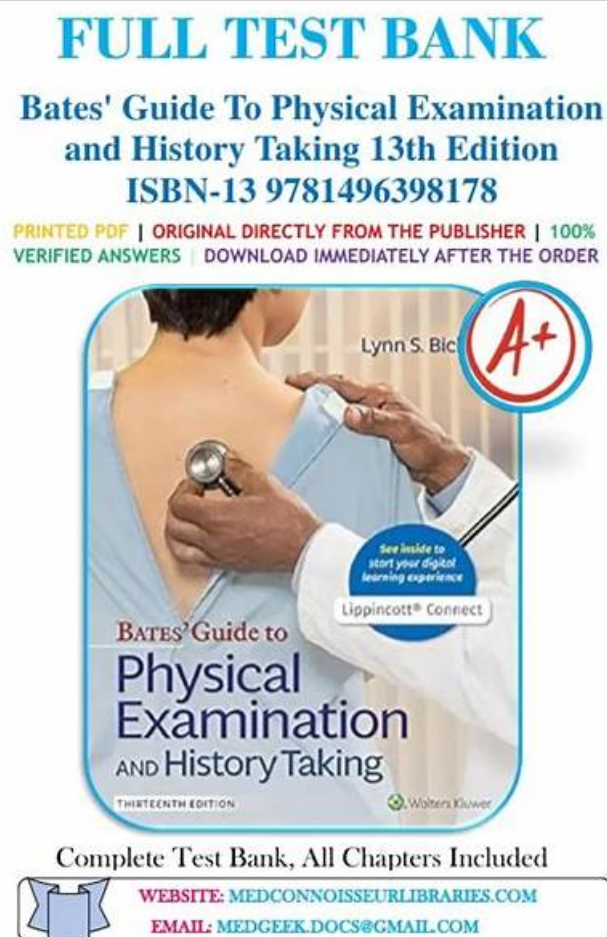


Latest 100-160 Test Guide & Certification Success Guaranteed, Easy Way of Training & New 100-160 Test Pass4sure



P.S. Free 2026 Cisco 100-160 dumps are available on Google Drive shared by ValidTorrent: https://drive.google.com/open?id=1j4mioYHxZ_Ag2IXDoOCkvpN7Mjsdb4sb

ValidTorrent is a professional website. It can give each candidate to provide high-quality services, including pre-sales service and after-sales service. If you need ValidTorrent's Cisco 100-160 exam training materials, you can use part of our free questions and answers as a trial to sure that it is suitable for you. So you can personally check the quality of the ValidTorrent Cisco 100-160 Exam Training materials, and then decide to buy it. If you did not pass the exam unfortunately, we will refund the full cost of your purchase. Moreover, we can give you a year of free updates until you pass the exam.

Cisco 100-160 Exam Syllabus Topics:

Topic	Details
Topic 1	<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 2	<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.
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"> • 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 5	<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.

>> Latest 100-160 Test Guide <<

New Cisco 100-160 Test Pass4sure & Examcollection 100-160 Free Dumps

ValidTorrent 100-160 Web-Based Practice Test: For the Cisco Certified Support Technician (CCST) Cybersecurity (100-160) web-based practice exam no special software installation is required. Because it is a browser-based Cisco 100-160 practice test. The web-based Cisco Certified Support Technician (CCST) Cybersecurity (100-160) practice exam works on all operating systems like Mac, Linux, iOS, Android, and Windows. In the same way, IE, Firefox, Opera and Safari, and all the major browsers support the web-based 100-160 practice test.

Cisco Certified Support Technician (CCST) Cybersecurity Sample Questions (Q155-Q160):

NEW QUESTION # 155

What is the primary goal of a threat actor in a cyber attack?

- A. To identify and mitigate security risks
- B. To exploit vulnerabilities in a system
- C. To gain unauthorized access to a network
- **D. To cause damage or disruption to a target**

Answer: D

Explanation:

The primary goal of a threat actor in a cyber attack is typically to cause damage, disruption, or gain some form of unauthorized advantage. They may aim to steal sensitive data, encrypt files for ransom, disrupt services, or compromise the integrity of a system. Understanding the motivations of threat actors helps in building effective defense strategies.

NEW QUESTION # 156

What is the main purpose of risk management in the context of cybersecurity?

- A. To transfer all cybersecurity risks to a third-party vendor.
- **B. To identify and prioritize potential cybersecurity risks for effective mitigation.**
- C. To eliminate all possible risks to an organization's cybersecurity.
- D. To ignore potential cybersecurity risks to minimize costs.

Answer: B

Explanation:

The main purpose of risk management in the context of cybersecurity is to identify and prioritize potential risks associated with a system, network, or application. By understanding the risks, organizations can develop effective mitigation strategies and allocate resources accordingly. Risk management involves assessing the likelihood and impact of potential risks, determining their significance to the organization, and implementing appropriate controls to mitigate or reduce those risks to an acceptable level.

NEW QUESTION # 157

Which of the following is a principle of data security?

- A. Data Masking
- **B. Encryption**
- C. Intrusion Detection System
- D. Firewall

Answer: B

Explanation:

Option 1: Correct. Encryption is a principle of data security that involves converting data into a form that is unreadable by unauthorized users. This helps protect the confidentiality of data.

Option 2: Incorrect. A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on predetermined security rules. While it plays a role in data security, it is not a principle of data security.

Option 3: Incorrect. An Intrusion Detection System (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports. While it plays a role in data security, it is not a principle of data security.

Option 4: Incorrect. Data masking is a technique that replaces sensitive data with fictitious data to protect the privacy of data. While it plays a role in data security, it is not a principle of data security.

NEW QUESTION # 158

What does data encryption in cybersecurity refer to?

- A. Backing up data periodically to prevent loss
- **B. Protecting data by converting it into an unreadable form**
- C. Transforming data into a format that can be easily accessed and read
- D. Collecting and analyzing data to identify patterns and trends

Answer: B

Explanation:

Data encryption is a fundamental technique in cybersecurity that involves converting data into an unreadable form using an encryption algorithm. This process ensures that even if unauthorized individuals gain access to the encrypted data, they cannot read or understand it without the appropriate decryption key. Data encryption helps protect sensitive and confidential information from unauthorized access or interception.

NEW QUESTION # 159

Which Windows app is a command-line interface that includes a sophisticated scripting language used to automate Windows tasks?

- A. Vim
- **B. PowerShell**
- C. MS-DOS
- D. Microsoft Management Console

Answer: B

Explanation:

The CCST Cybersecurity course identifies Windows PowerShell as both a command-line interface (CLI) and a robust scripting environment. It is used by system administrators for automation, configuration, and task scheduling.

"PowerShell is a Windows command-line shell and scripting language built on the .NET framework. It allows administrators to automate administrative tasks, manage system configurations, and execute complex scripts for system management." (CCST Cybersecurity, Endpoint Security Concepts, System Administration Tools section, Cisco Networking Academy) A is correct:

D (MS-DOS) is a legacy command shell with no advanced scripting features comparable to PowerShell.

• • • • •

New 100-160 Test Pass4sure: <https://www.validtorrent.com/100-160-valid-exam-torrent.html>

- BTW, DOWNLOAD part of ValidTorrent 100-160 dumps from Cloud Storage: https://drive.google.com/open?id=1j4mioYHxZ_Ag2IXDoOCkvpN7Mjsdb4sb