640-553 - Implementing Cisco IOS Network Security (IINS) “Official Edition”

Course Introduction 6m

Course Introduction

Module 01 - Introduction to Network Security Principles 5h 52m

Introduction to Network Security Principles
Examining Network Security Fundamentals
Threats to Security
Addressing Internal Threats
External Threats
Threat Capabilities - More Dangerous and Easier to Use
Size of the Problem
The Evolution of Intent
Vulnerable Custom Applications
Network Security Objectives
Confidentiality
Integrity
Availability
Information Classification
Classification Levels
Classification Criteria
Information Classification Procedures
Distribution of Classified Materials
Information Classification Roles
Security Controls
Administrative Controls
Technical Controls
Physical Controls
Type of Controls
Computer Crime Investigations
Computer Crime Complications
Collection of Evidence
Types of Law
Ethics
Liability
Legal and Government Policy Issues
Section 1 - Review
Examining Network Attack Methodologies
Vulnerabilities, Risks, and Exploits
Main Vulnerability Categories
The Human Vulnerability Factor
Adversaries
Hackers, Crackers, and Phreakers
Computer Security Hackers
Motivations
Academic Hackers
Hobby Hackers
Thinking Like a Hacker
The Purpose of Defense in Depth
What Is Defense in Depth?
Examples of Defense in Depth
Early Defense in Depth Example
Defense in Depth Technical Example

Defense in Depth Non-Example
IP Spoofing
IP Spoofing - A Technical Discussion
IP Spoofing - Types of Attack
IP Source Routing Options
Man-in-the-Middle Attacks
Demo - MITM
Confidentiality Violations
Ping Sweeps and Port Scans
Packet Sniffers
Emanations Capturing
Overt and Covert Channels
Overt Channel Example
Stenography
Covert Channel Example
Phishing, Pharming, and Identity Theft
Integrity Violations
Trust Exploitation
Port Redirection
Password Attacks
Availability Violations
Botnets
DoS and DDoS Attacks
DDoS Example
TCP SYN Flooding
DoS Attacks Using ICMP
Smurf Attack
Electrical Power
Computing Environment
Best Practices to Defeat Hackers
Section 2 - Review
Examining Operations Security
Operations Security
Secure Network Lifecycle
Initiation Phase
Acquisition and Development Phase
Implementation Phase
Operations and Maintenance Phase
Disposition Phase
Principles of Operations Security
Separation of Duties
Rotation of Duties
Trusted Recovery
Change and Configuration Control
Network Security Testing and the System Development Life Cycle
Security Testing Techniques
Common Testing Tools
Nmap
SuperScan by Foundstone
Disaster Recovery and Business Continuity Planning
Disaster Recovery
Disruptions
Backups
Section 3 - Review
Understanding and Developing a Comprehensive Network Security Policy
Figure Out What You Are Protecting

Why Do You Need a Security Policy?
Who Uses the Security Policy?
Components of a Comprehensive Security Policy
Governing Policy Comes from the Top
Technical and End-User Policies
Standards, Guidelines, and Procedures
Standards
Guidelines
Procedures
Responsibilities for the Security Policy
Threat Identification and Risk Analysis
Risk Analysis
Quantitative Risk Analysis Formula
Benefits of Risk Analysis
Threat Identification and Risk Analysis Example
Risk Management and Risk Avoidance
Manage the Risk
Avoid the Risk
Secure Network Design Factors
Realistic Assumptions
Realistic Assumptions Example
Least Privilege Concept
Least Privilege Example
Design and Implementation Simplicity
Simplicity Example
Security Awareness
Awareness
Education and Training
Results of Security Awareness
Section 4 - Review
Building Cisco Self-Defending Networks
Threat Evolution
A Blurred Network Perimeter
The SQL Slammer Worm 30 minutes After "Release"
Cisco Self-Defending Network Overview
Benefits of Cisco Self-Defending Networks
Collaborative Systems Enabling Unparalleled Security
Cisco Self-Defending Network Defined
Threat Control and Containment
Secure Communications - Secure Data, Voice, Video, and Wireless
Operational Control and Policy Management
Cisco Security Manager Overview
Cisco Security MARS
Secure Network Platform
Section 5 - Review
Module 01 - Review

Module 02 - Perimeter Security

4h 30m

Perimeter Security
Securing Administrative Access to Cisco Routers
Router Security Principles
How Routers Enforce Perimeter Security Policy
Cisco Integrated Services Routers
Cisco Integrated Services Router Features

Cisco Secure ACS Prerequisites

Cisco Secure ACS 4.1 Homepage

Network Configuration

Interface Configuration

External Databases

Windows Database

Unknown User Policy

Group Setup

User Setup

Adding a AAA Server

Creating a AAA Login Authentication Policy

Applying an Authentication Policy

Creating a AAA Exec Authorization Policy

Creating a AAA Network Authorization Policy

AAA Accounting Configuration

AAA Configuration for TACACS+ Example

debug tacacs

debug tacacs events

Demo - AAA Authentication

Demo - Authentication Servers

Demo - ACS Server

Section 4 - Review

Implementing Secure Management and Reporting

Considerations for Secure Management and Reporting

Secure Management and Reporting Architecture

Secure Management and Reporting Guidelines

Syslog Systems

Cisco Security MARS

Cisco Security MARS Process Flow

Implementing Log Messaging for Security

Cisco Log Severity Levels

Log Message Format

Enabling Syslog Logging

Using Logs to Monitor Network Security

SNMPv1 and SNMPv2 Architecture

Community Strings

SNMPv3 Architecture

SNMP Security Models and Levels

Enabling SNMP with Cisco SDM

SNMP Trap Receiver

Secure Shell

Enabling SSH Using Cisco SDM

VTY Settings

Configuring an SSH Daemon Using the CLI

Manually Configuring Data and Time Settings

Network Time Protocol

Enabling NTP with Cisco SDM

Section 5 - Review

Locking Down the Router

Vulnerable Router Services and Interfaces

Management Service Vulnerabilities

Security Audit Home Page

Performing a Security Audit

Performing a One-Step Lockdown

Locking Down a Router Using Cisco Auto Secure

Limitations and Cautions

Demo - Router Hardening
Section 6 - Review
Module 02 - Review

Module 03 - Network Security Using Cisco IOS Firewalls 2h 46m

Network Security Using Cisco IOS Firewalls
Introducing Firewall Technologies
What is a Firewall?
Expanding on the Definition
Firewall Benefits
Firewall Limitations
Firewalls in a Layered Defense Strategy
Static Packet Filtering Firewalls
Static Packet Filtering Example
Advantages and Disadvantages of Packet Filters
Application Layer Gateways
Proxy Server Communication Process
Advantages, Limitations, and Uses of Application Layer Gateways
Dynamic or Stateful Packet Filtering
Stateful Packet Filtering
Uses and Limitations of Stateful Packet Filters
Application Inspection Firewalls
Transparent Firewalls
Cisco IOS Firewall Features
Cisco Security Router Certifications
Cisco PIX 500 Series Security Appliances
Cisco ASA 5500 Series Adaptive Security Appliances
Firewall Best Practices
Section 1 - Review
Creating Static Packet Filters Using ACLs
Access Control Lists
Mitigating Threats Using ACLs
Outbound ACL Operation
Inbound ACL Operation
A List of Tests - Deny of Permit
Types of IP ACLs
Identifying ACLs
IP Access List Entry Sequence Numbering
ACL Configuration Guidelines
Wildcard Bits - How to Check the Corresponding Address Bits
Wildcard Bits to Match IP Subnets
Wildcard Bit Mask Abbreviations
Numbered Standard IPv4 ACL Configuration
Numbered Standard IPv4 ACL
Applying Standard ACLs to Control vty Access
Numbered Extended IPv4 ACL Configuration
Established Command
Displaying ACLs
Guidelines for Developing ACLs
ACL Caveats
ACL Editor - Access Rules
Standard Rule
Associate with an Interface (1)
Extended Rule
Associate with an Interface (2)
Routing Protocol Entries

IP Address Spoof Mitigation - Inbound
IP Address Spoof Mitigation - Outbound
Filtering ICMP Messages - Inbound
Filtering ICMP Messages - Outbound
Permitting Common Services
Router Service Traffic
Demo - ACL
Section 2 - Review
Configuring Cisco IOS Zone-Based Policy Firewall
Cisco IOS Zone-Based Policy Firewall
In the Beginning
Traditional Cisco IOS Firewall Stateful Inspection
The New Era: Cisco IOS Zone-Based Policy Firewall
Benefits of Zone-Based Policy Firewall
Zone-Based Policy Firewall Actions
Zone-Based Policy Firewall Rules for Application Traffic
Zone-Based Policy Firewall Rules for Router Traffic
Basic Firewall Configuration Wizard
Basic Firewall Interface Configuration
Applying Security Policy
Finishing the Wizard
Manually Configuring a Zone-Based Policy Firewall
Define Zones
Define Class Maps
Define Policy Maps
Assign Policy Maps to Zone Pairs
Reviewing the Cisco IOS Zone-Based Policy Firewall
Cisco IOS Zone-Based Firewall Policy Configuration
Viewing the Firewall Log
Monitoring the Cisco IOS Zone-Based Policy Firewall
Section 3 - Review
Module 03 - Review

Module 04 - Site-to-Site VPNs 4h 12m

Site-to-Site VPNs
Examining Cryptographic Services
Cryptology Overview
Cryptography History
Substitution Cipher
Vigenere Cipher
Transposition
One-Time Pads
Transforming Plaintext into Ciphertext
Cryptanalysis
Encryption Algorithm Features
Encryption Keys
Symmetric Encryption Algorithms
Asymmetric Encryption Algorithms
Block and Stream Ciphers
Choosing an Encryption Algorithm
Key Comparisons
Overview of Cryptographic Hashes
What Is Key Management?
Keyspaces
Key Length Issues
SSL Overview

SSL Tunnel Establishment
Section 1 - Review
Examining Symmetric Encryption
Symmetric Encryption Overview
Symmetric Encryption Key Lengths
Acceptable Key Lengths
DES
DES Modes
DES ECB vs. CBC Mode
DES Usage Guidelines
3DES
3DES Encryption Process
AES
SEAL
RC Algorithms
Section 2 - Review
Examining Cryptographic Hashes and Digital Signatures
Overview of Hash Algorithms and HMACs
What Is a Hash Function?
Hashing in Action
Hashed Message Authentication Code
HMAC in Action
Message Digest 5
Secure Hash Algorithm 1
MD5 and SHA-1 Compared
Hash and HMAC Best Practices
Overview of Digital Signatures
Digital Signatures in Action
Digital Signatures Example
Digital Signature Standard
Digital Signature Best Practices
Section 3 - Review
Examining Asymmetric Encryption and PKI
Asymmetric Encryption Overview
Asymmetric Encryption Algorithms
Public Key Confidentiality Scenario
Asymmetric Confidentiality Process
Public Key Authentication Scenario
Asymmetric Authentication Process
RSA Algorithm
RSA Digital Signatures
RSA Usage Guidelines
The DH Algorithm
The DH Key Exchange Algorithm
Trusted Third-Party Protocols
Trusted Third-Party Example
PKI Terminology and Components
PKI Topologies - Single - Root CA
PKI Topologies - Hierarchical Cas
PKI Topologies - Cross - Certified Cas
PKI and Usage Keys
PKI Server Offload
Overview of Standardization
X.509v3
Public-Key Cryptography Standards
Simple Certificate Enrollment Protocol

Crypto Map Parameters
Step 5: Configure IPSec Crypto Maps
Example: Crypto Map Commands
Applying Crypto Maps to Interfaces
Test and Verify IPSec
show crypto isakmp policy Command
show crypto ipsec transform-set Command
show crypto map Command
show crypto ipsec sa
Section 6 - Review
Configuring IPSec on a Site-to-Site VPN Using Cisco SDM
Introducing the Cisco SDM VPN Wizard Interface
Site-to-Site VPN Components
Launching the Site-to-Site VPN Wizard
Quick Setup
Step-by-Step Setup
Connection Settings
IKE Proposals
IPSec Transform Sets
Option 1: Single Source and Destination Subnet
Option 2: Using an ACL
Review the Generated Configuration
Test Tunnel Configuration and Operation
Monitor Tunnel Operation
Advanced Monitoring
Troubleshooting
Demo - IPSec
Section 7 - Review
Module 04 - Review

Module 05 - Network Security Using Cisco IOS IPS 54m

Network Security Using Cisco IOS IPS
Introducing IPS Technologies
Defining IDS and IPS
IDS and IPS Common Characteristics
IDS and IPS Operational Differences
Comparing IDS and IPS Solutions
Types of IDS and IPS Sensors
IPS Attack Responses
Event Monitoring and Management
Cisco IPS Management Software
Cisco IDS Event Viewer
Cisco Security MARS
HIPS Features
How HIPS Operates
Cisco HIPS Deployment
Network IPS Features
Cisco Network IPS Deployment
Comparing HIPS and Network IPS
Cisco IPS Appliances
Cisco IPS 4200 Series Sensors
Cisco ASA AIP-SSM
Cisco Catalyst 6500 Series IDSM-2
Cisco IPS AIM
IPS Signature Operational Characteristics
Signature Micro-Engines

Supported Signature Micro-Engines
Cisco Signature Alarm Types
Implementing Alarms in Signatures
IPS Configuration Best Practices
Section 1 - Review
Configuring Cisco IOS IPS Using Cisco SDM
Cisco IOS IPS Intrusion Prevention Technology
Primary Benefits of the Cisco IOS IPS Solution
Cisco IOS IPS Signature Features
Using Cisco SDM to Configure IPS
IPS Policies Wizard
IPS Config Location and Category
IPS Policy Summary
Cisco IOS IPS CLI Configuration
Setting Signature Severity
Configuring Signature Actions
Editing Signatures Using Cisco SDM
Support for SDEE and Syslog
Viewing SDEE Alarm Messages
Viewing Syslog IPS Alarms
Verifying IPS Policies
Verify IPS Operation
Section 2 - Review
Module 05 - Review

Module 06 - LAN, SAN, Voice, and Endpoint Security Overview 1h 53m

LAN, SAN, Voice, and Endpoint Security Overview
Examining Endpoint Security
Cisco Host Security Strategy
Software Security Concepts
Operating System Vulnerabilities
Application Vulnerabilities
Input Validation
Buffer Overflows
Types of Buffer Overflows
Worms, Viruses, and Trojan Horses
Anatomy of a Worm Attack
Worm and Virus - Exploit Comparison (~20 Yrs)
IronPort Perimeter Security Appliances
IronPort E-Mail Security Appliance
IronPort Web Security Appliance
Cisco NAC Products
NAC Framework
Cisco NAC Appliance Overview - Components
Cisco NAC Appliance Overview - Process Flow
Cisco NAC Appliance Overview - Agent
Cisco Security Agent Architecture
Appliance, Kernel, and Interceptors
Cisco Security Agent Interceptors
Cisco Security Agent Attack Response
Operating System Guidelines
Application Guidelines
Section 1 - Review
Examining SAN Security
What Is a SAN?
Why Use SANs?

Benefits of a SAN
SAN Basics
LUN Masking
World Wide Names
Fibre Channel Fabric Zoning
Virtual SANs
SAN Security Scope
SAN Management Threats
Fabric and Target Access Threats
Target Access Security - Zoning
IP Storage and Transmission Security
Section 2 - Review
Examining Voice Security
What is VoIP?
Business Case for VoIP
Components of a VoIP Network
Major VoIP Protocols
Threats to IP Telephony Endpoints
Spam over IP Telephony
SPIT Example
Fraud
SIP Vulnerabilities
Separate Voice VLAN
Protect IP Telephony with Firewalls
Protect IP Telephony with VPNs
Protect IP Telephony Endpoints
Protect IP Telephony Servers
Section 3 - Review
Mitigating Layer 2 Attacks
Why Worry About Layer 2 Security?
Domino Effect
VLAN Overview
VLAN Hopping by Rogue Trunk
VLAN Hopping by Double Tagging
Mitigating VLAN Hopping Network Attacks
Redundant Topology
Loop Resolution with STP
STP Operation
STP Root Bridge Selection
STP Manipulation
PortFast
BPDU Guard
Root Guard
Verifying BPDU Guard
CAM Table Overflow Attack
MAC Address Spoofing Attack
Port Security
Configuring Port Security
Configuring Port Security Aging
Port Security Example
Verifying Port Security
Notification of Intrusions
Switched Port Analyzer
Remote SPAN
Lan Storm
Storm Control

Layer 2 Security Best Practices
Demo - Layer 2 Security
Section 4 - Review
Module 06 - Review
Course Closure

Total Duration: 20 hrs 15 min