

# 100-160 Latest Test Practice | 100-160 Best Practice



P.S. Free 2026 Cisco 100-160 dumps are available on Google Drive shared by DumpsQuestion: [https://drive.google.com/open?id=1vqBCiF5dyCJ6mYvDsxsPU\\_zJod0mXbB](https://drive.google.com/open?id=1vqBCiF5dyCJ6mYvDsxsPU_zJod0mXbB)

If you are looking to advance in the fast-paced and technological world, DumpsQuestion is here to help you achieve this aim. DumpsQuestion provides you with the excellent Cisco 100-160 practice exam, which will make your dream come true of passing the Cisco Certified Support Technician (CCST) Cybersecurity certification exam on the first attempt.

If you don't professional fundamentals, you should choose our Cisco 100-160 new exam simulator online rather than study difficultly and inefficiently. Learning method is more important than learning progress when your goal is obtaining certification. For IT busy workers, to buy 100-160 new exam simulator online not only will be a high efficient and time-saving method for most candidates but also the highest passing-rate method.

>> 100-160 Latest Test Practice <<

## 100-160 Best Practice, 100-160 Latest Test Report

The services provided by our 100-160 test questions are quite specific and comprehensive. First of all, our test material comes from many experts. The gold content of the materials is very high, and the updating speed is fast. By our 100-160 exam prep, you can find the most suitable information according to your own learning needs at any time, and make adjustments and perfect them at any time. Our 100-160 Learning Materials not only provide you with information, but also for you to develop the most suitable for your learning schedule, this is tailor-made for you, according to the timetable to study and review. I believe you can improve efficiency.

## Cisco 100-160 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"><li>Endpoint Security Concepts: This section of the exam measures the skills of an Endpoint Security Specialist and includes securing individual devices, understanding protections such as antivirus, patching, and access control at the endpoint level, essential for maintaining device integrity.</li></ul>
Topic 2	<ul style="list-style-type: none"><li>Vulnerability Assessment and Risk Management: This section of the exam measures the skills of a Risk Management Analyst and entails identifying and assessing vulnerabilities, understanding risk priorities, and applying mitigation strategies that help manage threats proactively within an organization's systems</li></ul>
Topic 3	<ul style="list-style-type: none"><li>Incident Handling: This section of the exam measures the skills of an Incident Responder and centers on recognizing security incidents, responding appropriately, and containing threats—forming the essential foundation of incident response procedures.</li></ul>

Topic 4	<ul style="list-style-type: none"> <li>• <b>Essential Security Principles:</b> This section of the exam measures the skills of a Cybersecurity Technician and covers foundational cybersecurity concepts such as the CIA triad (confidentiality, integrity, availability), along with basic threat types and vulnerabilities, laying the conceptual groundwork for understanding how to protect information systems.</li> </ul>
Topic 5	<ul style="list-style-type: none"> <li>• <b>Basic Network Security Concepts:</b> This section of the exam measures the skills of a Network Defender and focuses on understanding network-level protections, including firewalls, VPNs, and intrusion detection and prevention systems, providing insight into how threats are mitigated within network environments.</li> </ul>

## Cisco Certified Support Technician (CCST) Cybersecurity Sample Questions (Q50-Q55):

### NEW QUESTION # 50

Which of the following logging mechanisms is commonly used in Windows environments to monitor system and application events?

- A. Syslog
- **B. Event Viewer**
- C. System and application logs
- D. Audit logs

**Answer: B**

Explanation:

The Event Viewer is a built-in tool in Windows operating systems that allows administrators to view and analyze logs of system and application events. It provides a central location for managing and reviewing various types of logs, including security, application, and system logs.

### NEW QUESTION # 51

The company web server collects information through a form. The form is accessed by using port 80. The form content is transferred to an encrypted database for storage. You are investigating a complaint that the form content has been compromised. What is the cause of the security breach?

- A. The web browser used to access the site was not updated to the latest version.
- **B. The website was accessed using HTTP, which is an unencrypted protocol.**
- C. The database was compromised.
- D. The data was transferred to the database using a nonsecure protocol.

**Answer: B**

Explanation:

The CCST Cybersecurity Study Guide explains that HTTP (port 80) transmits data in cleartext, making it susceptible to interception. Even if data is stored securely in an encrypted database, sensitive information can be compromised during transmission if HTTPS (port 443) is not used.

"When HTTP is used instead of HTTPS, all form inputs and transmitted data are sent in plaintext over the network, where they can be intercepted by attackers." (CCST Cybersecurity, Basic Network Security Concepts, Secure Protocols section, Cisco Networking Academy)

### NEW QUESTION # 52

Which of the following best describes the role of automated threat intelligence in a cybersecurity system?

- A. It provides advanced analytics for proactive threat mitigation
- B. It automates the detection and response to security incidents
- C. It enables real-time monitoring of threat landscapes
- **D. All of the above**

**Answer: D**

Explanation:

Automated threat intelligence plays a multifaceted role in a cybersecurity system. Firstly, it enables real-time monitoring of threat landscapes by continuously collecting and analyzing data from various sources. This allows organizations to stay updated on emerging threats and trends. Secondly, it automates the detection and response to security incidents by leveraging machine learning algorithms and predefined rules. Finally, automated threat intelligence provides advanced analytics for proactive threat mitigation, helping organizations anticipate and prevent potential security breaches.

#### NEW QUESTION # 53

What is the purpose of multi-factor authentication?

- A. To provide multiple layers of security by requiring users to provide more than one form of identification
- B. To prevent unauthorized access by encrypting user credentials
- C. To restrict access to certain users by requiring additional authorization
- D. To simplify the login process by only requiring one form of identification

Answer: A

Explanation:

Option 1: Correct. Multi-factor authentication adds an extra layer of security by requiring users to provide more than one form of identification, such as a password and a fingerprint or a security token.

Option 2: Incorrect. Multi-factor authentication does not simplify the login process, but rather adds an additional step to verify the user's identity.

Option 3: Incorrect. While multi-factor authentication can help restrict access to certain users, its main purpose is to provide an extra layer of security rather than additional authorization.

Option 4: Incorrect. While encryption is an important security measure, multi-factor authentication is specifically designed to provide multiple layers of security by requiring multiple forms of identification.

#### NEW QUESTION # 54

Which of the following elements are part of cybersecurity incident response?

- A. Detection, Analysis, Containment, Eradication
- B. Assessment, Authorization, Authentication, Accounting
- C. Prevention, Monitoring, Compliance, Remediation
- D. Identification, Recovery, Mitigation, Restoration

Answer: A

Explanation:

Cybersecurity incident response involves several key elements, including detection, analysis, containment, and eradication. Detection refers to the identification and recognition of a potential cybersecurity incident. Analysis involves examining the incident to understand its nature, impact, and cause. Containment entails taking immediate action to minimize further damage and prevent the incident from spreading. Eradication involves completely removing the threat or vulnerability from the system or network in order to eliminate the possibility of a recurring incident. These elements are crucial for an effective incident response strategy.

#### NEW QUESTION # 55

.....

DumpsQuestion offers real Cisco 100-160 Questions that can solve this trouble for students. Professionals have made the Cisco 100-160 questions of DumpsQuestion after working days without caring about themselves to provide the applicants with actual 100-160 exam questions DumpsQuestion guarantees our customers that they can pass the Cisco Certified Support Technician (CCST) Cybersecurity (100-160) exam on the first try by preparing from DumpsQuestion, and if they fail to pass it despite their best efforts, they can claim their payment back according to some terms and conditions.

**100-160 Best Practice:** <https://www.dumpsquestion.com/100-160-exam-dumps-collection.html>

- Cisco 100-160 Questions: Pass Exam With Good Scores [2026] ☐ Search for ➡ 100-160 ☐ and download it for free on ☀ [www.examcollectionpass.com](http://www.examcollectionpass.com) ☐ ☀ ☐ website ☐ 100-160 Exam Sample
- 100-160 Exam Sample ☐ 100-160 New Exam Bootcamp ☐ 100-160 Reliable Exam Topics ➡ Immediately open ☐

100-160 Latest Test Practice: Cisco Certified Support Technician (CCST) Cybersecurity - High-quality Cisco 100-160 Best Practice ☐ Download ( 100-160 ) for free by simply searching on ➡ [www.troytecdumps.com](http://www.troytecdumps.com) ☐ ☐ 100-160 Reliable Dumps Free

- BONUS!!! Download part of DumpsQuestion 100-160 dumps for free: [https://drive.google.com/open?id=1vqBCiF5dyCJ6mYvDsxsPU\\_zJod0mXbB](https://drive.google.com/open?id=1vqBCiF5dyCJ6mYvDsxsPU_zJod0mXbB)