How to Crack WEP Protected Wireless Access Points

Contents

1 Preface

In this document, I will summerize the steps required for cracking WEP protected wifi networks using an Atheros based wireless card, a patched version of the MadWifi driver, and the aircrack-ng suite. All of this information can be found at the aircrack-ng website.

2 Introduction

There are a few steps to cracking a WEP protected Access Point (AP). First off, you need to patch your MadWifi driver. Next, you'll need to find out some information about the AP you are trying to access. Next, you can actually perform the crack using the tools provided in the aircrack-ng suite.

3 Patching Your Driver

3.1 Check your current chipset

Use this command to make sure that you are using an Atheros based wireless card:

```
lspci | grep -i atheros
```

You should see a result that looks like this:

```
02:0c.0 Ethernet controller: Atheros Communications Inc. AR5212/AR5213
Multiprotocol MAC/baseband processor (rev 01)
```

If you get something like this, then you can move on to replacing your driver with a patched version that will allow it to inject packets. If you do not get a result similar to that above, then you most likely do not have an Atheros based wifi card and this section is of no use to you.

3.2 Patching and installing the MadWifi driver

For the most detailed explaination on how to perform this step, please see the aircrack-ng website[1]. The first step you need to do is bring your wireless card down.

```
ifconfig ath0 down
ifconfig wifi0 down
```

Next, check out the proper version of MadWifi-ng and get its patch:

```
svn -r 3745 checkout http://svn.madwifi-project.org/madwifi/trunk/ madwifi-ng
wget http://patches.aircrack-ng.org/madwifi-ng-r3745.patch
```

Now, apply the patch, uninstall the driver you were using before and install this one (you may need to use `sudo` in front of some of these commands):

[1] http://aircrack-ng.org/doku.php?id=madwifi-ng

```
cd madwifi-ng
patch -Np1 -i ../madwifi-ng-r3745.patch
./scripts/madwifi-unload
make
make install
depmod -ae
modprobe ath_pci
```

4 Enumerating Targets

4.1 Using kismet

Here is where you will gather the information you need about the AP that you are trying to connect to. For this task, I recommend you use a program called `kismet`. Kismet is a wireless AP scanner that gathers a lot of useful information about the access points that it sees. Once you have `kismet` installed, you will need to edit your `source` line in `/etc/kistmet/kismet.conf`. This is what mine looks like:

```
source=madwifi_b,wifi0,madwifi
```

Now, you will need to find out the following pieces of information about the AP you are trying to connect to. You will want to write these down:

- BSSID (MAC address of access point)
- ESSID (Wireless network name)
- Access point channel

Here is how to find this information using `kismet`:

1. Run the command, `kismet`
2. Press `space`
3. Press `S` to sort
4. Press `W` to sort by WEP
5. Now use the arrow keys to scroll down to an AP that has a `Y` under the `W` column and press `enter`.
6. You should now see all the information you need

5 Getting Access

You are now ready to actually start cracking the AP. I would recommend reading this tutorial for details on how this is done[2].

[2] http://www.aircrack-ng.org/doku.php?id=simple_wep_crack&DokuWiki=1028b58ed618f626a9a966f0e78ed235