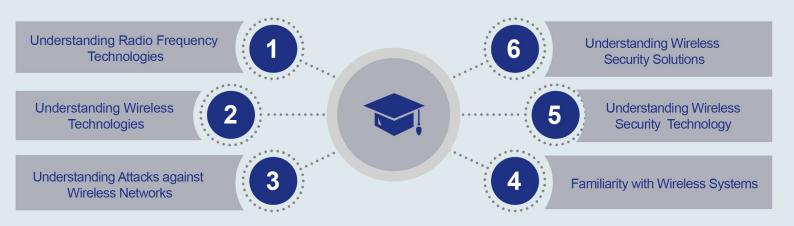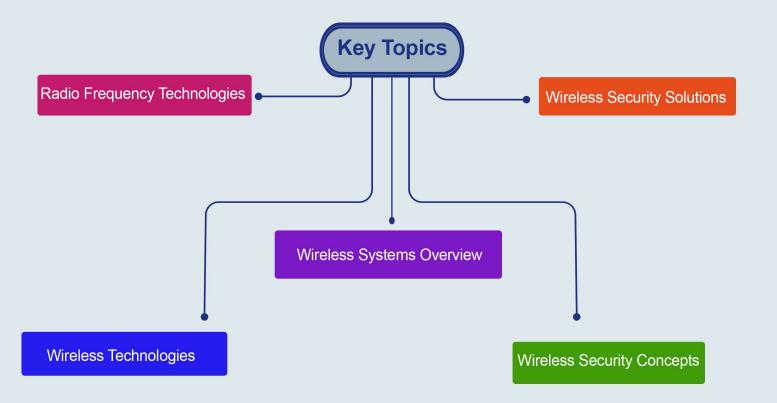**Terminus System**

About the Course

The wireless industry continues to grow in leaps and bounds with more and more gadgets evolving to be wireless. Unfortunately, the security that is implemented on wireless equipment is often lacking, resulting in severe security vulnerabilities. This is most often due to poor security awareness or a lack of understanding of the risks and ramifications. This course was created in an attempt to organize and summarize today's relevant Wi-Fi attacks and will provide you with a solid understanding of wireless insecurities.

Learning Objectives

1 Understanding Radio Frequency Technologies

2 Understanding Wireless Technologies

3 Understanding Attacks against Wireless Networks

4 Familiarity with Wireless Systems

5 Understanding Wireless Security Technology

6 Understanding Wireless Security Solutions

Terminus
System

Key Topics

Key Topics

Radio Frequency Technologies

Wireless Security Solutions

Wireless Systems Overview

Wireless Technologies

Wireless Security Concepts

Pre Requisites

- Information Security Concepts & Principles Course
- Network Securiy Course

What You Will Receive

Course Presentation File

Complementary Files

Wireless Security eBook

Who Should Attend

- Network Administrator
- Security Engineers
- CTOs
- System Administrators
- System Engineers
- Penetration Testers

Syllabus

Radio Frequency Technologies

- o RF Fundamentals
- o RF Math
- o Spread Spectrum Technologies

Wireless Technologies

- o 802.11 Standards and Amendments
- o Main 802.11 Protocols
- o 802.11 MAC Frame
- o Control Frames
- o Management Frames
- o Data Frames
- o Interacting with Networks

Wireless Systems

- o Architecture
- o Operating Modes
- o Infrastructure Network
- o Ad--Hoc Network
- o Wireless Distribution System
- o Monitor Mode
- o Packets and Network Interaction
- o Wireless Vulnerabilities

Wireless Attacks

- o Rogue Base Station
- o Scrambling
- o Jamming
- o Sniffing

Terminus
System

Syllabus

o Masquerading
o Content Modification
o Denial of Service (DoS) attacks
o Man-in-the-middle attacks
o ARP poisoning
o WEP Attacks
o WPA Attacks

Security Solutions

o Policy
o Design & Configuration
o Authentication
o Encryption
o IPS
o Access Control
o Message Modification Detection
o Message Replay Protection
o Secure Roaming
o Network Monitoring

Hands-on Training

- Lab 1: Find Hidden SSIDs using Aircrack-ng
- Lab 2: Cracking WEP via a Client
- Lab 3: Crack a WEP Network using Fern WiFi Cracker
- Lab 4: Crack a WPA2 Network using Aircrack-ng