200-201 Q&As

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Pass Cisco 200-201 Exam with 100% Guarantee

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

https://www.geekcert.com/200-201.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

Refer to the exhibit.

Which type of attack is being executed?

A. SQL injection

B. cross-site scripting

C. cross-site request forgery

D. command injection

Correct Answer: A

Reference: https://www.w3schools.com/sql/sql_injection.asp

QUESTION 2

What is the difference between a threat and a risk?

A. Threat represents a potential danger that could take advantage of a weakness in a system

B. Risk represents the known and identified loss or danger in the system

C. Risk represents the nonintentional interaction with uncertainty in the system

D. Threat represents a state of being exposed to an attack or a compromise, either physically or logically.

Correct Answer: A

A threat is any potential danger to an asset. If a vulnerability exists but has not yet been exploited--or, more importantly, it is not yet publicly known--the threat is latent and not yet realized.

QUESTION 3

Why should an engineer use a full packet capture to investigate a security breach?

A. It provides the full TCP streams for the engineer to follow the metadata to identify the incoming threat.

B. It collects metadata for the engineer to analyze, including IP traffic packet data that is sorted, parsed, and indexed.

C. It reconstructs the event allowing the engineer to identify the root cause by seeing what took place during the

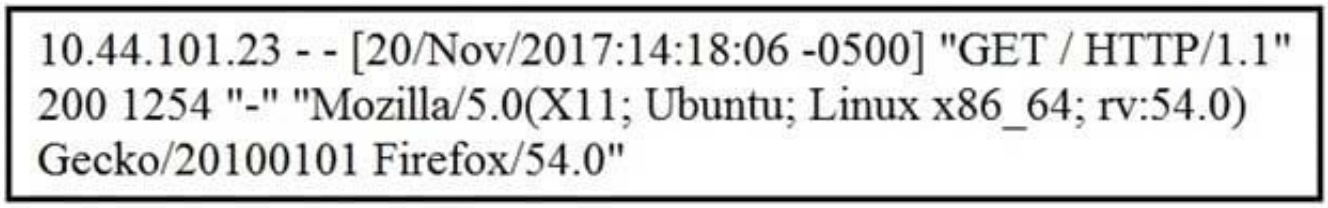
breach.

D. It captures the TCP flags set within each packet for the engineer to focus on suspicious packets to identify malicious activity.

Correct Answer: C

QUESTION 4

Refer to the exhibit.



What does the message indicate?

A. an access attempt was made from the Mosaic web browser

B. a successful access attempt was made to retrieve the password file

C. a successful access attempt was made to retrieve the root of the website

D. a denied access attempt was made to retrieve the password file

Correct Answer: C

QUESTION 5

A threat actor penetrated an organization\\'s network. Using the 5-tuple approach, which data points should the analyst use to isolate the compromised host in a grouped set of logs?

A. event name, log source, time, source IP, and host name

B. protocol, source IP, source port, destination IP, and destination port

C. event name, log source, time, source IP, and username

D. protocol, log source, source IP, destination IP, and host name

Correct Answer: B

Reference: https://blogs.cisco.com/security/the-dreaded-5-tuple