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 SCNP Security Certified Network Professional Boot Camp

Course Outline

LESSON 1: CRYPTOGRAPHY AND DATA SECURITY

- History of Cryptography
- Math and Algorithms
- Private Key Exchange
- Public Key Exchange
- Message Authentication
- Linux Filesystem and Navigation
- General Secure System Management
- User and Filesystem Security Administration
- Network Interface Configuration
- Security Scripting
- Useful Linux Security Tools
- Tasks:
    - Using Historical Crypto Systems
    - Polybius Cryptography
    - Installation of CrypTool
    - Classical Encryption Analysis
    - DES ECB and CBC Analysis
    - Private Key Exchange
    - Finding Diffie-Hellman Public Keys
    - Performing RSA Encryption and Decryption
    - Create Your RSA Key Pair
    - Creating RSA Keys
    - Encrypting and Decrypting with RSA
    - Cracking an RSA Encrypted Message
    - Encryption as Authentication

LESSON 2: HARDENING LINUX COMPUTERS

- Linux Filesystem and Navigation
- General Secure System Management
- User and Filesystem Security Administration
- Network Interface Configuration
- Security Scripting
- Useful Linux Security Tools
- Tasks:

  - Navigating in Linux
  - Exploring Man Pages
  - Exploring YaST
  - Viewing System Information
  - Modifying Process Behavior
  - Password Protection of Linux Startup
  - Stopping Unneeded Services
  - Modifying Process Runlevels
  - Mounting a Device
  - Installing Webmin with RPM
  - Installing John the Ripper from Source Code Archive
  - Updating your system with YOU (Yast Online Update) Tool
  - Creating and Modifying Users and Groups
  - Changing User Contexts with su
  - Viewing the Password Files
  - Managing Passwords
  - Viewing File Details
  - Creating Object Ownerships
  - Assigning Permissions
  - Verifying Permissions
  - Configuring umask Settings
  - Using PAM with vsFTPd
  - Logging Recent Login Activity
  - Configuring network interfaces
  - Managing Telnet with Xinetd
  - Controlling Access with TCP Wrappers
  - Demonstration of the Vulnerabilities of FTP and Telnet
  - Configuring an SSH Server
  - Configuring an SSH Client
  - Preventing root SSH logins by Modifying the sshd_config File
  - Using SCP to Securely Transfer Files
  - Sharing Data with NFS
  - Verifying Export Permissions
  - Configuring the Samba Server
  - I/O Redirection
  - Demonstration of vi and emacs
  - Writing simple shell scripts
  - Installing and Exploring Bastille
  - Starting Tripwire

LESSON 3: HARDENING WINDOWS SERVER 2003

- Windows 2003 Infrastructure Security
- Windows 2003 Authentication
- Windows 2003 Security Configuration Tools
- Windows 2003 Resource Security
- Windows 2003 Auditing and Logging
- Windows 2003 EFS
- Windows 2003 Network Security
- Tasks:
  - Configuring a Custom MMC and GPO
  - Editing a GPO

- Implementing Multiple GPOs
- Configuring NTLMv2 Authentication
- Securing Administrator Account Access
- Testing Administrative Access
- Verifying Password Requirements
- Analyzing Default Password Settings of Security Templates
- Creating a Custom Security Template
- Investigating the Security Configuration and Analysis Snap-In
- Implementing the Template
- Analyzing the Current Security Settings of the Local System
- Compromising NTFS Security
- Setting Registry Permissions
- Exporting Registry Information
- Blocking Registry Access
- Installing Security Configuration Wizard
- Using the Security Configuration Wizard
- Enabling Auditing
- Logging SAM Registry Access
- Viewing the Registry Audit
- Creating Events
- Viewing Event Logs
- Encrypting Files
- Investigating Printer Spooler Security
- Configuring TCP/IP in the Registry
- Configuring Port and Protocol Filtering
- Enabling Windows Firewall
- Configuring Windows Firewall
- Configure Server 2003

LESSON 4: ATTACK TECHNIQUES

- Network Reconnaissance
- Mapping the Network
- Sweeping the Network
- Scanning the Network
- Vulnerability Scanning
- Viruses, Worms, and Trojan Horses
- Gaining Control Over the System
- Recording Keystrokes
- Cracking Encrypted Passwords
- Revealing Hidden Passwords
- Social Engineering
- Gaining Unauthorized Access
- Hiding Evidence of an Attack
- Performing a Denial of Service
- Tasks:
    - Using Windows Tracing Tools
    - Using VisualRoute
    - Using SuperScan
    - Installing Linux Tools
    - Using Nmap
    - Using SuperScan

- Using nmap to Identify an Operating System
- Using nmap Front End
- Installing Nessus
- Configuring Nessus Scan
- Custom Nessus Scanning
- Network Scanning
- Windows to Windows Netcat
- Linux to Windows Netcat
- Using Software Keystroke Logging
- Using a Keystroke-logging Keyboard
- Installing LCP
- Creating User Accounts
- Cracking Passwords With LCP
- Revealing Hidden Passwords
- Discussing Social Engineering Examples
- Reviewing the Social Engineering Case Study
- Flooding with Udpflood

LESSON 5: SECURITY ON THE INTERNET AND THE WWW

- Describing the Major Components of the Internet
- Securing DNS Services
- Describing Web Hacking Techniques
- Tasks:
    - Defining Internet Components
    - Identifying Weak Points of the Internet
    - Famous Major Disruptions
    - Installing a DNS Server on Windows Server 2003
    - Creating a Primary Reverse Lookup Zones
    - Creating a Primary Forward Lookup Zone
    - Creating A and PTR Records in the DNS
    - Enabling Zone Transfers
    - Reviewing Pollution and Recursion Settings
    - Creating Secondary Zones
    - Filtering the Interface to Accept Only DNS Traffic
    - Creating an Active Directory Integrated Zone
    - Setting up a Stub Zone
    - Identifying Web Hacking Techniques
    - Installing IIS 6.0
    - Implementing a Website
    - Starting and Stopping the Web Server
    - Investigating IIS Security
    - Controlling Performance Settings
    - Controlling the Home Directory Settings
    - Controlling Access Settings
    - Installing the MBSA
    - Scanning a System Looking for Vulnerabilities
    - Applying a Patch to Mitigate an IIS 6.0 Vulnerability
    - Installing Apache 2.x on Suse Linux 10.0
    - Basic Configuring of the Apache Web Server
    - Securing your Apache Web Server – Installing Patches
    - Securing your Apache Web Server – Disabling Modules

  - Identifying User Vulnerabilities and Internet Security
  - Installing Internet Explorer 7
  - Viewing the General Settings for Your Browser
  - Viewing the Advanced Settings for Your Browser
  - Viewing the Zone Settings for Your Browser
  - Implementing Default Security Levels for Zones
  - Viewing Detailed Settings for the Security Level Low
  - Viewing Detailed Settings for the Security Level High
  - Adding Sites to a Zone
  - Viewing Cookie Handling Settings
  - Viewing Content Ratings
  - Properties of the Certificates Section
  - Viewing the Handling of Personal Information by a Browser
  - Dealing with Pop-ups
  - Basic Security Settings to Take Care of With Your Email Client

LESSON 6: PERFORMING A RISK ANALYSIS

- Concepts of Risk Analysis
- Methods of Risk Analysis
- The Process of Risk Analysis
- Techniques to Minimize Risk
- Continuous Risk Assessment
- Tasks:
  - Defining Risks and Threats for ABC, Inc
  - Performing Risk Analysis for ABC, Inc.
  - Defining Risk Analysis Roles for ABC, Inc
  - Minimizing the Risk of ABC, Inc
  - Investigating Continual Risk Assessment for ABC, Inc

LESSON 7: CREATING A SECURITY POLICY

- Concepts of Security Policies
- Policy Design
- Policy Contents
- An Example Policy
- Incident Handling and Escalation Procedures
- Partner Policies
- Tasks:
  - Task 7A-1 Defining the Benefits of a Security Policy for ABC, Inc
  - Designing a Security Policy for ABC, Inc
  - Creating a Physical Security Policy for ABC, Inc
  - Creating an Acceptable Use Statement for ABC, Inc
  - Describing Escalation Procedures for ABC, Inc
  - Creating the ABC, Inc.
  - Partner Policy

LESSON 8: ANALYZING PACKET SIGNATURES

- Signature Analysis
- Common Vulnerabilities and Exposures (CVE)
- Signatures
- Normal Traffic Signatures
- Abnormal Traffic Signatures

- Tasks:
  - Investigating CVE Benefits
  - Discussing IP Spoofing
  - Analyzing FTP Signatures
  - Analyzing a Trojan Horse Scan