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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A Mac laptop user notices that several files have disappeared from their laptop documents folder. While looking for the files, the user notices that the browser history was recently cleared. The user raises a case, and an analyst reviews the network usage and discovers that it is abnormally high.

Which step should be taken to continue the investigation?

A. Run the sudo sysdiagnose command

B. Run the sh command

C. Run the w command

D. Run the who command

Correct Answer: A

Reference: https://eclecticlight.co/2016/02/06/the-ultimate-diagnostic-tool-sysdiagnose/

QUESTION 2

```
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

QUESTION 3

What is the difference between process orchestration and automation?

A. Orchestration combines a set of automated tools, while automation is focused on the tools to automate process flows.

B. Orchestration arranges the tasks, while automation arranges processes.

C. Orchestration minimizes redundancies, while automation decreases the time to recover from redundancies.

D. Automation optimizes the individual tasks to execute the process, while orchestration optimizes frequent and repeatable processes.

Correct Answer: A

QUESTION 4

An analyst is alerted for a malicious file hash. After analysis, the analyst determined that an internal workstation is communicating over port 80 with an external server and that the file hash is associated with Duqu malware. Which

tactics, techniques, and procedures align with this analysis?

A. Command and Control, Application Layer Protocol, Duqu

B. Discovery, Remote Services: SMB/Windows Admin Shares, Duqu

C. Lateral Movement, Remote Services: SMB/Windows Admin Shares, Duqu

D. Discovery, System Network Configuration Discovery, Duqu

Correct Answer: A

QUESTION 5

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/