

Strategic Infrastructure Security

- **Course Number:** SCPSIS
- **Length:**

Certification Exam

There are no exams currently associated with this course.

Course Overview

This course picks up right where Tactical Perimeter Defense leaves off. The second course in the SCP line-up leads to a certification of Security Certified Network Professional (SCNP). It will give a network administrator the additional hands on skills needed to protect their network from the inside out. This course teaches you about prevention techniques as well as giving the candidate an understanding of risk analysis and security policy creation in a blended technology environment. This course is the official training for the SCNP exam and is designed to validate the foundational skills required by security professionals. These skills include, but are not limited to:

- Cryptography
- Hardening Linux Computers
- Hardening Windows Computers
- Ethical Hacking Techniques
- Security on the Internet and World Wide Web
- Performing a Risk Analysis
- Creating a Security Policy
- Analyzing Packet Signatures

Prerequisites

Before taking this course, candidates must first take Tactical Perimeter Defense.

Audience

This course is intended for those wanting to achieve the SCNP certification.

Course Outline

- **Lesson 1 - Cryptography and Data Security**
- Cryptography and Data Security
- History of Cryptography
- The number lock analogy
- Cryptography Terminology
- Caesar and Character Substitution
- Linguistic Patterns: frequency

- Polyalphabetic Ciphers
- Vigenère chart, to be used with a keyword
- Other Ciphers
- Others
- Rotor Machines
- Lessons learned from cracking Enigma
- Introduction to Cryptool
- Demo - Installing Cryptool
- Demo - Classical Encryption Analysis
- Topic 1B: Math and Algorithms
- Relatively Prime
- Mod Math
- Mod Math Examples
- Logic Operations
- Topic 1C: Private Key Exchange
- Keys
- Symmetric Keys
- DES in CBC mode
- Feistel structure
- Symmetric Algorithms
- Digital Encryption Standard (DES)
- DES Modes of Operation
- Demo - DES ECB and CBC Analysis
- Triple DES
- Advanced Encryption Standard: Rijndael
- Key Management
- Topic 1D: Public Key Exchange
- Asymmetric key cryptography
- The basic process of asymmetric key cryptography
- Public key cryptography requirements
- What is 'computationally infeasible'?
- Asymmetric vs. Symmetric - Comparison
- Diffie-Hellman
- Diffie-Hellman Example
- RSA
- RSA Example
- RSA Example, encrypt
- Demo - Create Your RSA Key Pair
- Demo - Creating RSA Keys
- Demo - Encrypting and Decrypting with RSA
- Demo - Cracking an RSA Encrypted Message
- Public Key Management
- Topic 1E: Message Authentication
- Lesson 1 Review
- **Lesson 2 - Hardening LINUX**
- Hardening LINUX

- Demo - Navigating in Linux
- Demo - Exploring YaST
- Topic 2B - Investigate Process Management in Linux
- Demo - Viewing System Information
- Demo - Modifying Process Behavior
- System Startup / Shutdown Security
- Demo - Password Protection of Linux Startup
- Topic 2B - Investigate Process Management in Linux (Cont.)
- Demo - Stopping Unneeded Services
- Demo - Modifying Process Runlevels
- Topic 2B - Investigate Process Management in Linux (Cont..)
- Demo - Mounting a Device
- Topic 2B - Investigate Process Management in Linux (Cont...)
- Demo - Installing Webmin via RPM
- Demo - Installing John the Ripper from Source Code
- Topic 2C – Manage Linux User and Filesystem Security
- Demo - Creating and Modifying Users and Groups
- Topic 2C – Manage Linux User and Filesystem Security (Cont.)
- Demo - Changing User Contexts With SU
- Topic 2C – Manage Linux User and Filesystem Security (Cont..)
- Shadow Password File
- Managing Passwords
- Demo - Viewing the Password Files
- Demo - Managing Passwords
- Topic 2C – Manage Linux User and Filesystem Security (Cont...)
- Demo - Viewing File Details
- File and Directory Permissions
- Five characters in the permission fields
- Binary, Octal Numbers, and Permissions
- Topic 2C – Manage Linux User and Filesystem Security (Cont....)
- Demo - Creating Object Ownership
- Demo - Assigning Permissions
- Demo - Verifying Permissions
- Umask Settings
- Demo - Configuring umask Settings
- Topic 2C – Manage Linux User and Filesystem Security (Cont.....)
- Demo - Using PAM with vsFTP
- Topic 2C - Manage Linux User and Filesystem Security (Cont.....)
- Demo - Logging Recent Login Activity
- Topic 2D - Manage Linux Security
- Demo - Configuring Network Interfaces
- Topic 2D - Manage Linux Security (Cont.)
- Demo - Managing Telnet with Xinetd
- Topic 2D - Manage Linux Security (Cont..)
- Demo - Controlling Access with TCP Wrappers
- Topic 2D - Manage Linux Security (Cont...)

- Demo - Configuring an SSH Server
- Demo - Configuring an SSH Client
- Topic 2D - Manage Linux Security (Cont....)
- Demo - Using SCP to Securely Transfer Files
- Demo - Preventing root SSH logins by Modifying the sshd_config file
- Securing Network Services
- Demo - Sharing Data with NFS
- Topic 2D - Manage Linux Security (Cont.....)
- Demo - Verifying Export Permissions
- Topic 2D - Manage Linux Security (Cont.....)
- Demo - Configuring the Samba Server
- Topic 2E - Create Scripts for Linux
- Demo - I/O Redirection
- Shell scripts
- Simple script examples
- Demo - Writing Simple Shell Scripts
- Topic 2F - Harden Linux
- Demo - Installing and Exploring Bastille
- Topic 2E - Create Scripts for Linux (Cont.)
- Lesson 2 Review
- **Lesson 3 - Hardening Windows**
- Hardening Windows
- Topic 3A – Examine the concepts of Windows 2003 infrastructure security
- Demo - Configuring a Custom MMC and GPO
- Demo - Editing a GPO
- Topic 3B – Examine the fundamentals of authentication in Windows 2003
- Demo - Configuring NTLMv2 Authentication
- Topic 3C – Implement Windows 2003 security configuration tools
- Demo - Securing Administrator Account Access
- Demo - Testing Administrative Access
- Group Policies
- Demo - Verifying Password Requirements
- Security Templates
- Demo - Analyzing Default Password Settings of Security Templates
- Demo - Creating a Custom Security Template
- Topic 3C - Implement Windows 2003 security configuration tools (Cont.)
- Demo - Investigating the Security Configuration and Analysis Snap-In
- Demo - Implementing the Template
- Demo - Analyzing the Current Security Settings of the Local System
- Topic 3D – Secure Windows 2003 resources
- Demo - Setting Registry Permissions
- Demo - Exporting Registry Information
- Demo - Blocking Registry Access
- Topic 3D – Secure Windows 2003 resources (Cont.)
- Demo - Installing Security Configuration Wizard
- Demo - Using the Security Configuration Wizard

- Topic 3E – Configure Windows 2003 auditing and logging
- Demo - Enabling Auditing
- Demo - Logging SAM Registry Access
- Topic 3E – Configure Windows 2003 auditing and logging (Cont.)
- Demo - Viewing the Registry Audit
- Topic 3E - Configure Windows 2003 auditing and logging (Cont..)
- Demo - Creating Events
- Demo - Viewing Event Logs
- Topic 3F - Examine and configure EFS on Windows 2003
- Demo - Encrypting Files
- Topic 3G - Examine the methods of securing network communications in a Windows 2003 network
- Demo - Configuring TCP/IP in the Registry
- Topic 3G - Examine the methods of securing network communications in a Windows 2003 network (Cont.)
- Demo - Configuring Port and Protocol Filtering
- Topic 3G - Examine the methods of securing network communications in a Windows 2003 network (Cont..)
- Demo - Enabling Windows Firewall
- Demo - Configuring Windows Firewall
- Demo - Configure Server 2003
- Lesson 3 Review
- **Lesson 4 - Attack Technique**
- Attack Techniques
- Topic 4A - Network Reconnaissance
- Information Learned in the Whois Lookup
- Topic 4B - Mapping the Network
- Demo - Using Windows Tracing Tools
- Using Graphical Tracing Tools
- Demo - Using VisualRoute
- Topic 4C: Sweeping the Network
- Ping Sweep Tools
- SuperScan 3.0 in default mode, before a scan begins
- Demo - Using Super Scan
- Topic 4D: Scanning the Network
- Demo - Installing Linux Tools
- Demo - Using Nmap
- Demo - Using SuperScan
- Identifying the Operating System and O/S Version
- Demo - Using Nmap to Identify an Operating System
- Demo - Using Nmap Front End
- Topic 4E - Perform Vulnerability Scanning
- Demo - Installing Nessus
- Topic 4E - Perform Vulnerability Scanning (Cont.)
- Demo - Configuring Nessus Scan
- Demo - Custom Nessus Scanning

- Demo - Network Scanning
- Topic 4F - Viruses, Worms, & Trojan Horses
- The Trojan Horse
- Famous Trojans
- Topic 4G - Gain Control over a Network System
- Demo - Windows to Windows Netcat
- Demo - Linux to Windows Netcat
- Topic 4H - Record Keystrokes
- Demo - Using Software Keystroke Logging
- Topic 4I - Crack Encrypted Passwords
- Topic 8J: Reveal Hidden Passwords
- Demo - Revealing Hidden Passwords
- Topic 4K: Social Engineering
- Topic 4L: Perform a Denial of Service
- Demo - Flooding with Udpflood
- Lesson 4 Review
- **Lesson 5 - Security on the Internet and the WWW**
- Security on the Internet and the WWW
- Major Components of the Internet
- Weak Points of the Internet
- Topic 5B - Secure DNS Servers
- Demo - Installing a DNS Server on Windows Server 2003
- Topic 5B - Secure DNS Servers (Cont.)
- Demo - Creating a Primary Reverse Lookup Zone
- Demo - Creating a Primary Forward Lookup Zone
- Demo - Creating A and PTR Records in the DNS
- Demo - Enabling Zone Transfers
- Demo - Reviewing Pollution and Recursion Settings
- Demo - Filtering the Interface to Accept Only DNS Traffic
- Topic 5B - Secure DNS Servers (Cont..)
- Best Practices for DNS Hardening
- Topic 5C - Identify attack points on the Internet, and Secure Web Servers
- IIS Security
- Demo - Installing IIS 6.0
- Demo - Implementing a Website
- Demo - Starting and Stopping the Web Server
- Topic 5C - Identify attack points on the Internet, and Secure Web Servers (Cont.)
- Demo - Investigating IIS Security
- Demo - Controlling Performance Settings
- Topic 5C - Identify attack points on the Internet, and Secure Web Servers (Cont..)
- Demo - Install the MBSA and Scan a system for vulnerabilities
- Demo - Applying a Patch to Mitigate and IIS 6.0 Vulnerability
- Topic 5C - Identify attack points on the Internet, and Secure Web Servers (Cont...)
- Demo - Installing Apache 2.x on SuSe Linux 10.0
- Demo - Basic Configuration of the Apache Web server
- Demo - Securing your Apache Web Server - Disabling Modules

- Apache Best Practices
- Topic 5D - Secure Internet Users
- Demo - Installing Internet Explorer 7.0
- Demo - Viewing the General Settings for Your Browser
- Demo - Viewing the Advanced Settings
- Default Security Settings
- Demo - Examine Security Levels for Zones
- Demo - Adding Sites to a Zone
- Other Features
- Email Security
- Demo - Basic Security Settings to Take Care of With Your Email Client
- Lesson 5 Review
- **Lesson 6 - Risk Analysis**
- Risk Analysis
- Topic 6A - Concepts of Risk Analysis
- Predicting Risk
- Quantifying Risk
- Minimize or Mitigate Risk
- Costs Versus Protection
- What is at Risk?
- What is a Threat?
- Vulnerability Analysis
- Likelihood of Occurrence
- Common Threats
- Topic 6B - Methods of Risk Analysis
- Qualitative Risk Analysis
- Facilitated Risk Analysis Process (FRAP)
- Vulnerability Levels
- Impact Levels
- Replacement Models
- Topic 6C: The Process of Risk Analysis
- Stage One: Inventory
- Stage Two: Threat Assessment
- Stage Three: Evaluation of Control
- Stage Four: Management
- Stage Five: Monitoring
- An Alternative Method
- General Techniques to Minimize Risk
- General Techniques
- Specific Minimization Techniques
- Topic 6E - Continual Risk Analysis
- Continuous Risk Assessment Process
- Security Technology Management
- Vulnerability Management
- Exploitation Management
- Systems Availability

- Lesson 6 Review
- **Lesson 7 - Security Policy**
- Security Policy
- Topic 7A - Concepts of Security Policies
- Policy Benefits
- How to Start
- A Question of Trust
- Policy Committee
- Are Policies Political?
- Topic 7B - The Policy Design
- Policy Standards
- 10 Sections
- Topic 7C - Policy Contents
- The Acceptable Use Policy
- The User Account Policy
- The Remote Access Policy
- The Information Protection Policy
- The Network Connection Policy
- The Strategic Partner Policy
- The Privileged Access Policy
- The Password Policy
- The Internet Access Policy
- The Internet Policy
- Miscellaneous Policies
- Topic 7D - An Example Policy
- Samples
- Topic 7E - Incident Handling and Escalation Procedures
- Sample Escalation Procedures for Security Incidents
- Incident Handling
- Topic 7F - Partner Policies
- Sample Partner Connection Policy
- Lesson 7 Review
- **Lesson 8 - Analyzing Packet Signatures**
- Analyzing Packet Signatures
- Topic 8A - Describe the Concepts of Signature Analysis
- Common Vulnerabilities and Exposures (CVE)
- CVE Classification
- Signatures
- Some Common Exploits
- Some Common Reconnaissance Scans
- Some Common DoS Attacks
- Topic 8D - Normal Traffic Signatures
- Ping Signatures
- Demo - Ping Signatures
- Web Signatures
- FTP Signatures

- Telnet Signature
- Topic 8E - Abnormal Traffic Signatures
- Ping Sweep
- Port Scan
- Backdoor Signatures
- Demo - Trojan Scans
- Nmap Scans
- Demo - Nmap scans
- Lesson 8 Review
- Course Closure