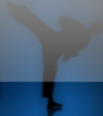


[WiFu]



www.offensive-security.com

BackTrack WiFu

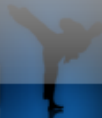
An Introduction to practical Wireless attacks

Based on Aircrack-ng



Mati Aharoni

Thomas d'Otreppe de Bouvette



Backtrack WiFu Course Description

Overview

The wireless industry is booming as more and more products and gadgets are evolving to be “wire free”. Access points, wireless music centers, wireless Skype phones etc are becoming average household goods. Unfortunately the security implementation procedures of wireless equipments are often lacking, resulting in severe security holes.

In practice, many companies and organizations still use and deploy vulnerable wireless setups. This is usually due to poor security awareness or a lack of understanding of the risks and ramifications. The course was created by Thomas d'Otreppe and Mati Aharoni in an attempt to organise and summarise today's relevant Wifi attacks. This course will provide you with a solid understanding of wireless insecurities, and also the latest tools and techniques used to exploit these insecurities. The course is mostly based on the Aircrack-ng suite, developed by Thomas d'Otreppe.

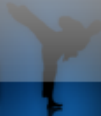
Prerequisites

Please read the following very carefully:

- There are **HARDWARE** pre-requisites 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 a WRT54GL Access Point and an Atheros PCMCIA / Mini PCI b/g wireless card. The ALFA Networks 500mw USB card is also strongly recommended. Please check our “recommended hardware” for this course: http://www.offensive-security.com/wifu_hardware.php
- Please note that Offensive Security does not sell hardware – We can merely recommend the

hardware models required for the course, and provide convenient links to amazon.

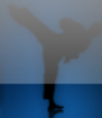
- A modern Laptop, able to run and boot backtrack.
- The student must have a solid understanding of TCP/IP and the OSI model and a reasonable level of familiarity with Linux, in order to complete the course.
- A fast Internet connection to view or download the Videos.



Course Description

"Offensive Security Wireless Attacks", also known as "BackTrack WiFu" is a course designed for penetration testers and security enthusiasts who need to learn to implement various active and passive Wireless (802.11 2.4 GHz) attacks. Please note that the course videos do not cover the first few WiFu lab guide modules which discuss 802.11 theory.

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, in case the student needs a refresher. Please note, we do not have a refund policy – it is **your** responsibility to make sure 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

Primary 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 cracking techniques, such as clientless attacks, cracking WEP via a wireless client, etc.

Secondary Objectives:

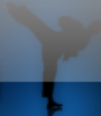
- The student will be familiarized with BackTrack wireless tools.
- The student will be introduced to other wireless attack tools such as Kismet and aircrack-ng.

Certification

Offensive Security Wireless Attacks – Backtrack WiFu introduces a new Offensive Security Certification – “**Offensive Security Wireless Professional**”.

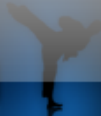
The certification exam requires the student to connect to our examination labs and attack WEP and WPA networks, under various hardened configurations.

Upon successful completion of the challenge, the student will receive an **OSWP** certificate, which testifies their competency of attack methods and techniques in a WEP and WPA hardened wireless environment.



Registration Process

- The registration process involves sending a no commitment preregistration mail, using our contact URL, at: <http://www.offensive-security.com/contact.php>
- This mail puts you in a waiting list in order of mail arrival.
- You will then be sent a registration form in which we will collect several personal details (Name, Surname, Address , Contact Information and non free Email). In addition, you will be asked to fill out a very short questionnaire.
- **You will be required to purchase or previously own suitable hardware for the course. Please visit http://www.offensive-security.com/wifu_hardware.php for more information.**
- Once we receive the registration form it will be reviewed, and will be subject to our approval. If approved, you will receive a confirmation mail from us. Please note that we reserve the right to refuse “Offensive Security” training, at our discretion.
- Once payment is approved, you will be sent an email with links to the Offensive Security WiFu course materials.



Offensive Security Wifu Course Overview

Please note that the WiFu videos begin from module 5 in the syllabus. Definitions, diagrams and capture dumps are not discussed in the videos. The following is a course outline describing the main topics discussed:

| |
|---|
| 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 description |
| 1.3.1.1 IEEE 802.11 |
| 1.3.1.2 IEEE 802.11b |
| 1.3.1.3 802.11a |
| 1.3.1.4 802.11g |
| 1.3.1.5 802.11n |
| 2. Wireless networks |
| 2.1 Wireless operating modes |
| 2.1.1 Infrastructure Mode |
| 2.1.2 Ad hoc network |
| 2.1.3 Monitor mode |
| 3. Packets and stuff |
| 3.1 Wireless packets - 802.11 MAC frame |



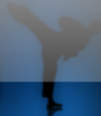
| |
|---------------------------------------|
| 3.1.1 Header |
| 3.1.1.1 Frame control |
| 3.1.1.2 Duration/ID |
| 3.1.1.3 Addresses |
| 3.1.1.4 Sequence Control |
| 3.1.2 Data |
| 3.1.3 FCS |
| 3.2 Control frames |
| 3.2.1 Common frames |
| 3.2.1.1 ACK |
| 3.2.1.2 PS-Poll |
| 3.2.1.3 RTS/CTS |
| Frames |
| Capture |
| 3.3 Management frames |
| 3.3.1 Beacon |
| 3.3.2.2 Response |
| 3.3.3 Authentication |
| 3.3.4 Association / Reassociation |
| 3.3.4.1 Association Request |
| 3.3.4.2 Reassociation Request |
| 3.3.4.3 Response |
| 3.3.5 Disassociate / Deauthentication |
| 3.3.6 ATIM |
| 3.3.7 Action frames |
| 3.4 Data frames |
| 3.4.1 Most common frames |
| 3.4.1.1 Data frame |



| |
|--|
| 3.4.1.2 Null frame |
| 3.5 Interacting with Networks |
| 3.5.1 Probe |
| 3.5.1.1 Wireshark capture |
| 3.5.1.2 Probe response |
| Open network |
| WEP networks |
| WPA networks |
| 3.5.2 Authentication |
| 3.5.2.1 Open Authentication |
| Wireshark capture |
| 3.5.2.2 Shared Authentication |
| Wireshark capture |
| 3.5.3 Association |
| 3.5.3.1 Wireshark capture |
| 3.5.4 Encryption |
| 3.5.4.1 Open networks |
| Connection to a network |
| Capture file analysis |
| 3.5.4.2 Wired Equivalent Privacy |
| RC4 |
| 3.5.4.3 WPA |
| Algorithms |
| Network connection |
| 4. Getting Started - Choosing Hardware |
| 4.1 Choosing hardware |
| 4.1.1 Different types of adapters |
| 4.1.1.1 External cards |



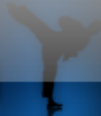
| | |
|--------------------------------------|-----------------------------------|
| 4.1.1.2 Internal cards | |
| MiniPCI | |
| MiniPCI Express | |
| PCI | |
| 4.1.2 Laptops | |
| 4.1.3 dB, dBm, dBi, mW, W | |
| 4.1.4 Antenna | |
| 4.2 Choosing a card | |
| 4.2.1 Atheros | |
| 4.2.1.1 TP-Link TL-WN610G | |
| 4.2.1.2 Ubiquiti SRC | |
| 4.2.2 Realtek 8187 | |
| 4.2.2.1 Alfa AWUS036H | |
| 4.3 Choosing an antenna | |
| 4.3.1 Antenna patterns | |
| 4.3.2 Omnidirectional | |
| 4.3.2.1 Omnidirectional 5dbi pattern | |
| 4.3.2.2 Omnidirectional 9dbi pattern | |
| 4.3.3 Directional antenna | |
| 4.3.3.1 Yagi | |
| 4.3.3.2 Planar | |
| 4.3.3.3 Sector | |
| 4.3.3.4 90° | |
| 4.3.3.5 120° | |
| 4.3.3.6 Grid | |
| 5. Aircrack-ng inside out | VIDEO TRAINING STARTS HERE |
| 5.2 Airmon-ng | |
| 5.2.1 Description | |



| |
|--|
| 5.2.2 Usage |
| 5.2.3 Usage Examples |
| 5.2.3.1 Typical Uses (non Madwifi-ng drivers) |
| 5.2.3.2 Madwifi-ng driver monitor mode |
| 5.2.4 Usage Tips |
| 5.2.5 A little word about madwifi-ng |
| 5.2.5.1 Known issues with Madwifi-ng |
| 5.2.6 Lab |
| 5.3 Airodump-ng |
| 5.3.1 Description |
| 5.3.2 Usage |
| 5.3.3 Usage Tips |
| 5.3.3.1 Airodump fields |
| More about “RXQ”: |
| More about “Lost”: |
| Various tips |
| 5.3.4 Usage Troubleshooting |
| 5.3.4.1 I am getting little or no data |
| Note for madwifi-ng |
| 5.3.4.2 airodump-ng keeps switching between WEP and WPA |
| 5.3.5 Lab |
| 5.4 Aireplay-ng |
| 5.4.1 Description |
| 5.4.2 Usage |
| 5.4.3 Usage Tips |
| 5.4.3.1 Optimizing injection speeds |
| 5.4.4 Usage Troubleshooting |
| 5.4.4.1 For madwifi-ng, ensure there are no other VAPs running |



| |
|---|
| 5.4.4.2 Aireplay-ng hangs with no output |
| 5.4.4.3 Slow injection, "rtc: lost some interrupts at 1024Hz" |
| 5.4.4.4 "Interface MAC doesn't match the specified MAC" |
| 5.4.4.5 General |
| 5.5.10 Aireplay Attack 9 -- Injection test |
| 5.5.10.1 Usage |
| 5.5.10.2 Usage Examples |
| Basic Injection Test |
| Hidden or Specific SSID |
| Attack Tests |
| 5.4.5 Aireplay Attack 0 - Deauthentication |
| 5.4.5.1 Usage |
| 5.4.5.1 Usage Examples - Typical Deauthentication |
| 5.4.5.2 Usage Tips |
| 5.4.5.5 Lab |
| 5.4.5 Aireplay Attack 1 - Fake authentication |
| 5.4.5.1 Usage |
| 5.4.5.2 Usage Examples |
| 5.4.5.3 Usage Tips |
| Setting MAC address |
| Examples of successful authentication |
| 5.4.5.4 Usage Troubleshooting |
| Identifying failed authentications |
| Re associating on periodic basis |
| Error Message "AP rejects open-system authentication" |
| Error Message "Denied (code 10), open (no WEP) ?" |
| MAC access controls enabled on the AP |
| Waiting for beacon frame |



| |
|---|
| Airodump-ng does not show the ESSID |
| Other problems and solutions |
| 5.4.6 Aireplay Attack 2 - Interactive packet replay |
| 5.4.6.1 Usage |
| 5.4.6.2 Usage Examples |
| Natural Packet Replay |
| Modified Packet Replay |
| Injecting Management Frames |
| 5.4.6.4 Usage Troubleshooting |
| 5.4.6.5 Lab |
| 5.4.7 Aireplay Attack 3 - ARP Request Replay Attack |
| 5.4.7.1 What is ARP? |
| 5.4.7.2 Usage |
| 5.4.7.3 Usage Example |
| 5.4.7.4 Usage Tips |
| 5.4.7.6 Lab |
| 5.4.8 Aireplay Attack 4 - KoreK chopchop |
| 5.4.8.1 Chopchop theory |
| 5.4.8.2 Usage |
| 5.4.8.3 Usage Examples |
| Example with sample output |
| Generating an ARP packet using the PRGA XOR stream |
| 5.4.8.4 Usage Tips |
| 5.4.8.5 Pros/Cons using Chopchop |
| 5.4.8.6 Usage Troubleshooting |
| 5.4.7.6 Lab |
| 5.5.9 Aireplay Attack 5 - Fragmentation Attack |
| 5.5.9.1 Usage |



| |
|---|
| 5.5.9.2 Usage Example |
| 5.5.9.3 Usage Tips |
| 5.5.9.4 Pro/Cons using fragmentation |
| 5.5.9.6 Lab |
| 5.5.11 I am injecting but the IVs don't increase! |
| 5.5.11.1 Solution |
| 5.5.11.2 Troubleshooting tips |
| 5.6 Packetforge-ng |
| 5.6.1 Description |
| 5.6.2 Usage |
| 5.6.2.1 Forge options: |
| 5.6.2.2 Source options: |
| 5.6.2.3 Modes (long modes use double dashes): |
| 5.6.3 Usage Example |
| 5.6.3.1 Generating an ARP request packet |
| 5.6.3.2 Generating a null packet |
| 5.6.4 Usage Tips |
| 5.6.5 Usage Troubleshooting |
| 5.6.6 Lab |
| 5.7 Aircrack-ng |
| 5.7.1 Description |
| 5.7.2 Air-cracking 101 |
| 5.7.2.1 PTW Attack |
| 5.7.2.2 FMS/ KoreK |
| 5.7.2.3 The fudge factor |
| 5.7.2.4 Dictionary Attacks |
| 5.7.4 Usage |
| 5.7.5 Usage Examples |



| |
|---|
| 5.7.5.1 WEP |
| 5.7.5.2 WPA |
| 5.7.6 Usage Tips |
| 5.7.6.1 General approach to cracking WEP keys |
| 5.7.6.2 How to determine which options to use |
| 5.7.6.3 How to use the key |
| 5.7.6.4 Sample files to try |
| 5.7.6.5 Other Tips |
| 5.7.7 Usage Troubleshooting |
| 5.7.7.1 Error message "Please specify a dictionary (option -w)" |
| 5.7.7.2 Negative votes |
| 5.7.7.3 "An ESSID is required. Try option -e" message |
| 5.7.7.4 The PTW method does not work |
| 5.8 Airdecap-ng |
| 5.8.1 Usage |
| 5.8.2 Usage Examples |
| 5.8.3 Usage Tips |
| 5.9 Airtun-ng |
| 5.9.1 Description |
| 5.9.2 Usage |
| 5.9.3 Scenarios |
| 5.9.3.1 wIDS |
| 5.9.3.2 WEP injection |
| 5.9.3.3 PRGA injection |
| 5.9.3.4 Connecting to Two Access Points |
| 5.9.3.5 Copy packets from the optional interface |
| Repeater Mode |
| Packet Replay Mode |



| |
|--|
| Injecting Management Frames |
| 5.11 Wesside-ng |
| 5.11.1 Description |
| 5.11.2 Usage |
| 5.11.3 Scenarios |
| 5.11.3.1 Standard Usage Example |
| 5.11.4 Usage Troubleshooting |
| 5.11.4.1 "ERROR Max retransmits" message |
| 5.10 Easside-ng |
| 5.10.1 Description |
| 5.10.1.1 Establish Connectivity |
| 5.10.1.2 What role does the buddy server play? |
| 5.10.1.3 Communication with the WIFI network |
| 5.10.1.6 Easside-ng compared to Wesside-ng |
| 5.10.2 Usage |
| 5.10.3 Scenarios |
| 5.10.3.1 Specific AP Usage Example |
| 5.10.3.2 Scanning for APs - Usage Example |
| 5.10.4 Usage Tips |
| 5.10.4.1 Combining Easside-ng and Wesside-ng |
| 5.10.4.2 Demonstrating Insecurity! |
| 5.10.5 Usage Troubleshooting |
| 5.10.6 Lab |
| 5.12 Other Aircrack-ng Tools |
| 5.12.1 ivstools |
| 5.12.2 Merge |
| 5.12.3 Convert |
| 6. Attacking wireless Networks |



6.1 WEP Cracking 101

6.1.1 Introduction

6.1.2 Assumptions

6.1.3 Equipment used

6.1.4 Solution

6.1.4.1 Solution Overview

6.1.4.2 Step 1

Start the wireless interface in monitor mode on AP channel

6.1.4.3 - Step 2

Start airodump-ng to capture the IVs

6.1.4.4 - Step 3

Use Aireplay-ng to perform a fake authentication with the AP

6.1.4.5 Step 4

Start Aireplay-ng in ARP request replay mode

6.1.4.6 Step 5

Run Aircrack-ng to obtain the WEP key

6.3 Cracking WEP via a wireless client

6.3.1 Introduction

6.3.2 Solution

6.3.2.1 Assumptions used

6.3.2.2 Equipment used

6.3.3 Scenarios

6.3.3.1 Scenario One

Pulling packets from captured data

6.3.3.2 Scenario Two

Interactively pulling packets from live communication

6.3.3.3 Scenario Three

Creating a packet from a chopchop replay attack



6.3.3.4 Scenario Four

6.4 Cracking WEP with no wireless clients

6.4.1 Introduction

6.4.2 Assumptions

6.4.3 Equipment used

6.4.4 Solution

6.4.4.1 Solution Overview

6.4.4.2 Step 1

Set the wireless card MAC address

6.4.4.3 Step 2

Start the wireless interface in monitor mode on AP channel

Troubleshooting Tips

6.4.4.4 Step 3

Use Aireplay-ng to perform a fake authentication with the AP

6.4.4.5 Step 4

Use Aireplay-ng chopchop or fragmentation attack to obtain PRGA

Helpful Tips

Troubleshooting Tips

6.4.4.6 Step 5

Use Packetforge-ng to create an ARP packet

Helpful Tips

6.4.4.7 Step 6

Start airodump-ng

6.4.4.8 Step 7

Inject the ARP packet

Troubleshooting Tips

6.4.4.9 Step 8

Run Aircrack-ng to obtain the WEP key



| |
|--|
| Troubleshooting Tips: |
| 6.4.5 Alternate Solution |
| 6.5 Cracking WEP with shared key |
| 6.5.1 Introduction |
| 6.5.3 Equipment used |
| 6.5.4 Solution |
| 6.5.4.1 Solution Background |
| 6.5.4.2 Solution Overview |
| 6.5.4.3 Step 1 |
| Start the wireless interface in monitor mode on AP channel |
| Troubleshooting Tips |
| 6.5.4.4 Step 2 |
| Start airodump-ng |
| 6.5.4.5 Step 3 |
| Deauthenticate a connected client |
| 6.5.4.6 Step 4 |
| Perform Shared Key Fake Authentication |
| Usage Tip |
| Troubleshooting Tips |
| 6.6 ARP amplification |
| 6.6.1 Introduction |
| 6.6.2 Solution |
| 6.6.2.1 Assumptions used |
| 6.6.2.2 Equipment used |
| 6.6.3 Scenarios |
| 6.6.3.1 Scenario One - One for one ARP packets |
| 6.6.3.2 Scenario Two - Two for one ARP packets |
| 6.6.3.3 Scenario Three - Three for one ARP packets |

6.6.4 Important note

6.7 Cracking WPA/WPA2

6.7.1 Introduction

6.7.3 Equipment used

6.7.4 Solution

6.7.4.1 Solution Overview

6.7.4.2 Step 1

Start the wireless interface in monitor mode

6.7.4.3 Step 2

Start airodump-ng to collect authentication handshake

6.7.4.4 Step 3

Use Aireplay-ng to deauthenticate the wireless client

Troubleshooting Tips

6.7.4.5 Step 4

Run Aircrack-ng to crack the pre-shared key

6.7.5 Lab