



# 350-201<sup>Q&As</sup>

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

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





## QUESTION 1

<p><b><u>Vulnerability #1</u></b></p> <p>A vulnerability in the Command Line Interpreter (CLI) of ACME Super Firewall (all models) could allow an attacker to execute a command which would overflow a buffer in memory. In order to carry out this attack, the attacker needs to fulfill all of the following conditions:</p> <ul style="list-style-type: none"><li>a) Be logged in to the device over telnet or SSH, or through the local console</li><li>b) Be logged in as a high-privileges administrative user</li></ul> <p>In order to trigger the vulnerability, the attacker has to execute a command on the device and supply a specially crafted argument to such command. Once the command is executed, an internal stack-based buffer overflow will be triggered. This buffer overflow may lead to code execution within the process space of the CLI parser, or may crash the device.</p> <p>All software versions are affected Fixes are available now There are no workarounds or mitigations</p>	<p><b><u>Vulnerability #2</u></b></p> <p>A vulnerability in the web-based management interface of the ACME Big Router models 1010 and 1020 could allow an attacker to bypass authorization checks and then access sensitive information on the device, modify the device's configuration, impact the availability of the system, create administrative level and regular level users on the device. In order to exploit this vulnerability, the attacker needs to:</p> <ul style="list-style-type: none"><li>a) Be able to reach port 80/tcp on an affected device</li><li>b) The web-based management interface needs to be enabled on the device</li></ul> <p>The attacker would then need to send a specially formed HTTP request to the web-based management interface of an affected system. The attacker does not need to log-in to the device before launching the attack.</p> <p>All software versions are affected There are no fixes available now Customers can disable the web-based management interface to prevent exploitation. Customers will still be able to manage, configure and monitor the device by using the Command Line Interface (CLI), but with reduced capabilities for monitoring.</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Refer to the exhibit. How must these advisories be prioritized for handling?

- A. The highest priority for handling depends on the type of institution deploying the devices
- B. Vulnerability #2 is the highest priority for every type of institution
- C. Vulnerability #1 and vulnerability #2 have the same priority
- D. Vulnerability #1 is the highest priority for every type of institution

Correct Answer: D

## QUESTION 2

The incident response team was notified of detected malware. The team identified the infected hosts, removed the malware, restored the functionality and data of infected systems, and planned a company meeting to improve the incident handling capability.

Which step was missed according to the NIST incident handling guide?

- A. Contain the malware
- B. Install IPS software
- C. Determine the escalation path



D. Perform vulnerability assessment

Correct Answer: D

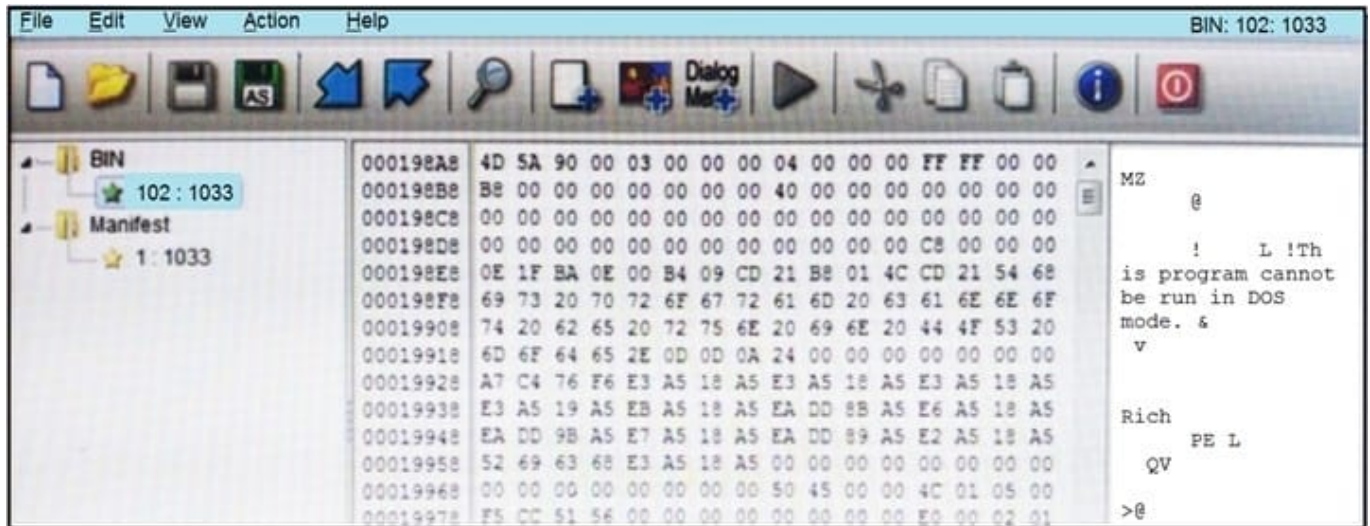
### QUESTION 3

An organization had a breach due to a phishing attack. An engineer leads a team through the recovery phase of the incident response process. Which action should be taken during this phase?

- A. Host a discovery meeting and define configuration and policy updates
- B. Update the IDS/IPS signatures and reimage the affected hosts
- C. Identify the systems that have been affected and tools used to detect the attack
- D. Identify the traffic with data capture using Wireshark and review email filters

Correct Answer: C

### QUESTION 4



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-](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.)

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 5

A SOC team receives multiple alerts by a rule that detects requests to malicious URLs and informs the incident response team to block the malicious URLs requested on the firewall. Which action will improve the effectiveness of the process?

- A. Block local to remote HTTP/HTTPS requests on the firewall for users who triggered the rule.
- B. Inform the user by enabling an automated email response when the rule is triggered.
- C. Inform the incident response team by enabling an automated email response when the rule is triggered.
- D. Create an automation script for blocking URLs on the firewall when the rule is triggered.

Correct Answer: A

[Latest 350-201 Dumps](#)

[350-201 VCE Dumps](#)

[350-201 Exam Questions](#)