

# 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](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 known 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

##### 1.1 IEEE

###### *1.1.1 Committees*

##### 1.1.2 IEEE 802.11

##### 1.2 802.11 Standards and Amendments

##### 1.3 Main 802.11 Protocols

###### *1.3.1 Detailed Protocol Descriptions*

#### 2. Wireless Networks

##### 2.1 Wireless Operating Modes

###### *2.1.1 Infrastructure Network*

###### *2.1.2 Ad-Hoc Network*

###### *2.1.3 Wireless Distribution System*

###### *2.1.4 Monitor Mode*

#### 3. Packets and Network Interaction

##### 3.1 Wireless Packets – 802.11 MAC Frame

###### *3.1.1 Header*

###### *3.1.2 Data*

###### *3.1.3 FCS*

##### 3.2 Control Frames

###### *3.2.1 Common Frames*

##### 3.3 Management Frames

###### *3.3.1 Beacon Frames*

###### *3.3.2 Probe Frames*

###### *3.3.2 Authentication*

###### *3.3.3 Association/Reassociation*

###### *3.3.4 Disassociation/Deauthentication*

###### *3.3.5 ATIM*

###### *3.3.6 Action Frames*

##### 3.4 Data Frames

###### *3.4.1 Most Common Frames*

##### 3.5 Interacting with Networks

###### *3.5.1 Probe*

###### *3.5.2 Authentication*

###### *3.5.3 Association*

###### *3.5.4 Encryption*

#### 4. Getting Started

##### 4.1 Choosing Hardware

###### *4.1.1 Adapter Types*

###### *4.1.2 dB, dBm, dBi, mW, W*

###### *4.1.3 Antennas*

##### 4.2 Choosing a Wireless Card

###### *4.2.1 Alfa AWUS036H*

##### 4.3 Choosing an Antenna

#### 4.3.1 Antenna Patterns

### 5. Linux Wireless Stack and Drivers

#### 5.1 ieee80211 vs. mac80211

##### 5.1.1 *ieee80211*

##### 5.1.2 *mac80211*

#### 5.2 Linux Wireless Drivers

##### 5.2.1 *Resolving AWUS036H Issues*

##### 5.2.2 *Loading and Unloading Drivers*

##### 5.2.3 *mac80211 Monitor Mode*

##### 5.2.4 *ieee80211 Monitor Mode*

### 6. Aircrack-ng Essentials

#### 6.2 Airmon-ng

##### 6.2.1 *Airmon-ng Usage*

##### 6.2.2 *Airmon-ng Usage Examples*

##### 6.2.2 *Airmon-ng Lab*

#### 6.3 Airodump-ng

##### 6.3.1 *Airodump-ng Usage*

##### 6.3.3 *Precision Airodump-ng Sniffing*

##### 6.3.4 *Airodump-ng Troubleshooting*

##### 6.3.5 *Airodump-ng Lab*

#### 6.4 Aireplay-ng

##### 6.4.1 *Aireplay-ng Usage*

##### 6.4.2 *Aireplay-ng Troubleshooting*

##### 6.4.3 *Optimizing Aireplay-ng Injection Speeds*

#### 6.5 Injection Test

##### 6.5.1 *Injection Test Usage*

##### 6.5.2 *Aireplay-ng Lab*

### 7. Cracking WEP with Connected Clients

#### 7.1 Initial Attack Setup

##### 7.1.1 *Airmon-ng*

##### 7.1.2 *Airodump-ng*

#### 7.2 Aireplay-ng Fake Authentication Attack

##### 7.2.1 *Fake Authentication Usage*

##### 7.2.2 *Fake Authentication Troubleshooting*

##### 7.2.3 *Running the Fake Authentication Attack*

##### 7.2.4 *Fake Authentication Lab*

#### 7.3 Aireplay-ng Deauthentication Attack

##### 7.3.1 *Deauthentication Attack Usage*

##### 7.3.2 *Deauthentication Troubleshooting*

##### 7.3.3 *Running the Deauthentication Attack*

##### 7.3.4 *Deauthentication Lab*

#### 7.4 Aireplay-ng ARP Request Replay Attack

##### 7.4.1 *What is ARP?*

##### 7.4.2 *ARP Request Replay Usage*

##### 7.4.3 *Running the ARP Request Replay Attack*

##### 7.4.4 *ARP Request Replay Attack Lab*

#### 7.5 Aircrack-ng

##### 7.5.1 *Aircrack-ng 101*

- 7.5.2 *Aircrack-ng Usage*
- 7.5.3 *Aircrack-ng Troubleshooting*
- 7.5.4 *Running Aircrack-ng*
- 7.5.5 *Aircrack-ng Lab*
- 7.6 Classic WEP Cracking Attack Summary

## **8. Cracking WEP via a Client**

- 8.1 Attack Setup
  - 8.1.1 *Attack Setup Lab*
- 8.2 Aireplay-ng Interactive Packet Replay Attack
  - 8.2.1 *Natural Packet Selection*
  - 8.2.2 *Modified Packet Replay*
  - 8.2.3 *Running the Interactive Packet Replay Attack*
  - 8.2.4 *Interactive Packet Replay Lab*
- 8.3 Cracking the WEP Key
  - 8.3.1 *Lab*
- 8.4 Cracking WEP via a Client Attack Summary

## **9. Cracking Clientless WEP Networks**

- 9.1 Attack Assumptions
- 9.2 Attack Setup
  - 9.2.1 *Attack Setup Lab*
- 9.3 Aireplay-ng Fragmentation Attack
  - 9.3.1 *Fragmentation Attack Usage*
  - 9.3.2 *Fragmentation Attack Troubleshooting*
  - 9.3.3 *Running the Fragmentation Attack*
  - 9.3.4 *Fragmentation Attack Lab*
- 9.4 Packetforge-ng
  - 9.4.1 *Packetforge-ng Usage*
  - 9.4.2 *Running Packetforge-ng*
  - 9.4.3 *Packetforge-ng Lab*
- 9.5 Aireplay-ng KoreK ChopChop Attack
  - 9.5.1 *ChopChop Theory*
  - 9.5.2 *Aireplay-ng KoreK ChopChop Usage*
  - 9.5.3 *Running the KoreK ChopChop Attack*
  - 9.5.4 *KoreK ChopChop Attack Lab*
- 9.6 Interactive Packet Replay and Aircrack-ng
  - 9.6.1 *Interactive Packet Replay*
- 9.7 Clientless WEP Cracking Lab
- 9.8 Clientless WEP Cracking Attack Summary

## **10. Bypassing WEP Shared Key Authentication**

- 10.2 Attack Setup
  - 10.2.1 *Attack Setup Lab*
- 10.3 Aireplay-ng Shared Key Fake Authentication
  - 10.3.1 *Deauthenticate a Connected Client*
  - 10.3.2 *Shared Key Fake Authentication*
  - 10.3.3 *Running the Shared Key Fake Authentication*
  - 10.3.4 *Shared Key Fake Authentication Lab*
- 10.4 ARP Request Replay and Aircrack-ng
  - 10.4.1 *ARP Request Replay*

- 10.4.2 *Aircrack-ng*
- 10.5 Bypassing WEP Shared Key Authentication Lab
- 10.6 WEP Shared Key Authentication Attack Summary

## **11. Cracking WPA/WPA2 PSK with Aircrack-ng**

- 11.1 Attack Setup
  - 11.1.1 *Attack Setup Lab*
- 11.2 Aireplay-ng Deauthentication Attack
  - 11.2.1 *Four-way Handshake Troubleshooting*
  - 11.2.2 *Deauthentication Attack Lab*
- 11.3 Aircrack-ng and WPA
  - 11.3.1 *"No valid WPA handshakes found"*
  - 11.3.2 *Aircrack-ng and WPA Lab*
- 11.4 Airolib-ng
  - 11.4.1 *Airolib-ng Usage*
  - 11.4.2 *Using Airolib-ng*
  - 11.4.3 *Airolib-ng Lab*
- 11.5 Cracking WPA Attack Summary

## **12. Cracking WPA with JTR and Aircrack-ng**

- 12.1 Attack Setup
  - 12.1.1 *Attack Setup Lab*
- 12.2 Editing John the Ripper Rules
  - 12.2.1 *Word Mangling Lab*
- 12.3 Using Aircrack-ng with John the Ripper
- 12.4 John the Ripper Lab
- 12.5 Aircrack-ng and JTR Attack Summary

## **13. Cracking WPA with coWPAtty**

- 13.1 Attack Setup
  - 13.1.1 *Attack Setup Lab*
- 13.2 coWPAtty Dictionary Mode
- 13.3 coWPAtty Rainbow Table Mode
- 13.4 coWPAtty Lab
- 13.5 coWPAtty Attack Summary

## **14. Cracking WPA with Pyrit**

- 14.1 Attack Setup
  - 14.1.1 *Attack Setup Lab*
- 14.2 Pyrit Dictionary Attack
- 14.3 Pyrit Database Mode
- 14.4 Pyrit Lab
- 14.5 Pyrit Attack Summary

## **15. Additional Aircrack-ng Tools**

- 15.1 Airdecap-ng
  - 15.1.1 *Airdecap-ng Usage*
  - 15.1.2 *Removing Wireless Headers*
  - 15.1.3 *Decrypting WEP Captures*
  - 15.1.4 *Decrypting WPA Captures*
  - 15.1.5 *Airdecap-ng Lab*
- 15.2 Aircrack-ng



- 15.2.1 *Airserv-ng Usage*
- 15.2.2 *Using Airserv-ng*
- 15.2.3 *Airserv-ng Troubleshooting*
- 15.2.4 *Airserv-ng Lab*
- 15.3 Airtun-ng
  - 15.3.1 *Airtun-ng Usage*
  - 15.3.2 *Airtun-ng wIDS*
  - 15.3.3 *Airtun-ng WEP Injection*
  - 15.3.4 *Airtun-ng PRGA Injection*
  - 15.3.5 *Connecting to Two Access Points with Airtun-ng*
  - 15.3.6 *Airtun-ng Repeater Mode*
  - 15.3.7 *Airtun-ng Packet Replay Mode*
  - 15.3.8 *Airtun-ng Lab*

## **16. Wireless Reconnaissance**

- 16.1 Airgraph-ng
  - 16.1.1 *CAPR*
  - 16.1.2 *CPG*
- 16.2 Kismet
- 16.3 GISKismet
- 16.4 Wireless Reconnaissance Lab

## **17. Rogue Access Points**

- 17.1 Airbase-ng
  - 17.1.1 *Airbase-ng Usage*
  - 17.1.2 *Airbase-ng Shared Key Capture*
  - 17.1.3 *Airbase-ng WPA Handshake Capture*
- 17.2 Karmetasploit
- 17.2 Karmetasploit Configuration
- 17.3 Man in the Middle Attack
- 17.4 Rogue Access Points Lab

## **Appendix A: Cracking WEP via a Client - Alternate Solutions**

- A.1 Pulling Packets from Captured Data
- A.2 Creating a Packet from a ChopChop Attack

## **Appendix B: ARP Amplification**

- B.1 Equipment Used
- B.2 One for One ARP Packets
- B.3 Two for One ARP Packets
- B.4 Three for One ARP Packets