INTRO TO CYBER SECURITY LAB

Wireless Exploitation Using AIRGEDDON

GROUP MEMBERS

- ***MUHAMMAD-ASIM***
- ***NOOR-UL-HASSAN***
- ***FARHAN KHAN***
- ***EMAN SAJID***
- ***AYESHA FATIMA***

Contents

Report on AirGeddon Project

1. Topic Introduction

Objective: To explore the functionality and applications of Airgeddon, a versatile tool designed for wireless network auditing and penetration testing.

Content:

This project discusses Airgeddon to demonstrate its capability in enhancing wireless network security. The increasing use of WiFi networks in modern society has made them a prime target for cyberattacks. Tools like Airgeddon are necessary to identify vulnerabilities and strengthen networks.

Motivation: The purpose of the project is to understand the procedures of wireless auditing and deploy effective measures in enhancing network security.

2. Description of Tool/Technique Used

Overview of Tool:

Name: Airgeddon

Version: Release 105 (version 11.40)

Why Chosen: The reason for using Airgeddon is that it can be adapted to perform such activities like wireless network auditing, handshakes, and assessing network strength. This tool comes with an intuitive interface, along with welldocumented information, so it can be used effectively by anyone, from new to experienced users.

Important Features Utilized:

1. Wireless network discovery
2. Deauthentication attacks
3. Capture of WPA/WPA2 handshake
4. Dictionary attack/Password Cracking
5. Fake AP creation

Example:

Airgeddon's enhanced wireless audits make it possible to simulate realistic attack scenarios for users; this makes it possible for them to improve their networks' defenses. Below is a screenshot of the tool while in action.

Requirements:

Some Requirements to carry the attacks are as follows:

Hardware Requirements:

1. **Wireless Network Adapter:**

An adapter capable of monitor mode and packet injection (e.g., Alfa AWUS036NHA or TP-Link TL-WN722N).

2. Secondary Wireless Interface (Optional):

Only required for conducting dual-interface tasks like simultaneous scanning and attacking.

3. System:

A desktop computer or laptop that possesses adequate processing capabilities and a minimum of 4GB of RAM.

Software Specifications:

1. OS:

Kali Linux. As it already has a plethora of built-in utilities that are set to use out of the box and, therefore compatible.

2. Airgeddon:

11.20 (Release 105) or latest

3. Dependencies:

Ensure that all the prerequisites to run Airgeddon are installed, such as `aircrack-ng`, `iwconfig`, and `mdk3`.

Networking Requirements:

1. Target Network:

A test network specifically created for learning purposes. Before conducting an audit on any network, ethical and legal permission is required to be acquired.

Skill Requirements:

1. Basic Linux knowledge

Knowledge of the directives required for moving around and deploying tools using a Linux platform.

2. Wireless Networking:

Understanding of Wi-Fi protocols, including WPA/WPA2 as well as its vulnerabilities

3. Ethics:

Familiarization with ethical hacking principles or best practices, along with local statutes to ensure safe use of tools.

Miscellaneous Requirements:

1. External Antenna (Optional):

To increase signal strength for weak networks.

2. Power Supply:

To provide constant power to carry out long operations.

3. Progress

Objective: Provide a chronological breakdown of the project milestones.

Date	Milestone	Description
Dec 8, 2024	Topic Selection	Chose the topic of Airgeddon for the project
Dec 10, 2024	Sample Attack Conducted	Performed an initial sample attack to understand tool functionality.
Dec 12, 2024	Issue Encountered	Identified a limitation of having only one wireless interface.
Dec 14, 2024	Mitigation of Issue	Arranged an additional wireless interface from a friend to proceed with the attacks.
Dec 17, 2024	Final Attack and Report	Conducted a full attack, documented the steps, and captured relevant screenshots for the report.

Details of Activities:

1. **Topic Selection:** The project topic, Airgeddon, was chosen on Dec 8, 2024, due to its relevance to wireless security.
2. **Sample Attack:** A sample attack was performed on Dec 10, 2024, to familiarize the team with the tool and its features. No major issues were encountered during this phase.
3. **Hardware Limitation:** On Dec 13, 2024, we realized that having only one wireless interface was insufficient for simultaneous scanning and attacking. This issue was addressed by borrowing an additional interface from a friend on Dec 14, 2024.
4. **Final Attack:** The final attack was performed on Dec 17, 2024, with both interfaces in use. Screenshots and detailed steps were recorded for documentation purposes.

4. Demonstration of Attacking Techniques

Objective:
To demonstrate Airgeddon's ability to identify and exploit vulnerabilities in a wireless network.

4.1 & 4.2 Deauth Attack and Handshake Capture

Goal:

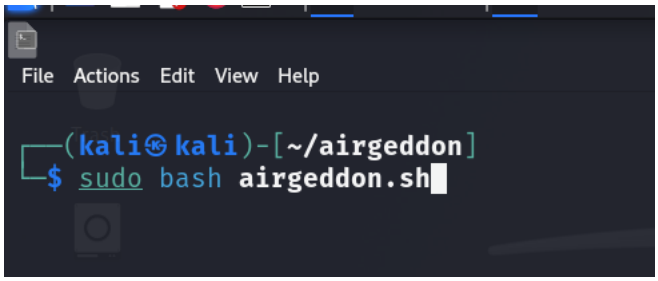
Perform a deauthentication attack to disconnect clients from a wireless network and capture the WPA/WPA2 handshake for further analysis.

Objective:

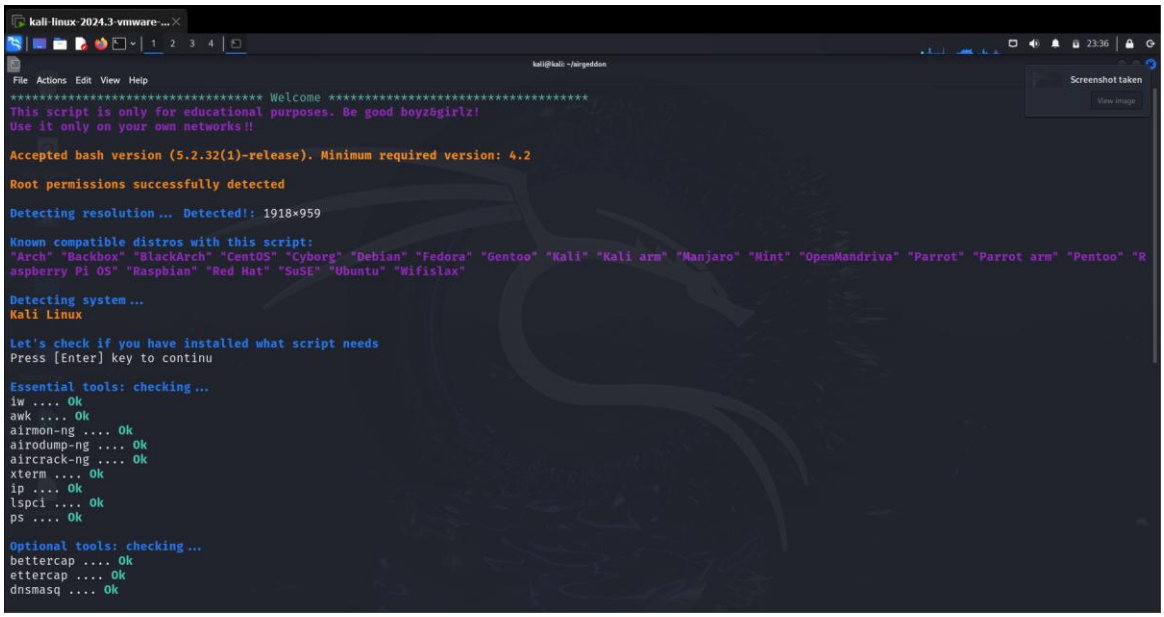
Conduct a deauthentication attack on the target network to briefly drop devices from the targeted network and capture the handshake packet when the devices try to reconnect to the attacked network as follows.

Detailed steps of Deauth attack and Handshake Capture:

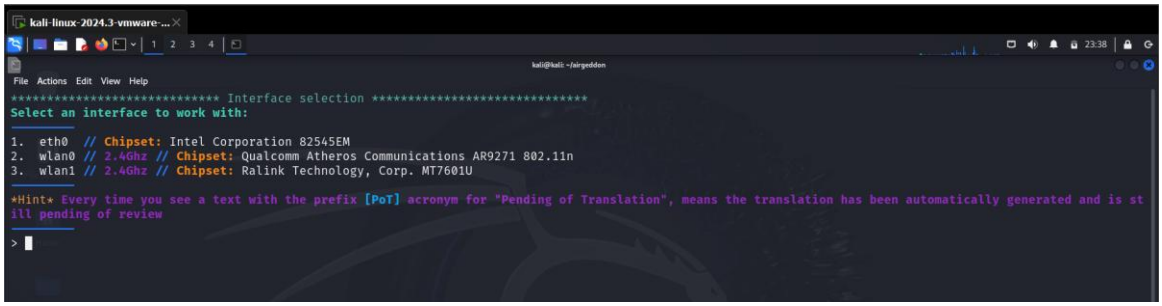
1. First start the airgeddon tool:



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

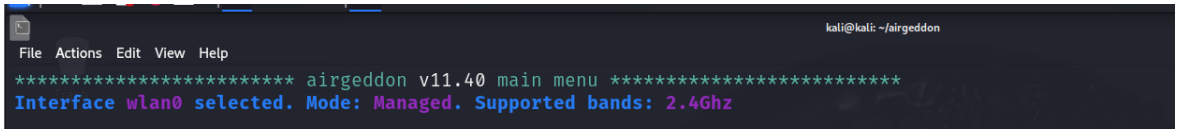


2. Now the tool/script will ask you to select an interface to conduct the attack.

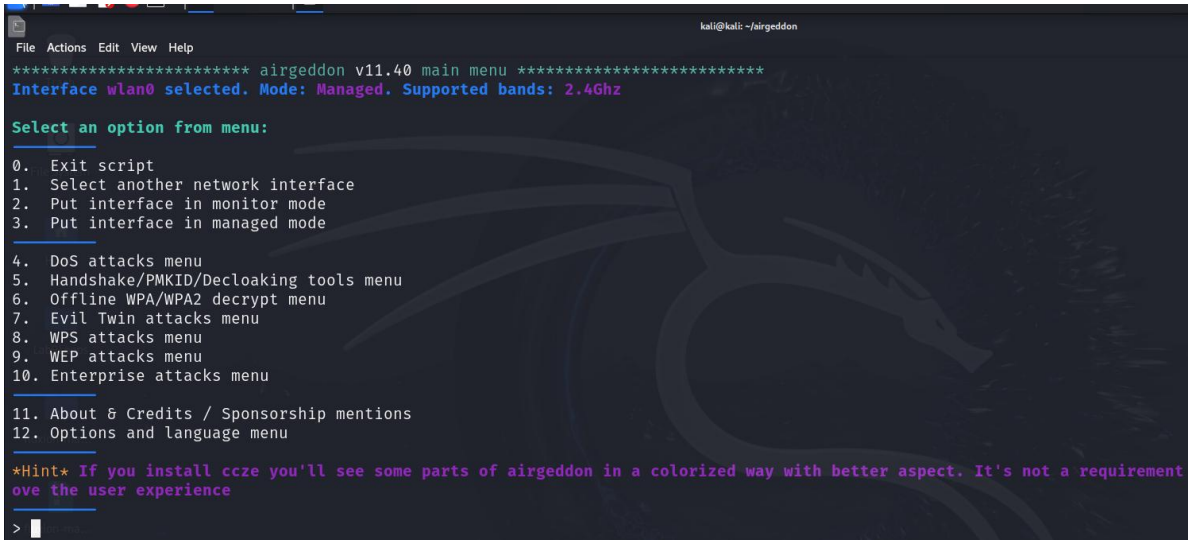


Note: if you are using kali virtual machine you will get the first interface as eth0(Do not select this one) and also you need to have two external wireless adapters to carry out a proper attack.

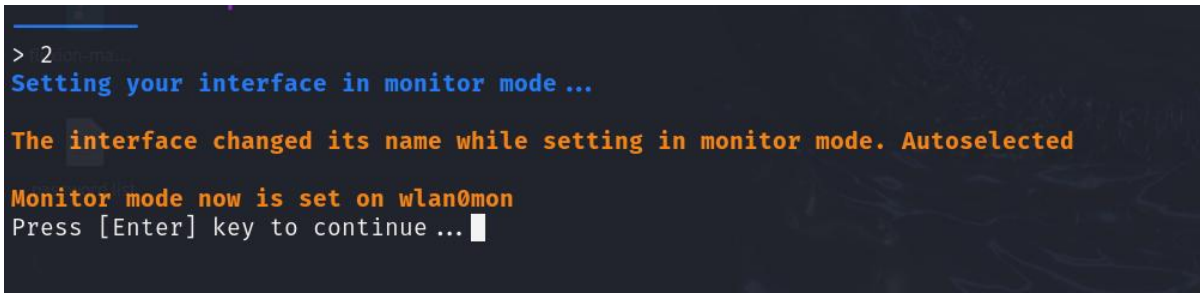
3. Select one of the two wireless interface. We have selected the 2nd one.



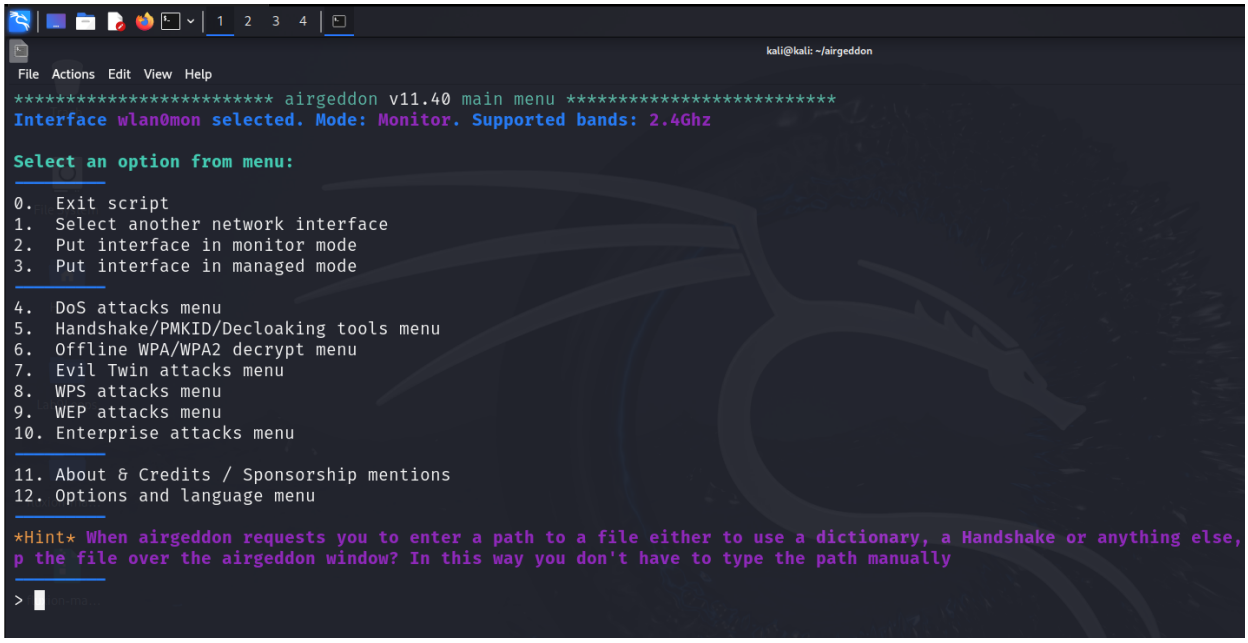
4. You will get the following interface:



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

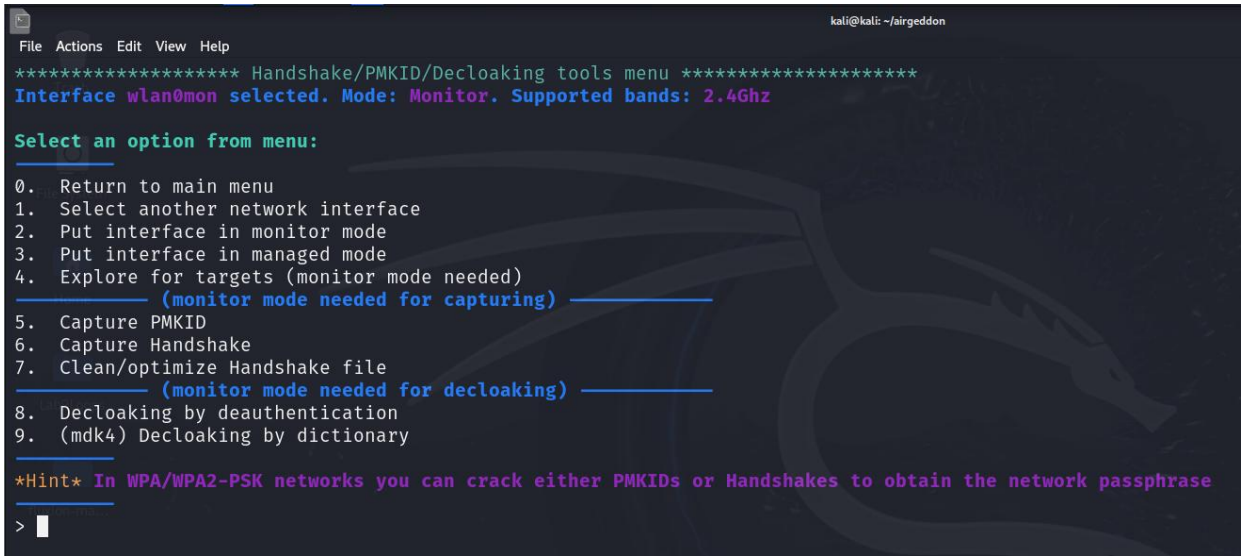


Press enter and you will be back to this interface:

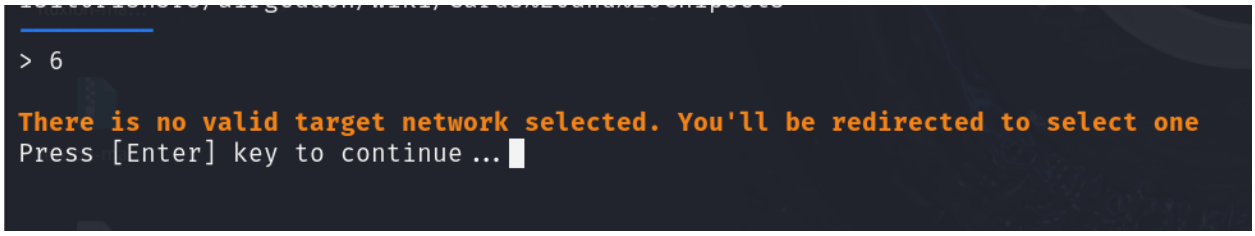


Note: But see on the top most of the terminal you will see that now your network interface is in monitoring mode (You are all set to go).

6. Now focus on the options from (4 - 10). You will see Handshake/PMKID/Deloaking tools menu. Press to enter in the menu.



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



There is no target network selected. Press enter and you will see a magic.

```
**************************** 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 "Mi
ed 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 the
 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 ...
```

Press enter to scan targets near you and wait for 30 seconds and then press Ctrl + C to stop scanning.

You will get the following interface:

```
kali@kali: ~/airgeddon
File  Actions  Edit  View  Help
********************************* Select target *********************************

  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

(*) Network with clients

Select target network:
>
```

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

8. Now select the target network in our case we will select **NTL Ground Floor** as we have the permission to attack this network (Never attack the network you don't have permission to) You will get the following options.

```
File  Actions  Edit  View  Help
**************************** 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
```

Note:

a. Deauth / disassoc amok mdk4 attack: This is a method used to disrupt the connection between a device and a wireless access point (AP). The "deauth" (de-authentication) and "disassoc" (disassociation) attacks send spoofed packets to disconnect users from the Wi-Fi network. The term "mdk4" refers to a tool that allows multiple types of wireless attacks, including this one.

b. Deauth airplay attack: Similar to the above, this attack specifically targets the Wi-Fi devices using a method to forcefully disconnect them from the network. "Airplay" is often associated with frameworks used in Wi-Fi testing,

targeting devices that are communicating over the air to induce reconnection attempts or to capture handshake data.

c. Auth DoS attack: An authentication denial-of-service (Auth DoS) attack aims to overwhelm a network with authentication requests, causing legitimate devices to be unable to connect. This attack exploits the way WPA/WPA2 authentication works and can be used to disrupt the availability of the network.

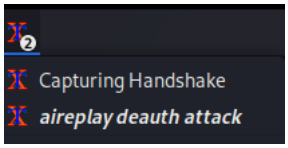
9. In our case we will be going with the 2nd method to deauth the clients connected to the network.

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

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

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 ...
```

Press enter to the start the attack.



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

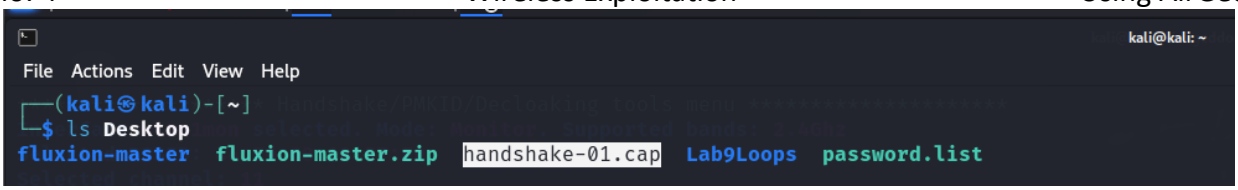
10. Now if the attack is successful you will be prompted to enter a path where to store the captured handshake file.

```
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-44:E9:68:10:57:E0.cap]
>
```

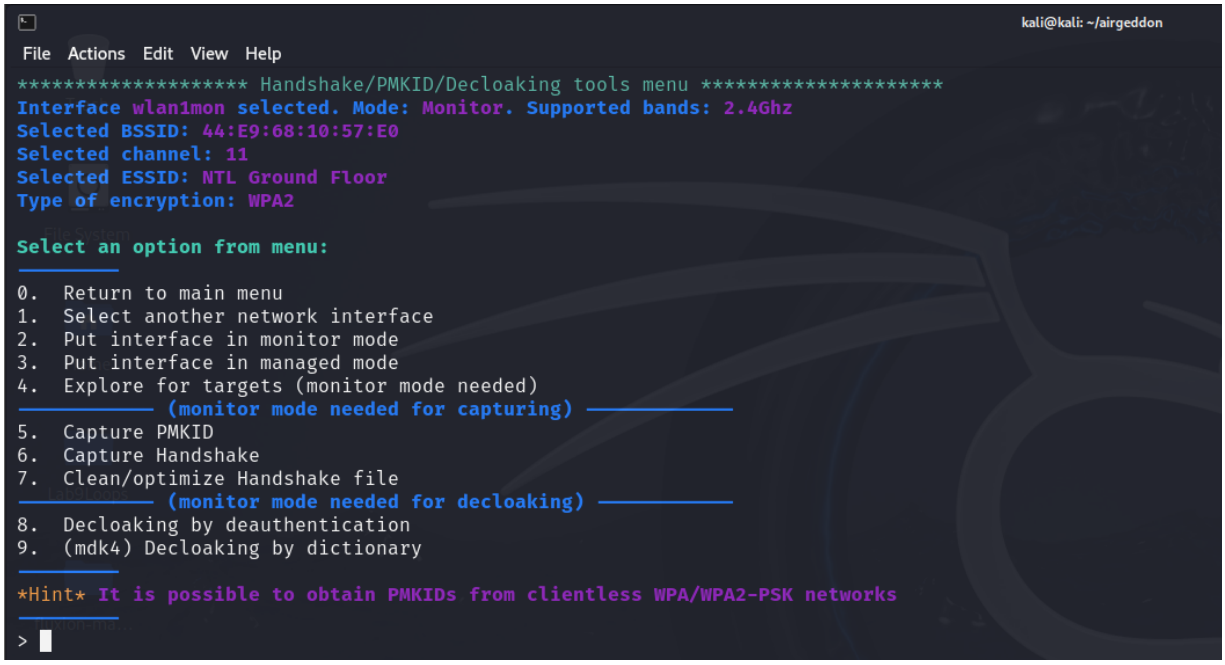
In our case we will give the Desktop for our convenience.

```
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 ...
```

To confirm that our file is stored in the specific directory.

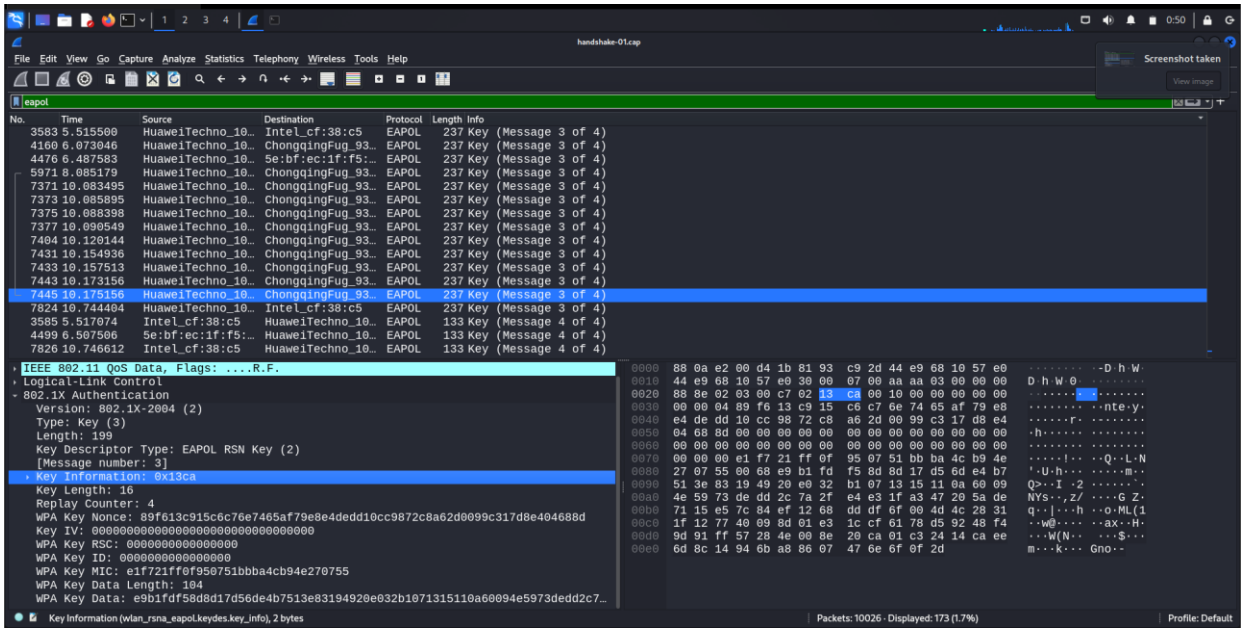


11. Focusing on our tool now you will get the following interface



But just focus on the top of the terminal, you will get the details about our target network. But for now we will go back to our main menu.

12. Handshake file details (We thought it will be better to add this)



As you can see we have the WPA key in encrypted form and that's all for this attack. Further information on how to decrypt this key or match the hash of the key is in the next sections.

Methodology:

•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

Use case:

This method illustrates how attackers can use the weaknesses of the network to steal encrypted authentication data. The configurations must be secure.

4.3 Dictionary Attack

- **Objective:** Crack the WPA/WPA2 password using the captured handshake.

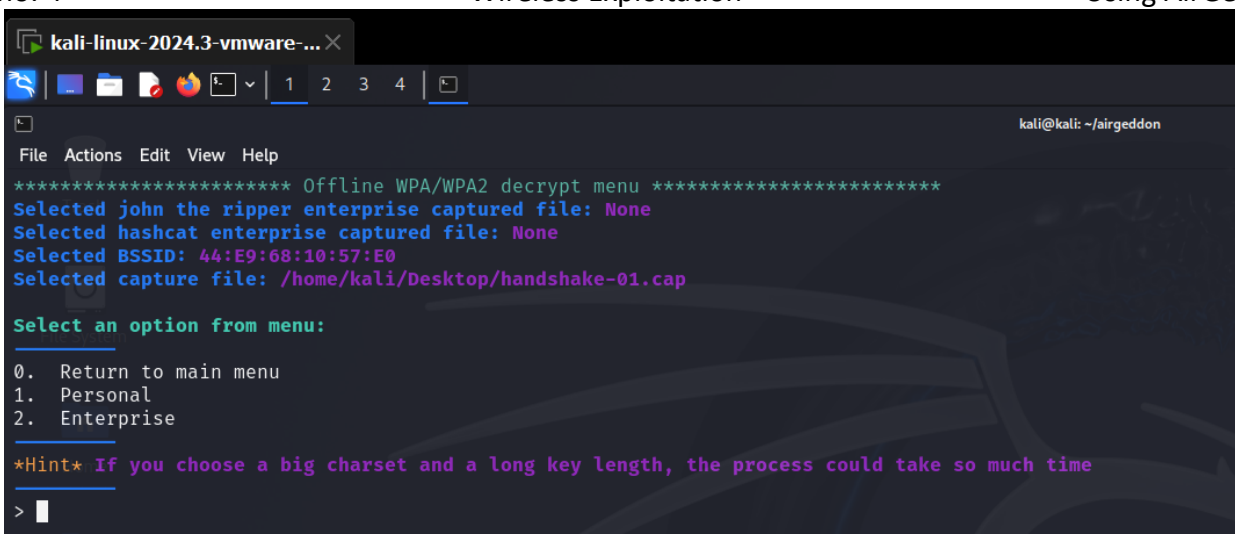
Methodology:

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

Detailed steps of Dictionary/Brute Force Attack:

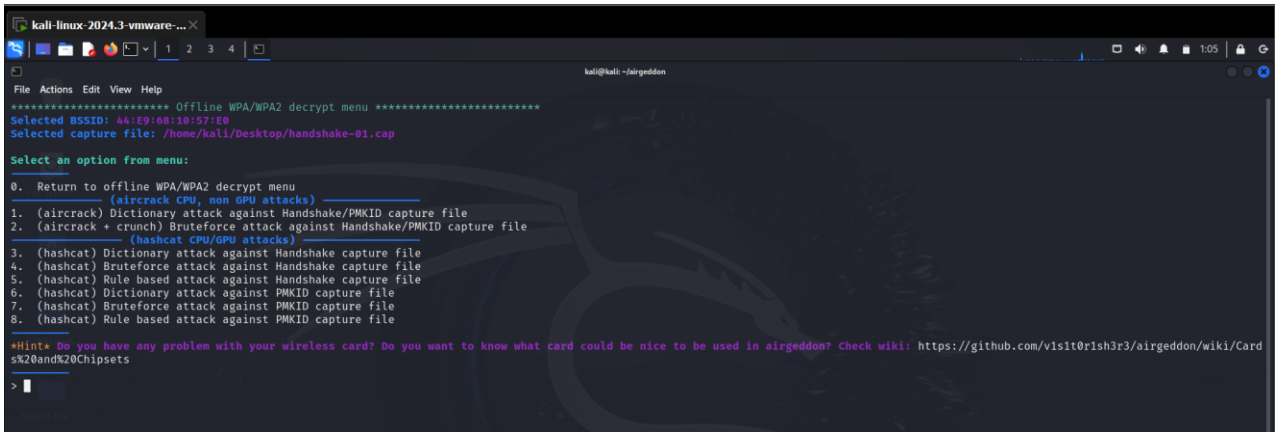
1. Coming back to the main menu:

2. Select the **<u>6. Offline WPA/WPA2 decrypt menu</u>** option.



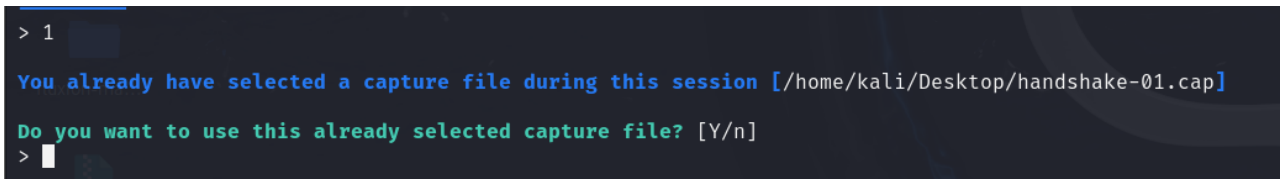
Focus on the top of the terminal where the information is given about the decrypt methods and the selected handshake file. Select the option depending on the network you attacked (if it was enterprise select 2nd option and if it is simple select the 1st option). In our case we have selected 1st option.

3. You will be treated with the following menu:



Note: There are lots of offline attacks you can perform using airgeddon. In this report we are covering "<u>(aircrack) Dictionary attack against Handshake/PMKID capture file</u>" _attack

4. Carrying the attack:



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

```
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]

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

Press Y to continue

5. Now you will get a prompt to enter the path for a file that contains password for dictionary attack (You can find one on the internet that contains compromised passwords). In my case I have a file stored on the Desktop.

```
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 ...
```

6. Press enter to start the attack.

```
kali@kali: ~/airgeddon
File  Actions  Edit  View  Help

                    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%

                    KEY NOT FOUND


  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
  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


Press [Enter] key to continue ...
```

Note: The dictionary attack will only be successful if your target network has a compromised password like “12345678” or “0000000” and like that.

Use case:

A dictionary attack is used to crack WPA/WPA2 passwords by systematically testing a list of pre-defined potential passwords against the captured handshake to find the correct one.

4.4 Evil Twin Attack

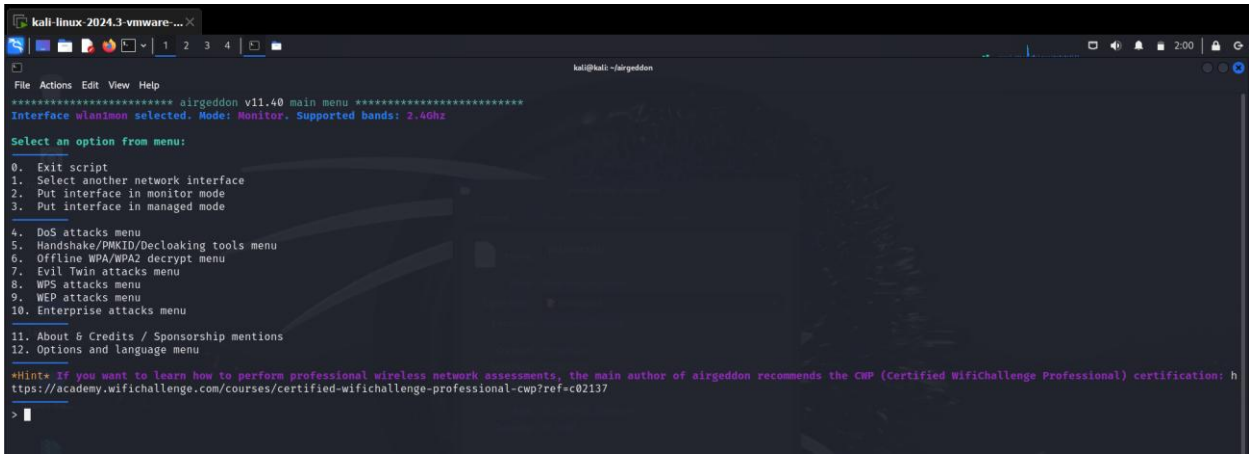
- **Objective:** Create a fake access point to trick users into sharing their Wi-Fi password.

Methodology:

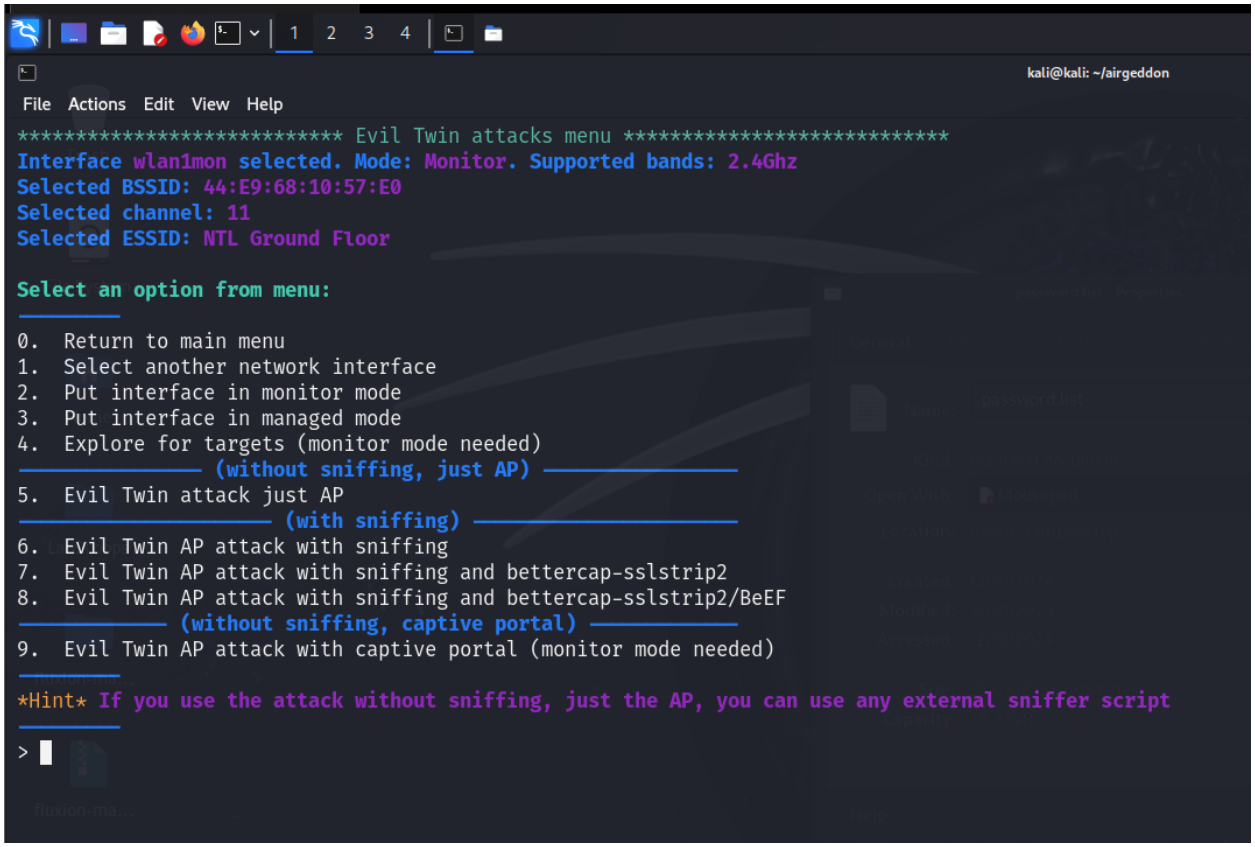
1. Configure Airgeddon to create a fake AP.
2. Broadcast the rogue AP and monitor connections.
3. Collect authentication details entered by unsuspecting users.

Details of the Evil Twin Attack:

1. Coming back to the main menu.



2. Select the Evil Twin Attack from the menu



You will get the following interface as shown in the above figure.

3. In this report we will be using the 9th option which is the Evil twin AP attack with captive portal (other topics are too advance to be cover in this report and will be out of scope of this report)

```
> 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 wlan1mon 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...
```

Press Enter to explore targets.

```
kali-linux-2024.3-vmware-...
1 2 3 4
kali@kali: ~/airgeddon
File Actions Edit View Help
********************************* Select target *********************************
  N.        BSSID        CHANNEL  PWR   ENC    ESSID

  1)*  44:E9:68:10:57:E0   11    38%   WPA2   NTL Ground Floor

Only one target detected. Autoselected
Press [Enter] key to continue...
```

We will be again attacking the **NTL Ground Floor** as we have the permission to attack this network

4. Now you will get the following menu:

```
File Actions Edit View Help
kali@kali: ~/airgeddon
***************************** Evil Twin deauth ******************************
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
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

>
```

You have to select one Deauth attack.

Note: The benefit of doing the deauth attack that the clients will be disconnected from the targeted network and will be connected to your fake access point.

```
> 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 countering "channel hopping" [y/N]
>
```

If you have an extra wireless interface you can enter Y.

```
File  Actions  Edit  View  Help
******************* Evil Twin AP attack with captive portal ********************

Only one additional interface able to be used detected. Autoselected
Press [Enter] key to continue...

This interface wlan0 is not in monitor mode

Interface will be tried to be changed to monitor mode automatically
Press [Enter] key to continue...

Setting your interface in monitor mode...

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

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

5. Press enter to continue

```
Selected interface enabled is in monitor mode. Attack can be performed
Press [Enter] key to continue...
```

6. Now the tool will ask you some things as follows.

```
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]
>
```

As we have the handshake file of the targeted network we will give the path to it.

```
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]
> y

Handshake captured file detected during this session [/home/kali/Desktop/handshake-01.cap]

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

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 the file or press [Enter] to accept the default proposal [
/root/evil_twin_captive_portal_password-NTL Ground Floor.txt]
>
```

7. Now you can see the tool automatically detected the captured handshake file and now asking a path to store the password file (In case the password hash matches with hash stored in the handshake file) give a path to (in our case we are using Desktop)
8. Now the tool will ask you about the language you want the captive portal to be in it.

```
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
13. Chinese

*Hint* If you want to learn how to perform professional wireless network assessments, the main
ttps://academy.wifichallenge.com/courses/certified-wifichallenge-professional-cwp?ref=c02137

>
```

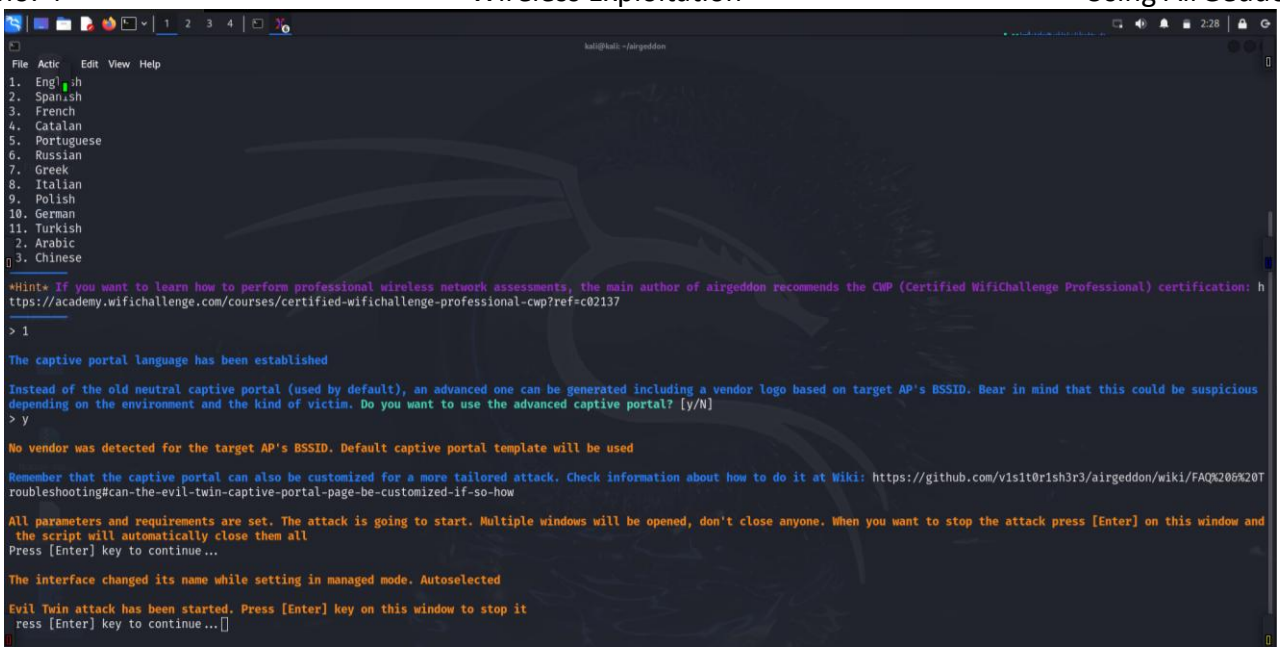
We will go with the **English.**

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

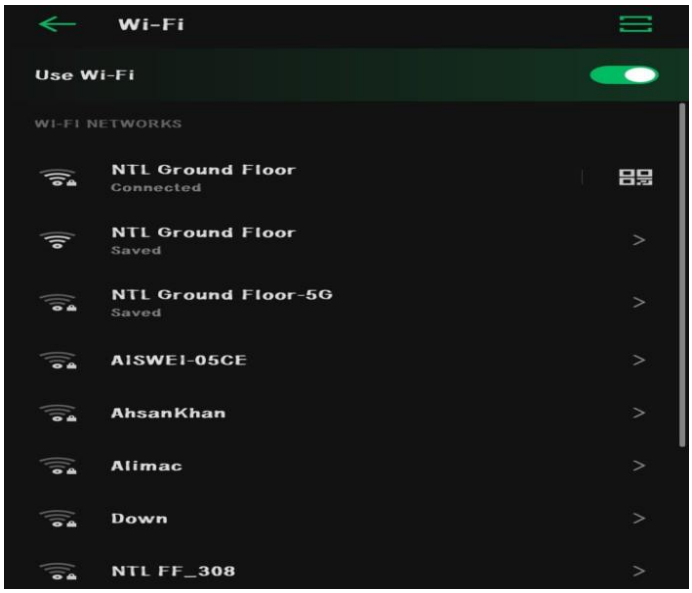
```
> 1

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]
>
```

10. Press Enter to start the attack and follow the instructions carefully:

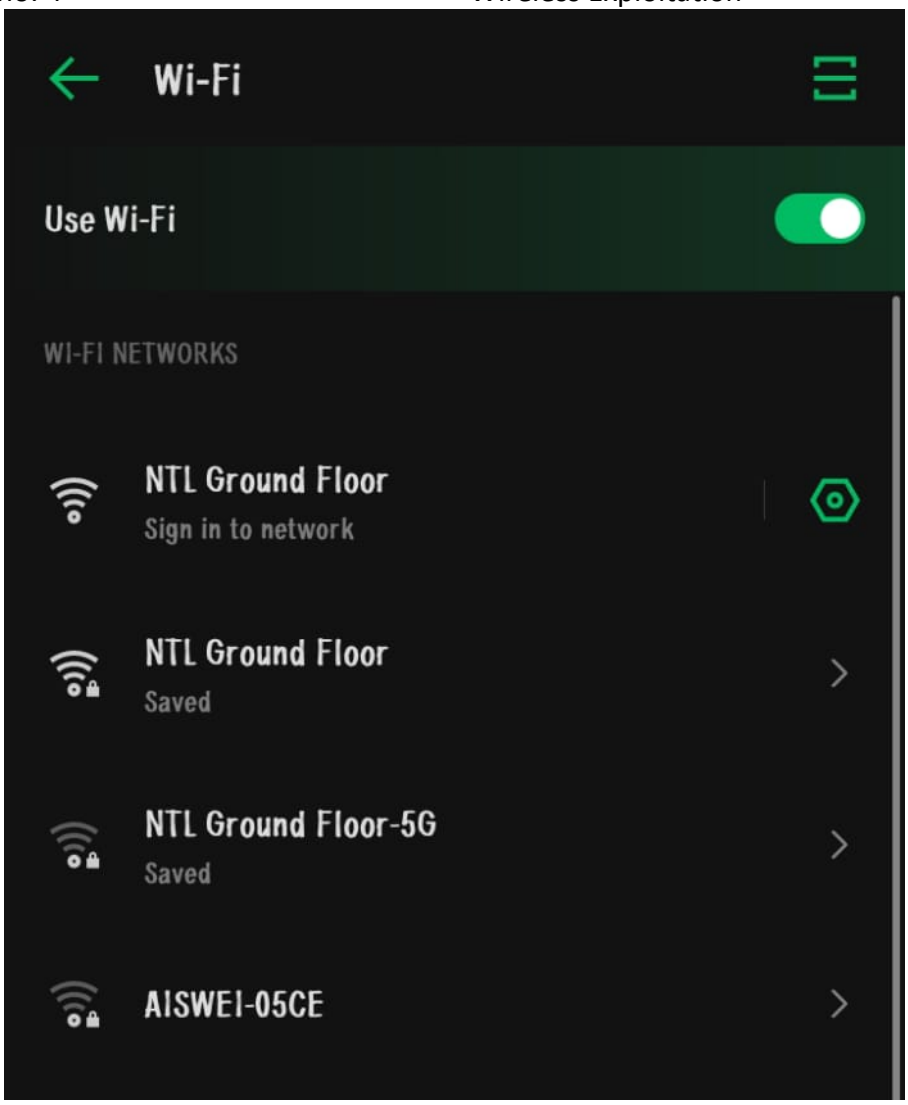
```
No vendor was detected for the target AP's BSSID. Default captive portal template will be used

Remember that the captive portal can also be customized for a more tailored attack. Check information about how to do it at Wiki: https://github.com/v1s1t0r1sh3r3/airgeddon/wiki/FAQ%206%20T
roubleshooting#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 anyone. When you want to stop the attack press [Enter] on this window and
 the script will automatically close them all
Press [Enter] key to continue...
```



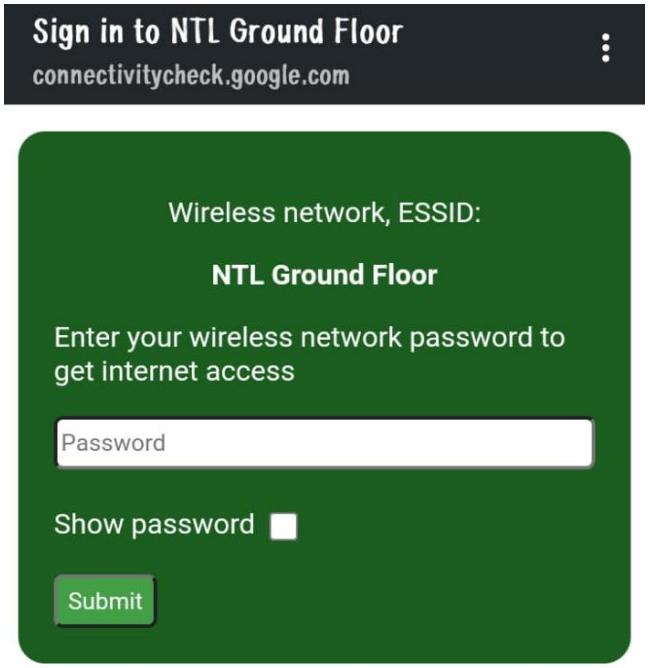
11. Now we will move on to an android device to show you what is going on.



A fake AP has created with the same name as of **NTL Ground Floor**

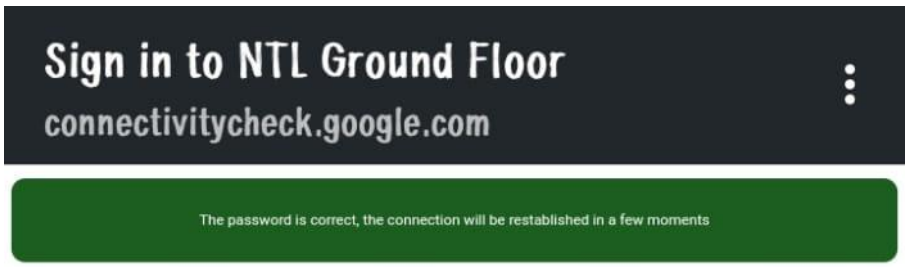


The android device is automatically connected to the Fake AP because the targeted network is jammed by our brute force attack and the following pop up will show up on the android device.

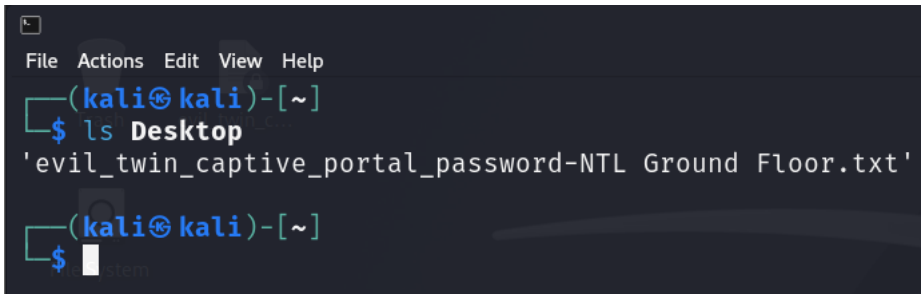


If the user enter wrong password it will be detected.

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



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



Open this file.

As you can see we got the correct the password and the attack was successful.

5. Airgeddon Limitations

Known Issues:

1. **Hardware Dependency:** Requires compatible wireless adapters for optimal performance.
2. **Ethical Considerations:** Improper use could lead to legal consequences.
3. **Manual Intervention:** Some tasks lack automation, increasing the complexity for beginners.
4. **Detection Risks:** Intrusion detection systems (IDS) can identify activities like deauthentication attacks.

6. Mitigation

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

Mitigation:

- Used an external antenna to boost signal reception.
- Optimized Airgeddon's settings for better range detection.

7. Conclusion

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.