



Wireless Security: Hands-on

As wireless technologies become ever more pervasive, the need to consider the risks they present should form part of any information security policy

What you will learn

- Discover the latest security standards and practices in WiFi
- Familiarise yourself with various hardware and software wireless tools
- Understand the threats to wireless networks, including rogue access points, denial of service (DoS) attacks and eavesdropping
- In-depth coverage of a comprehensive series of wireless security measures, including WEP, WPA / WPA2 and 802.11i
- Learn how hackers and auditors test wireless networks for vulnerabilities
- Explore how an attacker might attempt to subvert and bypass each type of security control
- Consider the security of other wireless technologies such as RFID and Bluetooth

Benefits

- Understand how hackers target wireless networks
- Our state-of-the-art class environment provides delegates with a first-hand opportunity to experiment with the tools of the trade
- The course culminates in a hands-on exercise to create a secure wireless network using digital certificates for authentication
- Delegates leave with knowledge they can apply outside the world of WiFi, such as how public key cryptography works
- The course is designed to educate for the purpose of properly defending systems from unauthorised wireless attacks

Who should attend

- Those responsible for, or with an interest in, the security of IT systems (both wired and wireless), including but not limited to: IT Managers, Systems/ Network Administrators, IT Security Professionals and Forensic/Network Investigators

To Book Call:

0870 600 1667

Duration: 2 days
Cost: £999 + VAT



CPE Credits: 16



MSc Credits: 15



Course style

Delegates learn how to secure wireless networks and then test them for vulnerabilities from both a theoretical and practical perspective. Open group discussion is strongly encouraged.

Prerequisites

- Basic understanding of TCP/IP networking.
- Previous use of wireless networks and Linux is desirable.

Course content highlights

WIRELESS NETWORK SECURITY

INTRODUCTION

- Overview of wireless technologies (e.g. Bluetooth, WiFi, WiMax)
- Wireless components and their functionality
- 802.11 architecture and commonly used terminology

WIRELESS VULNERABILITIES

- The dangers of using public WiFi networks
- Practical exercises on the equipment and tools used to gain access
- Unauthorised WiFi: rogue access points

SECURING WIRELESS NETWORKS

- How wireless networks can be protected against attack, including WEP, TKIP, CCMP and their relative strengths and weaknesses
- 802.11i and how the standard relates to WPA and WPA2
- 802.1X including EAP authentication methods, key management and RADIUS
- Practical exercise creating digital certificates for an 802.11i compliant network

TESTING THE LEVEL OF SECURITY

- “War driving” to audit WiFi networks
- Finding “hidden” networks
- Circumventing MAC Filtering
- Breaking WEP encryption
- Breaking WPA encryption
- Security considerations for Bluetooth, WiMax and RFID

Professional Training Authored By Experts