350-201 Q&As

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Pass Cisco 350-201 Exam with 100% Guarantee

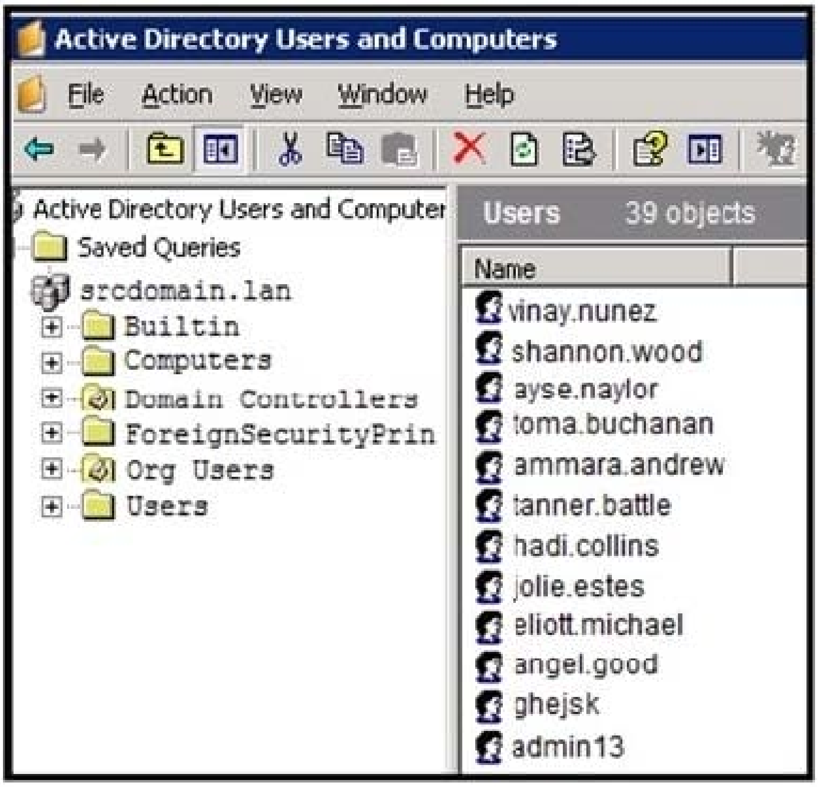
Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.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



Active Directory Users and Computer
Saved Queries
srcdomain.lan
Builtin
Computers
Domain Controllers
ForeignSecurityPrin
Org Users
Users

Users 39 objects

Name
vinay.nunez
shannon.wood
ayse.naylor
toma.buchanan
ammara.andrew
tanner.battle
hadi.collins
jolie.estes
eliott.michael
angel.good
ghejsk
admin13

Refer to the exhibit. An engineer is investigating a case with suspicious usernames within the active directory. After the engineer investigates and cross-correlates events from other sources, it appears that the 2 users are privileged, and their creation date matches suspicious network traffic that was initiated from the internal network 2 days prior.

Which type of compromise is occurring?

A. compromised insider

B. compromised root access

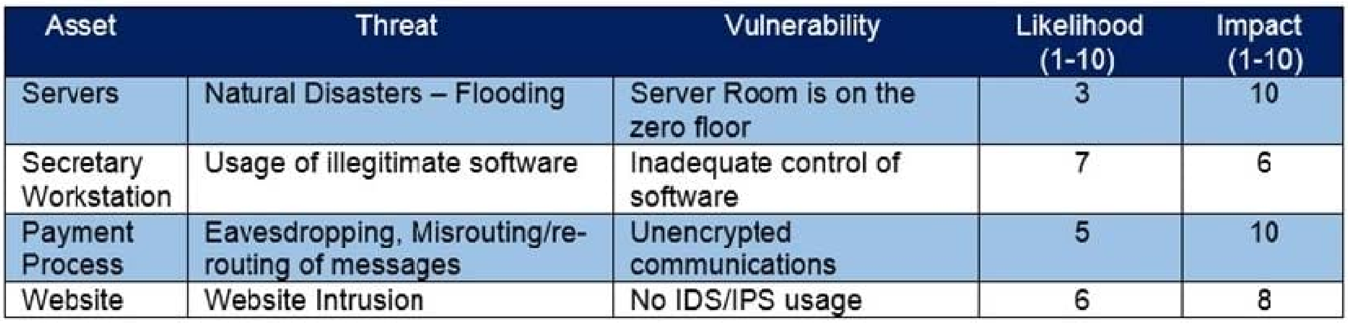
C. compromised database tables

D. compromised network

Correct Answer: D

QUESTION 2

Refer to the exhibit. Which asset has the highest risk value?



Asset	Threat	Vulnerability	Likelihood (1-10)	Impact (1-10)
Servers	Natural Disasters – Flooding	Server Room is on the zero floor	3	10
Secretary Workstation	Usage of illegitimate software	Inadequate control of software	7	6
Payment Process	Eavesdropping, Misrouting/re-routing of messages	Unencrypted communications	5	10
Website	Website Intrusion	No IDS/IPS usage	6	8

A. servers

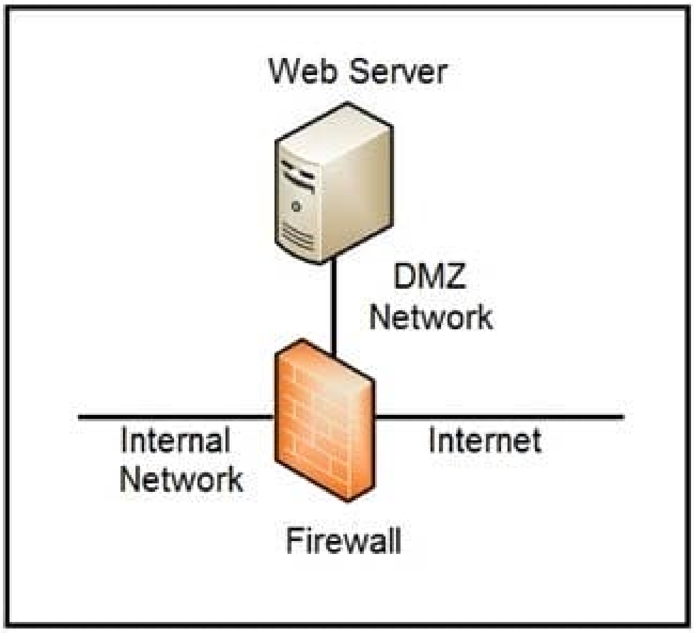
B. website

C. payment process

D. secretary workstation

Correct Answer: C

QUESTION 3



Refer to the exhibit. Which two steps mitigate attacks on the webserver from the Internet? (Choose two.)

A. Create an ACL on the firewall to allow only TLS 1.3

B. Implement a proxy server in the DMZ network

C. Create an ACL on the firewall to allow only external connections

D. Move the webserver to the internal network

Correct Answer: BD

QUESTION 4

An API developer is improving an application code to prevent DDoS attacks. The solution needs to accommodate instances of a large number of API requests coming for legitimate purposes from trustworthy services. Which solution should be implemented?

A. Restrict the number of requests based on a calculation of daily averages. If the limit is exceeded, temporarily block access from the IP address and return a 402 HTTP error code.

B. Implement REST API Security Essentials solution to automatically mitigate limit exhaustion. If the limit is exceeded, temporarily block access from the service and return a 409 HTTP error code.

C. Increase a limit of replies in a given interval for each API. If the limit is exceeded, block access from the API key permanently and return a 450 HTTP error code.

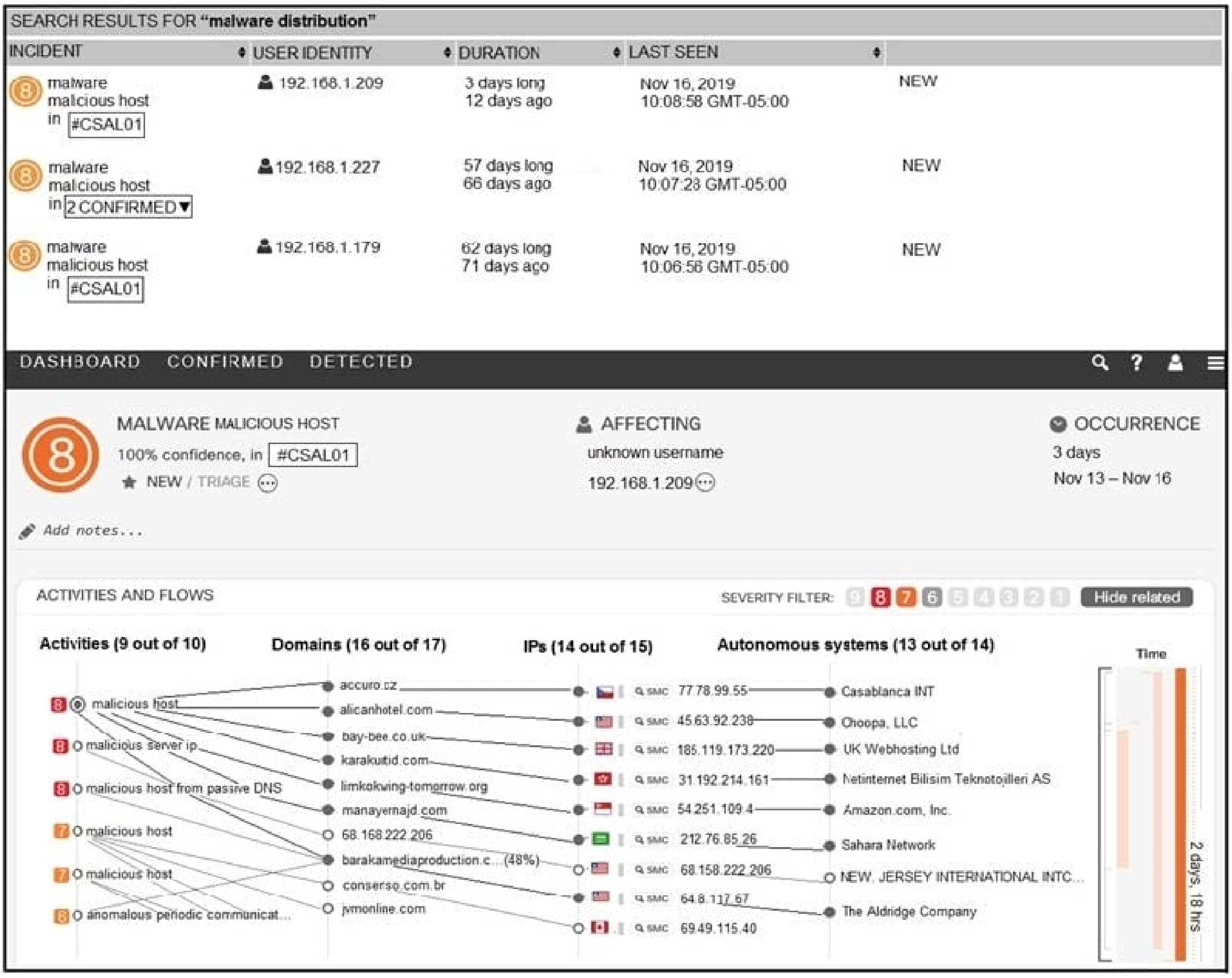
D. Apply a limit to the number of requests in a given time interval for each API. If the rate is exceeded, block access from the API key temporarily and return a 429 HTTP error code.

Correct Answer: D

Reference: https://www.whoishostingthis.com/resources/http-status-codes/

QUESTION 5

Refer to the exhibit. For IP 192.168.1.209, what are the risk level, activity, and next step?



SEARCH RESULTS FOR **"malware distribution"**

INCIDENT	USER IDENTITY	DURATION	LAST SEEN	
8 malware malcious host in #CSAL01	192.168.1.209	3 days long 12 days ago	Nov 16, 2019 10:08:58 GMT-05:00	NEW
8 malware malcious host in 2 CONFIRMED ▾	192.168.1.227	57 days long 66 days ago	Nov 16, 2019 10:07:28 GMT-05:00	NEW
8 malware malicious host in #CSAL01	192.168.1.179	62 days long 71 days ago	Nov 16, 2019 10:06:58 GMT-05:00	NEW

8 MALWARE MALICIOUS HOST
100% confidence, in #CSAL01
★ NEW / TRIAGE

AFFECTING
unknown username
192.168.1.209

OCCURRENCE
3 days
Nov 13 – Nov 16

Add notes...

ACTIVITIES AND FLOWS

SEVERITY FILTER: 9 8 7 6 5 4 3 2 1 Hide related

Activities (9 out of 10)
8 ◉ malicious host
8 ○ malicious server ip
8 ○ malicious host from passive DNS
7 ○ malicious host
7 ○ malicious host
6 ○ anomalous periodic communicat...

Domains (16 out of 17)
● accuro.cz
● alicanhotel.com
● bay-bee.co.uk
● karakutid.com
● limkokwing-tomorrow.org
● manayemajd.com
○ 68.168.222.206
● barakamediaproduction.c...(48%)
○ conserso.com.br
○ jvmonline.com

IPs (14 out of 15)
● SMC 77.78.99.55
● SMC 45.63.92.238
● SMC 185.119.173.220
● SMC 31.192.214.161
● SMC 54.251.109.4
● SMC 212.76.85.26
○ SMC 68.158.222.206
● SMC 64.8.117.67
○ SMC 69.49.115.40

Autonomous systems (13 out of 14)
● Casablanca INT
● Choopa, LLC
● UK Webhosting Ltd
● Netinternet Bilisim Teknotojileri AS
● Amazon.com, Inc.
● Sahara Network
○ NEW. JERSEY INTERNATIONAL INTC...
● The Aldridge Company

A. high risk level, anomalous periodic communication, quarantine with antivirus

B. critical risk level, malicious server IP, run in a sandboxed environment

C. critical risk level, data exfiltration, isolate the device

D. high risk level, malicious host, investigate further

Correct Answer: A

[350-201 VCE Dumps](https://www.geekcert.com/350-201.html) [350-201 Study Guide](https://www.geekcert.com/350-201.html) [350-201 Exam Questions](https://www.geekcert.com/350-201.html)