350-201 Q&As

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Pass Cisco 350-201 Exam with 100% Guarantee

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

https://www.leads4pass.com/350-201.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An engineer is utilizing interactive behavior analysis to test malware in a sandbox environment to see how the malware performs when it is successfully executed. A location is secured to perform reverse engineering on a piece of malware. What is the next step the engineer should take to analyze this malware?

A. Run the program through a debugger to see the sequential actions

B. Unpack the file in a sandbox to see how it reacts

C. Research the malware online to see if there are noted findings

D. Disassemble the malware to understand how it was constructed

Correct Answer: C

QUESTION 2

How does Wireshark decrypt TLS network traffic?

A. with a key log file using per-session secrets

B. using an RSA public key

C. by observing DH key exchange

D. by defining a user-specified decode-as

Correct Answer: A

Reference: https://wiki.wireshark.org/TLS

QUESTION 3

An organization had an incident with the network availability during which devices unexpectedly malfunctioned. An engineer is investigating the incident and found that the memory pool buffer usage reached a peak before the malfunction. Which action should the engineer take to prevent this issue from reoccurring?

A. Disable memory limit.

B. Disable CPU threshold trap toward the SNMP server.

C. Enable memory tracing notifications.

D. Enable memory threshold notifications.

Correct Answer: D

QUESTION 4

URIs:

- /invoker/JMXInvokerServlet
- /CFIDE/adminapi
- /?a=<script>alert%28%22XSS%22%29%3B</script>&b=UNION+SELECT+ALL+FROM+information_schema+AND+%27+or+SLEEP%285%29+or+%27&c=../../../../etc/passwd

Refer to the exhibit. At which stage of the threat kill chain is an attacker, based on these URIs of inbound web requests from known malicious Internet scanners?

A. exploitation

B. actions on objectives

C. delivery

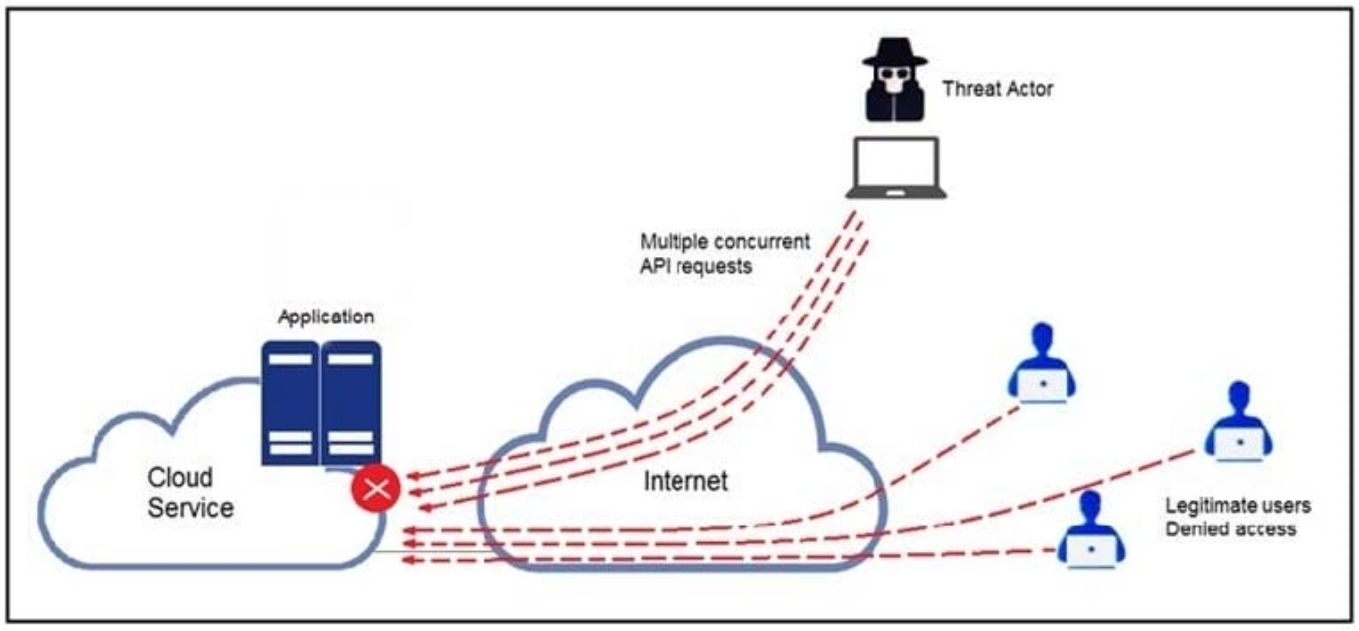
D. reconnaissance

Correct Answer: C

Reference: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-july2017.pdf

QUESTION 5

Refer to the exhibit. A threat actor behind a single computer exploited a cloud-based application by sending multiple concurrent API requests. These requests made the application unresponsive. Which solution protects the application from being overloaded and ensures more equitable application access across the end-user community?



A. Limit the number of API calls that a single client is allowed to make

B. Add restrictions on the edge router on how often a single client can access the API

C. Reduce the amount of data that can be fetched from the total pool of active clients that call the API

D. Increase the application cache of the total pool of active clients that call the API

Correct Answer: A