



Strategic Infrastructure Security

Duration:

Traditional Instructor Led Learning - 5.00 Day(s)

Mentored Learning - Flexible

Overview:

The Strategic Infrastructure Security course is designed to follow the hands-on skills utilized in the Tactical Perimeter Defense course and continues with hardening of strategic elements of your infrastructure, such as your Windows and Linux servers

At Course Completion:

- Detail the core issues of cryptography, including public and private key.
- Harden SuSe Linux 10 Server computers.
- Harden Windows Server 2003 computers.
- Utilize ethical hacking attack techniques.
- Secure DNS and web servers, and examine Internet and WWW security.
- Perform a risk analysis.
- Create a security policy.
- Analyze packet signatures.

Prerequisite(s) or equivalent knowledge:

Tactical Perimeter Defense

Outline:

Lesson 1: Cryptography

- History of Cryptography
- Math and Algorithms
- Private Key Exchange
- Public Key Exchange
- Message Authentication

Lesson 2: Hardening Linux Computers

- Linux Filesystem and Navigation
- Secure System Management
- User and Filesystem Security Administration
- Secure Network Management
- Security Scripting
- Using Linux Security Tools

Lesson 3: Hardening Windows Server 2003

- Windows Server 2003 Infrastructure Security
- Windows Server 2003 Authentication
- Windows Server 2003 Security Configuration Tools
- Windows Server 2003 Resource Security
- Windows Server 2003 Auditing and Logging
- Windows Server 2003 EFS
- Windows Server 2003 Network Security

Lesson 4: Attack Techniques

- Network Reconnaissance
- 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

Lesson 5: Security on the Internet and WWW

- Describing the Major Components of the Internet
- Securing DNS Services
- Describing Web Hacking Techniques
- Describing Methods Used to Attack Users

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

Lesson 7: Creating a Security Policy

- Concepts of Security Policies
- Policy Design
- Policy Contents
- An Example Policy
- Incident Handling and Escalation Procedures
- Partner Policies

Lesson 8: Analyzing Packet Signatures

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