CISCO 100-160

Cisco CCST Cybersecurity Certification Questions & Answers

Exam Summary – Syllabus – Questions

100-160

[Cisco Certified Support Technician (CCST) Cybersecurity](#)

40-50 Questions Exam – Variable (750-850 / 1000 Approx.) Cut Score – Duration of 50 minutes

Table of Contents:

Know Your 100-160 Certification Well:

The 100-160 is best suitable for candidates who want to gain knowledge in the Cisco Support Technician. Before you start your 100-160 preparation you may struggle to get all the crucial CCST Cybersecurity materials like 100-160 syllabus, sample questions, study guide.

But don't worry the 100-160 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the 100-160 syllabus?
- How many questions are there in the 100-160 exam?
- Which Practice test would help me to pass the 100-160 exam at the first attempt?

Passing the 100-160 exam makes you Cisco Certified Support Technician (CCST) Cybersecurity. Having the CCST Cybersecurity certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

Cisco 100-160 CCST Cybersecurity Certification Details:

Exam Name	Cisco Certified Support Technician (CCST) Cybersecurity
Exam Code	100-160
Exam Price	$125 USD
Duration	50 minutes
Number of Questions	40-50
Passing Score	Variable (750-850 / 1000 Approx.)
Exam Registration	**PEARSON VUE**
Sample Questions	**Cisco 100-160 Sample Questions**
Practice Exam	**Cisco Certified Support Technician (CCST) Cybersecurity Practice Test**

100-160 Syllabus:

Section	Objectives
Essential Security Principles	- Define essential security principles • Vulnerabilities, threats, exploits, and risks; attack vectors; hardening; defense-indepth; confidentiality, integrity, and availability (CIA); types of attackers; reasons for attacks; code of ethics - Explain common threats and vulnerabilities • Malware, ransomware, denial of service, botnets, social engineering attacks (tailgating, spear phishing, phishing, vishing, smishing, etc.), physical attacks, man in the middle, IoT vulnerabilities, insider threats, Advanced Persistent Threat (APT) - Explain access management principles • Authentication, authorization, and accounting (AAA); RADIUS; multifactor authentication (MFA); password policies - Explain encryption methods and applications • Types of encryption, hashing, certificates, public key infrastructure (PKI); strong vs. weak encryption algorithms; states of data and appropriate encryption (data in transit, data at rest, data in use); protocols that use encryption
Basic Network Security Concepts	- Describe TCP/IP protocol vulnerabilities • TCP, UDP, HTTP, ARP, ICMP, DHCP, DNS - Explain how network addresses impact network security • IPv4 and IPv6 addresses, MAC addresses, network segmentation, CIDR notation, NAT, public vs. private networks - Describe network infrastructure and technologies • Network security architecture, DMZ, virtualization, cloud, honeypot, proxy server, IDS, IPS - Set up a secure wireless SoHo network

Section	Objectives
	• MAC address filtering, encryption standards and protocols, SSID - Implement secure access technologies • ACL, firewall, VPN, NAC
Endpoint Security Concepts	- Describe operating system security concepts • Windows, macOS, and Linux; security features, including Windows Defender and host-based firewalls; CLI and PowerShell; file and directory permissions; privilege escalation - Demonstrate familiarity with appropriate endpoint tools that gather security assessment information • netstat, nslookup, tcpdump - Verify that endpoint systems meet security policies and standards • Hardware inventory (asset management), software inventory, program deployment, data backups, regulatory compliance (PCI DSS, HIPAA, GDPR), BYOD (device management, data encryption, app distribution, configuration management) - Implement software and hardware updates • Windows Update, application updates, device drivers, firmware, patching - Interpret system logs • Event Viewer, audit logs, system and application logs, syslog, identification of anomalies - Demonstrate familiarity with malware removal • Scanning systems, reviewing scan logs, malware remediation
Vulnerability Assessment and Risk Management	- Explain vulnerability management • Vulnerability identification, management, and mitigation; active and passive reconnaissance; testing (port scanning, automation) - Use threat intelligence techniques to identify potential network vulnerabilities

Section	Objectives
	• Uses and limitations of vulnerability databases; industry-standard tools used to assess vulnerabilities and make recommendations, policies, and reports; Common Vulnerabilities and Exposures (CVEs), cybersecurity reports, cybersecurity news, subscription services, and collective intelligence; ad hoc and automated threat intelligence; the importance of updating documentation and other forms of communication proactively before, during, and after cybersecurity incidents; how to secure, share and update documentation - Explain risk management • Vulnerability vs. risk, ranking risks, approaches to risk management, risk mitigation strategies, levels of risk (low, medium, high, extremely high), risks associated with specific types of data and data classifications, security assessments of IT systems (information security, change management, computer operations, information assurance) - Explain the importance of disaster recovery and business continuity planning • Natural and human-caused disasters, features of disaster recovery plans (DRP) and business continuity plans (BCP), backup, disaster recovery controls (detective, preventive, and corrective)
Incident Handling	- Monitor security events and know when escalation is required • Role of SIEM and SOAR, monitoring network data to identify security incidents (packet captures, various log file entries, etc.), identifying suspicious events as they occur - Explain digital forensics and attack attribution processes • Cyber Kill Chain, MITRE ATT&CK Matrix, and Diamond Model; Tactics, Techniques, and

Section	Objectives
	Procedures (TTP); sources of evidence (artifacts); evidence handling (preserving digital evidence, chain of custody) - Explain the impact of compliance frameworks on incident handling • Compliance frameworks (GDPR, HIPAA, PCI-DSS, FERPA, FISMA), reporting and notification requirements - Describe the elements of cybersecurity incident response • Policy, plan, and procedure elements; incident response lifecycle stages (NIST Special Publication 800-61 sections 2.3, 3.1-3.4)

Cisco 100-160 Sample Questions:

Question: 1

Which type of attack exploits human vulnerabilities to gain unauthorized access?

a) Phishing
b) Brute force
c) Denial of Service
d) Malware

Answer: a

Question: 2

Which metric is used in risk assessment to evaluate the severity of a vulnerability?

a) CVSS score
b) Response time
c) Threat level index
d) Packet loss percentage

Answer: a

Question: 3

Which of the following are examples of secure network protocols?

(Choose two)

a) SSH
b) HTTPS
c) FTP
d) Telnet

Answer: a, b

Question: 4

What is the main role of a Host-Based Intrusion Prevention System (HIPS)?

a) To block unauthorized users
b) To encrypt network traffic
c) To monitor and prevent suspicious activity on endpoints
d) To perform data backups

Answer: c

Question: 5

What tools can help identify network vulnerabilities? (Choose two)

a) Email clients
b) Word processors
c) Vulnerability assessment tools
d) Network scanners

Answer: c, d

Question: 6

Which protocol is commonly used for secure data transmission over the internet?

a) Telnet
b) HTTPS
c) FTP
d) HTTP

Answer: b

Question: 7

What are components of a comprehensive risk management process?

(Choose two)

a) Using outdated tools
b) Risk mitigation
c) Ignoring minor risks
d) Risk assessment

Answer: b, d

Question: 8

Which vulnerabilities can a risk assessment reveal? (Choose two)

a) Outdated software
b) Excessive packet loss
c) Misconfigured access controls
d) Insufficient power supply

Answer: a, c

Question: 9

What activities should occur during the preparation phase of incident handling? (Choose two)

a) Developing an incident response plan
b) Training the incident response team
c) Deleting outdated files
d) Replacing outdated hardware

Answer: a, b

Question: 10

What should an incident response team do immediately after detecting an incident?

a) Update threat intelligence databases
b) Prepare a final report
c) Eradicate the threat
d) Notify stakeholders

Answer: d

Study Guide to Crack Cisco CCST Cybersecurity 100-160 Exam:

- Getting details of the 100-160 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the 100-160 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the Cisco provided training for 100-160 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the 100-160 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on 100-160 practice tests is must. Continuous practice will make you an expert in all syllabus areas.