

SCNA Advanced Security Implementation

Course SCNA-ASI • 5 Days

▶ COURSE 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.

▶ AUDIENCE

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.

Advanced Security Implementation is designed to provide network administrators and security architects with an awareness of security-related issues and the essential skills they need to implement security in a given network. It is the first course offered in the second level of the Security Certified Program. This course is followed by Enterprise Security Solutions (ESS).

▶ PREREQUISITES

To ensure your success, you are strongly recommended to first take the following Security Certified Program courses or have equivalent knowledge:

- Hardening the Infrastructure
- Network Defense and Counter Measures

▶ OBJECTIVES

Upon successful completion of this course, students will be able to:

- Describe the fundamentals of trusted networks.
- Describe the concepts and principles of cryptography.
- Implement computer forensic tools.
- Identify current laws and legislation that influence computer security professionals.
- Describe biometric solutions, including fingerprint scanning, iris scanning, and vocal scanning.
- Describe strong authentication solutions and implement token-based strong authentication.
- Describe the function of digital certificates.
- Describe the implementation of digital signatures.

▶ COURSE 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



105 West Broad Street
Falls Church, Virginia 22046
Ph: 703.532.1000
Fax: 703.532.1001
Web: www.Knowledge.com

SCNA Advanced Security Implementation

Course SCNA-ASI • 5 Days

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



105 West Broad Street
Falls Church, Virginia 22046
Ph: 703.532.1000
Fax: 703.532.1001
Web: www.Knowlogy.com