C-ID Descriptor
Network Security – CCNA-Security

Descriptor Details

- **Descriptor Title**: Network Security – CCNA-Security
- **C-ID Number**: 167
- **Units**: 3
- **Date of Last Revision**: 2/26/2025 11:23:00 AM PST

General Description

This course equips students with the knowledge and skills needed to prepare for entry-level security specialist careers. This course is a hands-on, career-oriented e-learning solution that emphasizes practical experience. It is a blended curriculum with both online and classroom learning. Students will develop an in-depth understanding of network security principles as well as the tools and configurations required to secure a network. CCNA Security helps students develop the skills needed for entry-level network security career opportunities and prepare for the CCNA Security certification.

Prerequisites

No information provided

Corequisites

No information provided

Advisories

ITIS 150 - Computer Network Fundamentals
ITIS 151 – Routing and Switching Essentials
ITIS 160 – Introduction to Information Systems Security

Content

1. Modern Network Security Threats
    a. Securing Networks - Explain network security.
    b. Network Threats - Describe various types of threats and attacks.
    c. Mitigating Threats - Explain tools and procedures to mitigate the effects of malware and common network attacks.
2. Securing Network Devices
    a. Securing Device Access - Configure secure administrative access.
    b. Assigning Administrative Roles - Configure command authorization using privilege levels and role-based Command Line Interface (CLI).
    c. Monitoring and Managing Devices - Implement the secure management and monitoring of network devices.
    d. Using Automated Security Features - Use automated features to enable security on IOS-based routers.
3. Authentication, Authorization and Accounting (AAA)
    a. Purpose of AAA - Explain how AAA is used to secure a network.
    b. Local AAA Authentication - Implement AAA authentication that validates users against a local database.
    c. Server-Based AAA - Explain server-based AAA authentication and its communication protocols.
    d. Server-Based AAA Authentication - Implement server-based AAA authentication using TACACS+ and RADIUS protocols.
    e. Server-Based AAA Authorization and Accounting - Configure server-based AAA authorization and accounting.
4. Implementing Firewall Technologies
    a. Access Control Lists - Implement Access Control Lists (ACLs) to filter traffic and mitigate network attacks on a network.
    b. Firewall Technologies - Configure a classic firewall to mitigate network attacks.
    c. Zone-Based Policy Firewall - Implement Zone-Based Policy Firewall using CLI.
5. Implementing Intrusion Prevention (IPS)
    a. IPS Technologies - Explain how network-based IPS is used to help secure a network.
    b. IPS Signatures - Explain how signatures are used to detect malicious network traffic.
    c. Implementing IPS - Configure Cisco IOS IPS operations using CLI.
6. Securing the Local Area Network

a. Endpoint Security - Explain endpoint vulnerabilities and protection methods.
b. Layer 2 Security Considerations - Implement Layer 2 security features.

7. Cryptography
   a. Cryptographic Services - Explain how the types of encryption, hashes, and digital signatures work together to provide confidentiality, integrity, and authentication.
   b. Basic Integrity and Authenticity - Explain how cryptographic hashes are used to ensure data integrity and authentication.
   c. Confidentiality - Explain how encryption algorithms are used to ensure data confidentiality.
   d. Public Key Cryptography - Explain how a public key infrastructure is used to ensure data confidentiality and provide authentication.
8. Implementing Virtual Private Networks (VPNs)
   a. VPNs - Explain the purpose of VPNs.
   b. Internet Protocol Security (IPsec) VPN Components and Operation - Explain how IPsec VPNs operate.
   c. Implementing Site-to-Site IPSec VPNs with CLI - Configure a site-to-site IPsec VPN, with pre-shared key authentication, using CLI.
9. Implementing the Cisco Adaptive Security Appliance (ASA)
   a. Introduction to the ASA - Explain how the ASA operates as an advanced stateful firewall.
   b. ASA Firewall Configuration - Implement an ASA firewall configuration.
   c. ASA VPN Configuration - Implement an ASA VPN configuration.
10. Advanced Cisco Adaptive Security Appliance
    a. ASA Security Device Manager (ASDM) - Implement an ASA firewall configuration and VPNs using ASDM.
    b. ASA VPN Configuration - Configure remote-access VPNs on an ASA.
11. Managing a Secure Network
    a. Network Security Testing - Explain the various techniques and tools used for network security testing.
    b. Developing a Comprehensive Security Policy - Explain how to develop a comprehensive security policy.

Lab Activities

No information provided

Objectives

At the conclusion of this course, the student should be able to:

1. Explain network threats, mitigation techniques, and the basics of securing a network.
2. Secure administrative access on Cisco routers.
3. Secure administrative access with AAA.
4. Implement firewall technologies to secure the network perimeter.
5. Configure IPS to mitigate attacks on the network.
6. Describe LAN security considerations and implement endpoint and Layer 2 security features.
7. Describe methods for implementing data confidentiality and integrity.
8. Implement secure virtual private networks.
9. Implement an ASA firewall configuration using the CLI.
10. Implement an ASA firewall configuration and VPNs using ASDM.
11. Test network security and create a technical security policy.

Evaluation Methods

Evaluation will include hands-on projects and a combination of examinations, presentations, discussions, or problem-solving assignments.

Textbooks

- *CCNA Security Course Booklet Version 2.0*, Cisco Network Academy, Cisco Press
- Gargano, P., *31 Days Before Your CCNA Security Exam (Digital Study Guide)*, Cisco Press