

Who's watching your back?

Foundstone[®]
Professional Services A DIVISION OF McAfee

Training Datasheet

Ultimate Hacking Wireless

DURATION

- Four (4) Days

WHAT YOU'LL LEARN

- How intruders discover, disrupt service and compromise wireless networks
- The risks each individual faces when using wireless networks
- Security countermeasures and best practices to reduce risk

COURSE MATERIALS

- Student manual
- Class handouts
- Foundstone authored book
- Foundstone t-shirt
- Free Tools CD with course tools and scripts
- BackTrack the top rated bootable linux distribution

SUGGESTEDNEXTCOURSE(S)

- Ultimate Hacking
- Ultimate Hacking: Expert
- Incident Response & Forensics
- Ultimate Web Hacking

Our lives are constantly becoming more and more dependent on wireless technologies. Its convenience supports our ability to roam freely throughout our homes and offices, while enabling us to quickly check the news at our local coffee house or prior to boarding a flight. The use cases are nearly infinite; from vending machines, taxi cabs, and ticketing kiosks to wireless bridges facilitating building to building communication, wireless technologies have become a staple in our data communications. What is commonly taken for granted, however, is that this invisible facilitator can come at a price.

Foundstone's Ultimate Hacking: Wireless class takes an in-depth look at current attacks against wireless networks. The hands-on, Linux-based class starts off with an overview of the IEEE 802.11 protocol then dives deep into hardcore attacks used in the real world. By the end of the first day students will understand the underlying technology, the hardware needed to conduct an assessment, and the techniques used to sniff open communications. The next two days evaluate the popular IEEE 802.11 wireless security mechanisms and the methods to defeat each of them. On the last day, the class is taught the basic on the operation of Bluetooth and Radio-frequency identification technologies and then targets them through the eyes of an attacker. At the end of each topic student's perform hands on testing in a lab environment to gain experience and test their understanding with each attack. For the class to be applicable in real world scenarios, students are given a quick refresher about popular wired-side hacking techniques through-

out the class. At the end of the class each student is challenged in the final lab, which requires them to not only defeat wireless security mechanisms but to leverage that access and gain control over live targets within Foundstone's attack lab.

Foundstone closes each topic by discussing defense mechanisms for known attacks and providing strategic steps that can be taken to improve wireless network security. Throughout the class students will question the underlying security of all wireless networks.

- How confident are you that your wireless infrastructure can withstand the latest attacks?
- Can you afford to trust vendor claims?
- Are you truly aware of all your weaknesses?

Foundstone's Ultimate Hacking series goes wireless to help students see wireless networks the way hackers see them. Take control of the wireless environment. Learn the tools, techniques and methods attackers use in order to develop an effective defense against their increasingly sophisticated onslaught.

Who Should Take This Class

Anyone responsible for the planning, implementation, maintenance or assessment of 802.11/RFID/Bluetooth wireless networks would benefit from Ultimate Hacking Wireless.

Exercises

All topics are supported by hands-on

exercises specifically designed to increase knowledge retention. Classroom exercises provide the extensive hands-on experience needed to effectively identify, exploit, and secure complicated and obscure vulnerabilities..

Course Outline

Day 1

Module 1 – Introduction

- Introductions
- About Foundstone
- Purpose
- Course Objectives
- Classroom Etiquette

Module 2 – Environment and Setup

- Classroom and Computing environments
- Backtrack
- Linux Review

Module 3 – 802.11 Fundamentals

- History of 802.11
- 802.11 Design and Terminology
- Deployment and Architecture

Module 4 – 802.11 Discovery and Monitoring

- Wireless Card Operating Modes
- WLAN Discovery and Tools
- Rogue Access Points
- Site Surveying

Day 2

Module 5 – 802.11 Toolkit

- Laptops and PDAs
- Operating Systems
- Wireless Adapters and Access Points
- Antennas

Module 6 – Basic 802.11 Attacks

- Uncovering hidden SSIDs
- Defeating MAC Filtering
- Man in the Middle Attacks
- Attacking Captive Portals
- Device Theft

Module 7 – 802.11 Denial of Service Attacks

- Attacking the Physical Layer
- Attacking the Data Link Layer

Module 8 – Understanding and Attacking WEP

- Understanding WEP encryption
- Attacking WEP

Day 3

Module 9 – Understanding and Attacking WPA

- WPA Security
- Targeting WPA Enterprise
- EAP Attack Surface
- Hardware/Software Vulnerabilities
- EAP-FAST
- LEAP
- EAP-MD5
- EAP/TLS
- PEAP and EAP/TTLS

Module 10 – Bluetooth Fundamentals

- Bluetooth Introduction
- Terminology and Architecture
- Basic Communication
- Authentication and Encryption
- Profiles

Module 11 - Bluetooth Tools and Discovery

- Adapters
- Operating systems
- Additional Hardware
- Discovery

Day 4

Module 12 - Bluetooth Enumeration and Attacks Enumeration

- Enumeration
- Denial of Service Attacks
- Eavesdropping/Sniffing
- Paring Attacks
- Virus Propagation

Module 13 - RFID

- RFID Introduction
- RFID Architecture
- Discovering/Reading RFID devices
- Cloning RFID devices