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
- familirization with ethical hacking

DEMONSTRATION OF ATTACKING TECHNIQUES

Objective

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

ATTACK 01

DEAUTHENTICATION ATTACK & HANDSHAKE CAPTURE

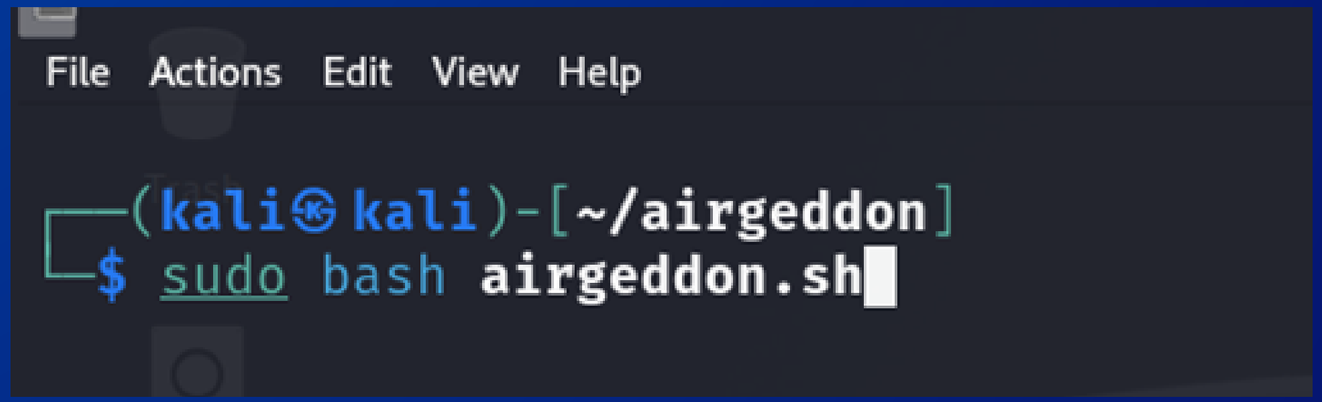
Performing deauthentic attack to Disconnect clients from a wireless network and capture the WPA/WPA2 handshake.

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.

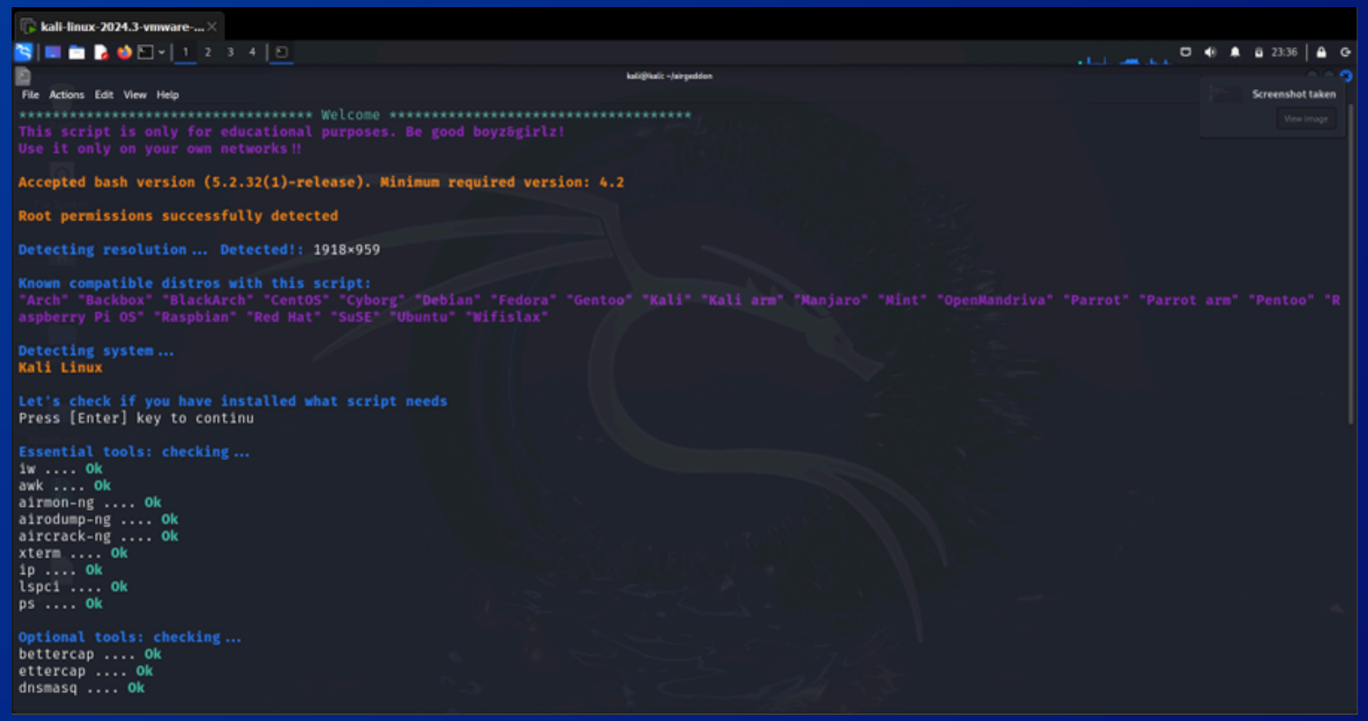
STEPS

1. First start the airgeddon tool



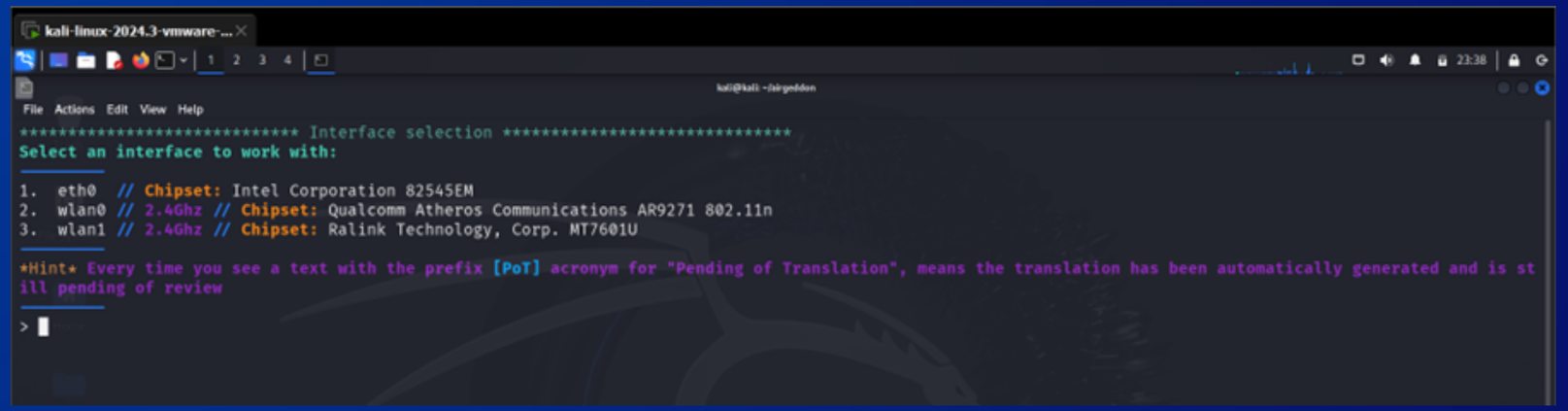
STEPS

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



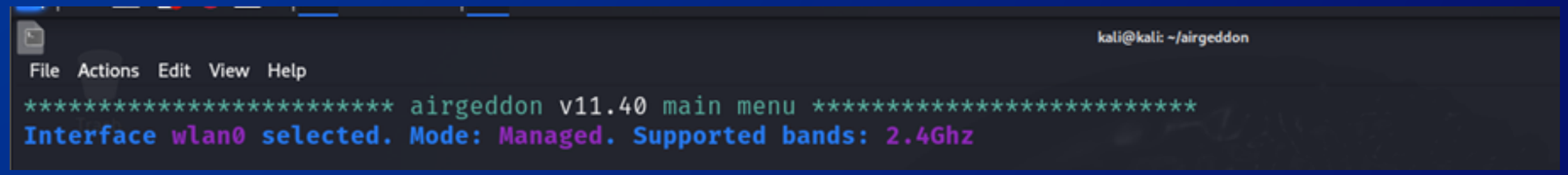
STEPS

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



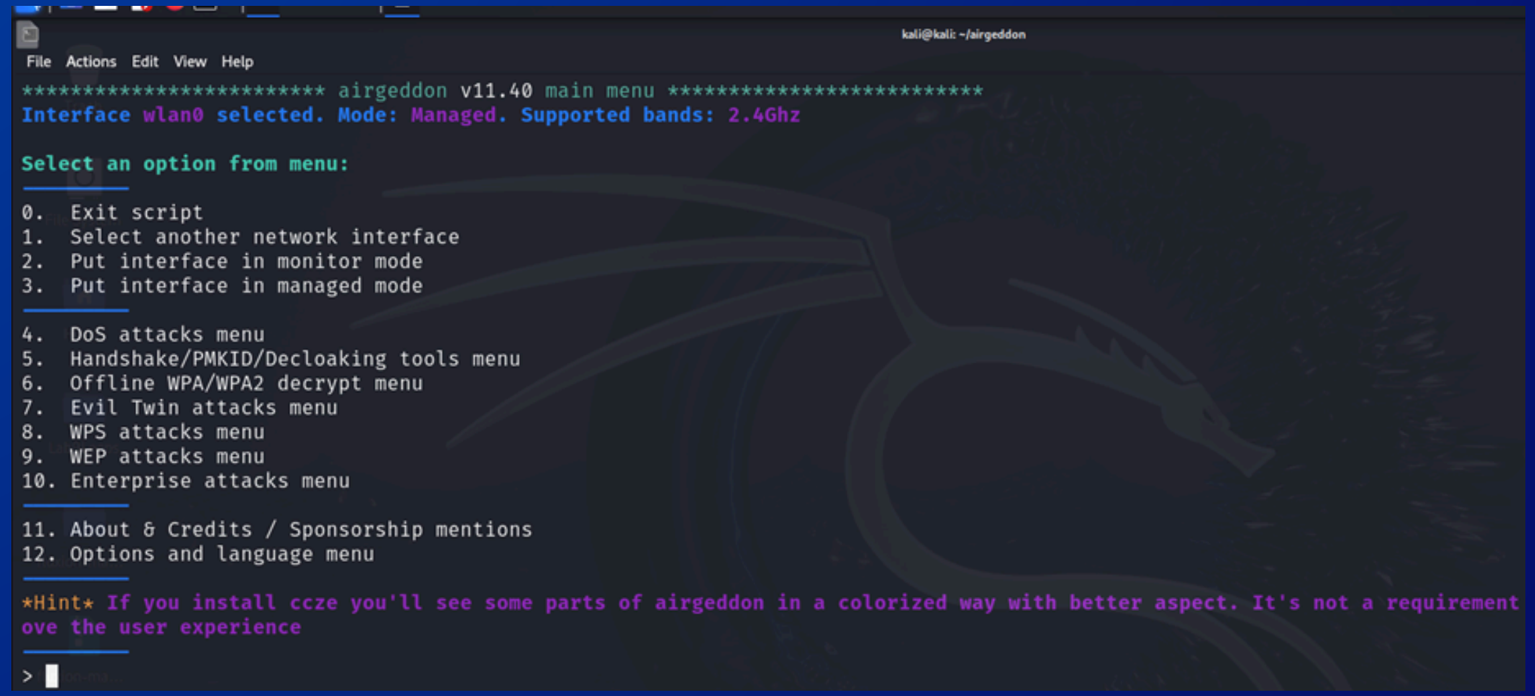
STEPS

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



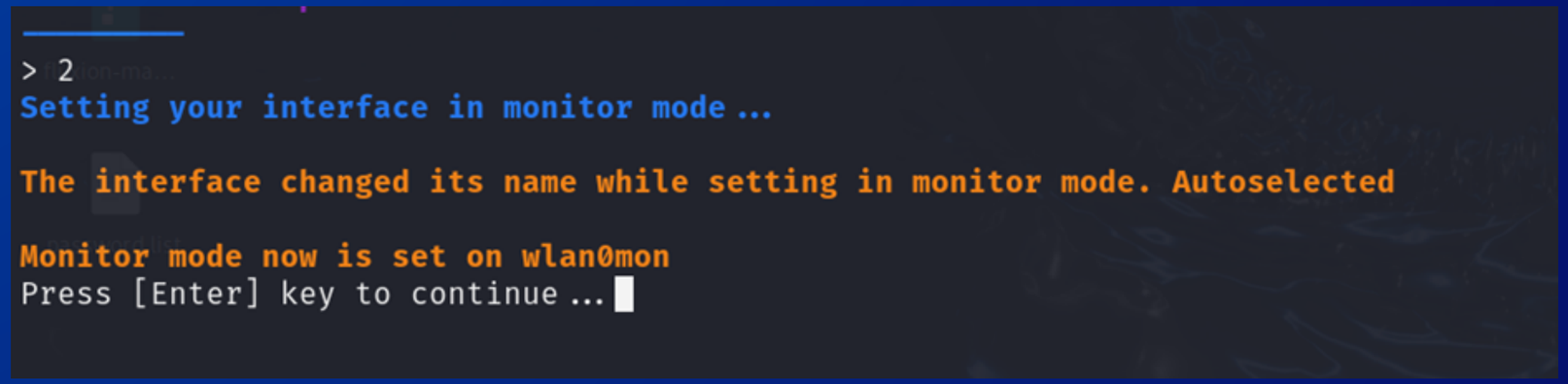
STEPS

4. You will get the following interface:



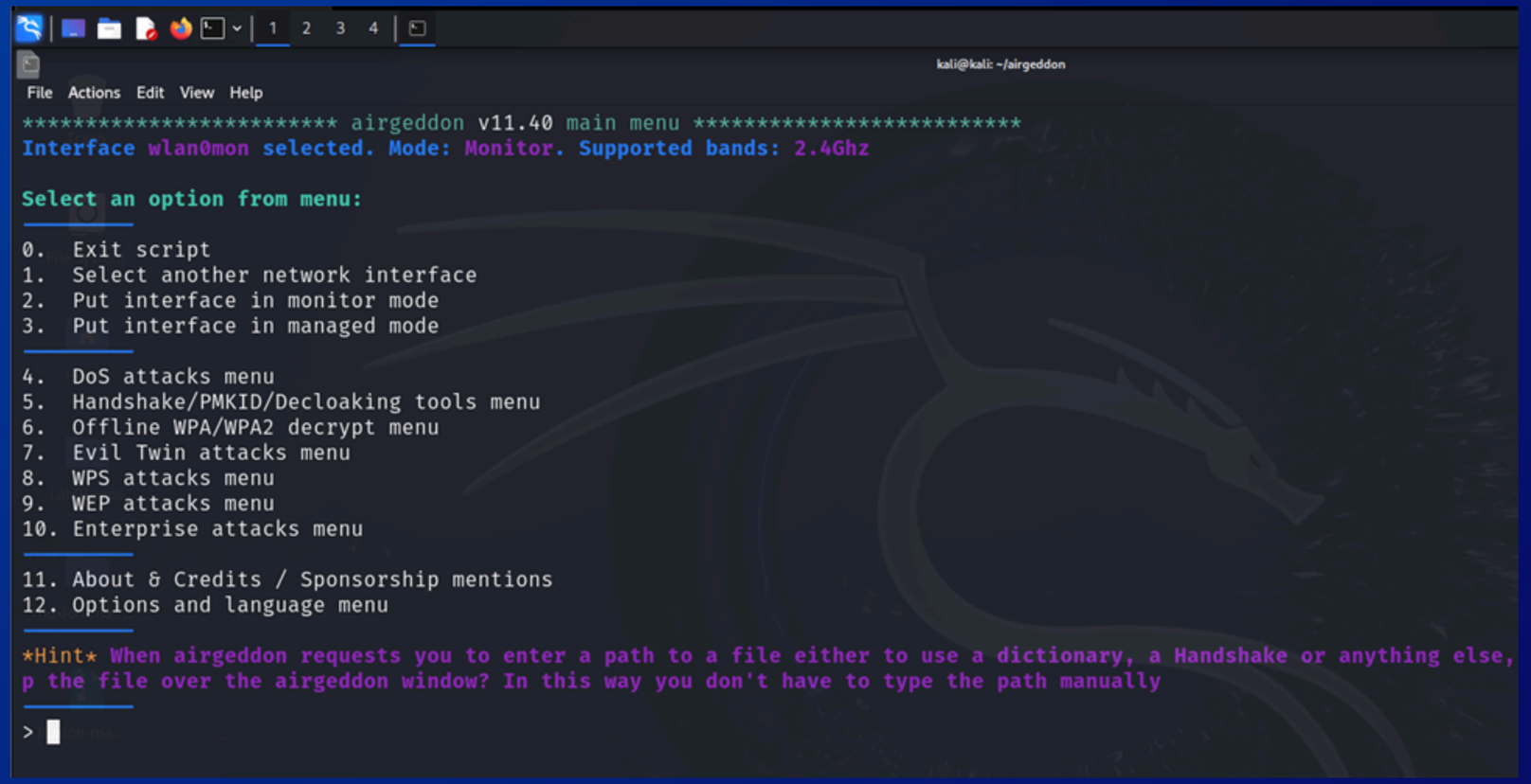
STEPS

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



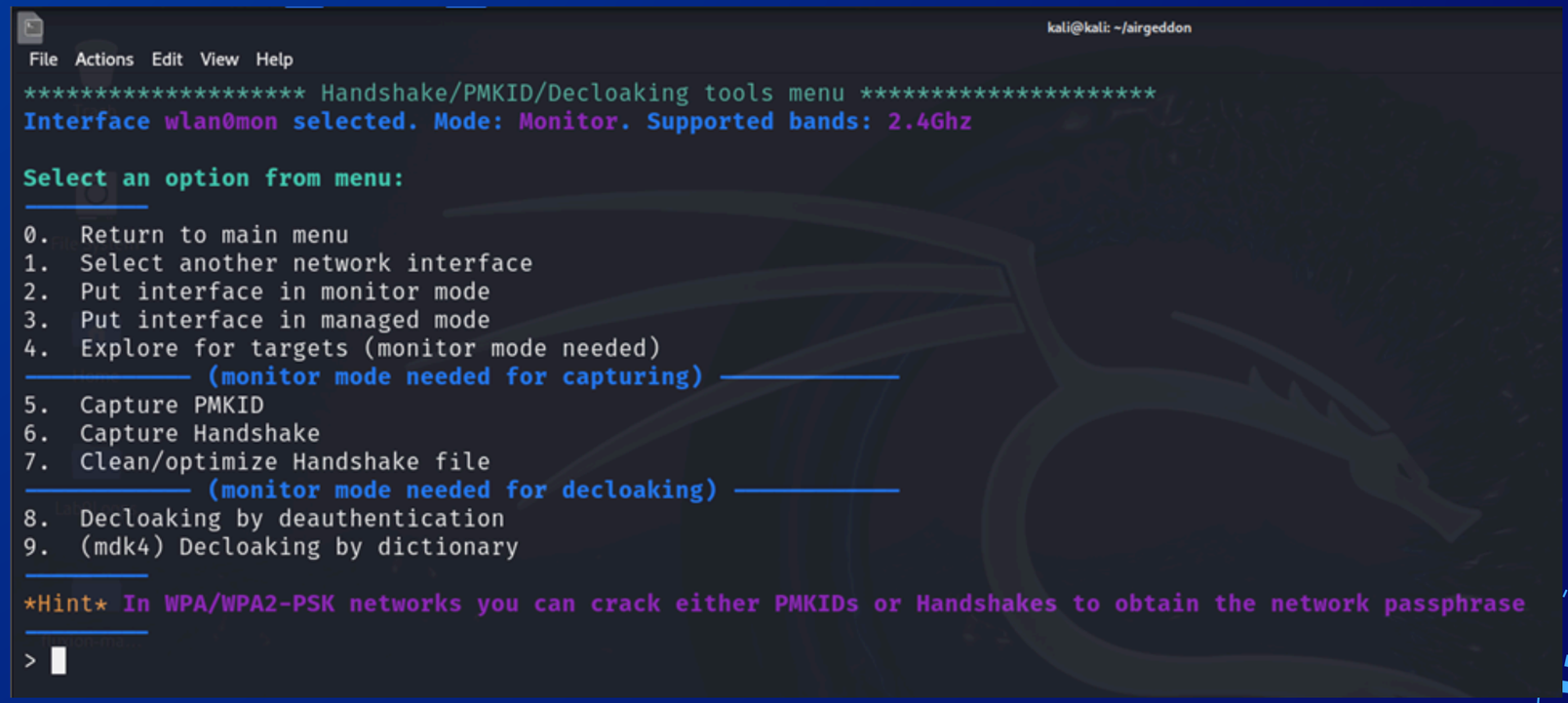
STEPS

press enter you will be back at the interface



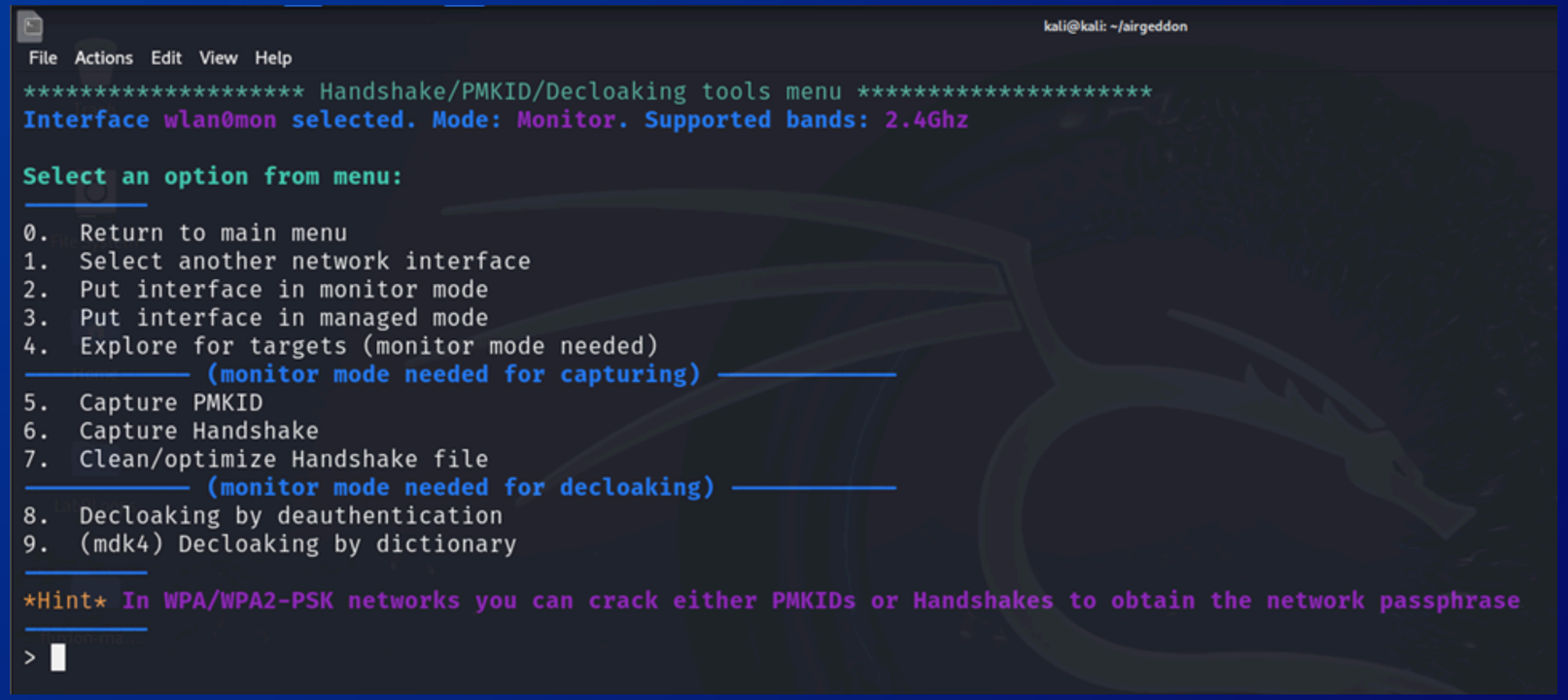
STEPS

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



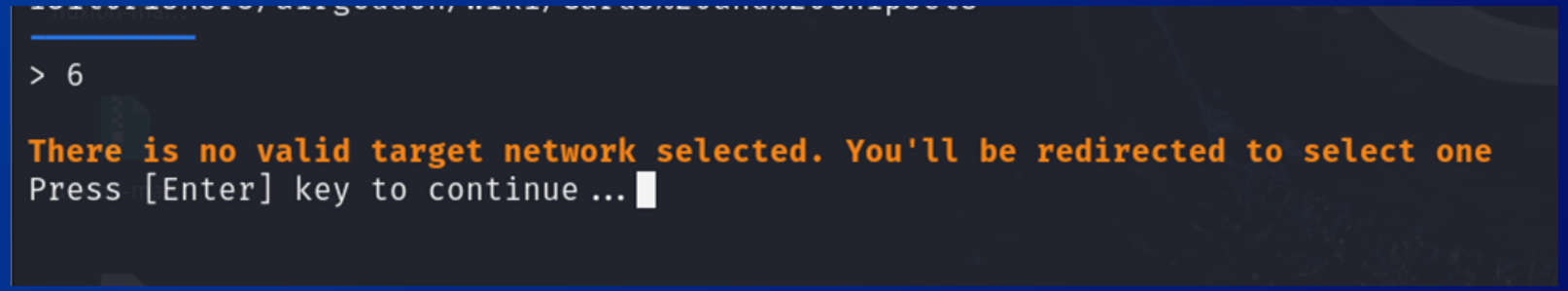
STEPS

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



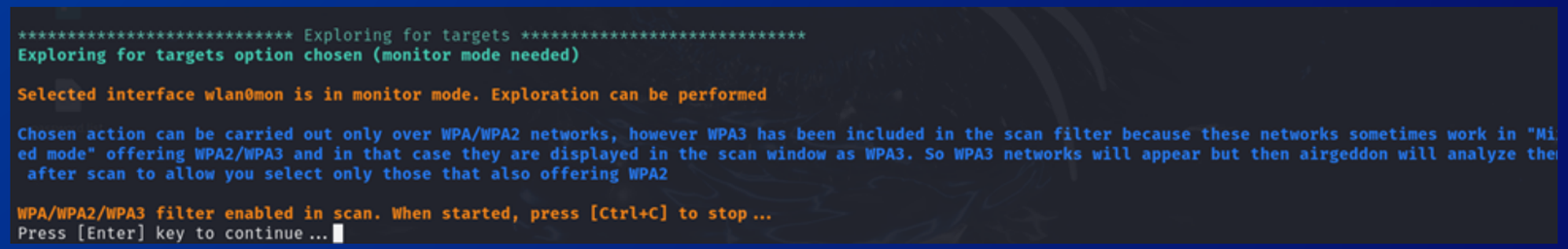
STEPS

There is no target network selected.



STEPS

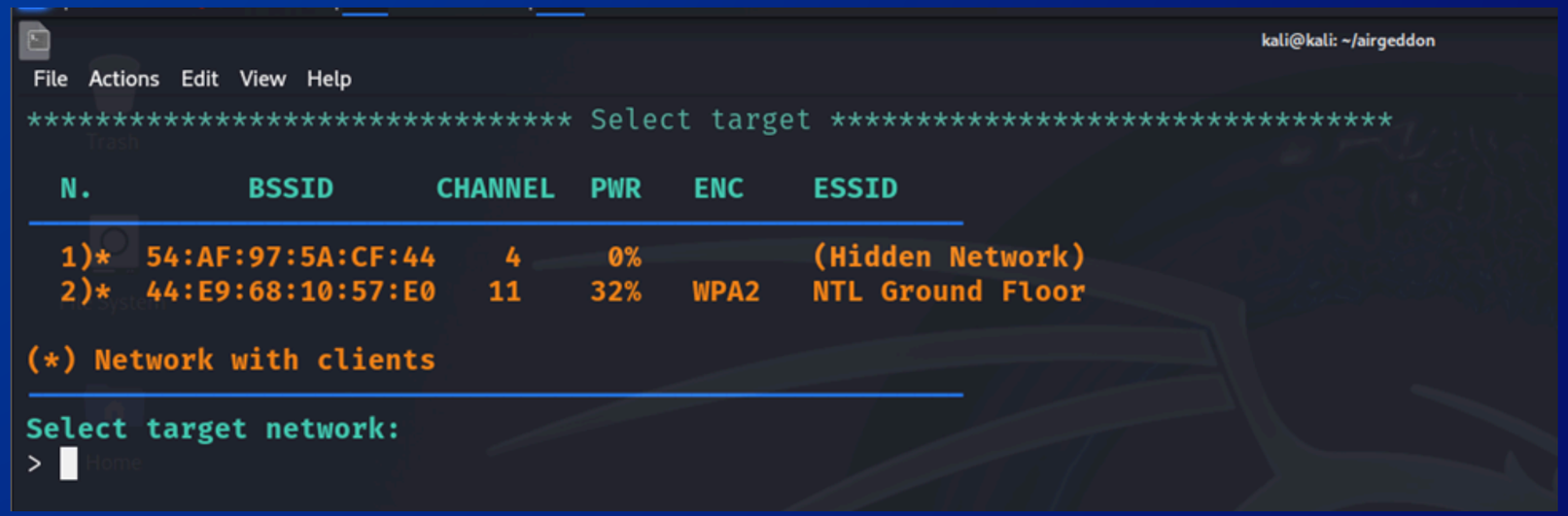
Press enter to scan targets near you



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

STEPS

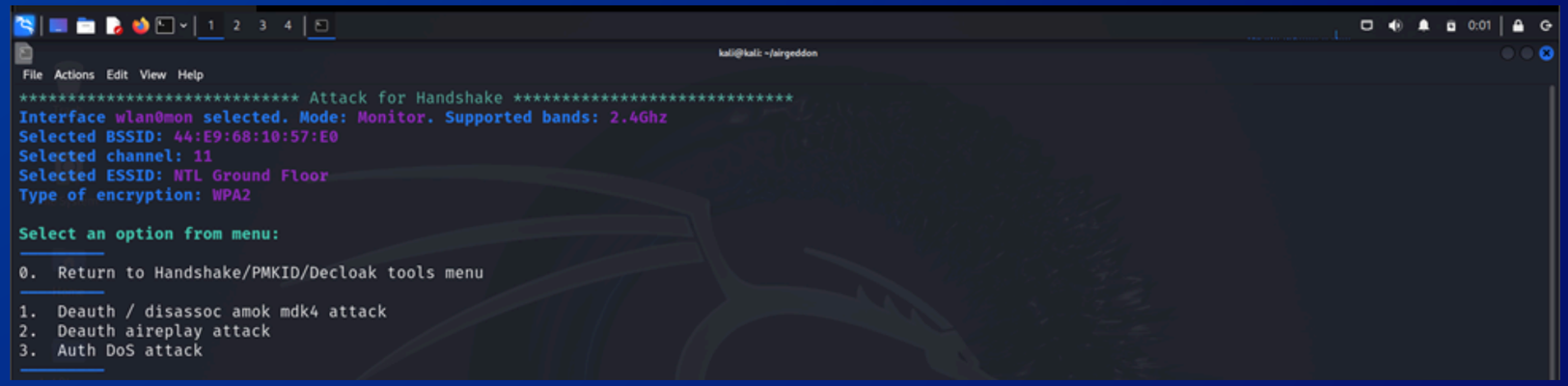
You will get the following interface:



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.



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

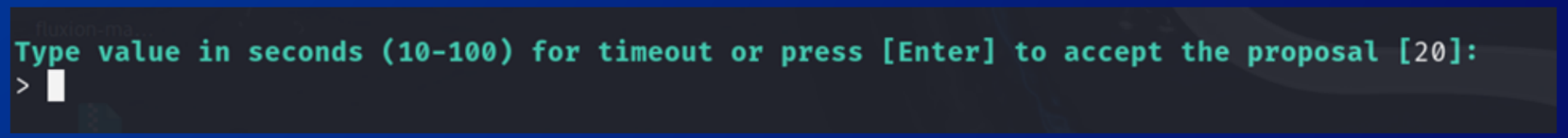
POINT TO BE NOTED

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

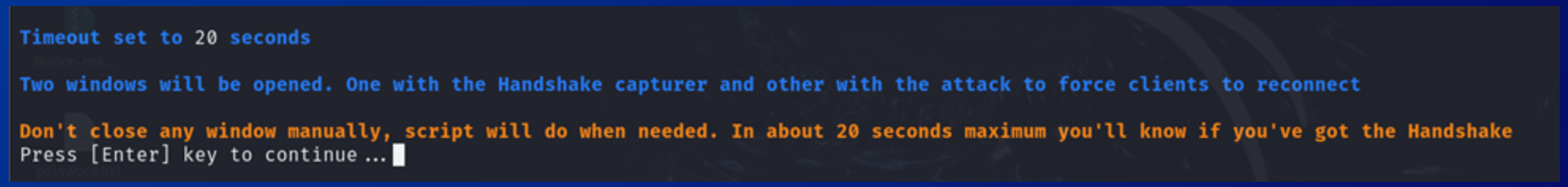
STEPS

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



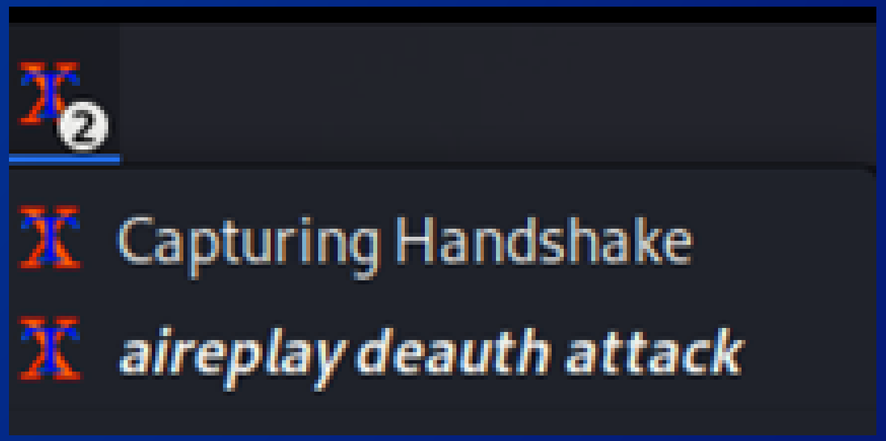
STEPS

- 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.



STEPS

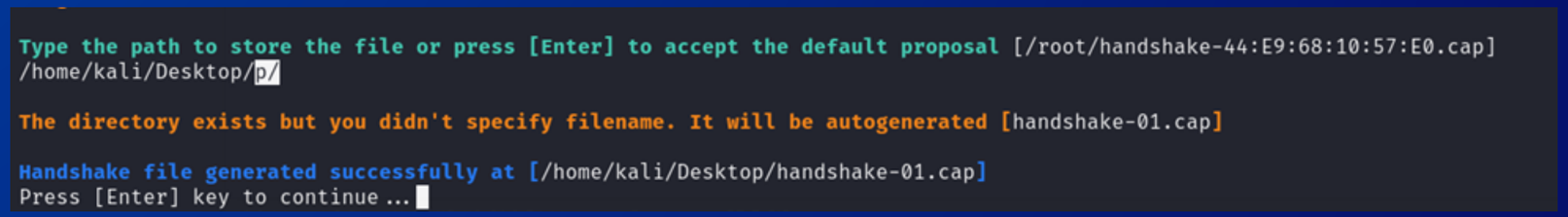
Press enter to the start the attack.



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

STEPS

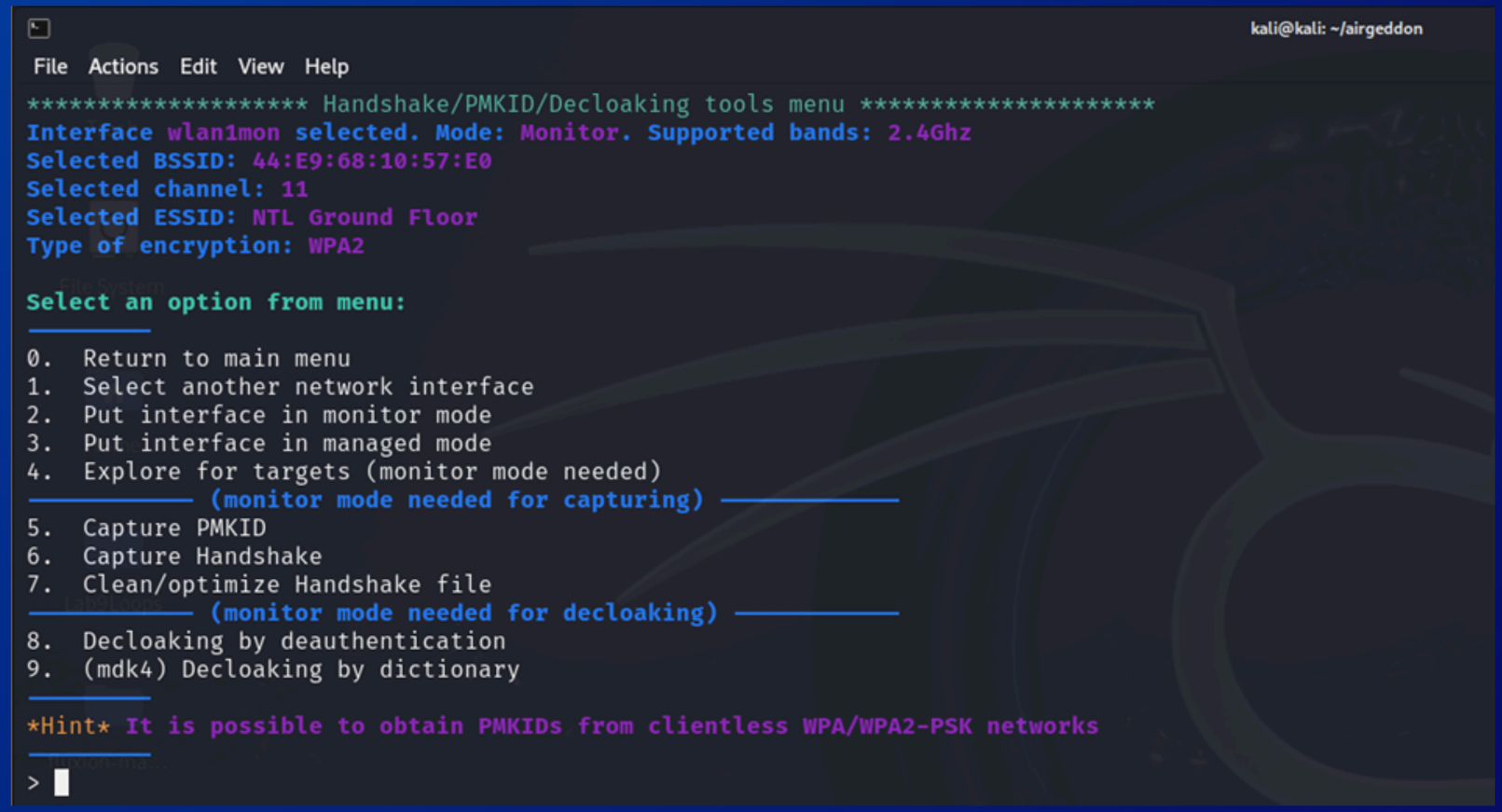
10. Now if the attack is successful you will be prompted to enter a path where to store the captured handshake file. In our case we will give the Desktop for our convenience.



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

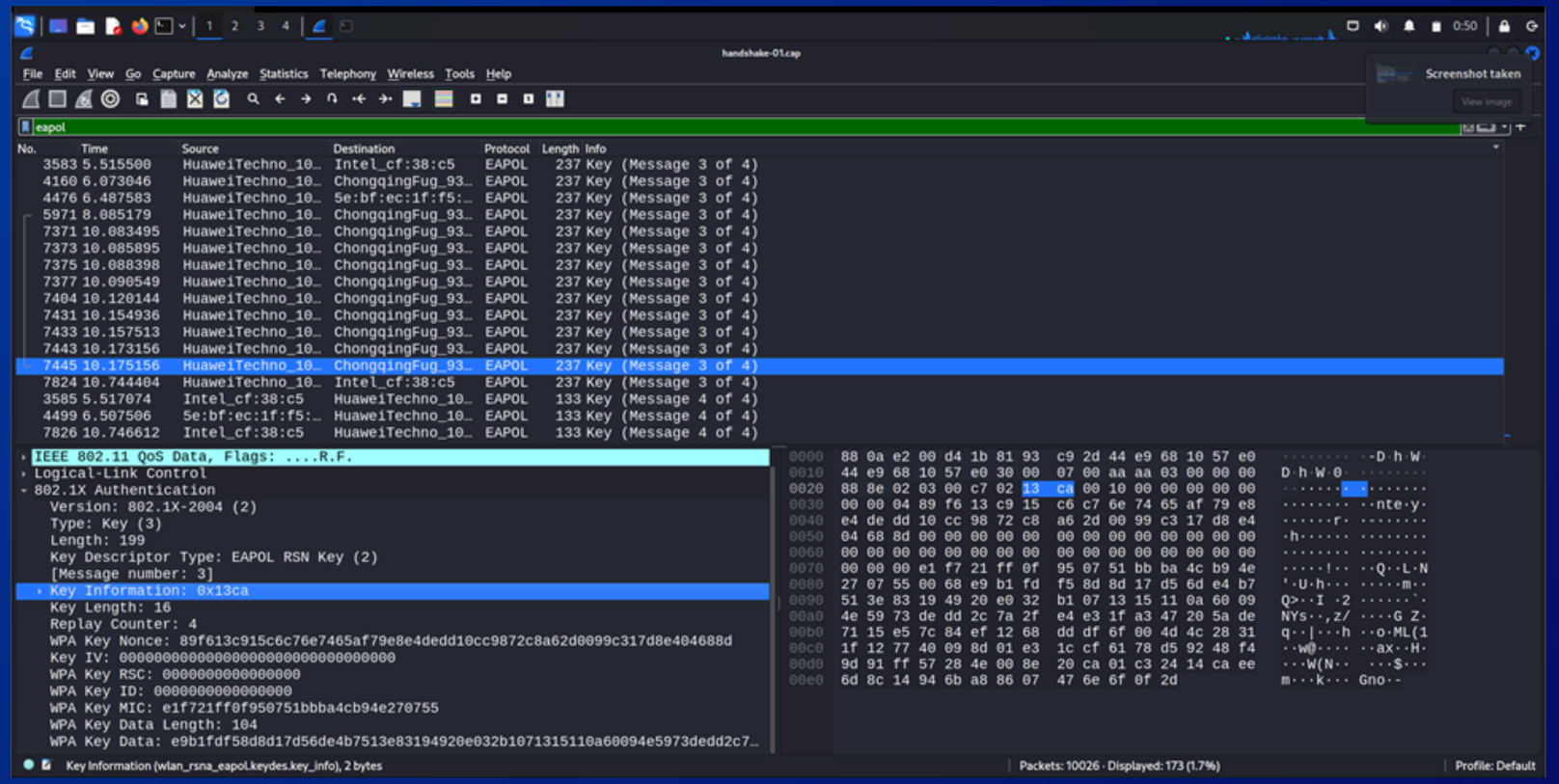
STEPS

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



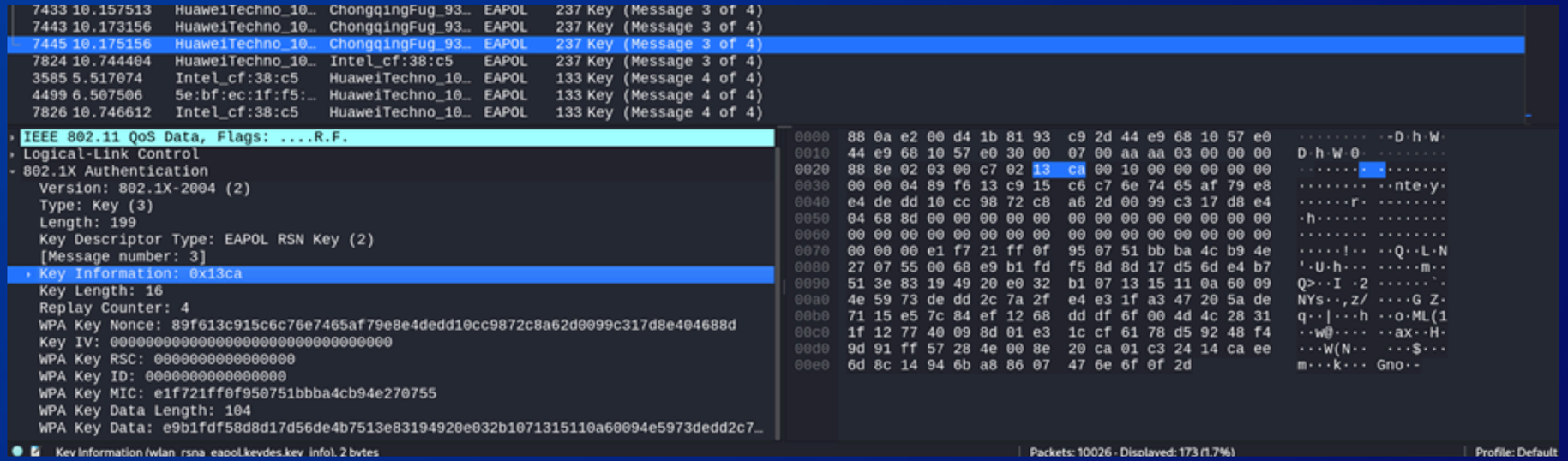
STEPS

12. Handshake file details



STEPS

Now we have the WPA key in encrypted form



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 th e captured handshake.

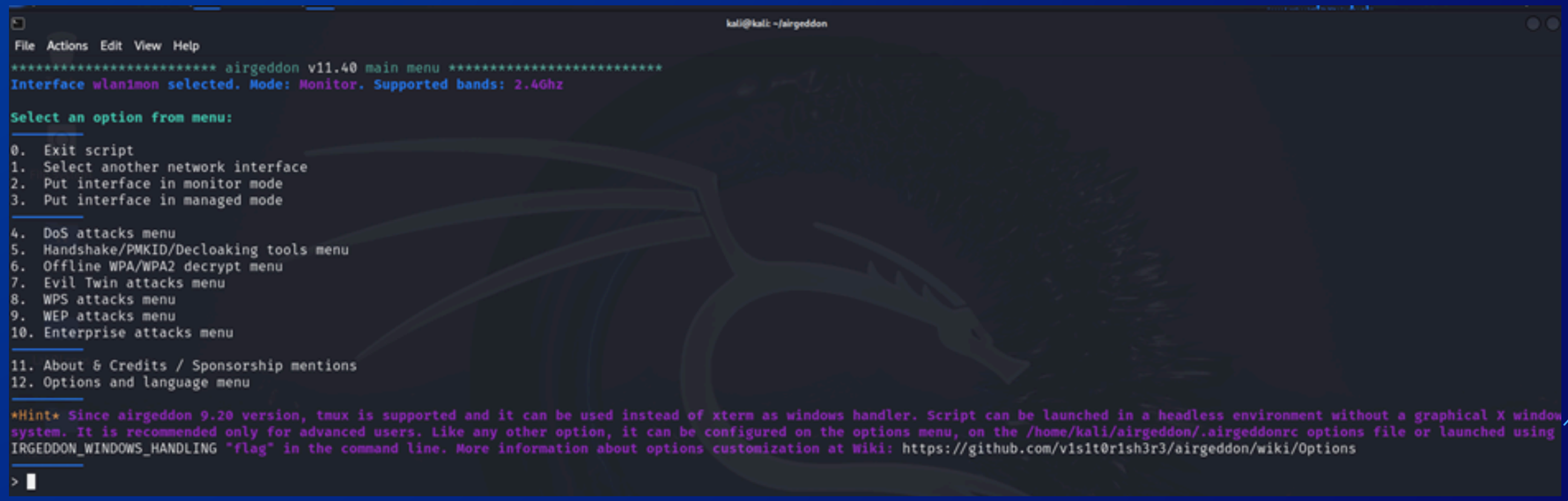
PROCEDURE

1. Load the handshake file into password-cracking (Provided with Airgeddon)

2 Attempt password guessing using a dictionary or brute force technique.

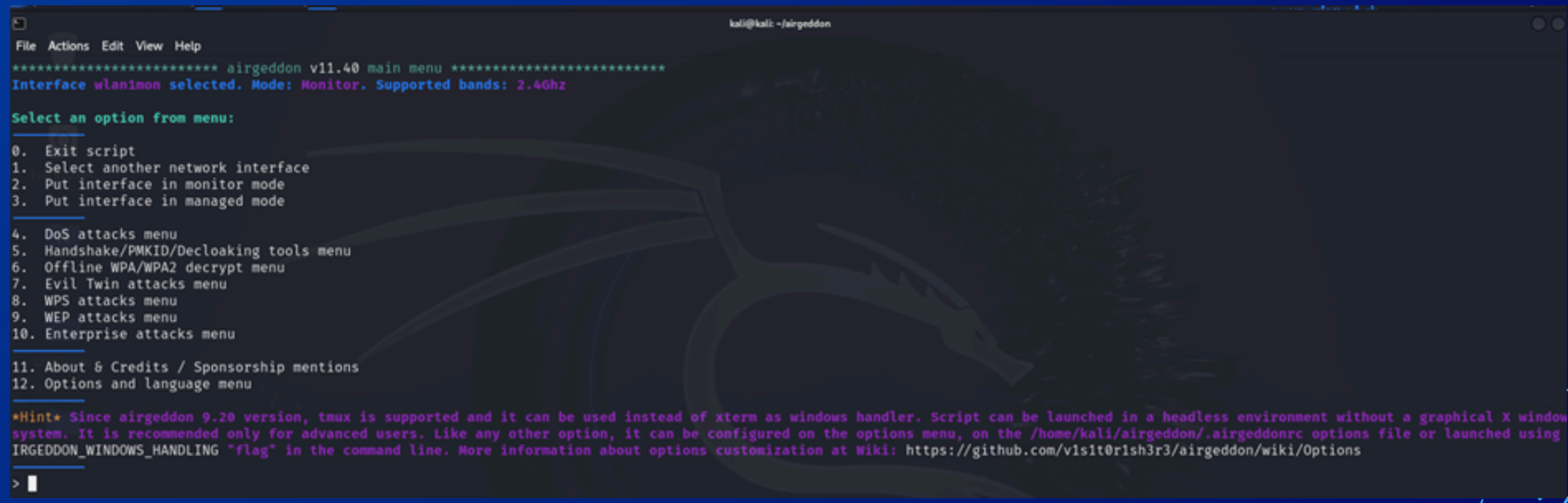
STEPS

coming back to our main menu



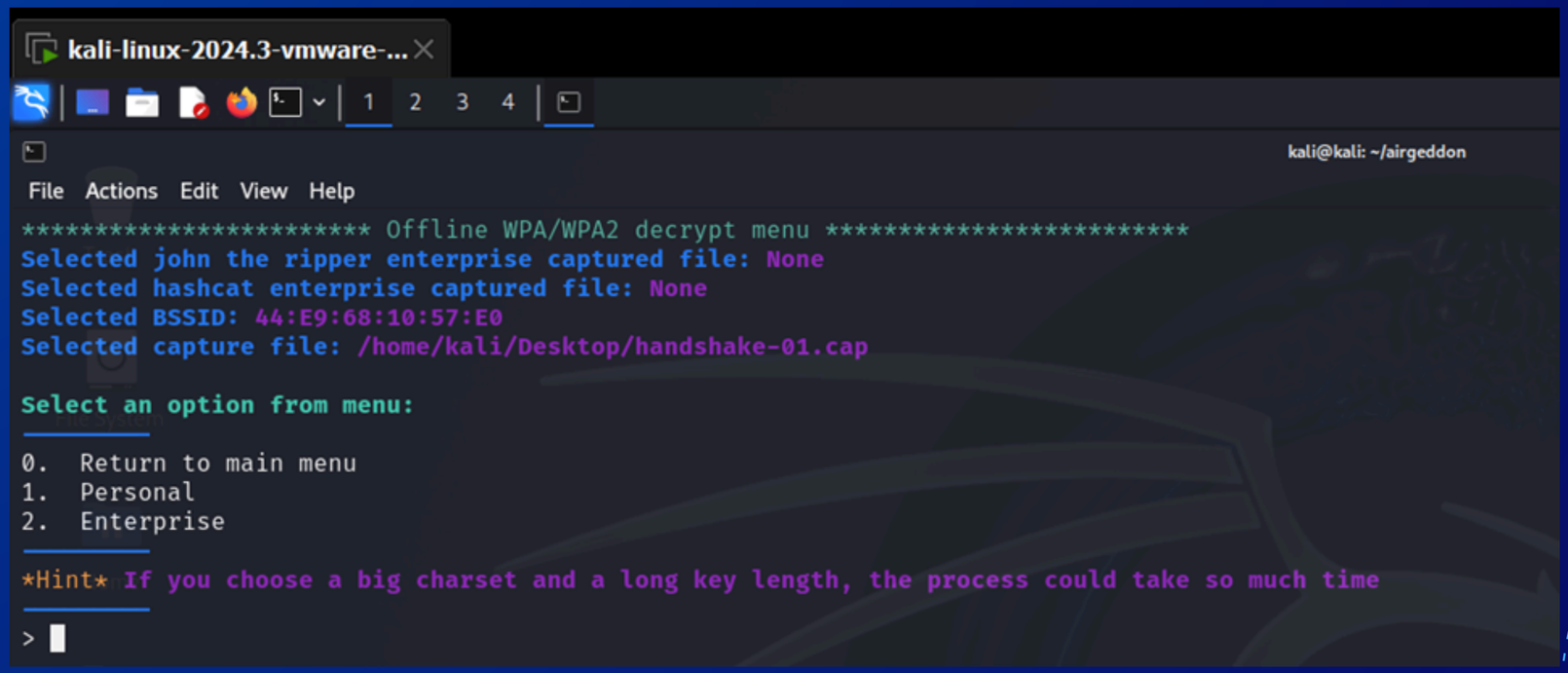
STEPS

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



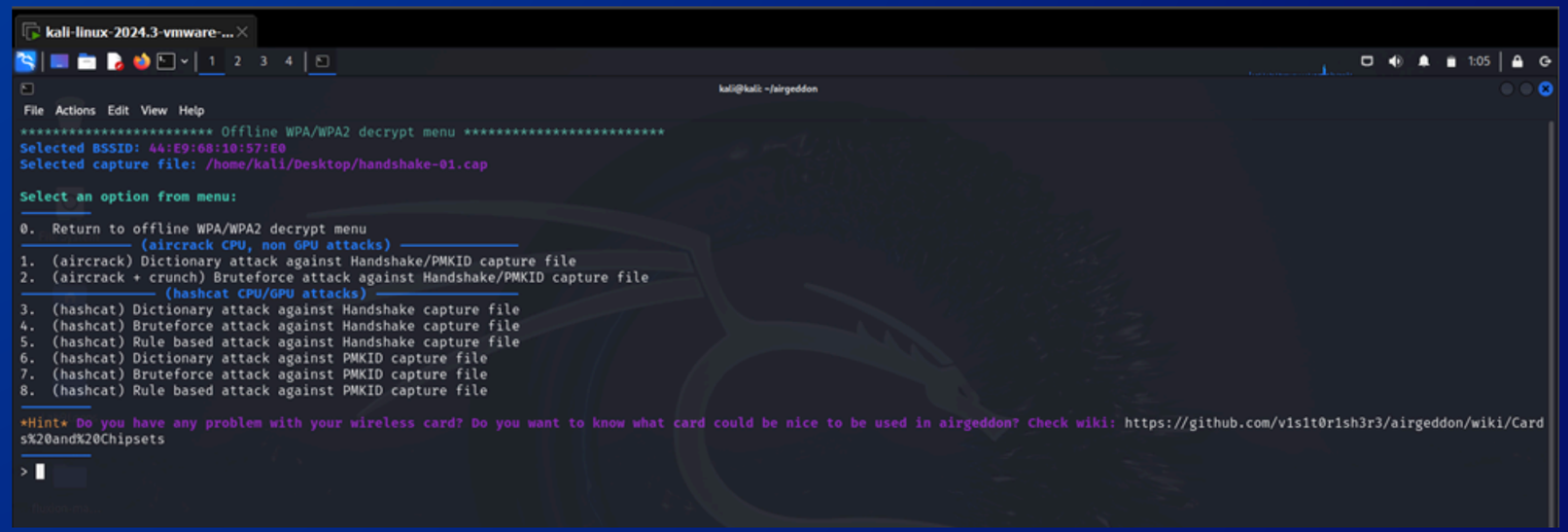
STEPS

Select the option depending on the network you attacked.
In our case we have selected 1st option.



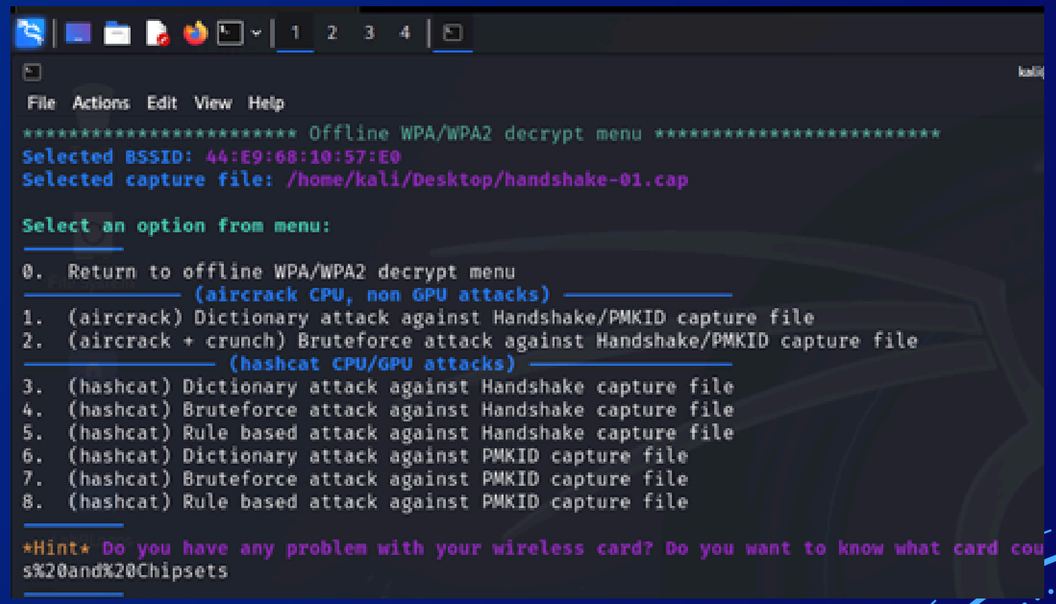
STEPS

3. You will be treated with the following menu:



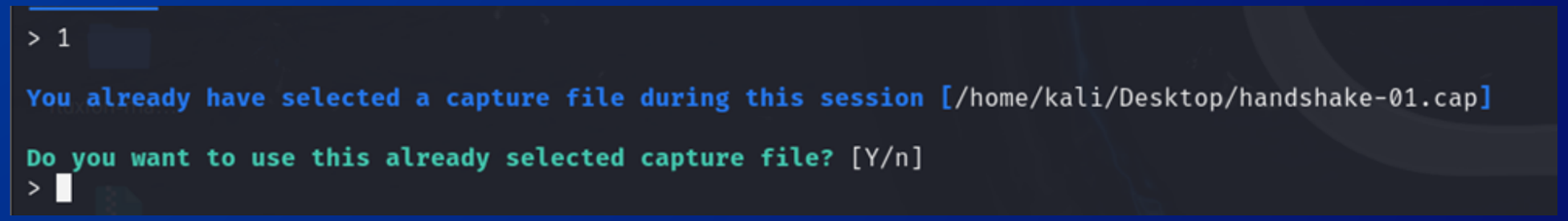
STEPS

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



STEPS

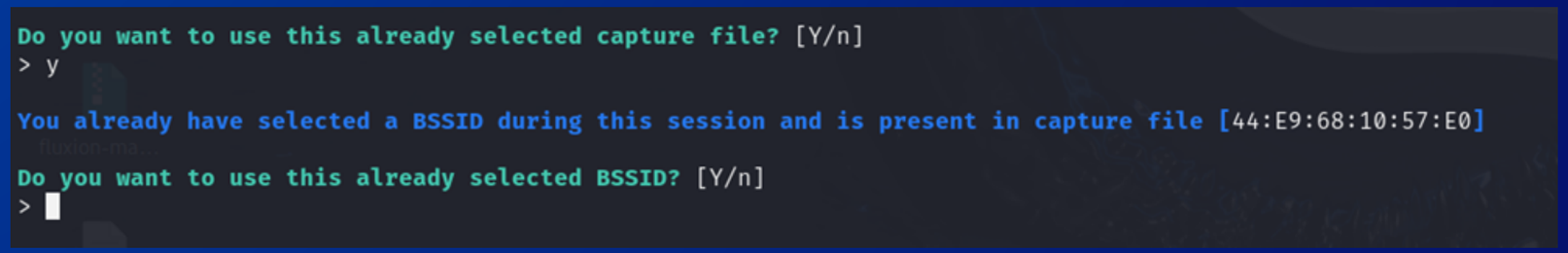
4. Iterating the attack:



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

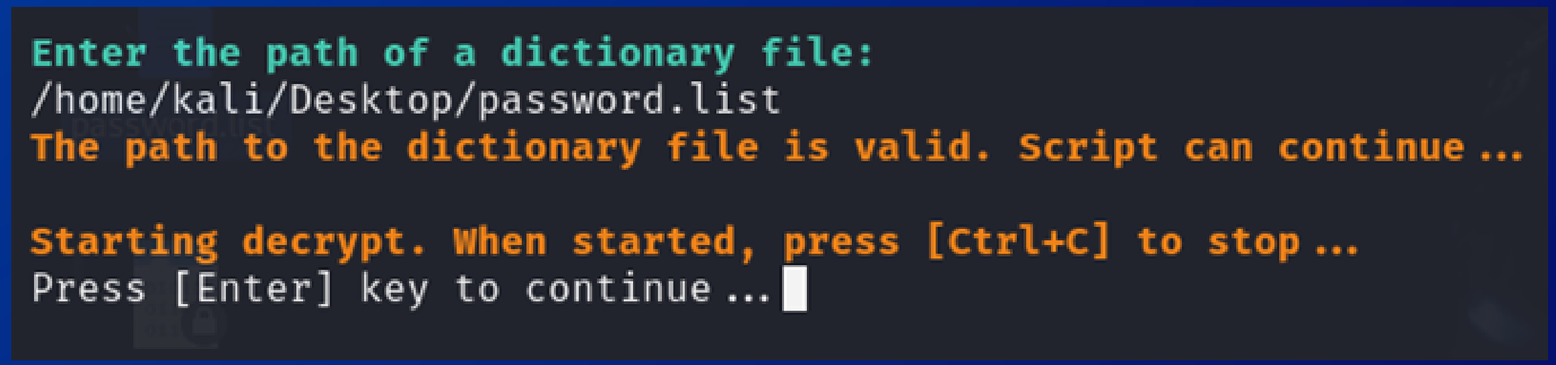
STEPS

press Y to continue



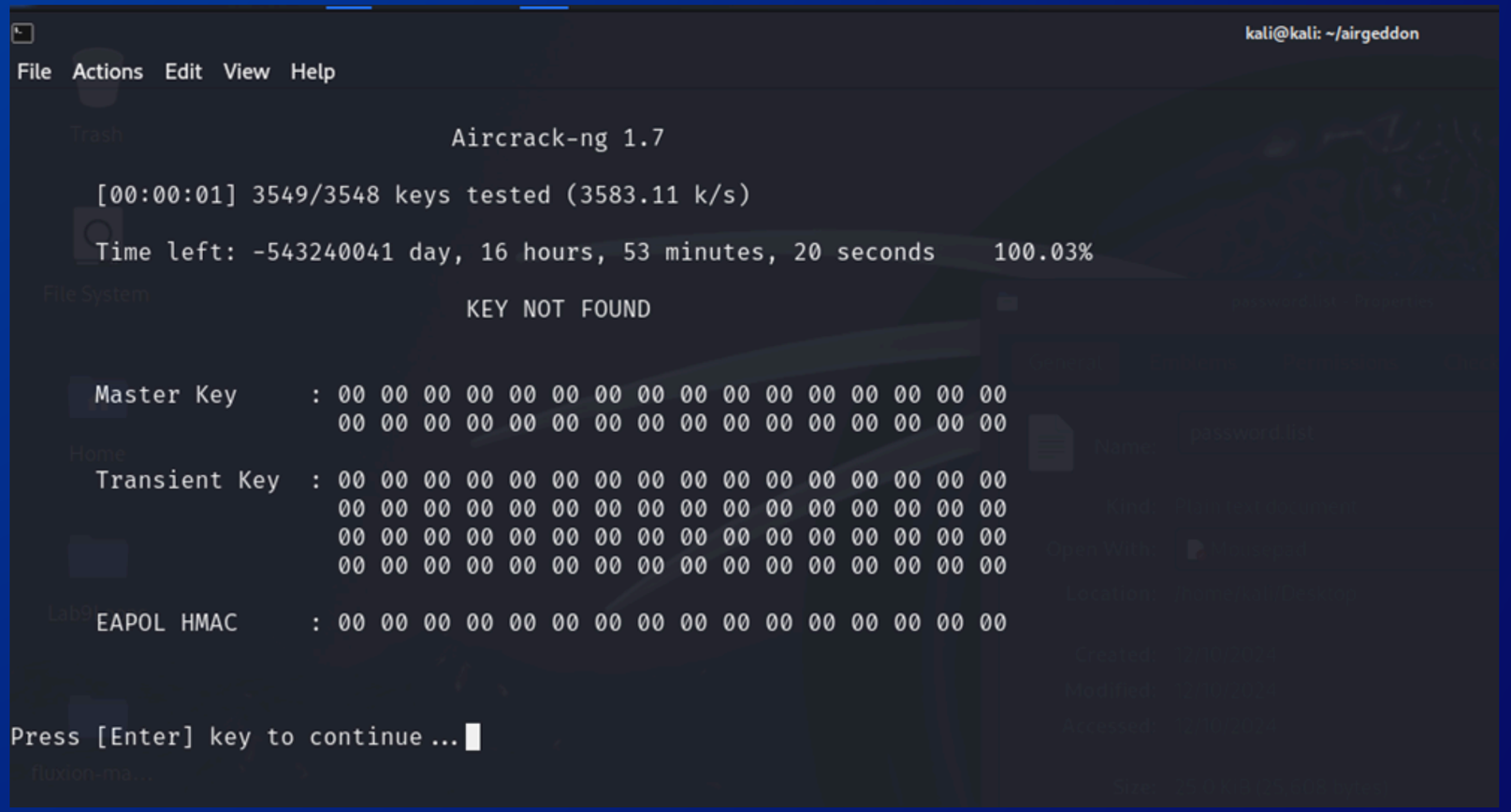
STEPS

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



STEPS

6. Press enter to start the attack.



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.

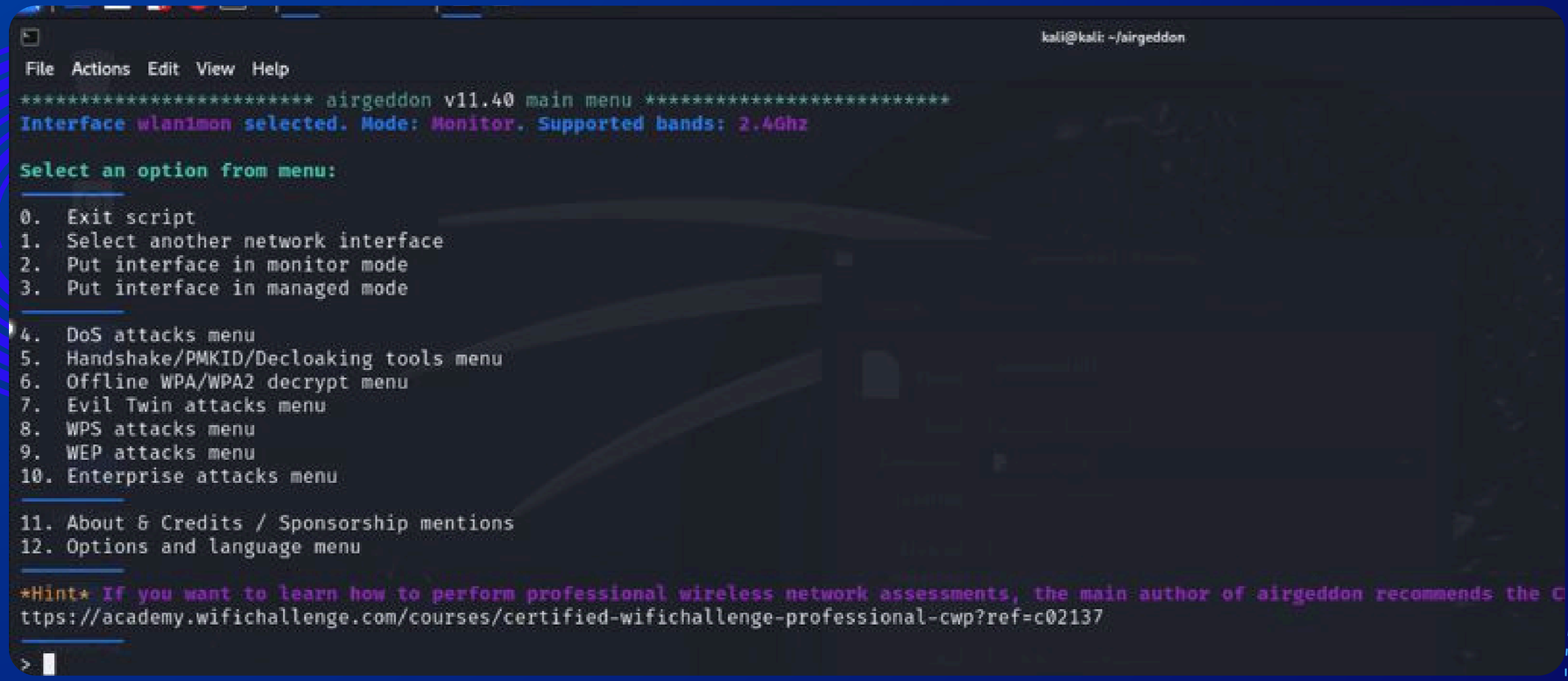
ATTACK 04

EVIL TWIN ATTACK

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

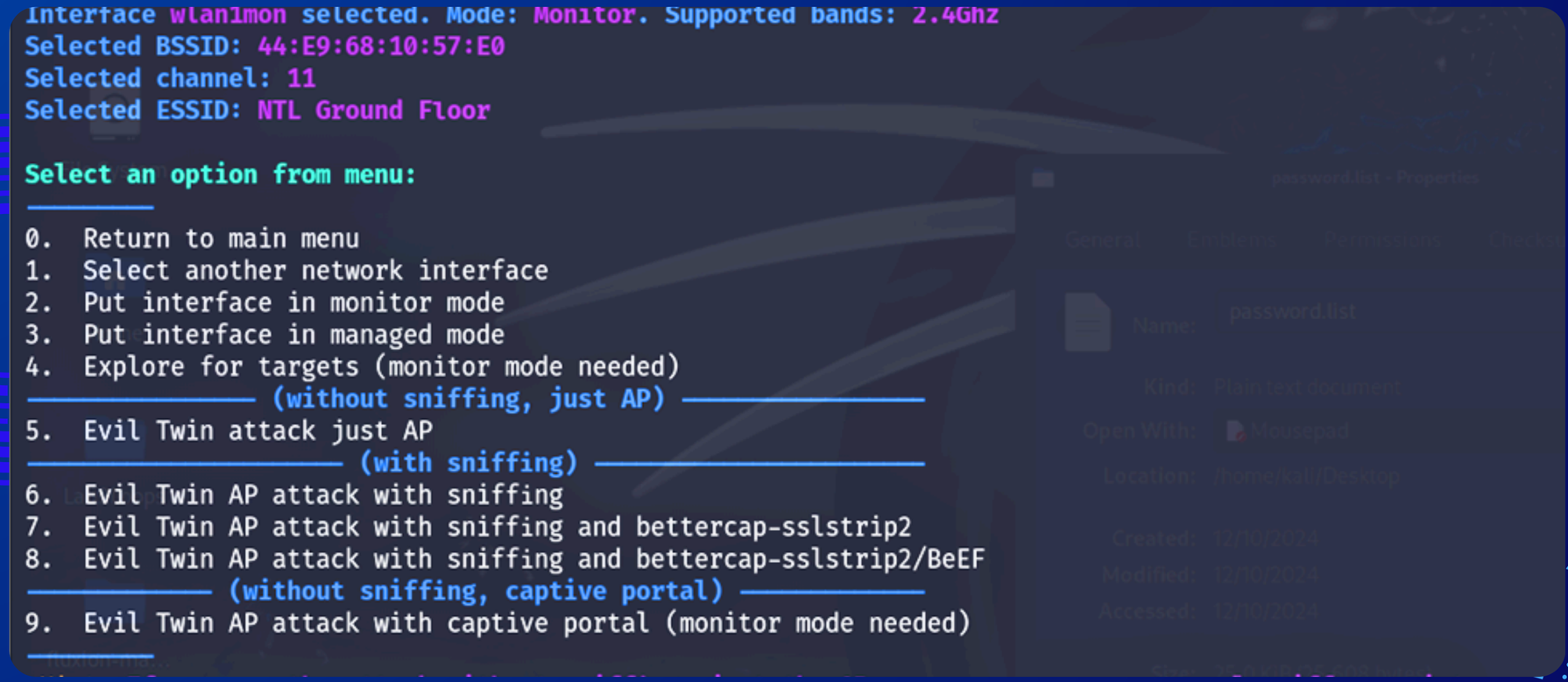
STEP#I

Come back to main menu



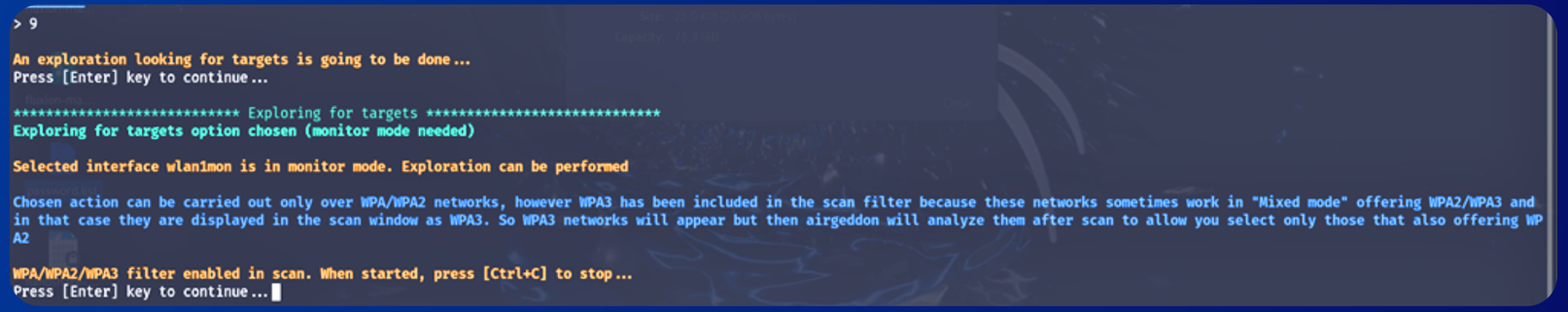
STEP#2

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

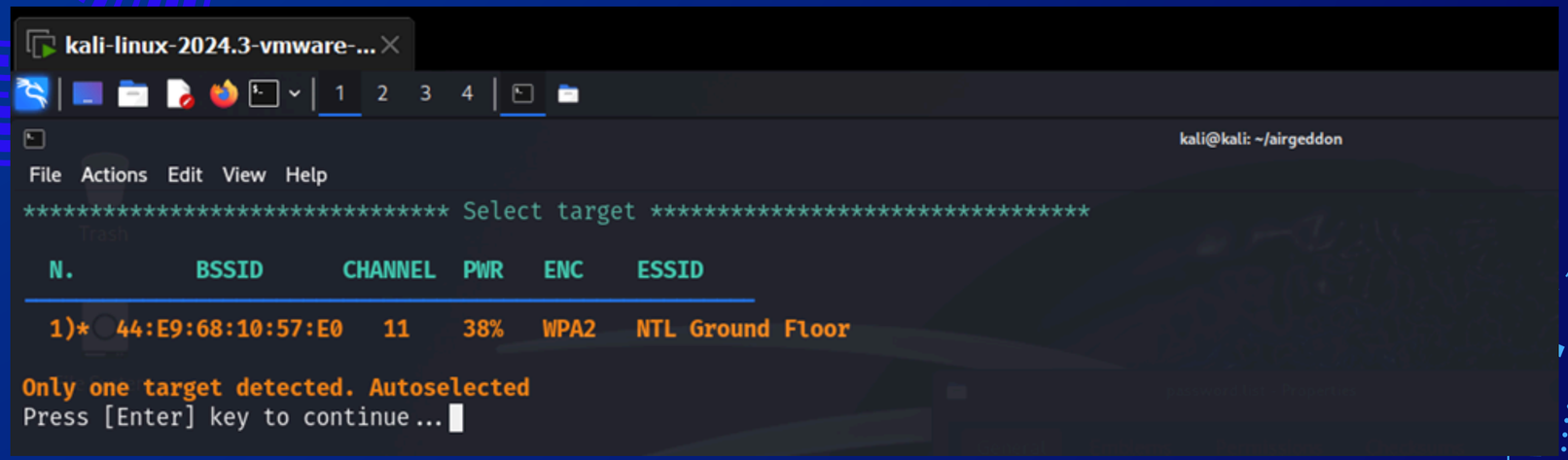


STEP#3

Press Enter to explore the targets

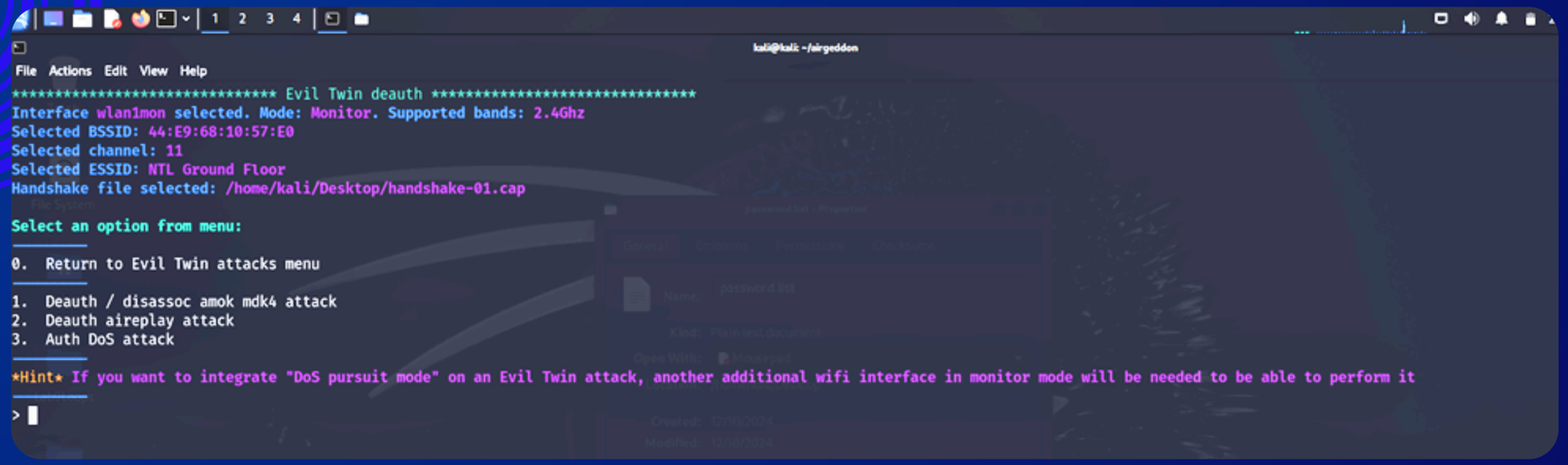


Select 1 because we have the premissions



STEP#4

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



STEP#4

If you have an extra adapter then press y.

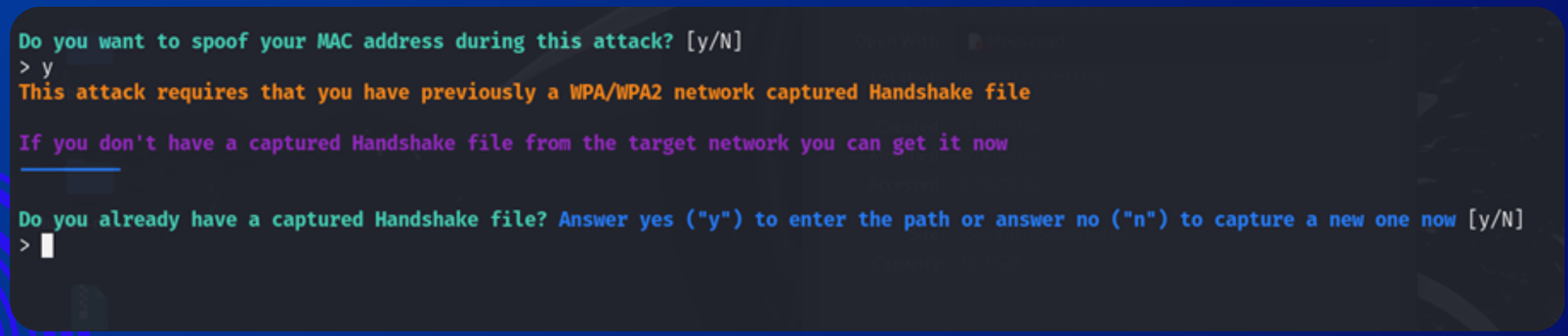
```
> 2

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

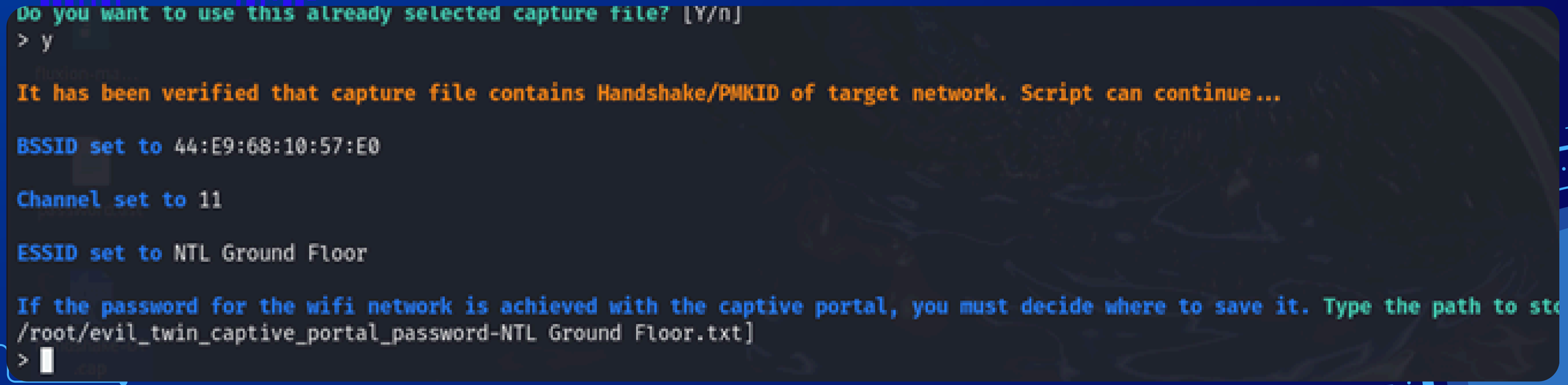
Press enter to enable monitor mode

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

This interface wlan0 is not in monitor mode

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...
```

STEP#5

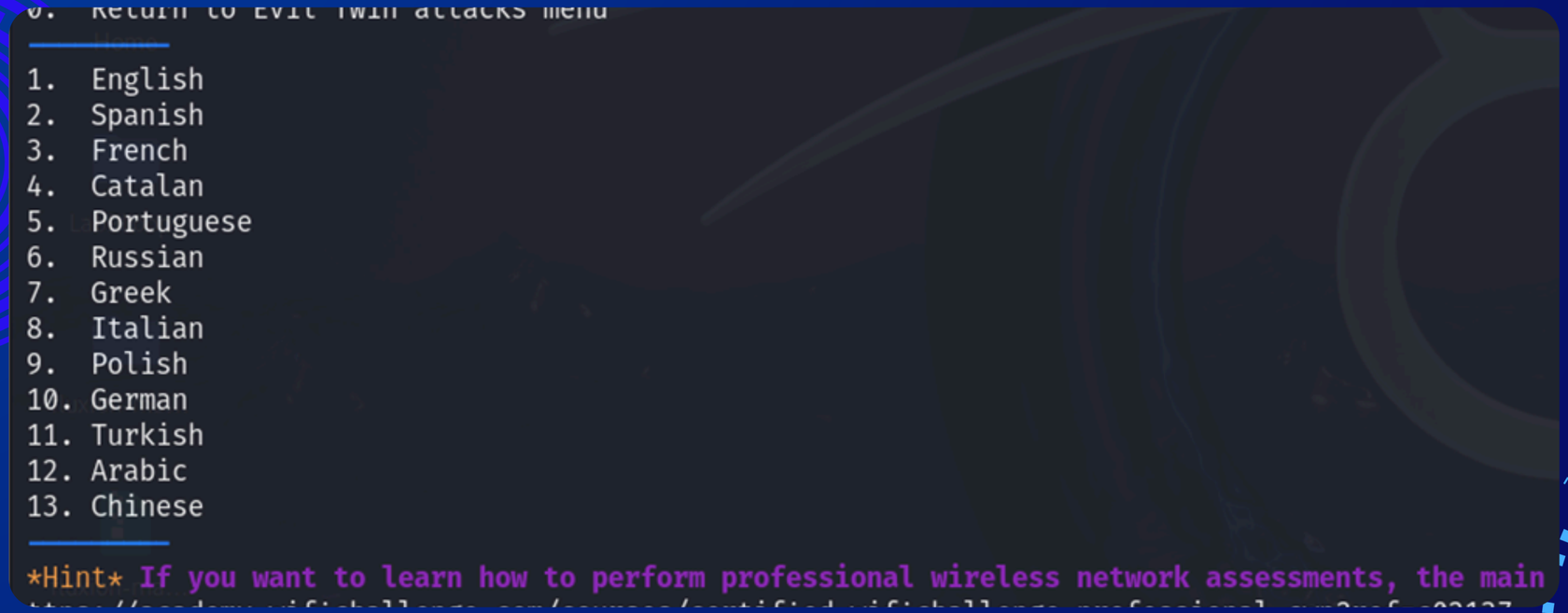
Now the tool will ask about handshake file and we have already captured the hand shake file so, we will paste the the path of handshake file





STEP#6

Then select the language



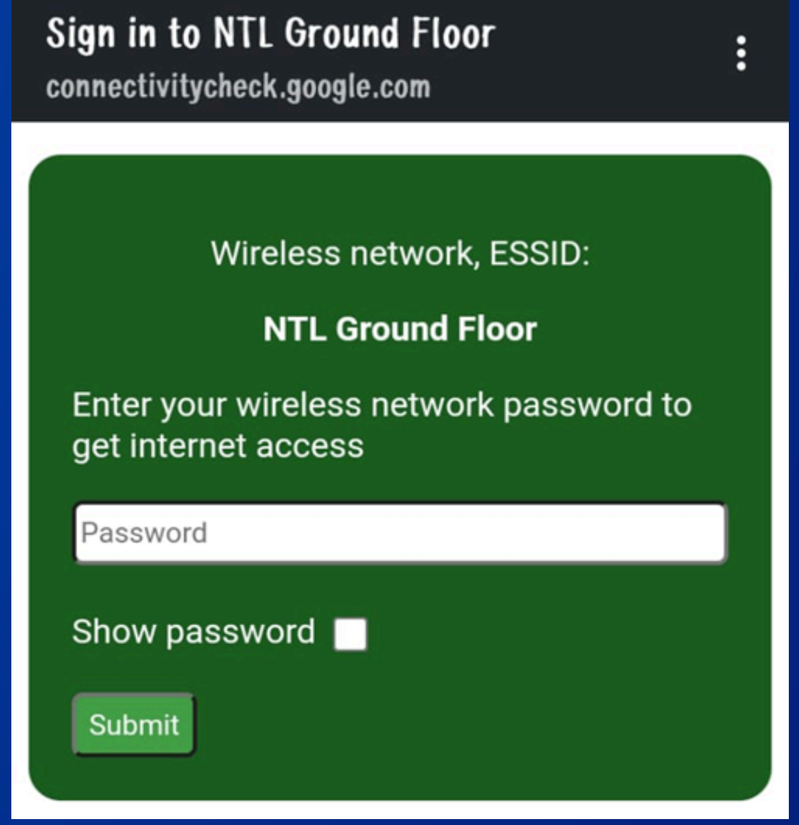
STEP#7

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

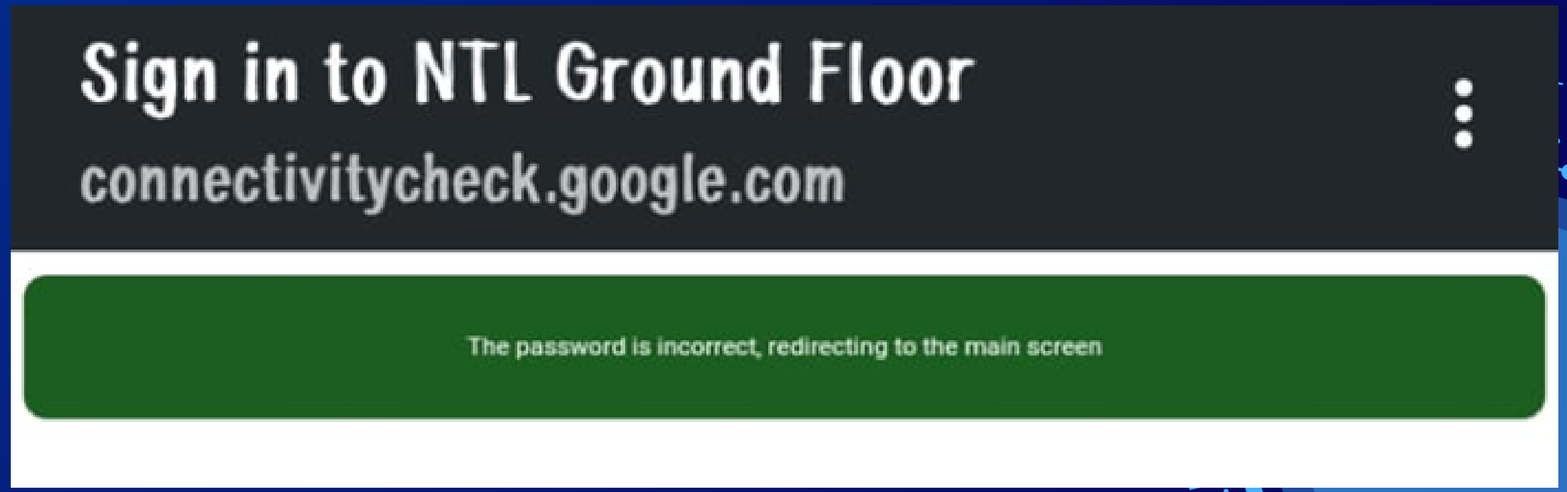
```
No vendor was detected for the target AP's BSSID. Default captive portal template will be used

Remember that the captive portal can also be customized for a more tailored attack. Check information about how to do
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 ar
 the script will automatically close them all
Press [Enter] key to continue...
```



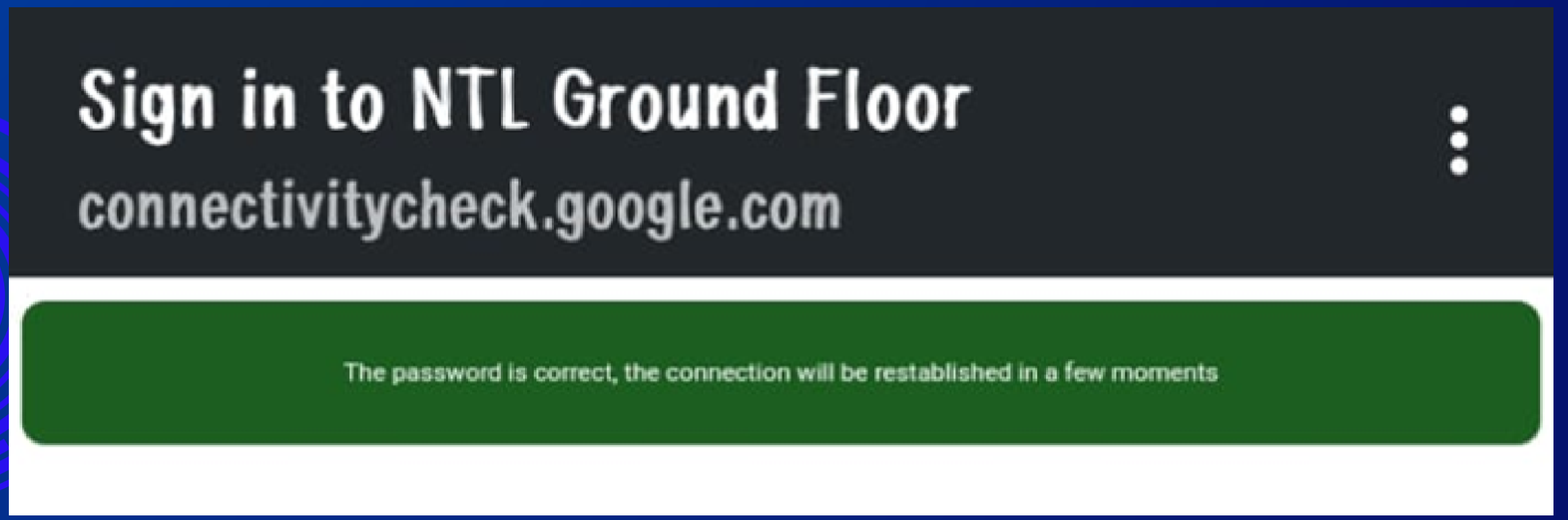
STEP#9

The user will go to this page and enter pasword

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

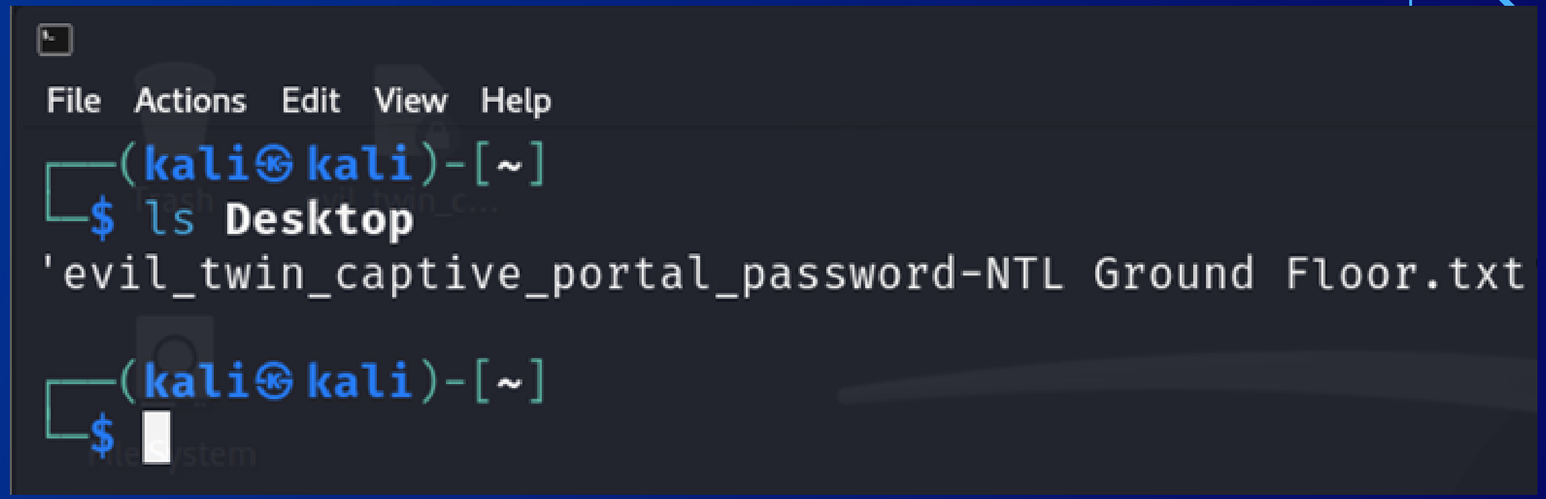


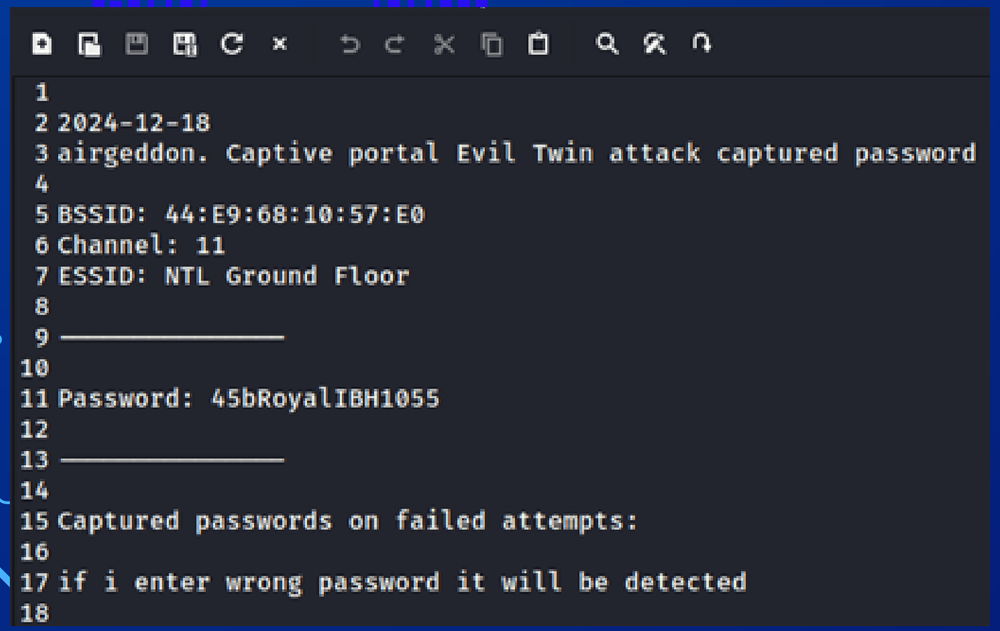
And if the user enters correct password he will have the following pop up on the android device that the password is correct.



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.





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.

Ethical Considerations

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

Manual Intervention

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

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: External Antenna

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

Solution: Optimized Settings

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

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