

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



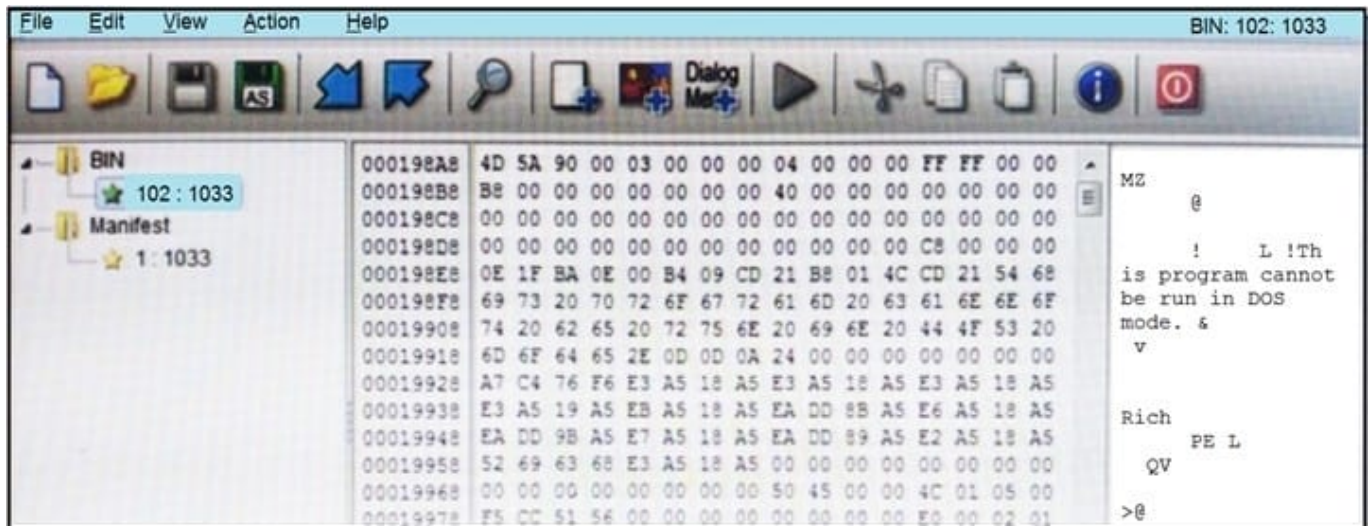
QUESTION 1

A malware outbreak is detected by the SIEM and is confirmed as a true positive. The incident response team follows the playbook to mitigate the threat. What is the first action for the incident response team?

- A. Assess the network for unexpected behavior
- B. Isolate critical hosts from the network
- C. Patch detected vulnerabilities from critical hosts
- D. Perform analysis based on the established risk factors

Correct Answer: B

QUESTION 2



Refer to the exhibit. An engineer is reverse engineering a suspicious file by examining its resources. What does this file indicate?

- A. a DOS MZ executable format
- B. a MS-DOS executable archive
- C. an archived malware
- D. a Windows executable file

Correct Answer: D

Reference: <https://stackoverflow.com/questions/2577545/why-is-this-program-cannot-be-run-in-dos-mode-text-present-in-dll-files#:~:text=The%20linker%20places%20a%20default,using%20the%20%2FSTUB%20linker%20option.andtext=This>

%20information%20enables%20Windows%20to,has%20an%20MS-DOS%20stub.

QUESTION 3

A customer is using a central device to manage network devices over SNMPv2. A remote attacker caused a denial of service condition and can trigger this vulnerability by issuing a GET request for the ciscoFlashMIB OID on an affected device.

Which should be disabled to resolve the issue?

- A. SNMPv2
- B. TCP small services
- C. port UDP 161 and 162
- D. UDP small services

Correct Answer: A

Reference: <https://nvd.nist.gov/vuln/detail/CVE-2018-0161>

QUESTION 4

What is the HTTP response code when the REST API information requested by the authenticated user cannot be found?

- A. 401
- B. 402
- C. 403
- D. 404
- E. 405

Correct Answer: A

Reference: <https://airbrake.io/blog/http-errors/401-unauthorized-error#:~:text=The%20401%20Unauthorized%20Error%20is,client%20could%20not%20be%20authenticated.>

QUESTION 5

```
pragma: no-cache
server: Apache
status: 200
strict-transport-security: max-age=31536000
vary: Accept-Encoding
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
x-test-debug: nURL=www.cisco.com, realm=0, isRealm=0, realmDomain=0, shortrealm=0
x-xss-protection: 1; mode=block
```

Refer to the exhibit. Where does it signify that a page will be stopped from loading when a scripting attack is detected?

- A. x-frame-options
- B. x-content-type-options
- C. x-xss-protection
- D. x-test-debug

Correct Answer: C

Reference: <https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/customize-http-security-headers-ad-fs>

[Latest 350-201 Dumps](#)

[350-201 Study Guide](#)

[350-201 Exam Questions](#)