



```
Interface: 192.168.1.29 --- 0x11
Internet Address      Physical Address     Type
192.168.1.10          d8-a7-56-d7-19-ea    dynamic
192.168.1.67          d8-a7-56-d7-19-ea    dynamic
192.168.1.1           01-00-5e-00-00-16    static
```

Refer to the exhibit. What is occurring in this network?

A. ARP cache poisoning

B. DNS cache poisoning

C. MAC address table overflow

D. MAC flooding attack

Correct Answer: A

QUESTION 9

Which regex matches only on all lowercase letters?

A. [a-z]+

B. [^a-z]+

C. a-z+

D. a*z+

Correct Answer: A

QUESTION 10

What is the relationship between a vulnerability and a threat?

A. A threat exploits a vulnerability

B. A vulnerability is a calculation of the potential loss caused by a threat

C. A vulnerability exploits a threat

D. A threat is a calculation of the potential loss caused by a vulnerability

Correct Answer: A

QUESTION 11

Which metric is used to capture the level of access needed to launch a successful attack?

A. privileges required

B. user interaction

C. attack complexity

D. attack vector

Correct Answer: A

QUESTION 12

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

A. destination IP address

B. TCP ACK

C. HTTP status code

D. URI

Correct Answer: D

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

Try our product !

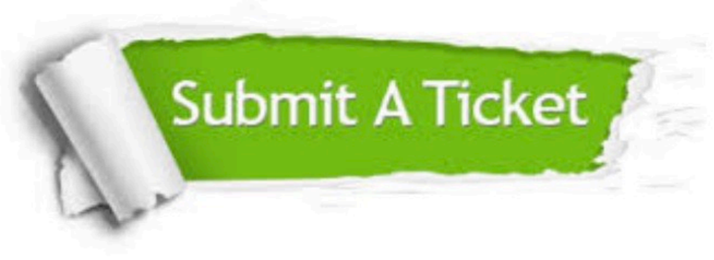
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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:



One Year Free Update

Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.

Money Back Guarantee

To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.