CWSP - Certified Wireless Security Professional

Duration: *4 Day(s)*

Course Overview

Using the latest enterprise wireless LAN security and auditing equipment in this hands-on course, learn, in detail, the most up-to-date WLAN intrusion and DoS tools and techniques. You will learn about functionality of the 802.11i amendment to the 802.11 standard, the inner-workings of each EAP type used with wireless LANs today, and every class and type of WLAN security solution available on the market from wireless intrusion prevention systems to wireless network management systems.

Review this course online at https://www.alta3.com/courses/CWSP

Objectives

- Understand the functionality of the 802.11i amendment to the 802.11 standard.
- Analyze the inner-workings of each EAP type used with wireless LANs.
- Identify and evaluate different WLAN security solutions available in the market.
- Implement security auditing tools and intrusion prevention systems for robust wireless networks.

Who Should Attend

- Network Security Engineers
- IT Security Specialists
- Wireless Network Administrators
- System Administrators

Prerequisites

Certified Wireless Network Administrator (CWNA)

Course Outline

Module 1 – Security Fundamentals

1. Security Basics
2. CWNA Security Review
3. Industry Organizations
4. Terminology
5. Wireless Vulnerabilities

Module 2 – Wireless Security Challenges

6. Network Discovery
7. Pseudo-Security
8. Legacy Security Mechanisms

9. Network Attacks
10. Recommended Practices

Module 3 – Security Policy

11. Defining Security Policies
12. Policy Enforcement
13. Policy Management
14. Policy Types

Module 4 – Understanding Authentication

15. Passphrase Authentication
16. AAA
17. RBAC
18. RADIUS
19. 802.1X
20. EAP

Module 5 – Authentication and Key Management

21. Robust Security Networks (RSN)
22. RSN Information Element
23. RSN Authentication and Key Management (AKM)

Module 6 – Encryption

24. Encryption Fundamentals
25. Encryption Algorithms
26. WEP
27. TKIP
28. CCMP

Module 7 – Security Design Scenarios

29. Virtual Private Networks (VPN)
30. Remote Networking
31. Guest Access Networks

Module 8 – Secure Roaming

32. Roaming Basics and Terminology
33. Preauthentication
34. PMK Caching
35. Opportunistic Key Caching (OKC)

36. 802.11r FT
37. Proprietary Roaming
38. Voice Enterprise

Module 9 – Network Monitoring

39. Wireless Intrusion Prevention Systems (WIPS)
40. WIPS Deployment Models
41. WIPS Policy
42. Threat Mitigation
43. Location Services
44. WNMS
45. Protocol Analysis
46. Spectrum Analysis