Wireless Networks:
Security Threats and Attacks

Duration **2 days**

How to protect yourself and your organisation in a world where the threats and risks have never been greater.

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 Find out how to best protect yourself and your organisation.

The Problem

Many of the techniques used to attack networks 10 years ago are still causing considerable damage today. These techniques have been reinvented and are frequently based on variations of basic themes or combinations of these used to form multi-vector and multi-payload attacks. The scale of interconnectivity that has evolved further compounds the damage that such attacks can cause. Further, wireless and mobile network access brings with it the opportunity for hackers to exploit many of these attacks, all be it in different forms. As networks have scaled in size and complexity so have attack vectors.

The Solution

This workshop will be run as a laboratory in which PCs running virtual machines which in turn run Backtrack5 Rev 2 will be used in conjunction with networking equipment such as a variety of access points, wireless interface devices, Bluetooth and Android equipment etc and a selection of these attacks will be created, tested and verified. Delegates will work in pairs and be guided through the process of carrying out a range of penetration attacks to which WPANs, WLANs and handheld mobile computers are particularly vulnerable.

Key Workshop Topics

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.

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.

Course Contents

Session 1
- Background to risks and vulnerabilities in use of wireless and mobile networks

Session 2
- Practical Workshop – Building and testing WEP, WPA and WPA2 wireless systems

Session 3
- Discussion and analysis of wireless/ mobile attacks, risks and vulnerabilities

Session 4
- Practical Workshop – Building and testing Bluetooth wireless/mobile systems

Session 5
- Practical Workshop – Building and testing Android wireless/mobile systems

Session 6
- Discussion and analysis of wireless/ mobile attacks in 3G/4G wide area networks

Overview of Tools

Individual PCs will run Backtrack 5 Rev 2 (2012) which is a Linux-based penetration testing suite which runs the following tools in a purely native environment:

- ***kismet***
  a wireless network detector and packet sniffer
- ***netstumbler***
  a tool for discovering fake access points
- ***airmon-ng***
  a tool that can help set a wireless adapter into monitor mode (rfmon)
- ***airodump-ng***
  a tool for capturing packets from an Access Point
- ***aireplay-ng***
  a tool for forging ARP requests
- ***aircrack-ng***
  a tool for decrypting WEP keys
- ***iwconfig***
  a tool for configuring wireless adapters in monitor mode and generation of fake ARP requests
- ***macchanger***
  a tool that allows one to view and/or spoof (fake) MAC address
- ***wireshark***
  a tool for passive collection and analysis of packets
- ***android exploit software***

The wireless adapter cards will allow both passive packet sniffing and active packet injection. In this laboratory, we will be using Alfa AWUS036H 802.11b/d Long-Range Wireless USB Adapters, Bluetooth mobile phones and Android handheld computers. A variety of CISCO, Linksys and D-Link Wireless Access Points will be used which will be configured with a variety of security options.

A variety of Bluetooth equipment with specifically configured Cambridge chipset USB Bluetooth adaptors will be used for the next part of the workshop.
Most importantly, modern Android devices will be used to demonstrate how private information can be extracted by the use of specific exploits and how such mobile devices can be subject to information theft and spam bot attacks.