



In today's network environments the implementation of wireless technologies is a serious undertaking. Improper planning can lead to an inadequate return on investment. Insufficient understanding of the security implications of wireless can lead to catastrophic results.

This course enables an individual to plan, select, and implement the appropriate wireless hardware and deploy the correct security controls to support a typical environment. A focus on RF(Radio Frequency) technologies in a vendor neutral environment with hands-on laboratories to reinforce concepts allows participants the broadest exposure to key concepts. This course is committed to be the most current in the industry with professionally developed laboratory exercises and real world hardware.

### Course Benefits

Following this Mile2 Official Course, participants will be prepared to design, implement, and administer wireless technologies and associated security controls that are typical in today's wireless networks. Additionally, awareness of the current threats against wireless networks will be investigated and countermeasures detailed. Course participants will have the ability to complete laboratories in all of the following areas:

- Selecting and implementing the appropriate wireless equipment for a given environment
- Performing a wireless site survey
- Employing various wireless authentication mechanisms
- examination ining various wireless security exploits
- Determining environmental factors that affect wireless performance
- Evaluating the latest wireless security standards
- Developing a wireless security policy

### Objective of Laboratory Scenarios:

This course is instructor-led; a portion being lecture, concepts, and demonstrations and an equal amount of practical, hands-on exercises to give participants the ability to reinforce concepts introduced in the workbook/lecture.

### Prerequisites:

- Knowledge of TCP/IP
- 12 months experience in Networking Technologies
- Computer Hardware Knowledge
- Typical Operating System Experience



# COURSE CONTENT

## Module 1: Wireless Concepts

- RF Fundamentals
- RF Mathematics
- RF Signal and Antenna Concepts
- RF Antenna Accessories
- Spread Spectrum Technologies
- IEEE 802.11 Standards
- 802.11 Industry Organizations
- 802.11 Protocol Architecture
- 802.11 MAC & Physical Layer Technologies
- Laboratory Scenario

## Module 2: Network Design, Installation and Management

- Wireless LAN Infrastructure and Client Devices
- 802.11 Network Design, Implementation, and Management
- Describe and demonstrate the different types of WLAN management systems and their features
- 802.11 Network Troubleshooting
- Laboratory Scenario

## Module 3: Site Survey

- 802.11 Network Site Survey Fundamentals
- 802.11 Network Site Survey Systems and Devices
- Laboratory Scenario

## Module 4: Wireless Security Basics

- The various methods of target locating and WLAN mapping
- Methods of information gathering
- Compare, contrast, and demonstrate hardware used to circumvent 802.11 Security
- How to recognize, perform, and prevent typical types of attacks
- The commonality and simplicity of attacks against wireless infrastructure devices
- Security vulnerabilities associated with public access or other unsecured wireless networks
- Laboratory Scenario

## Module 5: 802.1x Authentication

- Exploring legacy authentication protocols
- AAA server concepts
- The purpose and characteristics of 802.1X and EAPAuthentication design models and their scalability aspects
- Laboratory Scenario

## Module 6: Wireless Sniffing, Capture and Decryption

- How to select and use an 802.11 protocol analyzer
- Use of protocol analysis to capture sensitive information

- Explain and demonstrate security protocol circumvention against types of authentication and/or encryption
- Laboratory Scenario

### **Module 7: Enterprise Wireless Security**

- Describe secure infrastructure management protocols including WPA/WPA2/802.11i Security
- Network segmentation and its factors on WLAN network design Explain the role and importance of VLANs in an 802.11 WLAN infrastructure
- The purpose of and features in role-based access control (RBAC), including the configuration of RBAC in WLAN Switches/Controllers
- 802.11i Authentication and Key Management
- PKI and Authentication
- Describe and demonstrate layered security solutions
- Laboratory Scenario

### **Module 8: Wireless VPN Technologies**

- The concepts about VPNs
- VPN Protocols
- VPN Implementation
- The impact of L2, L3, and L7 security protocols on fast roaming and network throughput
- Laboratory Scenario

### **Module 9: Wireless Intrusion Detection**

- Security features of 802.11 WIPS
- Different types of 802.11 Wireless Intrusion Prevention Systems (WIPS)
- 802.11 WIPS baselining
- Identify the attacks and preventative measures of WIPS Fingerprinting
- Laboratory Scenario

### **Module 10: Security Policy**

- The phases of security policy development
- The purpose and goals of wireless LAN security policies
- Performing a risk assessment for a wireless LAN, including asset analysis and legal implications
- Performing an impact analysis for typical wireless LAN attack scenarios
- Appropriate installation locations for wireless LAN hardware
- Implementation of client-side security applications
- Layered security solutions
- The importance of on-going WLAN monitoring and documentation
- Security policy criteria related to wireless public-access network use
- Security implications of using non-standard security solution
- Given a set of business requirements, design a scalable secure wireless LAN solution

For information and registration, call 1-888-296-6682 Ext: 267  
or email [training@novaknowledge.com](mailto:training@novaknowledge.com)

