

100-160 Valid Practice Questions | Visual 100-160 Cert Exam



What's more, part of that Lead2PassExam 100-160 dumps now are free: https://drive.google.com/open?id=1My424dzyW_eG86tSmuiD0jqOLpHADwu1

Regardless of your weak foundation or rich experience, 100-160 exam torrent can bring you unexpected results. In the past, our passing rate has remained at 99%-100%. This is the most important reason why most candidates choose 100-160 test guide. Failure to pass the exam will result in a full refund. But as long as you want to continue to take the Cisco Certified Support Technician (CCST) Cybersecurity exam, we will not stop helping you until you win and pass the certification. In this age of the Internet, do you worry about receiving harassment of spam messages after you purchase a product, or discover that your product purchases or personal information are illegally used by other businesses? Please do not worry; we will always put the interests of customers in the first place, so 100-160 Test Guide ensure that your information will not be leaked to any third party.

The Cisco 100-160 certification exam is one of the hottest and career-oriented Cisco Certified Support Technician (CCST) Cybersecurity (100-160) exams. With the Cisco Certified Support Technician (CCST) Cybersecurity (100-160) exam you can validate your skills and upgrade your knowledge level. By doing this you can learn new in-demand skills and gain multiple career opportunities. To do this you just need to enroll in the Cisco 100-160 Certification Exam and put all your efforts to pass this important Cisco 100-160 Exam Questions.

>> 100-160 Valid Practice Questions <<

How Lead2PassExam will Help You in Passing the 100-160?

Our company is a well-known multinational company, has its own complete sales system and after-sales service worldwide. Our 100-160 real study guide have become a critically acclaimed enterprise, so, if you are preparing for the exam qualification and obtain the corresponding certificate, so our company launched 100-160 Exam Questions are the most reliable choice of you. The service tenet of our company and all the staff work mission is: through constant innovation and providing the best quality service, make the 100-160 question guide become the best customers electronic test study materials.

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"> • 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 and prevention systems, providing insight into how threats are mitigated within network environments.
Topic 3	<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 4	<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 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.

Cisco Certified Support Technician (CCST) Cybersecurity Sample Questions (Q244-Q249):

NEW QUESTION # 244

Which of the following is an essential component of information security assessments?

- A. Penetration testing
- B. Incident response planning
- C. All of the above
- D. User training

Answer: C

Explanation:

Information security assessments involve assessing the security posture of an IT system. Penetration testing, which involves simulating attacks to identify vulnerabilities, is an important component of such assessments. Additionally, user training is vital because human error or lack of awareness can often be a weak point in security. Understanding how to recognize and respond to potential threats is crucial. Lastly, incident response planning is essential to ensure that the organization is prepared to handle and mitigate any security incidents effectively. Therefore, all the options mentioned in the

NEW QUESTION # 245

Which of the following best describes asset management in the context of cybersecurity?

- A. Tracking software licenses
- B. Identifying and protecting valuable resources
- C. Monitoring user activity
- D. Managing network infrastructure

Answer: B

Explanation:

Asset management in a cybersecurity context involves identifying and protecting valuable resources within an organization. This includes identifying critical systems, data, and information that need to be protected from unauthorized access, modification, or destruction.

NEW QUESTION # 246

Which feature allows endpoints to communicate directly with each other, bypassing the network?

- A. Firewall
- B. VPN
- C. Peer-to-Peer
- D. IPS

Answer: C

Explanation:

Option 1: Incorrect. A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on predetermined security rules.

Option 2: Incorrect. An IPS (Intrusion Prevention System) is a network security device that monitors network traffic for malicious activity and takes immediate action to prevent attacks.

Option 3: Incorrect. A VPN (Virtual Private Network) is a secure connection between two or more endpoints over a public network, providing encryption and privacy for data communication.

Option 4: Correct. Peer-to-peer (P2P) is a decentralized communication model where endpoints can directly communicate with each other without the need for a central server or network infrastructure.

NEW QUESTION # 247

Which of the following is true regarding the incident response process?

- A. It is a reactive process that is only initiated after an incident has occurred.
- B. It is a one-time process that is only performed when an organization first establishes its security program.
- C. It is an iterative process that involves continuous improvement based on lessons learned.
- D. It is a proactive process that focuses on preventing incidents from occurring.

Answer: C

Explanation:

Option 1: Incorrect. The incident response process can be both proactive and reactive. While it does involve reacting to incidents that have already occurred, it also includes proactive measures to prevent incidents from happening again in the future.

Option 2: Incorrect. While incident response can involve proactive measures to prevent incidents, it is not solely focused on prevention. It also includes reacting to incidents that have already occurred.

Option 3: Correct. The incident response process is an iterative process that involves continuous improvement based on lessons learned. Organizations should regularly review and update their incident response plans to ensure they are effective and up to date.

Option 4: Incorrect. The incident response process is not a one-time process. It should be an ongoing and continuous process to address security incidents as they occur and to improve the incident response capabilities of the organization.

NEW QUESTION # 248

What is the primary reason for isolating an infected system from the network during malware removal?

- A. To prevent further spread of the malware
- B. To stop the infected system from collecting sensitive information
- C. To prevent unauthorized access to the system
- D. To avoid interference with malware removal tools

Answer: A

Explanation:

Isolating an infected system from the network is crucial to prevent the malware from spreading to other devices or networks. This containment measure helps in limiting the impact of the infection and prevents potential damage or data breaches.

NEW QUESTION # 249

.....

Visual 100-160 Cert Exam <https://www.lead2passexam.com/Cisco/valid-100-160-exam-dumps.html>

- What's more, part of that Lead2PassExam 100-160 dumps now are free: https://drive.google.com/open?id=1My424dzyW_eG86tSmuiD0jqOLpHADwul