# Cisco

## 350-201 Exam

**Performing CyberOps Using Core Security Technologies**

**Thank you for Downloading 350-201 exam PDF Demo**

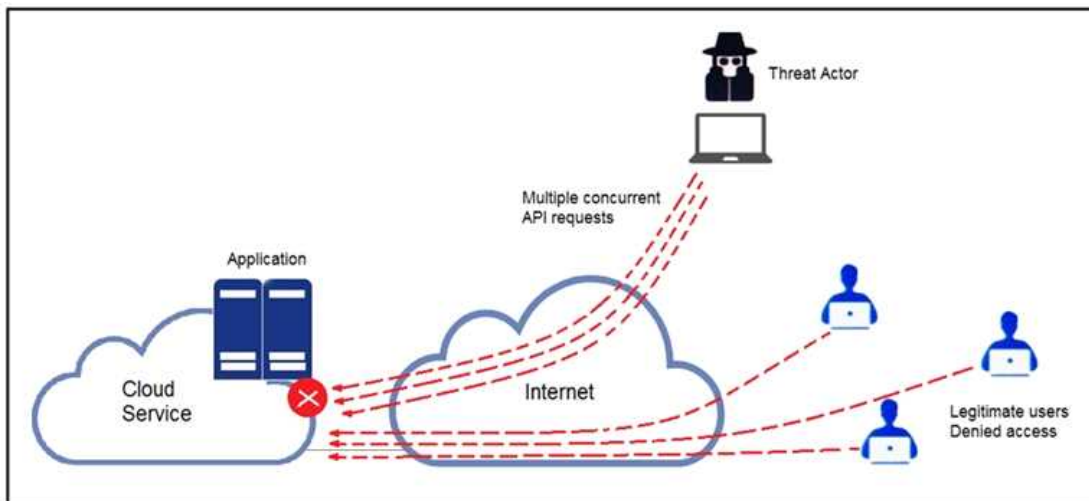You can also try our 350-201 practice exam software

**Download Free Demo**

https://prepbolt.com/350-201.html

# Version: 5.0

## 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

**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.

**Answer Area**

| | |
|---|---|
| run show access-list | Step 1 |
| run show config | Step 2 |
| validate the file MD5 | Step 3 |
| generate the core file | Step 4 |
| verify the image file hash | |
| check the memory logs | |
| verify the memory state | |

**Answer:**

Explanation:

**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

**Answer: C**

## Question: 4

Refer to the exhibit.

```
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 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?

A. packet sniffer
B. malware analysis
C. SIEM
D. firewall manager

**Answer: A**

## Question: 5

Refer to the exhibit.

**Analysis Report**

| | | | |
|---|---|---|---|
| ID | 12cbeee21b1ea4 | Filename | fpzryrf.exe |
| OS | 7601.1898.amd64fre.win7sp1_gdr.150316-1654 | Magic Type Analyzed As | PE32 executable (GUI) Intel 80386, for MS Windows exe |
| Started | 7/29/16 18:44:43 | SHA256 | e9ca08a3cc2f8c9748a9e9b304c9f5a16d830066e5467d3dd5927be36fec47da |
| Ended | 7/29/16 18:50:39 | | |
| Duration | 0:05:56 | SHA1 | a2de85810fd5ebcf29c5da5dd29ce03470772ad |
| Sandbox | phl-work-02 (pilot-d) | MD5 | dd07d778edf8d581ffaadb1610aaa008 |

**Warnings**

⊕ Executable Failed Integrity Check

**Behavioral Indicators**

| | | |
|---|---|---|
| ⊕ CTB Locker Detected | Severity: 100 | Confidence: 100 |
| ⊕ Generic Ransomware Detected | Severity: 100 | Confidence: 95 |
| ⊕ Excessive Suspicious Activity Detected | Severity: 90 | Confidence: 100 |
| ⊕ Process Modified a File in a System Directory | Severity: 90 | Confidence: 100 |
| ⊕ Large Amount of High Entropy Artifacts Written | Severity: 100 | Confidence: 80 |
| ⊕ Process Modified a File in the Program Files Directory | Severity: 80 | Confidence: 90 |
| ⊕ Decoy Document Detected | Severity: 70 | Confidence: 100 |
| ⊕ Process Modified an Executable File | Severity: 60 | Confidence: 100 |
| ⊕ Process Modified File in a User Directory | Severity: 70 | Confidence: 80 |
| ⊕ Windows Crash Tool Execution Detected | Severity: 20 | Confidence: 80 |
| ⊕ Hook Procedure Detected in Executable | Severity: 35 | Confidence: 40 |
| ⊕ Ransomware Queried Domain | Severity: 25 | Confidence: 25 |
| ⊕ Executable Imported the IsDebuggerPresent Symbol | Severity: 20 | Confidence: 20 |

Cisco Advanced Malware Protection installed on an end-user desktop has automatically submitted a low prevalence file to the Threat Grid analysis engine for further analysis. What should be concluded from this report?

A. The prioritized behavioral indicators of compromise do not justify the execution of the "ransomware" because the scores do not indicate the likelihood of malicious ransomware.
B. The prioritized behavioral indicators of compromise do not justify the execution of the

"ransomware" because the scores are high and do not indicate the likelihood of malicious ransomware.

C. The prioritized behavioral indicators of compromise justify the execution of the "ransomware" because the

scores are high and indicate the likelihood that malicious ransomware has been detected.

D. The prioritized behavioral indicators of compromise justify the execution of the "ransomware" because the scores are low and indicate the likelihood that malicious ransomware has been detected.

---

**Answer: C**

# Thank You for trying 350-201 PDF Demo

To try our 350-201 practice exam software visit link below

https://prepbolt.com/350-201.html

# Start Your 350-201 Preparation

Use Coupon "SAVE50" for extra 50% discount on the purchase of Practice Test Software. Test your 350-201 preparation with actual exam questions.