Hacking Wireless LANs

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 1 day course covering the following topics.

Introduction to wireless hacking

Understanding wireless standards
Overview of 802.11
MAC spoofing
Man-in-the-middle attacks
Denial of service attacks

Sniffing wireless networks

Wlan operating modes
Monitoring capable hardware
THC-rut
Airpcap
Airodump-ng

Analyzing captured traffic

Kismet
Ettercap
Wireshark

802.11 MAC

Authentication flood
Deauthentication flood

WEP attacks

FMS
Korek
PTW
Chop chop
Caffe latte

Leap attacks

THC leapcracker
Asleap
Dictionary attacks

Client attacks

Rogue APs
Airbase-ng
Evil twin AP
Airsnarf
Hotspotter
Identify rouge APs
Lorcon packet injection
TCP hijacking

WPA2 attacks

Cowpatty
Aircrack-ng

WPS attacks

Bully
Reaver-wps
Dumpper

Evade captive portals

DNS tunneling
ICMP tunneling

Attacking with CUDA

Pyrit
Cowpatty
Hashcat
Cal++

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 WLAN
- How penetration testing is your first line of defense

Duration

1 day

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 11 millions 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.

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.

zone-h
unrestricted information
www.zone-h.org