

Tactical Perimeter Defense

- **Course Number:** SCO-451
- **Length:**

Certification Exam

This course is associated with Exam **SCO-451**: Tactical Perimeter Defense.

Course Overview

This course is the starting point with the Security Certified Program (SCP). It is also part of the official training SCNS exam and is designed to validate the foundational skills required by security professionals. These skills include, but are not limited to:

- Advanced TCP/IP
- Routers and Access Control Lists
- Designing Firewalls
- Configuring Firewalls
- Configuring Virtual Private Networks
- Designing an Intrusion Detection System
- Configuring an Intrusion Detection System
- Securing Wireless Networks
- Network Defense Fundamentals

Prerequisites

SCNS is a required pre-requisite for going further towards the SCNP and SCNA certifications. It also tests the candidate's ability to work with, and implement, real world security technology.

Audience

This course is intended for those wanting to achieve the Security Certified Program, the SCNS certification and the SCNP certification.

Course Outline

- **Lesson 1 - Network Defense Fundamentals**
- Network Defense Fundamentals
- Five Key Issues of Network Security - Authorization and Availability
- Five Key Issues of Network Security - Authentication
- Five Key Issues of Network Security - Confidentiality
- Five Key Issues of Network Security - Integrity
- Five Key Issues of Network Security - Non-Repudiation

- Managing the Threats to Security
- Defensive Strategies
- The Castle Analogy
- The Defense Technologies
- Analyzing Defense
- Objectives of Access Control
- Access Control
- Authentication
- Authentication Token
- Example of a Challenge Response Token
- Time Based Tokens
- Core Defensive Technologies
- Define the Concepts of Network Auditing
- Concepts of Network Auditing
- Security Audits
- Independent Audit
- Quick Audit Results
- Managing Audit Data
- Lesson 1 Review
- **Lesson 2 - Advanced TCP/IP**
- Advanced TCP/IP
- TCP/IP Concepts
- TCP/IP Model Layers
- OSI Model Layers
- OSI Model vs. TCP/IP Model
- The TCP/IP Encapsulation Process
- RFCs (Requests for Comments)
- The Function of IP
- IP Address Classes
- Address Class Chart
- Private IP Address Ranges (RFC1918)
- IP Addressing
- Hexadecimal IP Addressing
- Hexadecimal Conversions
- The Subnet Mask
- Subnetting Example
- Routing
- VLSM and CIDR
- 'Slash' Notation
- X-casting
- Analyze the 3-Way Handshake
- TCP Control Flags
- Sequence and Acknowledgment Numbers
- Connection Establishment
- Connection Termination
- Ports

- IANA Assignments
- Port Numbers and Associated Services
- Trojan Associated Port Numbers
- Network Monitor
- Demo - Using Network Monitor
- Wireshark
- Demo - Installing and Starting Wireshark
- Wireshark Overview
- Demo - Using Wireshark
- TCP Connections
- Demo - Analyzing the Three-way Handshake
- Demo - Analyzing the Session Teardown Process
- Capture and Identify IP Datagrams
- IP Datagram
- Demo - Capturing and Identifying IP Datagrams
- Capture and Identify ICMP Messages
- Demo - Capturing and Identifying ICMP Messages
- Capture and Identify TCP Headers
- TCP Header
- Demo - Capture and Identify TCP Headers
- The UDP Header
- Demo - Working with UDP Headers
- Analyze Packet Fragmentation
- MTUs for Various Media
- Demo - Analyzing Fragmentation
- Analyzing Entire Sessions
- Demo - Complete ICMP Session Analysis
- Demo - Complete FTP Session Analysis
- Lesson 2 Review
- **Lesson 3 - Routers And Access Control Lists**
- Routers And Access Control Lists
- Fundamental Cisco Security
- Modes of Operation
- Navigating the Router
- Configuring Access Passwords
- Other Configuration Options
- SSH Overview
- SSH Configuration Options
- Routing Principles
- ARP Broadcast Between Two Nodes
- Router Returning the ARP Request
- Demo - Performing IP and MAC Analysis
- The Routing Process
- Routed vs. Routing Protocols
- Routing Protocol Metrics
- Routing Protocols

- Demo - Viewing a RIP Capture
- RIPv2
- Demo - Viewing a RIPv2 Capture
- Removing Protocols and Services
- Cisco Discovery Protocol (CDP)
- ICMP
- Creating Access Control Lists
- Access Control List Operation
- The Wildcard Mask
- Wildcard Mask Bits Defined
- Implement Access Control Lists
- Standard Access Control List Command Syntax
- Extended Access Control List Syntax
- ACL Scenarios
- Grant and Denial Examples
- Defending against Attacks with ACLs
- Logging Concepts
- Cisco Logging Options
- Log Priority
- Logging Examples
- ACL and VTY Logging
- Lesson 3 Review
- **Lesson 4 - Designing Firewall Systems**
- Designing Firewall Systems
- Examine Firewall Components
- Firewall Methodologies
- What a Firewall Cannot Do
- Implementation Options for Firewalls
- A Single Packet Filtering Device
- A Screened Host
- A Demilitarized Zone
- Create a Firewall Policy
- Firewall Policy
- Rule Sets and Packet Filters
- Locations of Packet Filters
- The Packet Filter Rules
- Considerations for Packet Filtering Devices
- Ports and Sockets
- Ports in Exchange of a Web Page
- Building Rules for the Firewall
- The Ack Bit
- Stateless and Stateful Packet Inspection
- Stateless Packet Filters
- Stateful Packet Filters
- Stateful Packet Filter Function
- Proxy Server

- Proxy Process
- Proxy Benefits
- Proxy Problems
- The Bastion Host
- Location of a Bastion Host
- Creating a Bastion Host to Run as a Firewall
- The Honeypot
- Honeypot Locations
- Goals of the Honeypot
- Lesson 4 Review
- **Lesson 5 - Configuring Firewalls**
- Configuring Firewalls
- Understanding Firewalls
- Firewalls and the OSI Model
- Common Types of Firewalls
- Building Firewall Rules
- What a Firewall Cannot Do
- Configuring Microsoft ISA Server 2006
- ISA Server 2006
- ISA Server 2006 Versions
- ISA Server 2006 Features
- Demo - Preparing for the ISA Server 2006 Install
- Demo - Install Microsoft ISA Server 2006
- Configuring ISA Server 2006
- ISA Server Management Console
- Demo - Exploring the Microsoft ISA Server 2006 Interface
- Demo - Exporting the Default Configuration
- ISA Server 2006 Firewall Policies
- Processing Firewall Policies
- Demo - Creating a Basic Access Rule
- ISA Server 2006 Access Rule Elements
- Demo - Creating a Protocol Rule Element
- Demo - Creating a User Rule Element
- Demo - Creating a Content Group Element
- Demo - Creating and Modifying Schedule Rule Elements
- Demo - Using Content Types and Schedule Rules
- ISA Server 2006 Network Rule Elements
- Demo - Creating a Network Rule Element
- ISA Server 2006 Publishing Rules
- Demo - Configuring a Web Publishing Rule
- ISA Server 2006 Caching
- Demo - Enabling and Configuring Caching
- Demo - Install Second Loopback Adapter
- Demo - Configure ISA in a Three-Legged DMZ
- Configure ISA Server Monitoring
- Demo - Working with Alerts

- Demo -Working with Reports
- ISA Server 2006 Logging
- Demo - Configuring Logging Options
- Final ISA Server 2006 Options
- Demo - ISA Server 2006 and the Security Configuration Wizard
- Demo - Configuring Packet Prioritization
- IPTables Concepts
- Chain Fundamentals
- Process of the Packets
- The Flow of the Chains
- Configuration Options
- Rule Management
- Rule Creation
- Other Options
- Rule Examples
- Example: Case Study
- Lesson 5 Review
- **Lesson 6 - Implementing IPsec and VPNs**
- Implementing IPsec and VPNs
- Internet Protocol Security
- Modes of Operation
- IPsec Policy Management
- Demo - Examining the MMC
- IPsec Policies
- Demo - Identifying Default IPsec Security Policies
- Demo - Saving a Customized MMC
- Secure Server (Require Security)
- Demo - Examining Security Methods
- Demo - Examining Policy Rules
- IPsec AH Implementation
- Demo - Creating the 1_REQUEST_AH(md5)_only Policy
- Demo - Editing the 1_REQUEST_AH(md5)_only Policy
- Demo - Configuring the Policy Response
- Demo - Configuring the Second Computer
- Demo - Setting Up the FTP Process
- Demo - Implementing the 1_REQUEST_AH(md5)_only Policy
- Demo - Analyzing the Request-only Session
- Demo - Configuring a Request-and-Respond IPsec Session
- Demo - Analyzing the Request-and-Respond Session
- Combining AH and ESP in IPsec
- Demo - Creating the 5_REQUEST_AH(md5)+ESP(des) IPsec Policy and the Response Policy
- Demo - Creating the 5_RESPOND_AH(md5)+ESP(des) IPsec Policy
- Demo - Configuring and Analyzing an IPsec Session Using AH and ESP
- Demo - Implementing the 7_REQUIRE_AH(sha)+ESP(sha+3des) Policy

- Demo - Implementing the 7_RESPOND_AH(sha)+ESP(sha+3des) Policy
- Demo - Implementing and Analyzing an AH(sha) and ESP(sha+3des) IPSec Session
- VPN Fundamentals
- VPN Elements
- IPSec and Tunneling Protocols
- Authentication Header (AH)
- Encapsulating Security Payload (ESP)
- Security Association (SA)
- IPSec Tunnel Mode
- VPN Security
- VPN Implementations and Firewalls
- VPN Authentication
- Configuring a VPN
- Demo - Configuring the VPN Server
- Demo - Configuring VPN Clients
- Lesson 6 Review
- **Lesson 7 - Designing an IDS**
- Designing an IDS
- The Goals of an Intrusion Detection System (IDS)
- IDS Abilities
- Some Intrusion Detection Definitions
- The IDS Matrix
- The Components of an Intrusion Detection System
- Realistic Goals of IDS
- Technologies and Techniques of Intrusion Detection
- Resources on the Network
- Acceptable & Unacceptable Use
- Information Collection and Analysis
- Host-based Intrusion Detection
- Centralized Host-based Design
- Distributed Host-based Design
- Network-based Intrusion Detection
- Network-based Design
- Traditional Network-based Design
- Distributed Network-based Design
- The Analysis
- Interval Analysis
- Real-Time Analysis
- How to Analyze
- How to Use an IDS
- What an Intrusion Detection System (IDS) Cannot Do
- Lesson 7 Review
- **Lesson 8 - Configuring IDS**
- Configuring IDS
- Snort Foundations
- Snort Fundamentals

- Snort Installation
- Snort Commands
- Demo - Installing Snort
- Demo - Initial Snort Configuration
- Demo - Capturing Packets with Snort
- Demo - Capturing Packet Data with Snort
- Demo - Logging with Snort
- Snort as an IDS
- Snort Rules
- Example Rules Using the Rule Header
- Rule Options
- Simple Rule Examples, adding Rule Options
- Snort Rule IDs (SID)
- Demo - Creating a Simple Ruleset
- Demo - Testing the Ruleset
- Rule Options
- Metadata Options
- Adding New Options
- Content Keyword
- Other Keywords
- Pre-configured Rules
- Demo - Examining Rules
- Configuring Snort to Use a Database
- Demo - Editing snort.conf
- Demo - Installing MySQL
- Demo - Creating the Snort Database
- Demo - Creating MySQL User Accounts
- Demo - Testing the New Configuration
- Demo - Configuring Snort as a Service
- Running an IDS on Linux
- Demo - Installing LAMP Components
- Apache and PHP
- Demo - Apache and PHP Test
- Demo - Configure Snort on Linux
- Configuring MySQL for Snort
- Demo - Testing Snort Connectivity to the Database
- Demo - Downloading AD0db and BASE
- Demo - Installing AD0db and BASE
- Demo - Configuring BASE
- Demo - Configuring the Firewall to Allow HTTP
- Demo - Generating Portscan Snort Events
- Demo - Generating Web Snort Events
- Lesson 8 Review
- **Lesson 9 - Securing Wireless Networks**
- Securing Wireless Networks
- Wireless Networking Fundamentals

- Wireless Media
- Radio Wireless Media
- IEEE 802.11
- WLAN Fundamentals
- Ad-hoc Mode
- Infrastructure Mode
- Configuring an Ad-Hoc WLAN
- 802.11 Framing
- Frame Format: 802.11 MAC Frame
- 802.11 Frame Details
- Address Fields Settings
- 802.11 Addressing
- The Addressing of Two Nodes in an Ad Hoc Network
- The Addressing in Infrastructure Mode
- The Addressing of Frames in a Wireless Bridge Network
- Configuring an Access Point
- Configure Infrastructure Clients
- WLAN Threats
- Wireless Security Solutions
- Exclusive OR (XOR)
- The Standard Operation of a Stream Cipher
- The WEP Encryption Process
- The WEP Decryption Process
- Example of the Plaintext/Ciphertext Attack on WEP
- Configuring WEP
- Security Solutions
- WEP and WPA Comparison
- WPA Process Using an Authentication Server
- Configuring WPA2
- Wireless Auditing
- Demo - Installing OmniPeek Personal
- Demo - Viewing OmniPeek Personal Captures
- Demo - Live OmniPeek Personal Captures
- Demo - Analyze Upper Layer Traffic
- Demo - Decrypting WEP
- Wireless PKI
- Example of how TLS Works between a Client and the Authentication Server
- Lesson 9 Review