

Use Cisco 100-160 Dumps to Have Great Outcomes In Cisco Exam



BTW, DOWNLOAD part of Real4test 100-160 dumps from Cloud Storage: <https://drive.google.com/open?id=1flvoYF41steS2oK1zy2eqcdKmgORnKUT>

Our 100-160 exam braindumps are famous for the advantage of high-efficiency and high-effective. And it is proved by the high pass rate. The 99% pass rate is a very proud result for us. If you join, you will become one of the 99% to pass the 100-160 Exam and achieve the certification. Believe in yourself, you can do it! Buy 100-160 study guide now and we will help you. Believe it won't be long before, you are the one who succeeded!

Cisco 100-160 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">• 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
Topic 2	<ul style="list-style-type: none">• 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.
Topic 3	<ul style="list-style-type: none">• 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.
Topic 4	<ul style="list-style-type: none">• Basic Network Security Concepts: 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• prevention systems, providing insight into how threats are mitigated within network environments.

Topic 5	<ul style="list-style-type: none">• Essential Security Principles: 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.
---------	--

>> 100-160 Training Courses <<

Valid 100-160 Test Simulator & 100-160 Exam Paper Pdf

One year free update for 100-160 pdf torrent is available, and you do not worry about missing the updated Cisco 100-160 study dumps. In addition, the content of 100-160 pdf download cover almost the key points which will be occurred in the actual test. Besides, you can install your 100-160 Online Test engine on any electronic device, so that you can study at anytime and anywhere. Thus your time is saved and your study efficiency is improved. Our 100-160 100-160 can ensure you 100% pass.

Cisco Certified Support Technician (CCST) Cybersecurity Sample Questions (Q193-Q198):

NEW QUESTION # 193

During a cybersecurity investigation, a log entry states, "Unauthorized access attempt blocked from IP address 123.45.67.89." What can be inferred from this log entry?

- A. The system detected suspicious traffic from IP address 123.45.67.89 for further investigation.
- B. The system experienced a denial-of-service attack from IP address 123.45.67.89.
- C. The system was compromised due to an unauthorized access attempt from IP address 123.45.67.89.
- **D. The system successfully prevented an unauthorized access attempt from a specific IP address.**

Answer: D

Explanation:

The log entry clearly states that the system blocked an unauthorized access attempt from a specific IP address, indicating that a security measure or mechanism successfully prevented the unauthorized access. This is a positive outcome for the system as it shows effective defense against potential threats.

NEW QUESTION # 194

What is the purpose of a VPN?

- A. To block unauthorized access
- B. To detect network vulnerabilities
- C. To authenticate users
- **D. To encrypt network traffic**

Answer: D

Explanation:

A VPN (Virtual Private Network) is used to create a secure connection between a user's device and a private network, such as a corporate network or the internet. It encrypts the data that is transmitted between the user and the network, ensuring that even if intercepted, the data is unreadable by unauthorized individuals.

NEW QUESTION # 195

Which command-line tool is used to query DNS records and obtain information about domain names?

- **A. nslookup**
- B. traceroute
- C. tcpdump
- D. netstat

Answer: A

Explanation:

The correct command-line tool for querying DNS records and obtaining information about domain names is nslookup. It can be used to check the security assessment information related to DNS configurations, verify the correct mapping of domain names to IP addresses, and troubleshoot any DNS-related issues.

NEW QUESTION # 196

A threat actor sets up a rogue access point (AP) at a local café. The rogue AP captures traffic and then forwards the traffic to the café AP.

Which type of attack does this scenario describe?

- A. Ransomware
- B. DDoS
- **C. Man-in-the-middle**
- D. Reconnaissance

Answer: C

Explanation:

The CCST Cybersecurity Study Guide describes a man-in-the-middle (MITM) attack as an attack where the adversary secretly intercepts and possibly alters communications between two parties, making them believe they are communicating directly. A rogue AP configured to pass traffic through itself before sending it on is a classic wireless MITM method.

"In a MITM attack, the attacker places themselves between the sender and receiver, intercepting and possibly altering data in transit. Rogue access points can facilitate MITM attacks in wireless environments." (CCST Cybersecurity, Basic Network Security Concepts, Wireless Threats section, Cisco Networking Academy) A is incorrect: Reconnaissance is information gathering, not active interception.

B is correct: This is a wireless MITM attack.

C is incorrect: DDoS aims to overwhelm a service, not intercept data.

D is incorrect: Ransomware encrypts data for extortion.

NEW QUESTION # 197

During a change management assessment, what should be evaluated?

- A. The effectiveness of the change management process
- B. The impact of proposed changes on system functionality
- C. The level of user acceptance and satisfaction with the changes
- **D. All of the above**

Answer: D

Explanation:

During a change management assessment, multiple aspects should be evaluated. Firstly, the impact of proposed changes on system functionality needs to be assessed to ensure that the changes do not negatively affect the overall performance or stability of the system. Secondly, the level of user acceptance and satisfaction with the changes should be evaluated to determine the effectiveness of the change management process and whether it meets the needs and expectations of the users. Assessing these aspects helps in identifying any areas that require improvement. Therefore, all the options mentioned in the

NEW QUESTION # 198

.....

The number of questions of the 100-160 study materials you have done has a great influence on your passing rate. As for our study materials, we have prepared abundant exercises for you to do. You can take part in the real 100-160 exam after you have memorized all questions and answers accurately. Also, we just pick out the most important knowledge to learn. Through large numbers of practices, you will soon master the core knowledge of the 100-160 Exam. It is important to review the questions you always choose mistakenly. You should concentrate on finishing all exercises once you are determined to pass the 100-160 exam.

Valid 100-160 Test Simulator: https://www.real4test.com/100-160_real-exam.html

