Certified Wireless Security Engineer

Description:

A **Wireless Security Engineer** designs, implements, and maintains secure wireless networks. 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.

Annual Salary Potential $85,967 AVG/year

Key Course Information

Live Class Duration: 5 Days
CEUs: 40
Language: English
Class Formats Available:

Instructor Led

Live Virtual Training

Suggested Prerequisites:

- Mile2's C)SP

- 12 months of Information Systems Management Experience

Modules/Lessons

Module 01 - Business and Technical Logistics

Module 02 - Wireless Security Fundamentals

Module 03 – Authentication

Module 04 – Encryption

Module 05 - WLAN Encryption Implementations

Module 07 - Reconnaissance and Enumeration

Module 08 - Network Assessment and Exploitation Techniques

(Modules 9 & 10 below)

Who Should Attend

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

Accreditations

www.mile2.com 10213 Wilsky Blvd, Tampa, FL 33625 813-920-6779

Upon Completion

Upon completion, Certified Wireless Security Engineer students will not only be able to establish industry acceptable Cyber Security & IS management standards with current best practices but also be prepared to competently take the C)WSE exam.

Exam Information

The Certified Wireless Security Engineer exam is taken online through Mile2's Learning Management System and is accessible on you Mile2.com account. The exam will take approximately 2 hours and consist of 100 multiple choice questions.

A minimum grade of 70% is required for certification.

Re-Certification Requirements

All Mile2 certifications will be awarded a 3-year expiration date. There are two requirements to maintain Mile2 certification:

1) Pass the most current version of the exam for your respective existing certification.

2) Earn and submit 20 CEUs per year in your Mile2 account.

Course FAQ's

Question: Do I have to purchase a course to buy a certification exam?

Answer: No

Question: Do all Mile2 courses map to a role-based career path?

Answer: Yes. You can find the career path and other courses associated with it at www.mile2.com.

Question: Are all courses available as self-study courses?

Answer: Yes. There is however 1 exception. The Red Team vs Blue Team course is only available as a live class.

Question: Are Mile2 courses transferable/shareable?

Answer: No. The course materials, videos, and exams are not meant to be shared or transferred.

Course and Certification Learning Options

www.mile2.com 10213 Wilsky Blvd, Tampa, FL 33625 813-920-6779

Detailed Outline:

Course Introduction

Module 01 - Business and Technical Logistics of Wireless Pen Testing

Section 01 - What is Penetration Testing?
Section 02 - Today's Threats
Section 03 - Pen Testing Methodology
Section 04 - Wireless Standards and Organizations

Module 02 - Wireless Security Fundamentals

Section 01 - Wireless Security Fundamentals
Section 02 - WLAN Security Policy
Section 03 - RF Components
Section 04 - RF Signal and Antenna Concepts
Section 05 - Spread Spectrum Technologies
Section 06 - IEE 802.11 Standards
Section 07 - IEEE 802.15 Standards Bluetooth

Module 03 - Authentication

Section 01 - WLAN Authentication Overview
Section 02 - 802.1x
Section 03 - EAP
Section 04 - Key Management

Module 04 - Encryption

Section 01 - Cryptography Overview
Section 02 - Symmetric Encryption
Section 03 - Asymmetric Cryptography

Module 05 - WLAN Encryption Implementations

Section 01 - WPA2
Section 02 - WPA3
Section 03 - Sniffing
Section 04 - Authentication Attacks
Section 05 - Threat Assessments

www.mile2.com 10213 Wilsky Blvd, Tampa, FL 33625 813-920-6779

Module 07 - Reconnaissance and Enumeration

Section 01 - What are we looking for?
Section 02 - Keeping Track of what we find!
Section 03 - Where/How do we find this information?
Section 04 - Passive Scanning: Are there tools to help?
Section 05 - Passive Recon Countermeasures
Section 06 - Reaching Out!
Section 07 - Port Scanning
Section 08 - Active Scanning: Are there tools to help?
Section 09 - Active Recon Countermeasures
Section 10 - Banner Grabbing
Section 11 - Enumeration

Module 08 - Network Assessment and Exploitation Techniques

Section 01 - Exploits
Section 02 - WiFi Tools
Section 03 - Wi-Fi Exploits
Section 04 - Exploit Framework

Module 09 - Evasion Techniques

Section 01 - Evading Firewalls
Section 02 - Evading Honeypots
Section 03 - Evading IDS

Module 10 - Monitoring and Auditing WLANS

Section 01 - Monitoring
Section 02 - Auditing
Section 03 - Secure Roaming
Section 04 - WLAN Security Recommendations and Designs

www.mile2.com 10213 Wilsky Blvd, Tampa, FL 33625 813-920-6779

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

www.mile2.com 10213 Wilsky Blvd, Tampa, FL 33625 813-920-6779