



Pass4IT

CISCO
350-201

QUESTIONS AND ANSWERS

FREE VERSION

(LIMITED CONTENT)

Thank you for downloading our reliable exam questions
for more exams you can visit:

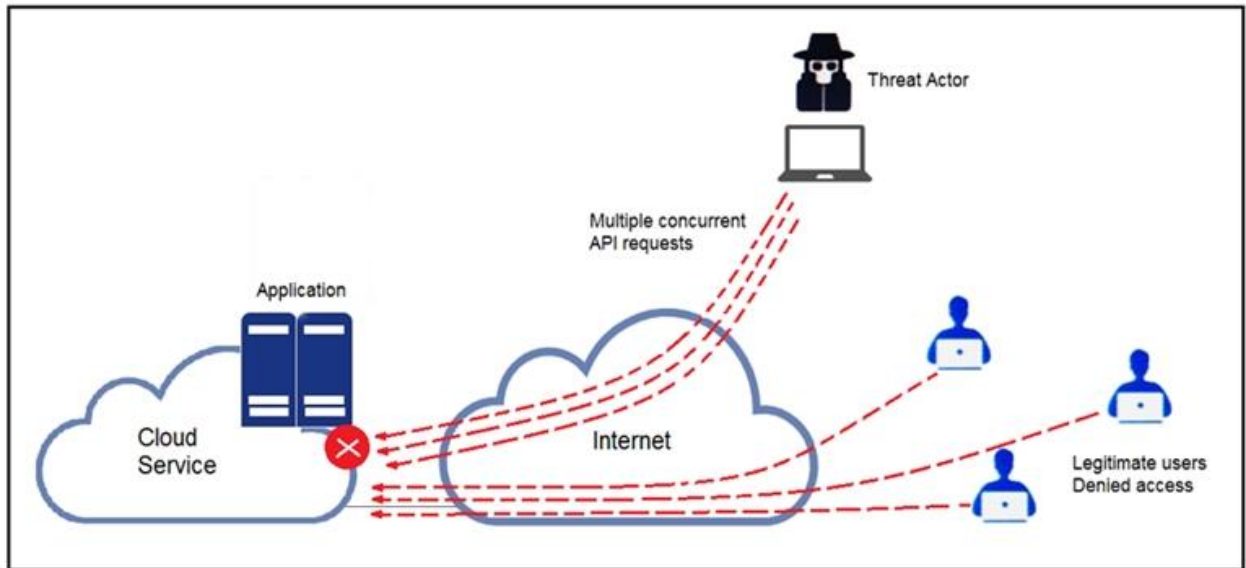
<https://www.pass4it.com/all-vendors>

Certification Provider: Cisco

Exam: Performing CyberOps Using Core Security Technologies (CBRCOR)

Question #1

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

Question #2

DRAG DROP -

An organization lost connectivity to critical servers, and users cannot access business applications and internal websites. An engineer checks the network devices to investigate the outage and determines that all devices are functioning. Drag and drop the steps from the left into the sequence on the right to continue investigating this issue. Not all options are used.

Select and Place:

Answer Area

- run show access-list
- run show config
- validate the file MD5
- generate the core file
- verify the image file hash
- check the memory logs
- verify the memory state

- Step 1
- Step 2
- Step 3
- Step 4

Correct

Answer:

Answer Area

- | | |
|----------------------------|-------------------------|
| run show access-list | run show config |
| run show config | check the memory logs |
| validate the file MD5 | verify the memory state |
| generate the core file | run show access-list |
| verify the image file hash | |
| check the memory logs | |
| verify the memory state | |

Question #3

A threat actor attacked an organization's Active Directory server from a remote location, and in a thirty-minute timeframe, stole the password for the administrator account and attempted to access 3 company servers. The threat actor successfully accessed the first server that contained sales data, but no files were downloaded. A second server was also accessed that contained marketing information and 11 files were downloaded. When the threat actor accessed the third server that contained corporate financial data, the session was disconnected, and the administrator's account was disabled. Which activity triggered the behavior analytics tool?

- A. accessing the Active Directory server
- B. accessing the server with financial data
- C. accessing multiple servers
- D. downloading more than 10 files

Correct Answer: C

Question #4

Refer to the exhibit. A security analyst needs to investigate a security incident involving several suspicious connections with a possible attacker. Which tool should the analyst use to identify the source IP of the offender?

TCP	192.168.1.8:54580	vk-in-f108:imaps	ESTABLISHED
TCP	192.168.1.8:54583	132.245.61.50:https	ESTABLISHED
TCP	192.168.1.8:54916	bay405-m:https	ESTABLISHED
TCP	192.168.1.8:54978	vu-in-f188:5228	ESTABLISHED
TCP	192.168.1.8:55094	72.21.194.109:https	ESTABLISHED
TCP	192.168.1.8:55401	wonderhowto:http	ESTABLISHED
TCP	192.168.1.8:55730	mia07s34-in-f78:https	TIME_WAIT
TCP	192.168.1.8:55824	a23-40-191-15:https	CLOSE_WAIT
TCP	192.168.1.8:55825	a23-40-191-15:https	CLOSE_WAIT
TCP	192.168.1.8:55846	mia07s25-in-f14:https	TIME_WAIT
TCP	192.168.1.8:55847	a184-51-150-89:http	CLOSE_WAIT
TCP	192.168.1.8:55853	157.55.56.154:40028	ESTABLISHED
TCP	192.168.1.8:55879	atl14s38-in-f4:https	ESTABLISHED
TCP	192.168.1.8:55884	208-46-117-174:https	ESTABLISHED
TCP	192.168.1.8:55893	vx-in-f95:https	TIME_WAIT
TCP	192.168.1.8:55947	stackoverflow:https	ESTABLISHED
TCP	192.168.1.8:55966	stackoverflow:https	ESTABLISHED
TCP	192.168.1.8:55970	mia07s34-in-f78:https	TIME_WAIT
TCP	192.168.1.8:55972	191.238.241.80:https	TIME_WAIT
TCP	192.168.1.8:55976	54.239.26.242:https	ESTABLISHED
TCP	192.168.1.8:55979	mia07s35-in-f14:https	ESTABLISHED
TCP	192.168.1.8:55986	server11:https	TIME_WAIT
TCP	192.168.1.8:55988	104.16.118.182:http	ESTABLISHED

- A. packet sniffer

B. malware analysis

C. SIEM

D. firewall manager

Correct Answer: A