Securing Cisco Wireless Enterprise Networks (CS-WISECURE)

Modality: Virtual Classroom

Duration: 3.5 Days

CLC: 30 Units

About this course:

The “Securing Cisco Wireless Enterprise Networks” course is put together to provide guidance for the implementation of Wi-Fi security architectures by configuring Cisco wireless components. This course includes labs to reinforce concepts with the help of WISECURE. Prime Infrastructure release 2.2, Identity Service Engine and other concepts.

Students who are looking for help to prepare for the Cisco: 300-375 WISECURE exam should enroll in this course.

Moreover, this course is part of the “Dual Wireless Certification” Boot Camp (CS-CCNA/CCNP)

Course Objectives:

The primary objective of this course is to teach students about the following:

- Designing and Identification of security strategies in a Wi-Fi design
- Wi-Fi Infrastructure Security
- Cisco ISE design and deployment
- Management Platforms
- End Point: Designing and deployment
- Client Security: designing and deployment
- Monitoring

Audience:

- Technicians
- Test Engineers
- Project Managers

- Wireless Support Engineers

Prerequisites:

The students interested in this course should have prior knowledge and understanding of the following:

- Understanding of Basic QoS
- Know-how of Cisco Identity Services Engine
- Voice Signaling Protocol
- LAN Switching
- Application Visibility

Course Outline:

Module 1 Define Security Approaches in a Wi Fi Design

- Security Areas in a Wi-Fi Design
- Security Challenges for IT Organizations
- Security Approaches in Wi-Fi Designs
- Policy Enforcement
- Cisco Prime Infrastructure
- Cisco ISE/ISE as a Policy Platform
- Network Access Challenges and Secure Access Control
- Network Monitoring
- Prime Infrastructure Converged Approach and Security Dashboard
- Cisco ISE Dashboard and ISE Alarms

Module 2 Design and Deploy Endpoint and Client Security

- Defining Endpoint, Client Standards and Features
- X.509 v3
- PKI
- IEEE 802.1X
- EAP, EAP-TLS and PKI with EAP-TLS
- PEAP and PEAP Deployment
- EAP-FAST
- RADIUS
- Configure WPA and WPA2 in a Wi-Fi Environment
- Security Mobility and Roaming

Module 3 Design and Deploy Cisco ISE and Management Platforms

- Cisco Network Security Architecture
- User Access Trends
- Cisco ISE Architecture, Components and Licensing
- End Device Analysis with Cisco ISE Profiling
- Create Policies in Cisco ISE
- Configure Guest Access
- Cisco CMX Visitor Connect
- Secure BYOD/BYOD Management and Monitoring
- Cisco ISE and ISE GUI

Module 4 Secure Wi Fi Infrastructure

- Current Standards and Features
- Client and Infrastructure Mode and MFP
- MFP vs IEEE802.11w
- VLANs vs ACLs
- MFP Configuration
- IEEE 802.11w PMF
- Identity-Based Networking
- SMNPv3 in Wi-Fi environment

Module 5 Design and Deploy Wi Fi Access Control

- Wi-Fi access control standards and features
- ACLs and Firewall Functionality
- Configure ACLs in Wi-Fi environment

Module 6 Design and Deploy Monitoring Capabilities

- Threat and Interference Mitigation Approaches in Wi-Fi
- Primary Security Concerns
- Rogue Detection and Mitigation in Wi-Fi Environment
- Management, Monitoring and Configuring Parameters
- Cisco CleanAir
- Cisco Prime Infrastructure Air Quality Monitoring and Reporting
- Monitoring RRM

Labs:

- Configuring WPA2 Access
- Configuring 802.1X Access
- Configuring RADIUS Integration
- Configuring a Basic Access Policy
- Configuring Hotspot Guest Access
- CWA and Self-Registered Guest Operations
- Configuring Secure Administrative Access
- Configuring a Basic Authentication Policy for an AP
- Implementing Profiling

- Profiling and Device Onboarding
- Cisco ISE Profiling Reports
- Guest Reports
- Live Logs and Client 360 View
- Security Report Operations
- Using System Security Verification Tools