

COURSE OUTLINE

CSCO-308

CCNA Security

3 Credits

HOWARD COMMUNITY COLLEGE

Description

This course concentrates on in-depth, theoretical understanding of network security principles as well as the tools and configuration available. This course emphasizes the practical application of skills needed to design, implement, and support network security. This course prepares students to take Implementing Cisco IOS Network Security (IINS) certification exam (640-543). Prerequisite: CCNA certification or CSCO-284. (2 hours lecture, 3 hours lab)

Overall Course Objectives

Upon completion of this course, the student will be able to:

1. Explain network threats, mitigation techniques, and the basics of securing a network.
2. Describe the fundamental principles of securing a network.
3. Describe the characteristics of worms, viruses, and Trojan horses and mitigation methods.
4. Describe common network attack methodologies and mitigation techniques such as Reconnaissance, Access, Denial of Service and DDoS.
5. Configure command authorization using privilege levels and role-based CLI.
6. Describe the purposes of AAA and the various implementation techniques.
7. Implement AAA using TACACS+ and RADIUS protocols.
8. Describe the purpose and operation of firewall technologies.
9. Implement CBAC, Zone-based policy Firewall using SDM and CLI.
10. Describe the purpose and operation of network-based and host-based Intrusion Prevention Systems.
11. Implement Cisco IOS IPS operations using SDM and CLI.
12. Describe endpoint vulnerabilities and protection methods.
13. Describe basic Catalyst switch vulnerabilities such as VLAN attacks, STP manipulation, CAM table overflow attacks, and MAC address spoofing attacks.
14. Describe the fundamentals of Wireless, VoIP and SANs, and the associated security considerations.
15. Describe how different types of encryption, hashes, and digital signature work together to provide confidentiality, integrity, and non-repudiation.
16. Describe the purpose and operation of VPN types.
17. Configure and verify a site-to-site IPSec VPN with pre-shared key authentication using SDM and CLI.
18. Configure and verify a remote access VPN.
19. Configure and verify SSL VPNs.
20. Establish a comprehensive security policy to meet the security needs of a given enterprise.

Major Topics

- I. Modern Network Security Threats
Fundamental Principles of a Secure Network
Worms, Viruses and Trojan Horses
Attack Methodologies

- II. Securing Network Devices
 - Privilege Levels and Role-Based CLI
 - Monitoring Devices
- III. Authentication, Authorization and Accounting (AAA)
 - Purpose of AAA
 - Configuring Local AAA
 - Configure Server-Based AAA
- IV. Implementing Firewall Technologies
 - Access Control Lists
 - Firewall Technologies
 - Context-Based Access Control
- V. Implementing Intrusion Prevention
 - IPS Technologies
 - Implementing IPS
- VI. Securing the Local Area Network
 - Layer 2 Security Considerations
 - Wireless, VoIP and SAN Security Considerations
- VII. Cryptography
 - Hashes and Digital Signatures and Authentication
 - Symmetric and Asymmetric Encryption
- VIII. Implementing Virtual Private Networks (VPN)
 - VPNs
 - IPSec VPN Components and Operation
 - Implementing Site-to-Site IPSec VPNs
 - Implementing a Remote Access VPN
 - Implementing SSL VPNs
- IX. Managing a Secure Network
 - Self-Defending Network
 - Building a Comprehensive Security Policy

Course Requirements

Grading/exams: Grading procedures will be determined by the individual faculty member but will include the following: Final grades will be based primarily on homework, lab exercises, lab practical and final exam.

Other Course Information

This course is a course in the Computer Support Technology program. This course is also intended for students who wish to become a Cisco Certified Network Associate Security (CCNA-Security).