Course Outline

ADVANCEDTRAINING
Inspire. Grow. Achieve.

Wireless Networks: Security Threats and Attacks

General Description

The last few years have seen a dramatic growth in the use of a vast variety of wireless and mobile network devices. With this growth has come a major increase in the range and complexity of security issues. The threats and risks have never been greater.

This 2-day workshop is a hands-on practical laboratory designed to demonstrate the vulnerabilities of wireless and mobile networks and to implement various active and passive attacks in order to carry out penetration tests on these systems. The laboratory makes use of the power and flexibility of a suite of wireless tools used to illustrate wireless insecurity, and focuses on understanding the inner workings, tools and methodologies of modern-day attacks to find out how to best protect yourself and your organization.

Audience

The program is designed for in-house presentation to groups. It is designed to be used both for initial induction and for periodic security refresher training.

This workshop is a hands-on practical laboratory designed to demonstrate the vulnerabilities of wireless and mobile networks and to implement various active and passive attacks in order to carry out penetration tests on these systems. This laboratory makes use of the power and flexibility of a suite of wireless tools used to illustrate wireless insecurity, and focuses on understanding the inner workings, tools and methodologies of modern-day attacks.

Outcomes

This workshop will commence by examining the characteristics of the different wireless and mobile networks including Bluetooth and other WPANs, Android, and IEEE802.11 variants of WLANs. The manner in which these networks can be compromised by attacks such as, sniffing, spyware, spoofing, hijacking, man-in-the-middle, buffer overflow, injection, brute force, denial of service (as well as the usual range of viruses, worms and Trojans) will be discussed.

Microsoft Partner
Gold Learning
Silver Desktop

☎ 1300 86 87246

1300 TO TRAIN

Course Details

Course code: STA
Duration: 2 days
Starting time: 9am
Finishing time: 4.30pm

Booking guidelines

Contact our learning consultants on 1300 86 87246 and we will assist you with your booking.

For more information about any of our training courses, contact our Learning Consultants
on 1300 86 87246 or email us on info@advancedtraining.com.au
Visit us on the web at www.advancedtraining.com.au

Course Outline

ADVANCEDTRAINING

- **Module 1**
  - Background to risks and vulnerabilities in use of wireless and mobile networks
- **Module 2**
  - Practical Workshop – Building and testing WEP, WPA and WPA2 wireless systems
- **Module 3**
  - Discussion and analysis of wireless/mobile attacks, risks and vulnerabilities
- **Module 4**
  - Practical Workshop – Building and testing Bluetooth wireless/mobile systems
- **Module 5**
  - Practical Workshop – Building and testing Android wireless/mobile systems
- **Module 6**
  - Discussion and analysis of wireless/ mobile attacks in 3G/4G wide area networks