Authorized 100-160 Certification, 100-160 Reliable Braindumps Ebook

What's more, part of that BootcampPDF 100-160 dumps now are free: https://drive.google.com/open?id=1jQqeGZPE4iOHo44NnjKg7oV2Pw2oMKji

The three formats of this Cisco 100-160 study material are the desktop Cisco 100-160 practice exam software, Cisco 100-160 web-based practice test, and a 100-160 Pdf Format. Below are their characteristics. BootcampPDF offers Cisco 100-160 practice exams of two types.

BootcampPDF also offers a demo of the Cisco 100-160 exam product which is absolutely free. Up to 1 year of free Cisco Certified Support Technician (CCST) Cybersecurity (100-160) questions updates are also available if in any case the sections of the Cisco 100-160 Actual Test changes after your purchase. Lastly, we also offer a full refund guarantee according to terms and conditions if you do not get success in the Cisco Certified Support Technician (CCST) Cybersecurity exam after using our 100-160 product.

>> Authorized 100-160 Certification <<

100-160 PDF dumps & 100-160 dumps training make for your success in the coming Cisco exam

If you buy 100-160 study materials, you will get more than just a question bank. You will also get our meticulous after-sales service. The purpose of the 100-160 study materials' team is not to sell the materials, but to allow all customers who have purchased 100-

160 study materials to pass the exam smoothly. The trust and praise of the customers is what we most want. We will accompany you throughout the review process from the moment you buy 100-160 Study Materials. We will provide you with 24 hours of free online services. All our team of experts and service staff are waiting for your mail all the time.

Cisco 100-160 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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	• 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	• 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	• 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.
Topic 5	• 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.

Cisco Certified Support Technician (CCST) Cybersecurity Sample Questions (Q278-Q283):

NEW QUESTION # 278
Which of the following features help to secure a wireless SoHo network from unauthorized access?

- A. SSID broadcast
- B. Weak encryption
- C. MAC filtering
- D. Default admin credentials

Answer: C

Explanation:
MAC filtering is a feature that allows a network administrator to specify which devices can connect to the wireless network based on their MAC (Media Access Control) addresses. By enabling MAC filtering, only devices with authorized MAC addresses will be allowed to connect, thereby enhancing network security. SSID (Service Set Identifier) broadcast refers to the network name being broadcasted, and hiding it doesn't provide significant security improvement. Default admin credentials should always be changed to prevent unauthorized access, making option C a weak answer choice. Weak encryption, such as WEP or TKIP, provides little security and should be avoided.

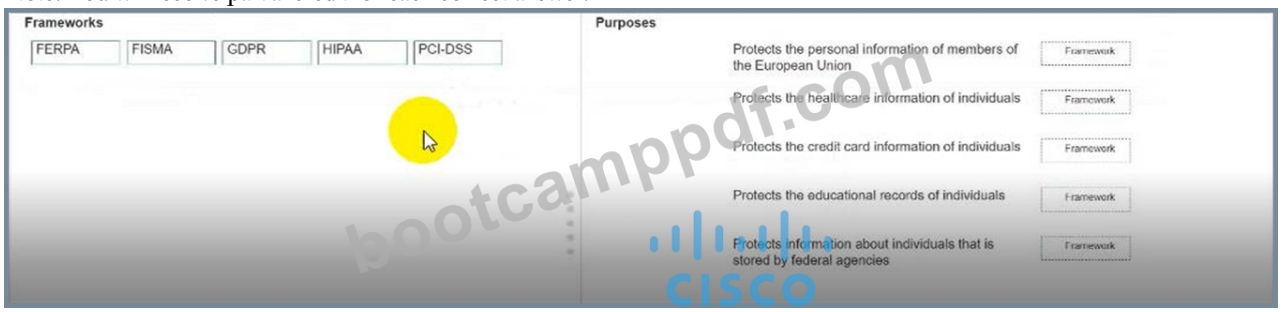
NEW QUESTION # 279
Which of the following is a common method used by threat actors to gain access in an Advanced Persistent Threat (APT)?

- A. Distributed Denial of Service (DDoS) attacks
- B. Firewall misconfigurations
- C. Social engineering techniques
- D. Application vulnerabilities

Answer: C

Explanation:
Social engineering techniques, such as phishing, spear phishing, or baiting, are commonly employed by threat actors to gain initial access in an APT. By tricking individuals or organizations into revealing sensitive information or executing malicious actions, attackers can bypass traditional security measures and gain a foothold in the target system.

NEW QUESTION # 280
Move each framework from the list on the left to the correct purpose on the right.
Note: You will receive partial credit for each correct answer.



Answer:

Explanation:

NEW QUESTION # 281
Why is it important to maintain the chain of custody when handling digital evidence?

- A. To prevent unauthorized access or tampering.
- B. To ensure the evidence is stored securely.
- C. To accelerate the analysis of the evidence.
- D. To recover lost or deleted data from the evidence.

Answer: A

Explanation:
Maintaining the chain of custody is crucial to ensure the integrity and admissibility of digital evidence in a legal case. It helps establish that the evidence has not been tampered with or accessed by unauthorized individuals, which ensures its reliability and credibility. By maintaining a strict chain of custody, any potential challenges to the evidence's validity can be effectively addressed by demonstrating that it has been handled in a controlled and secure manner.

NEW QUESTION # 282
Which of the following is a preventive control that can help in reducing the risk of future incidents?

- A. Conducting periodic employee training on incident response
- B. Regularly updating antivirus signatures
- C. Implementing strong access controls and authentication mechanisms
- D. Creating secure backups of critical data

Answer: C

Explanation:
Implementing strong access controls and authentication mechanisms is a preventive control that can help reduce the risk of future incidents. By ensuring that only authorized individuals have access to systems and data, the likelihood of unauthorized access or malicious activity is minimized. While regularly updating antivirus signatures, conducting employee training, and creating secure backups are also important preventive measures, the focus here is on access controls and authentication mechanisms.

NEW QUESTION # 283
.....