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.pass4itsure.com/350-201.html

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

QUESTION 1

A security incident affected an organization\\'s critical business services, and the customer-side web API became unresponsive and crashed. An investigation revealed a spike of API call requests and a high number of inactive sessions during the incident. Which two recommendations should the engineers make to prevent similar incidents in the future? (Choose two.)

A. Configure shorter timeout periods.

B. Determine API rate-limiting requirements.

C. Implement API key maintenance.

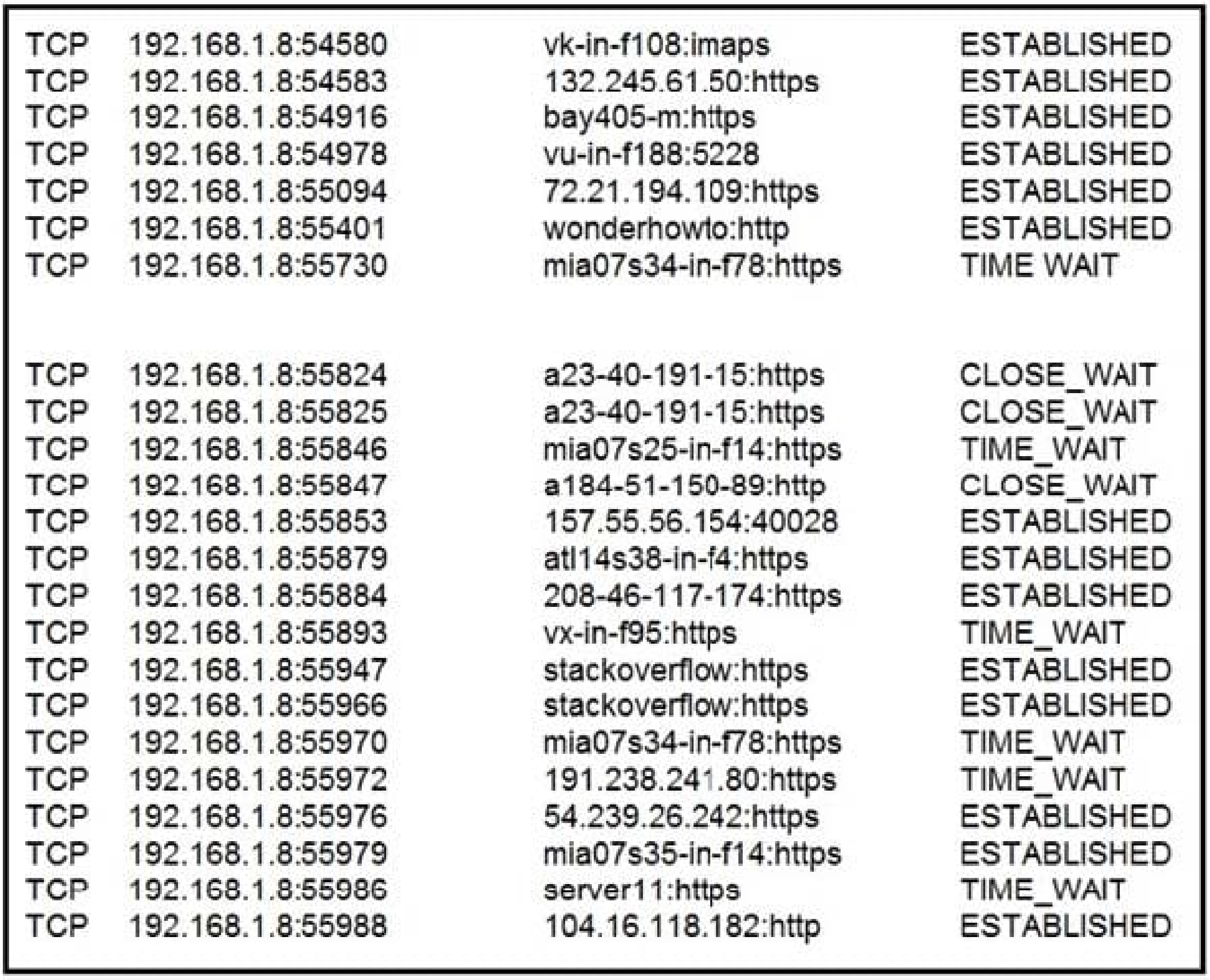
D. Automate server-side error reporting for customers.

E. Decrease simultaneous API responses.

Correct Answer: BD

QUESTION 2

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

QUESTION 3

A SOC analyst is notified by the network monitoring tool that there are unusual types of internal traffic on IP subnet 103.861.2117.0/24. The analyst discovers unexplained encrypted data files on a computer system that belongs on that specific subnet.

What is the cause of the issue?

A. DDoS attack

B. phishing attack

C. virus outbreak

D. malware outbreak

Correct Answer: D

QUESTION 4

A security architect is working in a processing center and must implement a DLP solution to detect and prevent any type of copy and paste attempts of sensitive data within unapproved applications and removable devices. Which technical architecture must be used?

A. DLP for data in motion

B. DLP for removable data

C. DLP for data in use

D. DLP for data at rest

Correct Answer: C

Reference: https://www.endpointprotector.com/blog/what-is-data-loss-prevention-dlp/

QUESTION 5

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