UCSEC - Implementing Cisco Unified Communications Security v1.0

1. Vulnerabilities of Cisco Unified Communications Networks and Security Fundamentals

Lesson 1: Assessing Vulnerabilities of Cisco Unified Communications Networks

- Threats to Cisco Unified Communications solution
- Types of Attackers and Attacks
- Security Weaknesses of Cisco Unified Communications networks
- Examples of Identity Spoofing Attacks
- Examples of DoS Attacks
- Examples of Privilege Escalation Attacks
- Examples of Eavesdropping Attacks
- Examples of Data Manipulation
- Examples of Phone Attacks

Lesson 2: Describing Security Implementation Strategies

- Risk Assessment
- Security Implementation Guidelines
- Security Policy Benefits
- Auditing
- Accountability

Lesson 3: Describing Cryptographic Services and Functions

- Cryptography Overview
- Symmetric Encryption
- Asymmetric Encryption
- Hashes
- Hashed Message Authentication Codes (HMACs)
- Digital Signatures

Lesson 4: Describing Key Management and PKI

- Key Management Issues
- PKI Overview
- PKI Operation
- PKI Considerations
- PKI Examples

Lesson 5: Describing IPsec and Cisco AnyConnect SSL VPN

- IPsec and Cisco AnyConnect SSL Overview
- IPsec Characteristics
- IPsec Operation
- IPsec Considerations
- Special IPsec Implementation

- Cisco AnyConnect SSL Characteristics
- Cisco AnyConnect SSL Operation
- Cisco AnyConnect SSL Considerations

2. Network Infrastructure Security

Lesson 1: Implementing Network Separation and Packet Filtering

- Security Domains
- Overview of Network Separation Methods
- Voice VLAN Implementation
- Cisco IOS Firewall Implementations
- NAT in Cisco Unified Communications
- Stateless Packet Filter
- Stateful Packet Filter
- Deep Packet Inspection
- Application Proxies
- Softphone Network Separation Considerations

Lesson 2: Implementing Switch Security Features

- Overview of Switch Security Features
- 802.1X Characteristics
- 802.1X Operations
- 802.1X Implement

Lesson 3: Implementing Cisco AnyConnect SSL VPNs in Cisco Unified Communications Networks

- IP Phone VPN Client Overview
- IP Phone VPN Client Trust Requirements
- IP phone VPN Client Considerations
- IP phone VPN Client Implementation
- IP phone VPN Client Verification

3. Cisco Unified Communications Manager and Endpoint Security Features

Lesson 1: Hardening Cisco Unified Communications Endpoints

- General Device Hardening
- Overview of Cisco Unified Communications Manager Endpoint Hardening
- Settings Button Access
- PC Port Access
- GARP Configuration
- IP Phone Web Server Access
- Gateway Hardening

Lesson 2: Implementing Toll-Fraud Prevention

- Toll-Fraud Prevention Overview
- Call Classification

- External-to-External Transfers
- Ad Hoc Conferences
- CoS for Voice-Mail Ports, Call Forward and Unified Mobility
- Forced Authorization Codes
- Monitoring and Accounting
- Gateways and Cisco Unified Communications Manager Express Toll-Fraud prevention

Lesson 3: Implementing Native Cisco Unified Communications Manager Security Features

- Signed Firmware
- SIP Digest Authentication
- Secure SIP Trunks
- IPsec Support in Cisco Unified Communications Manager
- Security by Default Overview
- Security by Default Components
- Security by Default Operation
- Security by Default Consideration

Lesson 4: Implementing Cisco Unified Communications Manager Security Features Based on Security Tokens

- Roots of Certificates
- Certificate Trust List
- Cisco CTL Client
- CTL Interaction with Initial Trust List
- Overview of Security Features Based on Security Tokens
- Secure Signalling
- Secure Real-Time Transport Protocol
- Phone Configuration File Encryption
- Secure Conferences
- Impact of Encrypted Signalling

4. Secure Cisco Unified Communications Integration and Features

Lesson 1: Implementing SRTP to Gateways and Signalling Protection by IPsec

- Secure Gateway Overview
- IPsec Protection between Cisco Unified Communications Manager and VPN Device
- SIP-TLS and SRTP to SIP Gateways
- SRTP to MGCP Gateways
- SRTP to H.323 Gateways
- Implementing IPsec for Signalling

Lesson 2: Implementing Secure Signalling and SRTP in SRST and Cisco Unified Communications Manager Express

- Secure SRST Trust Requirements
- Trusted SRST Gateway
- Trust IP Phones

- Secure SRST Operation
- Secure SRST Implementation
- Secure Cisco Unified Communications Manager Express PKI
- Cisco Unified Communications Manager Express Security Features
- Secure Cisco Unified Communications Manager Express Implementation

Lesson 3: Implementing Trusted Relay Points

- Trusted Relay Point Overview
- Trusted Relay Point Characteristics
- Trusted Relay Point Components
- Trusted Relay Point Operations
- Trusted Relay Point Implement

Lesson 4: Implementing Proxies for Secure Signalling and SRTP

- Proxy Overview
- Cisco Unified Border Element Overview
- Cisco Unified Border Element Security Features
- Cisco Unified Border Element Configuration
- TLS Proxy Overview
- TLS Proxy Configuration
- Verifying TLS Proxy
- Phone Proxy Overview
- Phone Proxy Configuration
- Comparison of Cisco Unified Border Element, TLS Proxy, and Phone Proxy

Labs:

- Lab 1-1: Identifying Security Weaknesses in a Cisco Unified Communications Network
- Lab 2-1: Implementing Firewalls
- Lab 2-2: Implementing 802.1X
- Lab 2-3: Implementing Cisco AnyConnect SSL VPNs
- Lab 3-1: Implementing Cisco Unified Communications Manager Security Features Based on Security Tokens
- Lab 4-1: Implementing SRTP to Gateways and Signalling Protection by IPsec
- Lab 4-2: Implementing Secure SRST and Secure Cisco Unified Communications Manager Express
- Lab 4-3: Implementing Trusted Relay Points
- Lab 4-4: Implementing Proxies for Signalling and RTP