



Tactical Perimeter Defense

Duration:

Traditional Instructor Led Learning - 5.00 Day(s)

Mentored Learning - Flexible

Overview:

This course is designed to provide network administrators and certification candidates with hands-on tasks on the most fundamental perimeter security technologies. The course covers the issues every administrator must be familiar with.

At Course Completion:

- Describe the core issues of building a perimeter network defense system. - Investigate the advanced concepts of the TCP/IP protocol suite. - Secure routers through hardening techniques and configure Access Control Lists. - Design and configure multiple firewall technologies. - Examine and implement IPSec and Virtual Private Networks. - Design and configure an Intrusion Detection System. - Secure wireless networks through the use of encryption systems.

Prerequisite(s) or equivalent knowledge:

Security+ Certification (2008 Objectives)

Prerequisite Comments:

Fundamental working knowledge of networking concepts, and foundational security knowledge

Outline:**Lesson 1: Network Defense Fundamentals**

- Defense fundamentals
- Defensive Technologies
- Objectives of Access Control
- The Impact of Defense
- Network Auditing Concepts

Lesson 2: Advanced TCP/IP

- TCP/IP Concepts
- Analyzing the Three-way Handshake
- Capturing and Analyzing IP Datagrams
- Capturing and Analyzing ICMP Messages
- Capturing and Analyzing TCP Headers
- Capturing and Analyzing UDP Headers
- Analyzing Packet Fragmentation
- Analyzing an Entire Session

Lesson 3: Routers and Access Control Lists

- Fundamental Cisco Security
- Routing Principles

- Removing Protocols and Services
- Creating Access Control Lists
- Implementing Access Control Lists
- Logging Concepts

Lesson 4: Designing Firewalls

- Firewall Components
- Creating a Firewall Policy
- Rule Sets and Packet Filters
- Proxy Servers
- The Bastion Hosts
- The Honeypots

Lesson 5: Configuring Firewalls

- Understanding Firewalls
- Configuring Microsoft ISA Server 2006
- IPTables Concepts
- Implementing Firewall Technologies

Lesson 6: Implementing IPsec and VPNs

- Internet Protocol Security
- IPsec Policy Management
- IPsec AH Implementation
- Combining AH and ESP in IPsec
- VPN Fundamentals
- Tunneling Protocols
- VPN Design and Architecture
- VPN Security
- Configuring a VPN

Lesson 7: Designing an Intrusion Detection System

- Goals of an Intrusion Detection System
- Technologies and Techniques of Intrusion Detection
- Host-based Intrusion Detection
- Network-based Intrusion Detection
- The Analysis
- How to use an IDS
- What an IDS Cannot Do

Lesson 8: Configuring IDS

- Snort Foundations
- Snort Installation
- Snort as an IDS
- Configuring Snort to Use a Database
- Running an IDS on Linux

Lesson 9: Securing Wireless Networks

- Wireless Networking Fundamentals
- Wireless LAN (WLAN) Fundamentals
- Wireless Security Solutions
- Wireless Auditing

Wireless Trusted Networks