

ITSY 2071 Tactical Perimeter Defense – SCNS Certification

Course Description:

The Tactical Perimeter Defense (TPD) class is the starting point with the Security Certified Program (SCP). TPD is a required pre-requisite for the SCNP and SCNA certifications. TPD focuses on the critical defensive technologies that are the foundation of securing network perimeters, such as firewalls, intrusion detection, and router security. This course prepares students to work with, and implement, real world security technology.

Prerequisites:

Security+ or equivalent knowledge/experience.

Length of Course:

48-hours.

Course Learning Objectives:

Students will learn how to

- 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.

Rationale:

Information security is today's most critical requirement in IT networks. Security Certified Programs created certifications and curricula to develop and validate skills of computer and network security professional. The SCP courses and certifications are designed not just around knowledge-based theory, like so many others, rather around the actual technical skills required by practitioners.

Texts for the Course: Tactical Perimeter Defense [included]

Evaluation:

Those who participate in class discussions and miss no more than three class meetings will be awarded 4.8 continuing education units. The Student also will be prepared for the SCNS certification. The SCNS certification exam purchase and registration are be the responsibility of the student. The exam may be scheduled and taken anytime following the course at any PearsonVue or Prometric testing centers.

To become SCNS certified, candidates must successfully pass one exam: SC0-451.
[Learn more about SCNS Certification.](#)

Course Content:

Lesson 1: Network Defense Fundamentals

1. Network Defense
2. Defensive Technologies
3. Objectives of Access Control
4. The Impact of Defense
5. Network Auditing Concepts

Lesson 2: Advanced TCP/IP Concepts

1. Analyzing the Three-way Handshake
2. Capturing and Identifying IP Datagrams
3. Capturing and Identifying ICMP Messages
4. Capturing and Identifying UDP Headers
5. Analyzing Packet Fragmentation
6. Analyzing an Entire Session

Lesson 3: Routers and Access Control Lists

1. Fundamental Cisco Security
2. Routing Principles
3. Removing Protocols and Services
4. Creating Access Control Lists
5. Implementing Access Control Lists
6. Logging Concepts

Lesson 4: Designing Firewalls

1. Firewall Components
2. Create a Firewall Policy
3. Rule Sets and Packet Filters
4. Proxy Server
5. The Bastion Host
6. The Honeypot

Lesson 5: Configuring Firewalls

1. Understanding Firewalls
2. Configuring Microsoft ISA Server 2006
3. IPTable Concepts
4. Implementing Firewall Technologies

Lesson 6: Implementing IPsec and VPNs

1. Internet Protocol Security
2. IPsec Policy Management
3. IPsec AH Implementation
4. Combining AH and ESP in IPsec
5. VPN Fundamentals
6. Tunneling Protocols
7. VPN Design and Architecture
8. VPN Security
9. Configuring a VPN

Lesson 7: Designing and Intrusion Detection System

1. The Goals of an Intrusion Detection System
2. Technologies and Techniques of Intrusion Detection
3. Host-based Intrusion Detection
4. Network-based Intrusion Detection
5. The Analysis
6. How to Use an IDS
7. What an IDS Cannot Do

Lesson 8: Configuring an IDS

1. Snort Foundations
2. Snort Installation
3. Snort as an IDS
4. Configuring Snort to Use a Database
5. Running an IDS on Linux

Lesson 9: Securing Wireless Networks

1. Wireless Networking Fundamentals
2. Wireless LAN (WLAN) Fundamentals
3. Wireless Security Solutions
4. Wireless Auditing
5. Wireless Trusted Networks