

## **Module 1: Preparing to Secure Information**

### **Lessons**

- Explaining How Assets Are Attacked
- Explaining How Assets Are Secured

### **Lab A: Preparing to Secure Information**

## **Module 2: Implementing Security-Enhanced Computing Baselines**

### **Lessons**

- Introduction to Trusted Computing Bases
- Establishing a Security Baseline
- Monitoring a Security Baseline
- Helping to Secure Computers Physically
- Maintaining a Security Baseline

### **Lab A: Maintaining Baseline Security**

## **Module 3: Helping to Protect Information Using Authentication and Access Control**

### **Lessons**

- Introduction to Access Control
- Implementing an Authentication Strategy
- Implementing an Access Control Strategy

### **Lab A: Securing Accounts (MBSA)**

## **Module 4: Using Cryptography to Help Protect Information**

### **Lessons**

- Introduction to Cryptography
- Using Symmetric Encryption
- Using Hash Functions
- Using Public Key Encryption

### **Lab A: Using Cryptography to Help Protect Information**

**Module 5: Using a PKI to Help Protect Information**

**Lessons**

- Introduction to Certificates
- Introduction to Public Key Infrastructure
- Deploying and Managing Certificates

**Lab A: Using Certificates**

**Module 6: Securing Internet Applications and Components**

**Lessons**

- Helping to Protect Web Servers
- Configuring Security for Common Internet Protocols
- Configuring Security for Web Browsers
- Configuring Security for Databases

**Lab A: Securing Web Servers**

**Lab B: Protecting Clients from Active Content**

**Module 7: Implementing Security for E-Mail and Instant Messaging**

**Lessons**

- Securing E-Mail Servers
- Securing E-Mail Clients
- Securing Instant Messaging

**Lab A: Securing Mail Servers**

**Module 8: Managing Security for Directory Services and DNS**

**Lessons**

- Helping protect Directory Services Against Common Threats
- Helping Protect DNS Against Common Threats

**Lab A: Managing Security for Directory Services and DNS**

## **Module 9: Securing Data Transmission**

### **Lessons**

- Identifying Threats to Network Devices
- Implementing Security for Common Data Transmission
- Implementing Security for Remote Access
- Implementing Security for Wireless Network Traffic

### **Lab A: Securing Data Transmission**

### **Lab B: Using IPSec to Secure Data Transmission**

## **Module 10: Implementing and Monitoring Security for Network Perimeters**

### **Lessons**

- Introduction to Network Perimeters
- Implementing Security on Inbound and Outbound Network Traffic
- Monitoring Network Traffic

### **Lab A: Implementing and Monitoring Security for Network Perimeters**

## **Module 11: Managing Operational Security**

### **Lessons**

- Establishing Security Policies and Procedures
- Educating Users about Security Policies
- Applying Security Policies to Operational Management
- Resolving Ethical Dilemmas When Helping to Protect Assets

### **Lab A: Managing Operational Security**

## **Module 12: Preserving Business Continuity**

### **Lessons**

- Preparing to Recover from Disasters
- Communicating the Impact of Risks
- Performing a Security-Enhanced Backup and Recovery

### **Lab A: Preserving Business Continuity**

### **Module 13: Responding to Security Incidents**

#### **Lessons**

- Identifying Security Incidents
- Responding to Security Incidents
- Investigating Security Incidents

#### **Lab A: Responding to Security Incidents**

**Contact the training coordinator for pricing and details at 613-563-NOVA (6682) Ext:250 Or [training@nova-networks.com](mailto:training@nova-networks.com)**

Nova Networks can also customize this course to topics of your choice which will reduce the course cost.

#### **Copyright Statement**

This site is Copyright © 2004 Nova Networks Inc. Reproduction of any part of this site for personal or commercial purposes without permission is strictly prohibited. The information at this site may be downloaded onto a disk or printed for your personal use provided that you include this copyright notice on each copy and that you make no alterations to any of the pages and do not use any of the information in any other work or publication whatsoever whether the publication is paper based or electronic. No part of the information may be distributed or copied for any commercial purpose.