أكاديمية اتصالات
etisalat academy
Skills | Solutions | Results

Certified Wireless Security Engineer

Duration: 4 Days | Language: English

Course Delivery: Classroom

Course Overview

Wireless networks offer many conveniences that are not available in wired networks, but there are security risk associated with those conveniences that businesses need to understand. The Certified Wireless Security Engineer is prepared to identify those risk that wireless networks present for a business and to create and implement a plan to mitigate those risk.

The C)WSE course will give students real-world experience with solving security vulnerabilities in wireless networks. This is accomplished by students completing hands-on lab exercises with the tools and methodologies that actual malicious hackers use to compromise wireless networks

Prerequisites

C)SS: Security Sentinel, C)ISSO: Information Systems Security Officer, OR 12 months of experience in networking technologies and security.

Course Outline

1. WLAN Security Overview
   - Standards Organization
   - OSI Layers (ISO Standard)
   - 802 Project (IEEE)
   - ISOC Hierarchy (IETF)
   - Wi-Fi Alliance
   - Wi-Fi Certified Programs
   - 802.11 Security Basics
   - 802.11 Security History
   - Summary

2. Legacy Security
   - Overview
   - Authentication Open System Authentication
   - Authentication Open System and 802.1X/EAP
   - Authentication Shared Key
   - Static WEP and IV Key
   - WEP Transmission Key
   - WEP Encryption Process
   - Common WEP Attacks
   - VPN and WLAN Client Access
   - VPNs
   - VPN Comparison
   - Aggressive Mode PSK Attacks

- Aggressive PSK Cracking
- MAC Filters Changing a MAC Address
- SSID Segmentation
- SSID Cloaking
- Labs

3. Encryption Ciphers and Methods
- Overview
- Introduction
- Encryption
- Cryptographic Definitions
- Encryption Algorithm
- Implementation
- Symmetric Encryption
- Symmetric Downfalls
- Symmetric Algorithms
- Crack Times
- Asymmetric Encryption
- Public Key Cryptography Advantages
- Asymmetric Algorithm Disadvantages
- Asymmetric Algorithm Examples
- Key Exchange
- Symmetric versus Asymmetric
- Using the Algorithm Types Together
- Attack Vectors
- WLAN Encryption Methods
- MAC Protocol Data Unit (MSDU)
- WEP MPDU
- WEP Encryption Process
- WEP Decapsulation
- TKIP Modification to WEP
- TKIP Cryptographic Encapsulation
- TKIP Decapsulation
- TKIP MPDU
- CCMP
- CCMP MPDU
- Additional Authentication Data
- CCMP Encapsulation
- CCMP Decapsulation
- Labs

4. Layer 2 Authentication Methods in Enterprise Networks
Overview
AAA
Types of Credentials
Authentication
Examples of Credentials
802.1X Components
Supplicant Types
Authenticator
WLAN Bridging and 802.1X
Authentication Proxy
Typical Authentication Servers

Supplicant Identity Credential
Legacy Authentication Protocols
Extensible Authentication Protocol
EAPOL Messages
802.11 Association and 802.1X/EAP
Generic EAP Exchange
Weak EAP Protocols
EAP-LEAP
Strong EAP Protocols
EAP-PEAP Process
EAP-TTLS Process
EAP-TLS Process
EAP-FAST Process
PACs
EAP Comparison Chart
EAP Methods for Cellular Networks

5. 802.11 Layer 2 Dynamic Encryption Key Generation
- Overview
- 802.1X/EAP and Dynamic Keys
- Advantages
- Dynamic WEP Process
- Robust Security Network Associations
- RSNA in IBSS (Ad-hoc)
- RSN Information Element
- RSNIE (Cipher Suites)
- RSNIE (AKM)
- AKM Overview
- AKM Discovery
- AKM Master Key Generation
- AKM Temporal Key Generation
- RSN Key Hierarchy
- Master Keys
- Pairwise Key Hierarchy
- Group Key Hierarchy
- 4-way Handshake
- Group Key Handshake
- Station to Station Link (STSL)
- RSNA Security Associations
- WPA/WPA2 Personal
- Passphrase to PSK Mapping
- Roaming and Dynamic Keys
- Labs

6. SOHO 802.11 Security
- Overview
- WPA/WPA2 Personal
- Pre-shared Keys (PSK) and Passphrases
- WPA/WPA2 Personal Risks
- Wi-Fi Protected Setup (WPS)
- WPS Architecture
- Setup Options

- Configuration Modes
- Guidelines and Requirements for PIN
- PBC Demonstration
- SOHO Security Best Practices
- Labs

7. Fast Secure Roaming
   - Overview
   - Client Roaming Thresholds
   - AP-to-AP Re-association
   - Problems with Autonomous AP-to-AP Roaming
   - PMKSA without Fast Roaming
   - PMK Caching
   - Pre-authentication
   - Opportunistic PMK Key Caching (OKC)
   - Proprietary FSR CCKM
   - Fast BSS Transition
   - FT Protocols
   - Message Exchange Methods
   - Key Holders
   - Key Hierarchy
   - FT Key hierarchy-WLAN controller
   - FT Key hierarchy-Supplicant
   - Information Elements
   - Fast BSS transition information element
   - FT Initial Mobility Domain Association
   - Over-the-air Fast BSS Transition
   - Over: the: DS Fast BSS Transition
   - Fast BSS Transition Summary
   - Wi-Fi Voice Personal and Enterprise
   - Enterprise Grade Voice over Wi-Fi Requirement
   - Features Required
   - Layer3 Roaming
   - Mobile IP
   - Single Channel
   - Architecture (SCA) Roaming

8. Common Attacks
   - Overview
   - Unauthorized Rogue Access Rogue Devices
   - Bridged Ad Hoc (IBSS)
   - Attacks which can be launched through rogue AP
   - Rogue AP Attack Risks
   - Rogue AP Prevention
   - Eavesdropping
   - Eavesdropping Risks
   - Eavesdropping Prevention
   - Authentication Attacks
   - Denial of Service Attacks
   - MAC Spoofing
   - Wireless Hijacking (Evil Twin Attack)
   - Encryption Cracking

- Peer-to-peer attacks
- Management Interface Exploits
- Vendor Proprietary Attacks
- Physical Damage and Theft
- Social Engineering Attacks
- Public Access and WLAN Hotspots
- Labs

9. Auditing WLAN Security
    - Overview
    - What is Security Audit?
    - 2.4 GHz ISM Interferers
    - Narrow Band Interference
    - Wide Band Interference
    - All-Band Interference
    - OSI Layer2 Audit
    - List of L2 Information collection
    - Layer2 Protocol Analyzer
    - Penetration Testing
    - Wired Infrastructure Audit
    - Social Engineering Audit
    - WIPS Audit
    - Documenting the Audit
    - Documents required prior to audit
    - Example Recommendations
    - WLAN Toolkit of an Auditor
    - Common Software Tools
    - Automated Tool (SILICA)

10. Wireless Security Monitoring
    - Overview
    - WIDS / WIPS Infrastructure Components
    - WIDS/WIPS Architecture Models
    - Overlay WIDS/WIPS
    - Integrated WIDS/WIPS
    - Integrated-Enabled WIDS/WIPS
    - Wireless Network Management System
    - Sensor Placement
    - Device Classification
    - Rouge Detection
    - Rogue Types
    - Rogue Mitigation
    - Device Tracking
    - Device Tracking Techniques
    - WIDS/WIPS Signature Analysis
    - WIDS/WIPS Behavioral Analysis
    - WIDS/WIPS Protocol Analysis
    - WIDS/WIPS Spectrum Analysis
    - WIDS/WIPS Forensics Analysis
    - WIDS/WIPS Performance Analysis
    - Monitoring
    - Policy Enforcement
    - Types of Alarms and Notifications

- Severity Levels of
- Alarms and Notifications
- Typical Notification Tools
- 802.11n
- 802.11n Security Concerns
- Management Frame Protection
- 802.11w
- 802.11w Shared Secret Key
- Labs

11. WLAN Security
    - Overview
    - Wireless Infrastructure Components
    - Autonomous AP
    - WLAN Controllers
    - WLAN-VLAN Assignment
    - WLAN-Dynamic VLAN Assignment
    - Split MAC
    - Mesh Networks
    - WLAN Bridging
    - Hybrid WLAN APs
    - Dynamic RF
    - Hot Standby/Failover
    - Device Management
    - Management Protocols
    - RADIUS/LDAP Servers
    - Radius Features and Components
    - Radius Integration
    - EAP Type Selection
    - Deployment Architectures and Scaling
    - Built-in RADIUS Servers
    - Timer Values
    - PKI
    - CA Hierarchy