Cisco Networking Academy®, Constanta, Romania

CCNA® Security

Description:
The Cisco Networking Academy® CCNA® Security course provides a next step for individuals wanting to enhance their CCENT-level skills and help meet the growing demand for network security professionals. The curriculum provides an introduction to the core security concepts and skills needed for installation, troubleshooting, and monitoring of network devices to maintain the integrity, confidentiality, and availability of data and devices.

Skills and Competencies
Here are some examples of tasks students will be able to perform after completing each course:
- Students develop an in-depth, theoretical understanding of network security principles as well as the tools and configurations available.
- The course emphasizes the practical application of skills needed to design, implement, and support network security.
- Hands-on labs help students develop critical thinking and complex problem-solving skills.
- Packet Tracer simulation-based learning activities promote the exploration of networking security concepts and allow students to experiment with network behavior, asking "what if" questions.
- Innovative assessments provide immediate feedback to support the evaluation of knowledge and acquired skills.

Table of Contents:

Chapter 1: Modern Network Security Threats
1.0 Introduction
1.1 Securing Networks
1.2 Network Threats
1.3 Mitigating Threats
1.4 Chapter Summary

Chapter 2: Securing Network Devices
2.0 Introduction
2.1 Securing Device Access
2.2 Monitoring and Managing Devices
2.3 Using Automated Security Features
2.4 Chapter Summary

Chapter 3: Authentication, Authorization and Accounting
3.0 Introduction
3.1 Purpose of AAA
3.2 Local AAA Authentication
3.3 Server-Based AAA
3.4 Server-Based AAA Authentication
3.5 Server-Based AAA Authorization and Accounting
3.6 Chapter Summary

Chapter 4: Implementing Firewall Technologies
4.0 Introduction
4.1 Access Control Lists
4.2 Firewall Technologies
4.3 Zone-Based Policy Firewalls
4.4 Chapter Summary

Chapter 5: Implementing Intrusion Prevention
5.0 Introduction
5.1 IPS Technologies
5.2 IPS Signatures
5.3 Implement IPS
5.4 Chapter Summary

Chapter 6: Securing the Local Area Network
6.0 Introduction
6.1 Endpoint Security
6.2 Layer 2 Security Considerations
6.3 Chapter Summary

Chapter 7: Cryptographic Systems
7.0 Introduction
7.1 Cryptographic Services

7.2 Basic Integrity and Authenticity
7.3 Confidentiality
7.4 Public Key Cryptography
7.5 Chapter Summary

Chapter 8: Implementing Virtual Private Networks
8.0 Introduction
8.1 VPNs
8.2 IPsec VPN Components and Operation
8.3 Implementing Site-to-Site IPsec VPNs with CLI
8.4 Chapter Summary

Chapter 9: Implementing the Cisco Adaptive Security Appliance
9.0 Introduction
9.1 Introduction to the ASA
9.2 ASA Firewall Configuration
9.3 Chapter Summary

Chapter 10: Advanced Cisco Adaptive Security Appliance
10.0 Introduction
10.1 ASA Security Device Manager
10.2 ASA VPN Configuration
10.3 Chapter Summary

Chapter 11: Managing a Secure Network
11.0 Introduction
11.1 Network Security Testing
11.2 Developing a Comprehensive Security Policy
11.3 Chapter Summary

Contact: Foundation for promoting Information and Communication Technology (ICT Foundation)
Constanta, Romania
www.fict.ro