ASM Educational Center (ASM) *Est. 1992*

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | **Phone**: 301-984-7400 | **Fax**: 301-984-7401
Web: www.asmed.com | **E-mail**: info@asmed.com

Authorized SCNS Security Certified Network Specialist Boot Camp

Course Outline

LESSON 1: NETWORK DEFENSE FUNDAMENTALS

- Network Defense
- Defensive Technologies
- Objectives of Access Control
- The Impact of Defense
- 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

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

- Fundamental Cisco Security
- Authentication and Authorization
- Configuring Access Passwords
- Routing Principles
- Removing Protocols and Services
- Creating Access Control Lists
- Implementing Access Control Lists
- Logging Concepts
- 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

- Firewall Components
- Create a Firewall Policy
- Rule Sets and Packet Filters
- Proxy Server
- The Bastion Host
- The Honeypot
- Tasks:
    - Firewall Planning
    - Creating a Simple Firewall Policy
    - Firewall Rule Creation
    - Diagram the Proxy Process
    - Describing a Bastion Host
    - Honeypot Configuration

LESSON 5: CONFIGURING FIREWALLS

- Understanding Firewalls
- Configuring Microsoft ISA Server
- IPTables Concepts
- Implementing Firewall Technologies
- Tasks:
    - Install Microsoft ISA Server
    - Exploring the Microsoft ISA Server 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 with the Security Configuration Wizard
  - Configuring Packet Prioritization
  - Uninstalling ISA Server
  - Working with Chain Management

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
- 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 the 1_REQUEST_AH(md5)_only Policy
  - Editing the 1_REQUEST_AH(md5)_only Policy
  - Configuring the Policy Response
  - Configuring the Second Computer
  - Setting Up the FTP Process
  - Implementing the 1_REQUEST_AH(md5)_only Policy
  - Analyzing the Request-only Session
  - Configuring a Request-and-Respond IPSec Session
  - Analyzing the Request-and-Respond Session
  - Creating the 5_REQUEST_AH(md5)+ESP(des) IPSec Policy
  - and the Response Policy
  - Creating the 5_RESPOND_AH(md5)+ESP(des) IPSec Policy
  - Configuring & Analyzing an IPSec Session Using AH & ESP
  - Implementing the 7_REQUIRE_AH(sha) +ESP(sha+3des) Policy

- Implementing the 7_RESPOND_AH(sha) +ESP(sha+3des) Policy
- Implementing and Analyzing an AH(sha)
- and ESP(sha+3des) 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
- Restoring the Classroom Setup

LESSON 7: DESIGNING AN INTRUSION DETECTION SYSTEM

- The 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
- 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

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

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