SCNA Advanced Security Implementation

Duration:
Traditional Instructor Led Learning - 5.00 Day(s)
Mentored Learning - Flexible

Overview:
This course is designed to provide the foundation knowledge to network administrators and security professionals who are seeking to learn about advanced security issues surrounding PKI and biometrics.

Prerequisite(s) or equivalent knowledge:

SCNP Hardening the Infrastructure
SCNP Network Defense and Counter Measures

Outline:

Lesson 1: Introduction to Trusted Networks

The Need For Trusted Networks
Authentication and Identification
Public Key Infrastructure
Applications of PKI

Lesson 2: Cryptography and Data Security

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

Lesson 3: Computer Forensics

Incident Response
Computer Forensic Fundamentals
Hard Disk Structure
Forensic Tools
Investigating Computers
Computer Forensics Solutions

Lesson 4: Law and Legislation

Intellectual Property
Categories and Types of Law
Process of Handling Evidence
Information Security-related Laws and Acts

Lesson 5: Biometrics—Who You Are

- The Process of Biometrics Today
- Accuracy of Biometrics
- Applications of Biometrics
- Fingerprint Scanning
- Facial Scanning
- Iris and Retinal Scanning
- Vocal Scanning
- Further Biometric Technologies
- Techniques for Compromising Biometrics

Lesson 6: Strong Authentication

- Why Strong Authentication
- Authentication Tokens
- RSA SecurID
- Smart Cards

Lesson 7: Digital Certificates

- Paper Certificates and Identity Cards
- Authorities that Issue Physical Certificates
- The Importance of Protecting the Identity of the CA
- Differences between Physical and Digital Certificates
- Standards for Digital Certificates
- X.509 as an Authentication Standard
- Case Study—VeriSign's Digital Certificates

Lesson 8: Digital Signatures

- Signatures as Identifiers
- Features of Digital Signatures
- Digital Signatures in Practice
- Standards for Digital Signatures
- Digital Signatures and PKI