Aircrack-ng

getting_started

Tutorial: Getting Started

Version: 1.01 September 25, 2009
By: darkAudax

Introduction

Many people ask “How do I get started?”. This tutorial is intended to answer that question.

It is not intended to be a detailed “How To” tutorial, rather it is a road map to get you from where you are to the desired destination of using aircrack-ng. Once you get going, there is an abundance of materials on the wiki describing the tools in great detail and tutorials for various tasks.

This tutorial is focused on linux. Yes, I realize that linux is a problem for many people. Unfortunately Microsoft Windows simply does a poor job supporting the aircrack-ng suite. This is primarily due to the proprietary nature of the operating system and wireless card drivers. See Tutorial: Aircrack-ng Suite under Windows for Dummies for more details. Bottom line, don't use the aircrack-ng suite under Windows. There is little or no support for it.

The basic process consists of three steps:

- Determine the chipset in your wireless card
- Determine which of the three options you will use to run the aircrack-ng suite
- Get started using the aircrack-ng suite

The first step of determining the wireless card chipset is covered in the “Determining the Wireless Card Chipset” section below.

Next, you need to decide which method you will use to run the aircrack-ng suite. The three options are:

1. Linux distribution of your choice plus the aircrack-ng suite
2. Live CD which contains a version of the aircrack-ng suite
3. VMWare image which contains a version of the aircrack-ng suite

There is a section below describing each option in more detail plus the advantages and disadvantages of each.

Finally, once you have aircrack-ng running, follow the “Using Aircrack-ng Suite” section below.

If you have problems, see the “Resources” section.

I would like to acknowledge and thank the Aircrack-ng team [http://trac.aircrack-ng.org/wiki/Team] for producing such a great robust tool.

Please send me any constructive feedback, positive or negative.

Have fun!

Determining the Wireless Card Chipset

The first step is determining which chipset your current wireless card contains. “Chipsets” are the electronics on a card which allow the card to function wirelessly. Not all chipsets are supported by aircrack-ng. Even if the chipset is supported, some of the functions may not work properly.

To determine the chipset of your card, follow Tutorial: Is My Wireless Card Compatible?. You need to know what chipset your card has in order to determine if it is supported by aircrack-ng.

Once you have determined the chipset in your wireless card, use Compatible Cards to determine if the chipset is compatible with the aircrack-ng suite. If it is, then it tells you which software drivers are required for your particular card.

If you don't have an existing wireless card or are considering purchasing another one, this same page has comments on various chipsets and cards which are known to work with aircrack-ng.

Linux Distribution of Your Choice

There are a large number of linux distributions available. They should all properly support the aircrack-ng suite.

Once you have your favorite linux distribution installed and functioning well, it is time to patch your wireless card driver. In the previous step you had determined the chipset in your wireless card. Lookup which driver is required for that particular chipset on Compatible Cards.

Then follow the installation instructions on the Installing Drivers page specific to your chipset. There is troubleshooting information on both this page and the individual driver pages.

Install the aircrack-ng suite using these instructions.

Once your wireless card is working well, jump to the “Using Aircrack-ng Suite” section below.

Advantages

- aircrack-ng is almost certainly guaranteed to work
- Provides the ability to run the latest versions of aircrack-ng and any wireless driver
- Provides the most flexibility

Disadvantages

- Requires much deeper knowledge of linux

Live CD

A live CD is a complete running linux distribution which you download and burn onto a CD. You then boot from this CD. Once booted and logged in, you are able to run the aircrack-ng suite with your wireless card. Knowing the chipset of your wireless card (determined in the first step), select a live CD which contains the patched version of the driver for your particular card. This is a key requirement. Needless to say, the live CD must also contain a copy of the aircrack-ng suite.

Here is a list of live CDs that are known to include the aircrack-ng suite.

Once you have booted from the CD and your wireless card is working well, jump to the “Using Aircrack-ng Suite” section below.

Advantages

- Works with any host operating system.
- No knowledge need to get aircrack-ng and the drivers working.
- Very portable.

Disadvantages

- Old version of aircrack-ng is included. May contain bugs and/or be missing features.
- Old versions of drivers are included. May contain bugs and/or be missing features.

VMWare Image

VMWare is a commercial product example of computer virtualization. Virtualization is running a “virtual computer” instance under a host operating

system. VMWare supports a variety of host operating systems.

Here are the the currently available VMWare virtual machines [http://download.aircrack-ng.org/vmware-aircrack-ng-v4.7z]. Here are the installation instructions.

Once you have installed and booted from the VMWare image and your wireless card is working well, jump to the “Using Aircrack-ng Suite” section below.

Advantages

- No knowledge need to get aircrack-ng and the drivers working.
- Very portable.

Disadvantages

- Works with a limited set of host operating systems.
- Only USB devices are supported.
- Old version of aircrack-ng is included. May contain bugs and/or be missing features. (but can be updated with some knowledge)
- Old versions of drivers are included. May contain bugs and/or be missing features. (but can be updated with some knowledge)

Using the Aircrack-ng Suite

You should always start by confirming that your wireless card can inject packets. This can be done by using the injection test.

Then start by following the Simple WEP Crack Tutorial.

Once you have mastered that technique, you can follow the other tutorials to learn aircrack-ng in more detail.

Resources

The most common source of problems is the human factor. Meaning typos, failure to follow instructions, skipping steps and so on. Always, always double check what you have done. Most times this will resolve your problem.

The Wiki [http://aircrack-ng.org/doku.php] is your primary source of information and troubleshooting tips. It provides very detailed documentation on each aircrack-ng tool plus troubleshooting tips throughout. There is a large set of tutorials to walk you through tasks in detail.

The Forum [http://forum.aircrack-ng.org/] is also an excellent source for finding solutions to problems. It is extremely important to first attempt to resolve a problem yourself prior to posting. Your question will be ignored if the answer is easily available on the wiki or forum. Conversely, people will try their best to

help you if you demonstrate you researched the problem first and could not solve it. Also be sure to supply the details of your setup and what you have tried when you post.

For live discussion, you can join IRC: #aircrack-ng on Freenode [irc://irc.freenode.net/aircrack-ng]. Just go ahead and ask your question, “don't ask to ask”. people will try their best to help you if you demonstrate you researched the problem first and could not solve it.

For both the Forum and IRC, remember that we don't support or endorse people accessing networks that do not belong them. We will not help anybody to break into a network or do anything illegal. This is the fastest way to get permanently banned.

You may also find the Videos helpful.

getting_started.txt · Last modified: 2009/09/25 20:58 by darkaudax