Hacking Wireless LAN's

WIRELESS HACKING

With the use of laptop computers and PDA's and mobile devices increasingly on the rise, the places where people perform computing are spreading. Network connectivity has become an integral part of computing. It is easy therefore to see why wireless networking is being employed on an increasingly larger scale. Wireless networks are a growing target for hackers creating numerous security challenges such that flaws and vulnerabilities can be exploited by malicious hackers to gain access into wireless system architectures.

The Wireless Hacking course is a new and unique course that will help IT professionals develop and implement secure networks by understanding current standard vulnerabilities and how attacks are planned and perpetrated.

Training Overview

Wireless Hacking will help you understand how to improve WLAN security by showing the ways networks are attacked. You will examine current 802.11 standard security flaws and learn possible countermeasures. The course is ideally divided into three parts: a detailed description of the hardware needed to perpetrate the attack; how to perform network mapping and site surveying; and then to learn how attacks are performed.

Who should attend?

- IT Managers
- IT Security Specialists
- Security Officers
- EDP Managers
- Wireless Network Administrators
- Individuals and enthusiasts interested in this topic

zone-h
unrestricted information

Course Contents

An intensive 2-day course covering the following topics.

Introduction to wireless hacking
- Wireless technology worldwide - WLAN's insecurity
- Why analyzing a WLAN
- Wardriving - Warchalking
- Wireless penetration testing methodology

Protocol 802.11
- Protocol analysis (802.11a, 802.11b, 802.11g) - Protocol architecture
- DSSS, FHSS, OFDM technologies
- Frame 802.11

Live session: traffic analysis

Assembling the arsenal: hardware 802.11
- PDA's vs. laptops
- Wireless cards
- Chipsets: Prism, Cisco Aironet, Hermes, Symbol, Atheros

RF behavior
- Gain, loss, reflection, refraction, other
- Antennas: sectorial, omnidirectional, directional
- Rf cables and connectors
- EIRP calculation: practical exercises

Live session: how to build a pringles antenna

802.11 drivers and utilities
- Linux wireless extensions - Linux-wlan-ng utilities – Hostap - Windows

Network mapping and site surveyng: 'wardriving'
- Active scanning in wireless network discovery
- Monitor mode network discovery and traffic analysis tools
- Kismet – Airtraf – Airfart - Netstumbler
- RF signal strength monitoring tools

Live session: wardriving

Securing wireless networks (live)
- WEP algorithm - Hide SSID - MAC filtering - WEP – WPA
- WPA2 - 802.11i

Algorithm vulnerabilities (live)
- WEP – WPA - WPA2

Planning the attack
- Network footprinting
- Site surveying: considerations and planning
- Proper attack timing and battery power preservation
- Stealth issues in wireless penetration testing

Assembling the arsenal: tools of trade (live)
- Encryption cracking tools
- WEP crackers
- AirSnort – Wepattack - Aircrack
- Tools to retrieve WEP keys stored on the client hosts: LucentRegCrypto
- Traffic injection tools used to accelerate WEP cracking

Dos attack: - Airjack - File2air - void11 – macflood

Breaking through (live)
- Bypassing closed ESSIDs, MAC and protocols filtering
- Wireless frame generating tools
- AirJack - File2air - FakeAp

Various means of key recovery (live)
- WEP bruteforcing - The FMS attack - The Korek Attack

Hardware administration
- Main hardware configuration parameters - Best practices

Bluetooth technology
- Protocol and stack – Vulnerabilities - Possible scenarios

What You Will Learn

- How to think like a hacker to improve protection of your system
- How to exploit WLAN standard vulnerabilities
- Typical techniques used to gain access into a wireless LAN
- How penetration testing is your first line of defense

Duration

2 days

Prerequisites

A background in wireless networks

About Zone-H

Zone-H is an independent and open-source digital observatory, considered today as the most authoritative voice on cybercrime in the Internet. The www.zone-h.org homepage registers about 35,000 single accesses and a total of nearly 800,000 clicks, on an average day.

In addition to information and analysis on cyber terrorism and cybercrime, Zone-H offers the IT community, IT Security services and educational programs, providing a constant stream of web monitoring activities, including daily advisories, statistics, updates and news. The data merge into one of the biggest digital archives in the world, including, to date, over 2 million recorded attacks and information on attacker profiles, motivations and methodologies of intrusion.

Zone-H presents a realistic and "no-hat" perspective on web trends, supported by a worldwide community of more than 50 experts, among which are IT professionals, journalists, students and scholars. Zone-H websites are available in 13 different editions: English, Italian, French, Russian, Brazilian, Slovak, Spanish, Japanese, Slovenian, Turkish, German, Latvian and Croatian.

The Zone-H worldwide education and training programs focus on the fundamental aspects of IT Security. The program addresses a wide ranging international audience, promoting "ethical hacking" techniques and utilizing our own unique proprietary cybercrime observatory, to provide a research-based source of training information.