Course Summary: Tactical Perimeter Defense

Overview

The Tactical Perimeter Defense course is designed to provide network administrators and certification candidates with hands-on tasks on the most fundamental perimeter security technologies. The network perimeter is often the first line of defense in an organization's network. This course covers the issues every administrator must be aware of to protect their network. .

Prerequisite

Before you begin the SCNS certification track, it is recommended that, at a minimum, you have attained CompTIA's Security+ certification or have equivalent training along with additional hands-on experience. The Tactical Perimeter Defense course and it's SCNS certification exam build on concepts and skills learned in the Security+ certification.

Course Objectives

- 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.

Lesson 1: Network Defense Fundamentals

In this lesson you will be introduced to the core concepts of network security. You will examine the technologies of defending a network, and how those technologies may be used to create a layered defense of the network. You will also identify the foundations of network auditing.

Topics: Describe the five keys of network security; Defensive technologies in network defense; Creating a layered defense and its effect on the performance of the network; Access control method objectives; Network auditing concepts

Tasks: Identifying Non-repudiation Issues, Describing the Layers of a Defended Network, Describing the Challenge Response Token Process, Describing the Problems of Additional Layers of Security, Describing Network Auditing

---

Lesson 2: Advanced TCP/IP

There is one primary set of protocols that runs networks and the Internet today. In order to manage the security of a network, you must become familiar with the details of how TCP/IP functions, including core concepts, such as addressing and subnetting. We also discuss advanced concepts such as session establishment and packet analysis.

Topics: Define the core concepts of TCP/IP, Analyze sessions of TCP, Analyze the protocols of TCP, IP, ICMP, UDP, discuss fragmentation, and complete a full session analysis.

Tasks: Layering and Address Conversions, Routers and Subnetting, Using Network Monitor, Installing and starting Wireshark, Using Wireshark, Analyzing the Three-way Handshake, Analyzing the Session Teardown Process, Capturing and Identifying IP Datagrams, Capturing and Identifying ICMP Messages, Capturing and Identifying TCP Headers, Working with UDP Headers, Analyzing Fragmentation, Performing a Complete ICMP Session Analysis, Performing a Complete FTP Session Analysis

Lesson 3: Routers and Access Control Lists
In this lesson you will be introduced to the functioning of routers and routing protocols. The examples in this lesson are shown on Cisco Routers, specifically the 2500 series. You will examine the issues of securing routers and routing protocols. You will remove unneeded services and create access control lists to manage and secure the network. The lesson ends with the creation of logging options on the Cisco router.

Topics: Routing Principles, Fundamental router security configuration, Removing services and protocols, the function and implementation of Access Control Lists on a Cisco router and logging on a Cisco router.

Tasks: Configuring Passwords, Configuring Login Banners, Configuring SSH on a Router, Configuring the SSH Client, Performing IP and MAC Analysis, Viewing a RIP Capture, Viewing a RIPv2 Capture, Turning Off CDP, Hardening ICMP, Removing Unneeded Services, Creating Wildcard Masks, Creating Access Control Lists, Configuring Buffered Logging, Configuring Anti-spoofing Logging

Lesson 4: Designing Firewalls
In this lesson you will be introduced to the concepts and technologies used in designing firewall systems. You will identify the methods of implementing firewalls in different scenarios using different technologies. The strategies and concepts in this lesson are important in understanding later lessons.

Topics: Firewall design and implementation principles, creating firewall policies, proxy servers, using rule sets for packet filtering, bastion hosts in relation to network security, and the function honeypots.

Tasks: Firewall Planning, Creating a Simple Firewall Policy, Firewall Rule Creation, Diagram the Proxy Process, Describing a Bastion Host, and Honeypot Configuration.

Lesson 5: Configuring Firewalls
In this lesson you will first review firewalls from a conceptual viewpoint to learn about the types of firewalls, how each of these types work, and what protection they can provide for your network. After you understand the foundational concepts you will go through a series of exercises to actually implement two different firewall solutions using Microsoft’s Internet Security and Acceleration server, which runs on top of the Windows platform and IPTables which runs on top of the Linux platform. This will provide you with the practical working knowledge to implement a firewall in your network environment.

Topics: Standard firewall functionality and common implementation practices, Microsoft ISA Server 2006, Linux IPTables, application of firewall concepts and practices.

Tasks: Install Microsoft ISA Server 2006, Exploring the Microsoft ISA Server 2006 Interface, Exporting the Default Configuration, Creating a Basic Access Rule, Creating a Protocol Rule Element, Creating a User Rule Element, Creating a Content Group Rule Element, Creating and Modifying Schedule Rule Elements, Using Content Types and Schedules in Rules, Creating a Network Rule Element, Configuring a Web Publishing Rule, Enabling and Configuring Caching, Install Second Microsoft Loop Back Adapter and Assign an IP Address, Working with Alerts, Working with Reports, Configuring Logging Option, Securing ISA Server 2006 with the Security Configuration Wizard, Configuring Packet Prioritization, Uninstalling ISA Server 2006, Working with Chain Management

Lesson 6: Implementing IPSec and VPNs
In this lesson you will be introduced to the concepts of IPSec. You will examine and configure the Microsoft Management Console and identify the predefined IPSec policies in Windows Server 2003. You will create new policies and implement IPSec to specifically use AH, ESP, or both in Transport Mode. Finally, you will analyze IPSec traffic in Network Monitor.

In this lesson, you will also examine Virtual Private Networks (VPNs) and some of the security issues related to them.

Topics: IPSec in a network environment, IPSec policy management, IPSec AH Configurations, IPSec AH and ESP configurations, VPN business drivers and technology components, VPN design and implementation issues, VPN and firewall architecture VPN options in Windows 2003, additional tunneling protocols,

Tasks:
Describing the Need for IPSec, Examining the MMC, Identifying Default IPSec Security Policies, Saving a Customized MMC, Examining Security Methods, Examining Policy Rules, Creating various AH and ESP Policies, Configuring the Policy Response, Configuring the Second Computer, Setting Up the FTP Process, Analyzing the Request-only Session, Configuring a Request-and-Respond IPSec Session, Analyzing the Request-and-Respond Session, IPSec Session, Assigning Tunneling Protocols, Assigning Additional Tunneling Protocols, Examining VPN-related RFCs, Viewing Firewall-related RFCs, Configuring the VPN Server, Configuring VPN Clients, Establish the VPN.

Lesson 7: Designing an Intrusion Detection System
In this lesson you will be introduced to the concepts surrounding one of the areas critical to the defensive network protection scheme—the Intrusion Detection System. This system, in conjunction with the firewall technologies in place, is the basis for a very solidly defended network. The Intrusion Detection System will be used to detect when an intruder is attempting penetration of the network or tampering with the firewalls.

Topics: Technologies and techniques of intrusion detection, Host-based IDS, Network-based IDS, Intrusion Detection analysis, What an IDS cannot do

Tasks: Describing Alarms, Discussing IDS Concepts, Describing Centralized Host-based Intrusion Detection, Discussing Sensor Placement, Discussing Data Analysis, Discussing Intrusion Detection Uses, Discussing Incident Investigation.

Lesson 8: Configuring an IDS
In this lesson you will implement IDS. There are many different types of IDSes, and for this lesson, you will use perhaps the most famous free IDS tool—Snort. Snort is a tool that is designed to monitor TCP/IP networks, looking for suspicious traffic and direct network attacks. It enables system administrators to collect enough data to make informed decisions on the best course of action in the event that an intrusion is detected.

Topics: Snort as an IDS, Snort on a stand-alone computer, Snort rules, Snort IDS and a MySQL database, IDS on Linux.

Tasks: Installing Snort, Initial Snort Configuration, Capturing Packets with Snort, Capturing Packet Data with Snort, Logging with Snort, Creating a Simple Ruleset, Testing the Ruleset, Examining Pre-configured Rules, Examining DDoS Rules, Examining Backdoor Rules, Examining Web Attack Rules, Examining IIS Rules, Editing Snort.Conf, Installing MySQL, Creating the Snort Database, Creating MySQL User Accounts, Testing the New Configuration, Configuring Snort as a Service, Installing LAMP

Components, Apache and PHP Test, Configure Snort on Linux, Configuring MySQL for Snort, Testing Snort Connectivity to the Database, Downloading ADOdb and BASE, Installing ADOdb and BASE, Configuring BASE, Configuring the Firewall to Allow HTTP, Generating Portscan Snort Events, Generating Web Snort Events

---

Lesson 9: Securing Wireless Networks
In this lesson you will learn to implement and secure a wireless network. You will examine the components of the network, and how to configure these components. You will detail the security options required for making wireless networks part of your trusted enterprise. You will perform wireless network analysis using leading wireless tools, and examine how to create a trusted wireless network.

Topics: Wireless networking and Wireless LANs, Wireless security solutions, Wireless Network Audits, Wireless Trusted Network, Wireless PKI.

Tasks: Examining Satellite Orbits, Choosing a Wireless Media, Installing the Linksys WPC54G WNIC, Installing the Netgear WPN511, Enabling the Ad-Hoc Network, Installing the Linksys WAP54G Access Point, Configuring the Linksys Client, Configuring the Netgear Client, Installing the Netgear WPN824 Access Point, Configuring WEP on the Network Client, Configure WPA2 on the Access Point, Configuring WPA2 on the Network Client, Installing NetStumbler, Identifying Wireless Networks, Installing OmniPeeK Personal, Viewing OmniPeek Personal Captures, Viewing Live OmniPeek Personal Captures, Analyze Upper Layer Traffic, Decrypting WEP, Choosing a Wireless Trusted Network

---

Related SCP Exam: ***SC0-451 – Tactical Perimeter Defense***

Examination Domain	Percentage of Exam
1.0 – Network Defense Fundamentals	5%
2.0 - Hardening Routers and Access Control Lists	10%
3.0 – Implementing IPSec and Virtual Private Networks	10%
4.0 – Advanced TCP/IP	15%
5.0 – Securing Wireless Networks	15%
6.0 - Designing and Configuring Intrusion Detection Systems	20%
7.0 - Designing and Configuring Firewall Systems	25%
Total	**100%**
