Cracking the WPA password using Aircrack-ng

Purpose: Usually they are trying to get a handshake, which is saved as a cap file. After you have the cap file already (which contains the password encrypted) you can use either a dictionary attack or a brute-force attack.

-Dictionary attack – after I have the handshake. Cap file I am using Aircrack-ng tool.

I am using some of the biggest dictionary files, found online. They contain millions of passwords. The program is trying to match the encrypted password (the hash) with the hash from the password in the dictionary.

The main weakness of wireless networking is that all messages between the hosts are transmitted on air. So if a malicious user is sniffing the air for packets he will always get the password key (encrypted) after this he has all the time in the world to try millions of different words in dictionaries in order to crack it. So, the more complicated is your pass, the better!

In case you cannot capture the handshake, here is an explanation on what could be wrong and how to fix it!

I Cannot Capture the Four-way Handshake!

It can sometimes be tricky to capture the four-way handshake. Here are some troubleshooting tips to address this:

- Your monitor card must be in the same mode as the both the client and Access Point. So, for example, if your card was in “B” mode and the client/AP were using “G” mode, then you would not capture the handshake. This is especially important for new APs and clients which may be “turbo” mode and/or other new standards. Some drivers allow you to specify the mode. Also, iwconfig has an option “modulation” that can sometimes be used. Do “man iwconfig” to see the options for “modulation”. For information, 1, 2, 5.5 and 11Mbit are 'b', 6, 9, 12, 18, 24, 36, 48, 54Mbit are 'g'.
- Sometimes you also need to set the monitor-mode card to the same speed. IE auto, 1MB, 2MB, 11MB, 54MB, etc.
- Be sure that your capture card is locked to the same channel as the AP. You can do this by specifying “-c <channel of AP>” when you start airodump-ng.
- Be sure there are no connection managers running on your system. This can change channels and/or change mode without your knowledge.
- You are physically close enough to receive both access point and wireless client packets. The wireless card strength is typically less than the AP strength.
- Conversely, if you are too close then the received packets can be corrupted and discarded. So you cannot be too close.
- Make sure to use the drivers specified on the wiki. Depending on the driver, some old versions do not capture all packets.

- Ideally, connect and disconnect a wireless client normally to generate the handshake.
- If you use the deauth technique, send the absolute minimum of packets to cause the client to reauthenticate. Normally this is a single deauth packet. Sending an excessive number of deauth packets may cause the client to fail to reconnect and thus it will not generate the four-way handshake. As well, use directed deauths, not broadcast. To confirm the client received the deauthentication packets, use tcpdump or similar to look for ACK packets back from the client. If you did not get an ACK packet back, then the client did not “hear” the deauthentication packet.
- Try stopping the radio on the client station then restarting it.
- Make sure you are not running any other program/process that could interfere such as connection managers, Kismet, etc.
- Review your captured data using the WPA Packet Capture Explained tutorial to see if you can identify the problem. Such as missing AP packets, missing client packets, etc.

Unfortunately, sometimes you need to experiment a bit to get your card to properly capture the four-way handshake. The point is, if you don't get it the first time, have patience and experiment a bit. It can be done!

Another approach is to use **Wire shark** to review and analyze your packet capture. This can sometimes give you clues as to what is wrong and thus some ideas on how to correct it. The WPA Packet Capture Explained tutorial is a companion to this tutorial and walks you through what a “normal” WPA connection looks like. As well, see the FAQ for detailed information on how to use Wire shark.

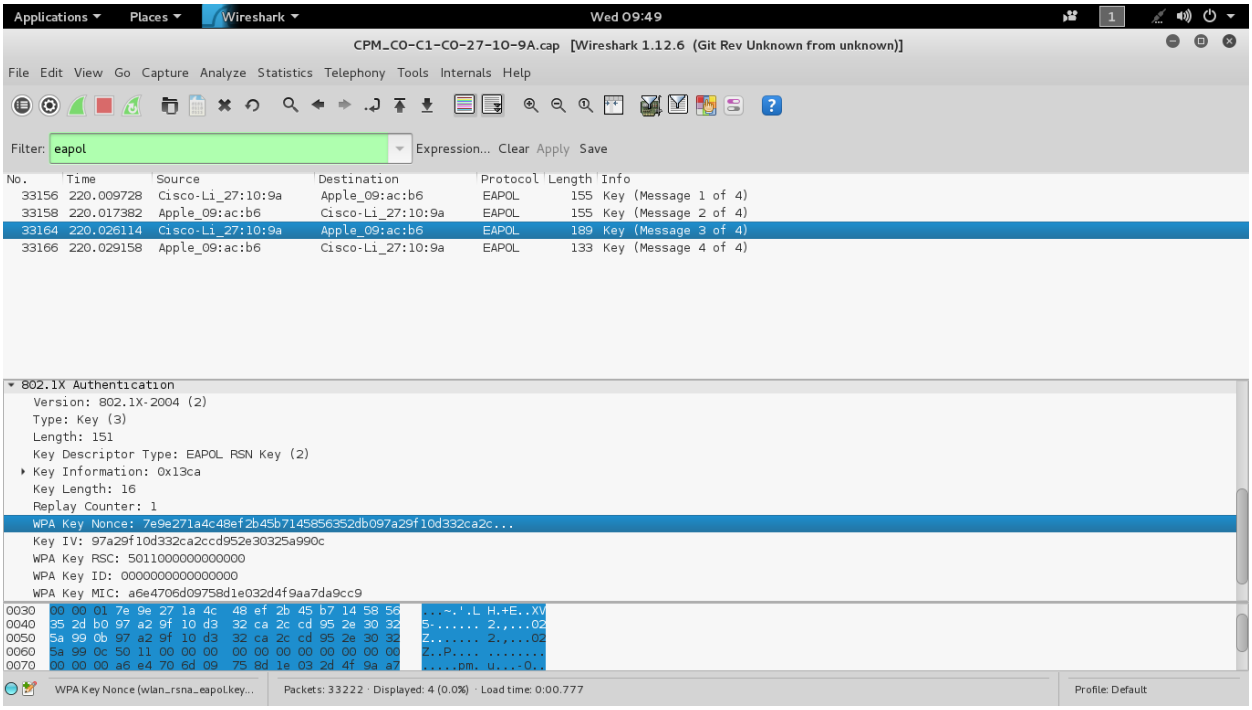
In an ideal world, you should use a wireless device dedicated to capturing the packets. This is because some drivers such as the RTL8187L driver do not capture packets the card itself sends. Also, always use the driver versions specified on the wiki. This is because some older versions of the drivers such as the RT73 driver did not capture client packets.

When using Wireshark, the filter “eapol” will quickly display only the EAPOL packets. Based on what EAPOL packets are actually in the capture, determine your correction plan. For example, if you are missing the client packets then try to determine why and how to collect client packets.

You can download the ready captured handshake file from Fronter.

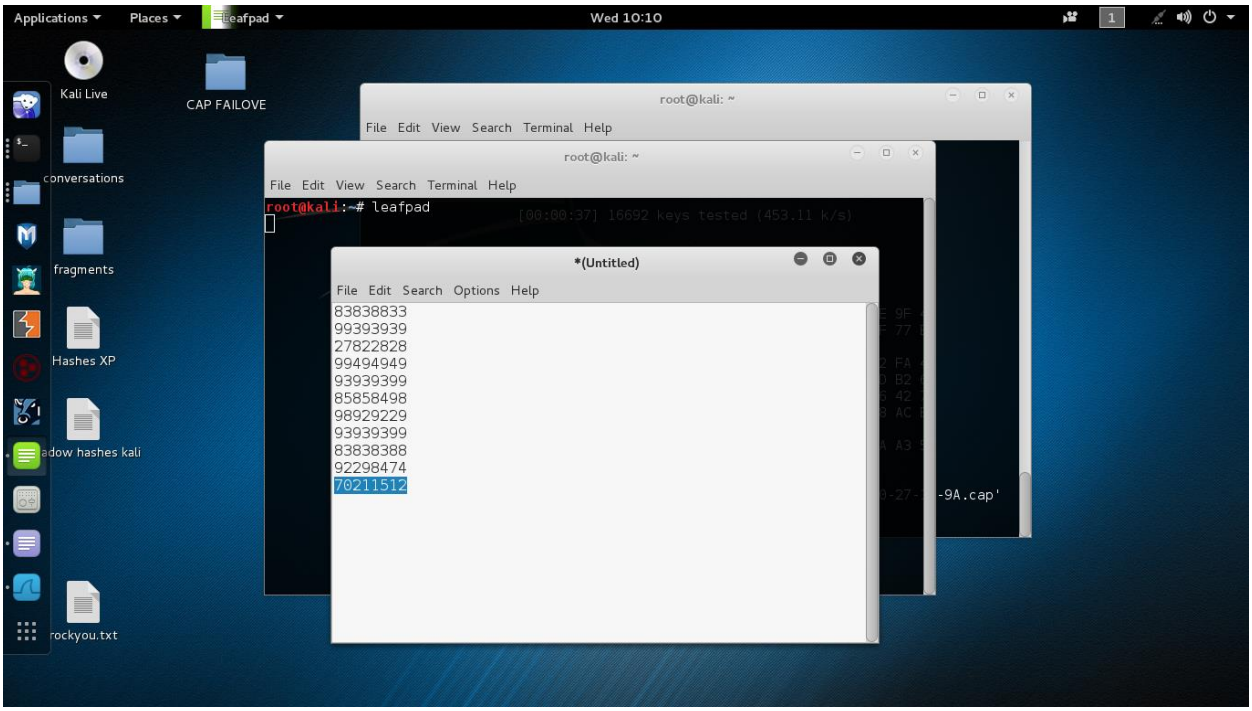
First open up a terminal and type in Wireshark.

Then ,open up the cap.file and type in EAPOL in the wire shark field.You can see the 4 way handshake now.



1.Open up a terminal a type in leafpad

2.Create your own dictionary file ,just like this:



Include the real password in the list :70211512

3.Run aircrack-ng against the cap file , using the dictionary.txt file you created (the command is:

aircrack-ng <drag and drop the cap file> -w <drag and drop the dictionary file>

Mine looks like this:

aircrack-ng '/root/Desktop/CAP FAILOVE/CPM_C0-C1-C0-27-10-9A.cap' -w'/root/Desktop/mycreateddictionary'

4.Locate the file rockyou.gz on your computer.(it's in usr/share/wordlists)

5.Open up a new terminal and run gunzip rockyou.gz to unzip the files

6.Run aircrack-ng against the cap file ,using the rockyou.txt file.The tool will run all passwords from the wordlist against the cap file.If the password is not in the wordlist ,it will not be found.

Brute force the WPA handshake file with Hashcat

If you cannot break the key with dictionary attack you can use brute force attack.

Hashcat is the fastest tool available (according to its developers) It is using the GPU –your video card power. Accordingly the more powerful is your video card, the faster the process will be. If you have 2 or more video cards interconnected (cross –fire) then the computing power is more.

Download for Windows from here : https://hashcat.net/oclhashcat/

Usage:

```
?l = abcdefghijklmnopqrstuvwxyz

?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ

?d = 0123456789

?s = !”#$%&'()*+,-./:;⇔?@[\]^_`{|}~



?a = ?l?u?d?s
```

?1 = small characters

?u = only uppercase

?s = symbols

?a = anything (takes the most time – years)

So lets say you password is `12345678`. You can use a custom MASK like `?d?d?d?d?d?d?d?d`

If your password is all letters in CAPS such as: `ABCFEFGH` or `LKHJHIOP` or `ZBTGYHQS` ..etc. then you can use the following MASK:

```
?u?u?u?u?u?u?u?u
```

If your password is all letters in lowercase such as: `abcdefgh` or `dfghpoiu` or `bnmiopty` ..etc. then you can use the following MASK:

```
?l?l?l?l?l?l?l?l
```

If you somehow know the few characters in the password, this will make things a lot faster. For every known letter, you save immense amount of computing time. MASK's allows you to combine this. Let's say your 8 character password starts with abc, doesn't contain any special characters. Then you can create a MASK rule file to contain the following:

```
abc?l?l?l?l?l

abc?u?u?u?u?u

abc?d?d?d?d?d

abc?l?u??d??d?l

abc?d?d?l?u?l
```

Next step will be converting the `.cap` file to a format cudaHashcat or oclHashcat or Hashcat on Kali Linux will understand.
Here's how to do it:

To convert your `.cap` files manually in Kali Linux, use the following command

```
wpaclean <out.cap> <in.cap>
```

Please note that the `wpaclean` options are the wrong way round. < `out.cap` > < `in.cap` > instead of < `in.cap` > < `out.cap` > which may cause some confusion.

Next

We need to convert this file to a format cudaHashcat or oclHashcat or Hashcat on Kali Linux can understand.

To convert it to `.hccap` format with " `aircrack-ng` " we need to use the `-J` option

```
aircrack-ng <out.cap> -J <out.hccap>
```

Note the `-J` is a `capitol J` not `lower case j`.

The file is already converted and can be found on Fronter with the name : thebest.hccap.

Now , to launch the attack use the following :
Using Brute Force MASK attack.

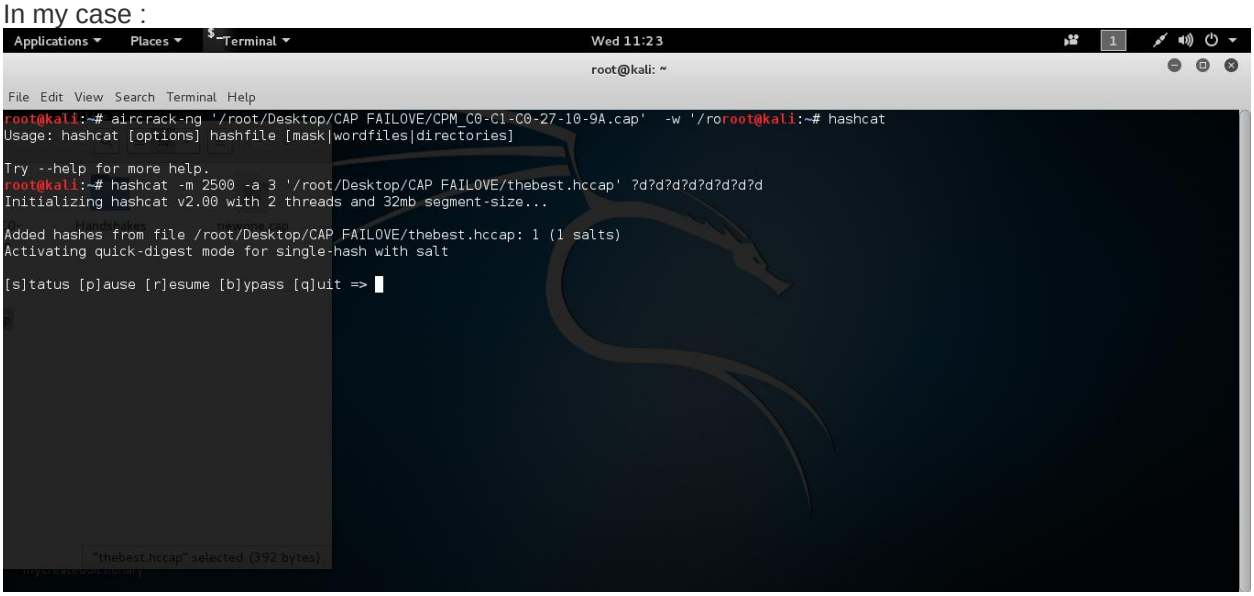
To crack WPA WPA2 handshake file using cudaHashcat or oclHashcat or Hashcat, use the following command (you can substitute cudahashcat with the other 2 tools)

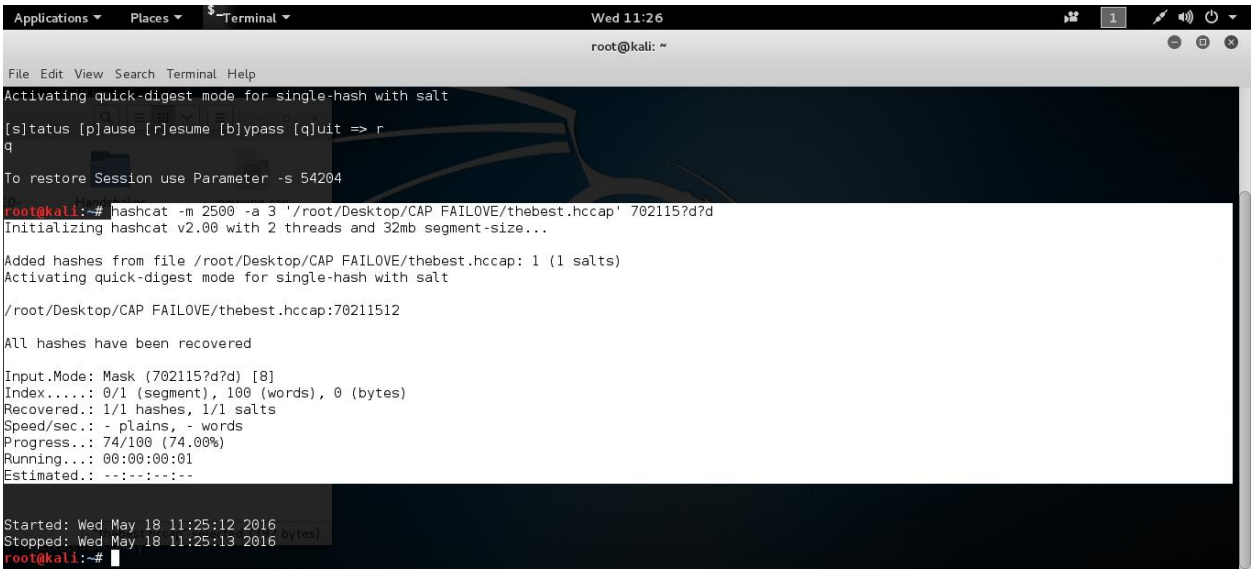
Sample:

```
cudahashcat -m 2500 -a 3 capture.hccap ?d?d?d?d?d?d?d?d
```

Where `-m = 2500` means we are attacking a WPA2 WPA handshake file.
`-a = 3` means we are using `Brute Force Attack mode` (this is compatible with MASK attack).
`capture.hccap` = this is your `converted .cap` file. We generated it using `wpaclean` and `aircrack-ng`.
`?d?d?d?d?d?d?d?d` = This is your MASK where `d = digit`. That means this password is all in numbers. i.e. `7896435` or `12345678` etc.

In my case :





First I run it with all only digits mask. This needs 99999999 possible guesses and needs some time don`t want to wait though.

Then, to make the process faster I input the first 6 digits and leave the last 2 unknown. It took only 1 second to recover the hashes.

Hashcat stores all cracked hashes in a file. To see it type in: **cat hashcat.pot**

And you see the result:

/root/Desktop/CAP FAILOVE/thebest.hccap:**70211512**

Successfully uncovered the password.