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:

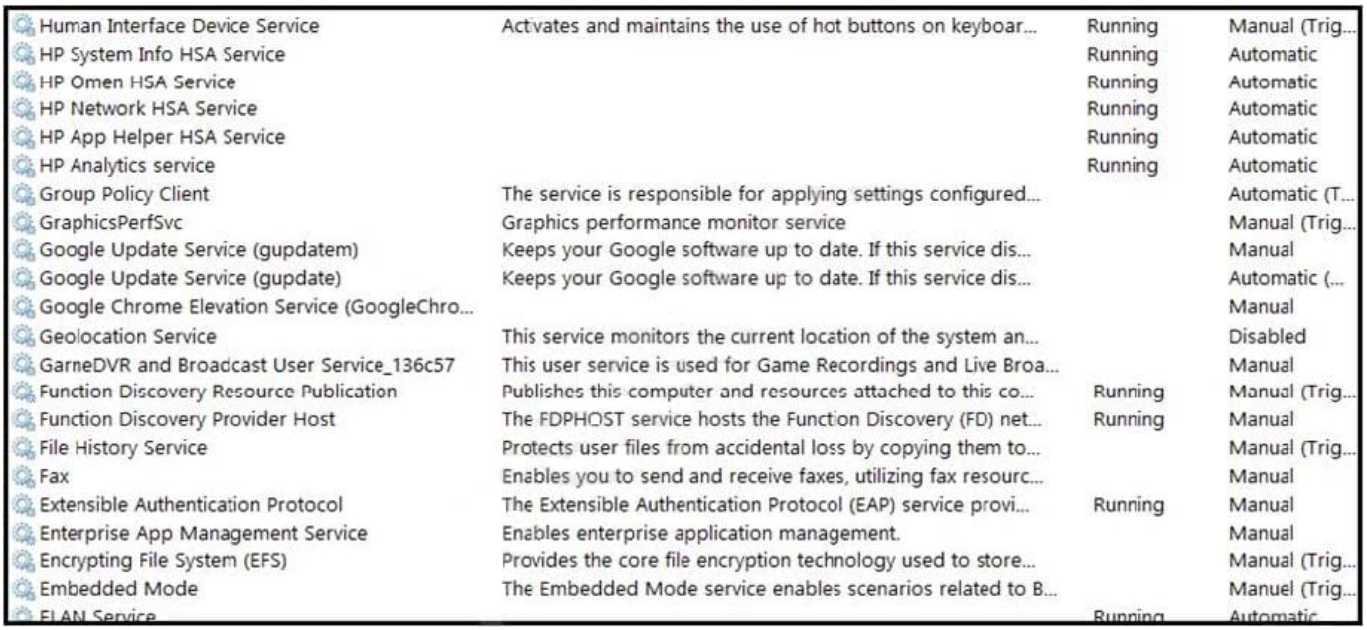
https://www.leads4pass.com/350-201.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Refer to the exhibit. An engineer received multiple reports from employees unable to log into systems with the error: The Group Policy Client service failed to logon – Access is denied. Through further analysis, the engineer discovered several unexpected modifications to system settings. Which type of breach is occurring?



Human Interface Device Service	Activates and maintains the use of hot buttons on keyboar...	Running	Manual (Trig...
HP System Info HSA Service		Running	Automatic
HP Omen HSA Service		Running	Automatic
HP Network HSA Service		Running	Automatic
HP App Helper HSA Service		Running	Automatic
HP Analytics service		Running	Automatic
Group Policy Client	The service is responsible for applying settings configured...		Automatic (T...
GraphicsPerfSvc	Graphics performance monitor service		Manual (Trig...
Google Update Service (gupdatem)	Keeps your Google software up to date. If this service dis...		Manual
Google Update Service (gupdate)	Keeps your Google software up to date. If this service dis...		Automatic (...
Google Chrome Elevation Service (GoogleChro...			Manual
Geolocation Service	This service monitors the current location of the system an...		Disabled
GarneDVR and Broadcast User Service_136c57	This user service is used for Game Recordings and Live Broa...		Manual
Function Discovery Resource Publication	Publishes this computer and resources attached to this co...	Running	Manual (Trig...
Function Discovery Provider Host	The FDPHOST service hosts the Function Discovery (FD) net...	Running	Manual
File History Service	Protects user files from accidental loss by copying them to...		Manual (Trig...
Fax	Enables you to send and receive faxes, utilizing fax resourc...		Manual
Extensible Authentication Protocol	The Extensible Authentication Protocol (EAP) service provi...	Running	Manual
Enterprise App Management Service	Enables enterprise application management.		Manual
Encrypting File System (EFS)	Provides the core file encryption technology used to store...		Manual (Trig...
Embedded Mode	The Embedded Mode service enables scenarios related to B...		Manual (Trig...
ELAN Service		Running	Automatic

A. malware break

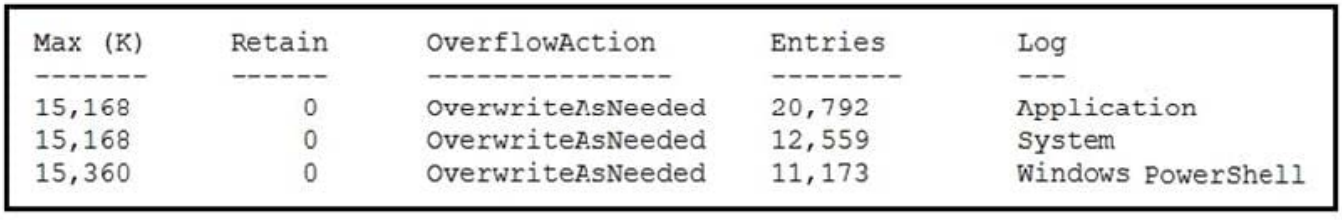
B. data theft

C. elevation of privileges

D. denial-of-service

Correct Answer: C

QUESTION 2



Max (K)	Retain	OverflowAction	Entries	Log
15,168	0	OverwriteAsNeeded	20,792	Application
15,168	0	OverwriteAsNeeded	12,559	System
15,360	0	OverwriteAsNeeded	11,173	Windows PowerShell

Refer to the exhibit. An employee is a victim of a social engineering phone call and installs remote access software to allow an "MS Support" technician to check his machine for malware. The employee becomes suspicious after the remote technician requests payment in the form of gift cards. The employee has copies of multiple, unencrypted database files, over 400 MB each, on his system and is worried that the scammer copied the files off but has no proof of

it. The remote technician was connected sometime between 2:00 pm and 3:00 pm over https.

What should be determined regarding data loss between the employee\\'s laptop and the remote technician\\'s system?

A. No database files were disclosed

B. The database files were disclosed

C. The database files integrity was violated

D. The database files were intentionally corrupted, and encryption is possible

Correct Answer: C

QUESTION 3

A SOC team is informed that a UK-based user will be traveling between three countries over the next 60 days. Having the names of the 3 destination countries and the user\\'s working hours, what must the analyst do next to detect an abnormal behavior?

A. Create a rule triggered by 3 failed VPN connection attempts in an 8-hour period

B. Create a rule triggered by 1 successful VPN connection from any nondestination country

C. Create a rule triggered by multiple successful VPN connections from the destination countries

D. Analyze the logs from all countries related to this user during the traveling period

Correct Answer: D

QUESTION 4

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

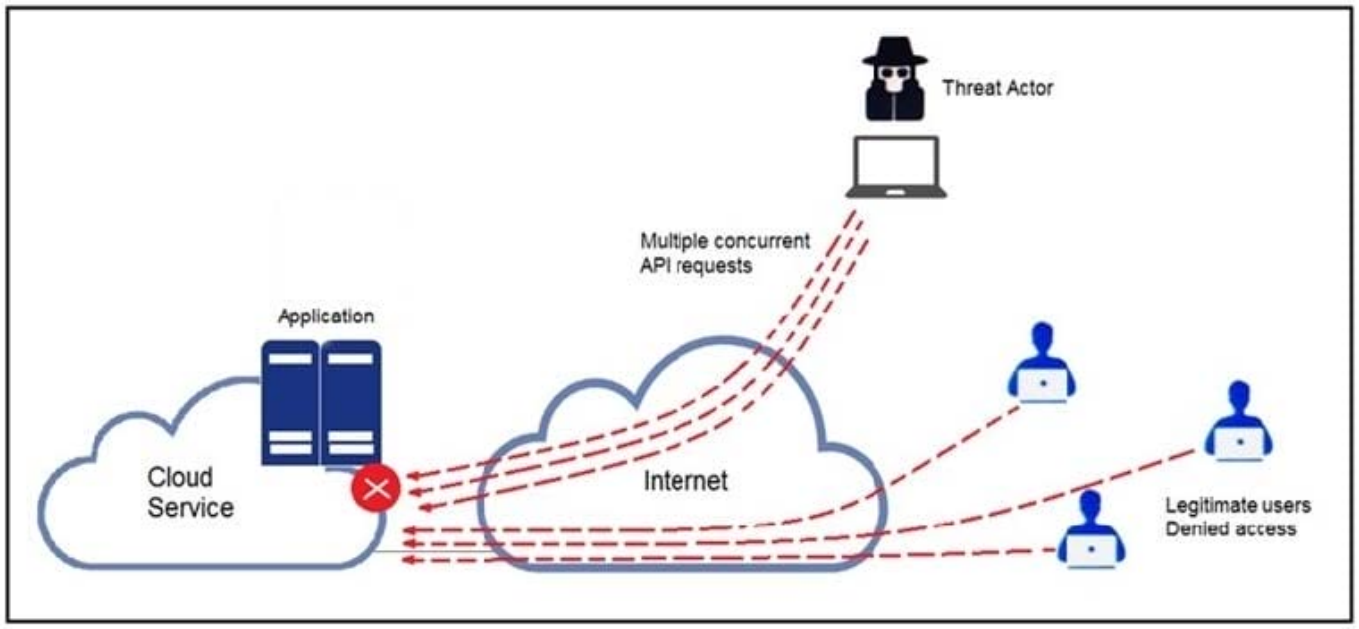
Correct Answer: A

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

QUESTION 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