Offensive Security

Wireless Attacks - WiFu

v. 3.0

Mati Aharoni

Devon Kearns

Thomas d'Otreppe de Bouvette

Course Overview

The wireless industry continues to grow in leaps and bounds with more and more gadgets evolving to be wireless. Access points, media centers, phones, and even security systems are commonplace in the average household. Unfortunately, the security that is implemented on wireless equipment is often lacking, resulting in severe security vulnerabilities.

In practice, many companies and organizations still use and deploy vulnerable wireless gear, often in their default configurations. This is most often due to poor security awareness or a lack of understanding of the risks and ramifications.

This course was created in an attempt to organize and summarize today's relevant Wi-Fi attacks and will provide you with a solid understanding of wireless insecurities along with the latest tools and techniques used to exploit these insecurities.

Prerequisites

Please read the following very carefully:

- There are HARDWARE prerequisites for this course. Each student is expected to purchase or previously own a wireless access point and a suitable "injection capable" wireless card. To ensure hardware compatibility, we recommend the use of an access point that can be configured with WPA/WPA2 encryption and WEP encryption with both open and shared key authentication. The ALFA Networks 500mW USB card is also strongly recommended. Please refer to our "recommended hardware" for this course at the following: http://www.offensive-security.com/wifu_hardware.php
- Please note that Offensive Security does not sell hardware. We merely recommend the hardware models that are known to work for this course.
- A modern laptop or desktop is required that can boot and run BackTrack.

- The student must have a solid understanding of TCP/IP and the OSI model as well as a reasonable level of familiarity with Linux in order to complete the course.
- A fast Internet connection is required to download the course videos.

Course Description

Offensive Security Wireless Attacks also know as “WiFu”, is a course designed for penetration testers and security enthusiasts who need to learn to implement various active and passive wireless attacks.

It is vital that you meet the technical prerequisites as stated above; otherwise you might find yourself lost as the course progresses. In many cases, previous knowledge is assumed and theoretical explanations are shortened or referenced rather than thoroughly explained.

Please note, we do not have a refund policy - it is **your** responsibility to ensure you meet the mentioned technical requirements. However, if you do meet the technical requirements, this course will very quickly expose you to the world of wireless insecurity and teach you the inner workings, tools, and methodologies of modern day attackers.

Course Objectives

- The student will gain insight into the wireless offensive security field, which will expand awareness for the need of **real world** security solutions.
- The student will learn to implement attacks against WEP encrypted networks.
- The student will learn to implement attacks against WPA encrypted networks.
- The student will learn to implement advanced attacks such as PRGA key extraction and one-way packet injection.
- The student will learn alternate WEP and WPA cracking techniques.
- The student will be introduced to various wireless reconnaissance tools and learn to implement different rogue access point attacks.
- The student will be familiarized with the BackTrack wireless tools

Certification

Successful completion of the certification exam earns the student the Offensive Security Wireless Professional (OSWP) certification.

The certification exam requires the student to connect to our examination labs and attack WEP and WPA networks under various hardened configurations.

Upon successful completion of the exam, the student will receive an OSWP certificate, which testifies their competency in attack methods and techniques in WEP and WPA environments.

Course Outline

A Note from the Author

Before we Begin

1. IEEE 802.11

2. Wireless Networks

3. Packets and Network Interaction

4. Getting Started