Course Catalog
2012-2013

CCNA SECURITY

CSLiT

.....Connecting Technology

CCNA Security

This course is comprised of the CISCO CCNA Security Curriculum. The CCNA Security curriculum prepares students for the Implementing CISCO IOS Network Security (IINS) certification exam (640-553), leading to the CCNA Security certification.

CCNA Security course is the ultimate training program for engineers pursuing the Cisco Certified Network Associate Security (CCNA Security) certification. Cisco Certified Network Associate Security (CCNA Security) validates associate-level knowledge and skills required to secure Cisco networks. With a CCNA Security certification, a network professional demonstrates the skills required to develop a security infrastructure, recognize threats and vulnerabilities to networks, and mitigate security threats.

Course Objectives

On completion of this course, students should have the skills to:

- Describe the security threats facing modern network infrastructures
- Secure network device access
- Implement AAA on network devices
- Mitigate threats to networks using ACLs
- Implement secure network management and reporting
- Mitigate common Layer 2 attacks
- Implement the CISCO IOS firewall feature set
- Implement the CISCO IOS IPS feature set
- Implement site-to-site IPSec VPNs
- Administer effective security policies

Who Should Attend

The target audience for this course is:

- IT networking professionals.
- People with a background in deploying and supporting networking infrastructure (routers and switches).

CCNA Security provides a next step for CCNA Discovery or CCNA Exploration students who want to expand their CCNA-level skill set to prepare for a career in network security

Prerequisite

It is recommended that students have a technical background in networking, particularly routers. This may be achieved by at least a year working with routers at the command line and/or completing a recent CISCO CCNA course.

Course Duration

36 Hours, 12 Classes, 3 Hours per class

Course Details

Lesson 01: Describe the security threats facing modern network infrastructures

- Describe and list mitigation methods for common network attacks
- Describe and list mitigation methods for Worm, Virus, and Trojan Horse attacks
- Describe the Cisco Self Defending Network architecture

Lesson 02: Secure Cisco routers

- Secure Cisco routers using the SDM Security Audit feature
- Use the One-Step Lockdown feature in SDM to secure a Cisco router
- Secure administrative access to Cisco routers by setting strong encrypted passwords, exec timeout, login failure rate and using IOS login enhancements
- Secure administrative access to Cisco routers by configuring multiple privilege levels
- Secure administrative access to Cisco routers by configuring role based CLI
- Secure the Cisco IOS image and configuration file

Lesson 03: Implement AAA on Cisco routers using local router database and external ACS

- Explain the functions and importance of AAA
- Describe the features of TACACS+ and RADIUS AAA protocols
- Configure AAA authentication
- Configure AAA authorization
- Configure AAA accounting

Lesson 04: Implement secure network management and reporting

- Use CLI and SDM to configure SSH on Cisco routers to enable secured management access
- Use CLI and SDM to configure Cisco routers to send Syslog messages to a Syslog server

Lesson 05: Mitigate common Layer 2 attacks

- Describe how to prevent layer 2 attacks by configuring basic Catalyst switch security features

Lesson 06: Implement the Cisco IOS firewall feature set using SDM

- Describe the operational strengths and weaknesses of the different firewall technologies
- Explain statefull firewall operations and the function of the state table
- Implement Zone Based Firewall using SDM

Lesson 07: Implement the Cisco IOS IPS feature set using SDM

- Define network based vs. host based intrusion detection and prevention
- Explain IPS technologies, attack responses, and monitoring options
- Enable and verify Cisco IOS IPS operations using SDM

Lesson 08: Implement site-to-site VPNs on Cisco Routers using SDM

- Describe the building blocks of IPSec and the security functions it provides
- Configure and verify an IPSec site-to-site VPN with pre-shared key authentication using SDM

CSLiT
.....Connecting Technology