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.pass2lead.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

A company recently completed an internal audit and discovered that there is CSRF vulnerability in 20 of its hosted applications. Based on the audit, which recommendation should an engineer make for patching?

A. Identify the business applications running on the assets

B. Update software to patch third-party software

C. Validate CSRF by executing exploits within Metasploit

D. Fix applications according to the risk scores

Correct Answer: D

QUESTION 2

An engineer is moving data from NAS servers in different departments to a combined storage database so that the data can be accessed and analyzed by the organization on-demand. Which data management process is being used?

A. data clustering

B. data regression

C. data ingestion

D. data obfuscation

Correct Answer: A

QUESTION 3

An engineer wants to review the packet overviews of SNORT alerts. When printing the SNORT alerts, all the packet headers are included, and the file is too large to utilize. Which action is needed to correct this problem?

A. Modify the alert rule to "output alert_syslog: output log"

B. Modify the output module rule to "output alert_quick: output filename"

C. Modify the alert rule to "output alert_syslog: output header"

D. Modify the output module rule to "output alert_fast: output filename"

Correct Answer: A

Reference: https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256andX-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20201231%2Fuse

ast-1%2Fs3%2Faws4_requestandX-Amz-Date=20201231T141156ZandX-Amz-Expires=172800andX-Amz-SignedHeaders=hostandX-Amz-Signature=e122ab6eb1659e13b3bc6bb2451ce693c0298b76c1962c3743924bc5fd83d382

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

```
def get_umbrella_dispos(domains):
    # put in right format to pass as argument in POST request
    values = str(json.dumps(domains))
    req = requests.post(investigate_url, data=values, headers=headers)
    # time for timestamp of verdict domain
    time = datetime.now().isoformat()
    # error handling if true then the request was HTTP 200, so successful
    if(req.status_code == 200):
      print("SUCCESS: request has the following code: 200\n")
      output = req.json()

      [                                                              ]

      if(domain_status == -1):
        print("The domain %(domain)s is found MALICIOUS at %(time)s\n" % {'domain': domain, 'time': time})
      elif(domain_status == 1):
        print("The domain %(domain)s is found CLEAN at %(time)s\n" %
          {'domain': domain, 'time': time})
      else:
        print("The domain %(domain)s is found UNDEFINED / RISKY at %(time)s\n" %
          {'domain': domain, 'time': time})
  else:
    print("An error has occurred with the following code %(error)s, please consult the following link:
    https://docs.umbrella.com/investigate-api/"%
          {'error': req.status_code})
```

Refer to the exhibit. Which code snippet will parse the response to identify the status of the domain as malicious, clean or undefined?

A.
```
for domain in domains[]:
        domain_status = domain_output["status"]
```

B.
```
while domain in domains:
    domain_status = domain_output["status"]
```

C.
```
for domain in domains:
    domain_output = output[domain]
    domain_status = domain_output["status"]
```

D.
```
while domains in domains:
    domain_output = output[domain]
    domain_status = domain_output["status"]
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: C

350-201 VCE Dumps 350-201 Study Guide 350-201 Braindumps