C)WSE: Certified Wireless Security Engineer

Course ID #: 7000-822-ZZ-Z

Hours: 35

Course Content

Course Description:

In this course, you will cover how a Wireless Security Engineer designs, implements, and maintains secure wireless networks. You will also learn how they assess security risks and vulnerabilities, configure security solutions, and ensure the confidentiality, integrity, and availability of data transmitted over wireless networks. This includes implementing security protocols such as WPA2, 802.1X, and others, monitoring network activity for security threats, and responding to security incidents. They also stay up to date with emerging security trends and technologies to continuously improve the security posture of their organization's wireless network.

Course Objectives:

Upon successful completion of this course students will:

- Be able to establish industry acceptable Cyber Security & IS management standards with current best practices
- Be prepared to competently take the C)WSE exam

Prerequisites:

- C)SP
- 12 months of Information Systems Management Experience

Target Audience:

- Coders
- Application Engineers
- IS Managers
- Developers
- Programmers

Topics:

Lesson 1: Business and Technical Logistics of Wireless Pen Testing

- What is Penetration Testing?
- Today's Threats
- Pen Testing Methodology
- Wireless Standards and Organizations

Lesson 2: Wireless Security Fundamentals

- Wireless Security Fundamentals
- WLAN Security Policy
- RF Components
- RF Signal and Antenna Concepts
- Spread Spectrum Technologies
- IEE 802.11 Standards
- IEEE 802.15 Standards Bluetooth

C)WSE: Certified Wireless Security Engineer

Course ID #: 7000-822-ZZ-Z

Hours: 35

Lesson 3: Authentication
- WLAN Authentication Overview
- 802.1x
- EAP
- Key Management

Lesson 4: Encryption
- Cryptography Overview
- Symmetric Encryption
- Asymmetric Cryptography

Lesson 5: WLAN Encryption Implementations
- WPA2
- WPA3
- Sniffing
- Authentication Attacks
- Threat Assessments

Lesson 6: Reconnaissance and Enumeration
- What are we looking for?
- Keeping Track of what we find!
- Where/How do we find this information?
- Passive Scanning: Are there tools to help?
- Passive Recon Countermeasures
- Reaching Out!
- Port Scanning
- Active Scanning: Are there tools to help?
- Active Recon Countermeasures
- Banner Grabbing
- Enumeration

Lesson 7: Network Assessment and Exploitation Techniques
- Exploits
- WiFi Tools
- Wi-Fi Exploits
- Exploit Framework

Lesson 8: Evasion Techniques
- Evading Firewalls
- Evading Honeypots
- Evading IDS

Lesson 9: Monitoring and Auditing WLANS
- Monitoring
- Auditing
- Secure Roaming
- WLAN Security Recommendations and Designs

Labs listed on following page…

C)WSE: Certified Wireless Security Engineer

Course ID #: 7000-822-ZZ-Z

Hours: 35

Cyber Range Wireless Labs:

Lab 01 - Introduction to Pen Testing Setup
Lab 02 - Using Tools for Reporting (Optional)
Lab 03 - Wireless Authentication Capture
Lab 04 - Information Gathering (Optional)
Lab 05 - Detecting Live Systems - Scanning Techniques
Lab 06 - Enumeration
Lab 07 - Wireless Scanning with Different Systems
Lab 08 - Decrypting Wi-Fi Traffic
Lab 09 - Cracking WPA2
Lab 10 - Windows System Hacking
Lab 11 - Advanced Vulnerability and Exploitation Techniques
Lab 12 - AntiVirus Bypass
Lab 13 - Cracking Passwords from a Linux System
Lab 14 - Network Sniffing/IDS
Lab 15 - WiFi Audit with hcxdumptool
Final Lab - WarDrive, Scanning, Setup Evil Twin, Enterprise Attack

Accreditations:

Register for this class by visiting us at:
www.tcworkshop.com or calling us at 800-639-3535