



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

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





QUESTION 1

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 2

Vulnerability #1

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:

- a) Be logged in to the device over telnet or SSH, or through the local console
- b) Be logged in as a high-privileges administrative user

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.

All software versions are affected

Fixes are available now

There are no workarounds or mitigations

Vulnerability #2

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:

- a) Be able to reach port 80/tcp on an affected device
- b) The web-based management interface needs to be enabled on the device

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.

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.

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 3

An organization installed a new application server for IP phones. An automated process fetched user credentials from the Active Directory server, and the application will have access to on-premises and cloud services. Which security threat should be mitigated first?

- A. aligning access control policies
- B. exfiltration during data transfer
- C. attack using default accounts
- D. data exposure from backups

Correct Answer: B

QUESTION 4

A security analyst receives an escalation regarding an unidentified connection on the Accounting A1 server within a monitored zone. The analyst pulls the logs and discovers that a Powershell process and a WMI tool process were started on the server after the connection was established and that a PE format file was created in the system directory.

What is the next step the analyst should take?

- A. Isolate the server and perform forensic analysis of the file to determine the type and vector of a possible attack
- B. Identify the server owner through the CMDB and contact the owner to determine if these were planned and identifiable activities
- C. Review the server backup and identify server content and data criticality to assess the intrusion risk
- D. Perform behavioral analysis of the processes on an isolated workstation and perform cleaning procedures if the file is malicious

Correct Answer: C

QUESTION 5

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

[Latest 350-201 Dumps](#)

[350-201 VCE Dumps](#)

[350-201 Study Guide](#)