National College of Ireland

Configuration Manual

MSc Research Project
MSc in Cybersecurity

Abhinav Wakhloo
Student ID: x21156956

School of Computing
National College of Ireland

Supervisor: Arghir Nicolae Moldovan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: ……. Abhinav Wakhloo……

Student ID: ……x21156956……..……

Programme: ……MSc in Cybersecurity…… **Year:** …2022-2023..

Module: ……MSc Research Project……..……

Lecturer: ……Arghir Nicolae Moldova……..……..……

Submission Due Date: ……..1/2/2023……..……

Project Title:…… Client-side Evil-Twin access point detection using beacon-frame delay and wireless network parameter deviation
……..……

Word Count: ……1784…… **Page Count:** ……36……..……..……

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: …Abhinav Wakhloo……

Date: …1/2/2023……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Abhinav Wakhloo
Student ID: x21156956

1 Introduction

This configuration manual articulates the methodology and the implementation of the proposed setup illustrated in the thesis by providing comprehensive information on installing the required software tools and dependencies and configuring the dependent hardware. The proposed model includes various wireless adapters and security and social engineering tools. This manual serves as a guide to help prepare the various adapters and provides the required commands and steps to initialize, install, and use the various tools.

2 System Configuration

The setup requires a Debian-based Linux distribution running as a virtual machine on top of the base host machine. The virtualization software used is Parallels Desktop 17.

Host Machine	M1 MacBook Pro
Processor	8-core CPU with 4 performance cores and 4 efficiency cores
System Architecture	ARM-64
Operating System	Ventura 13.0.1
RAM	8 GB

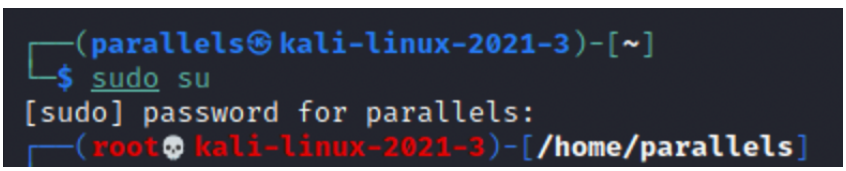
Virtual Machine	Kali Linux
Processor	2-core CPU
System Architecture	ARM-64
Operating System	Kali 2022.4
RAM	2 GB

3 Installation and Setup

3.1 Checking the Adapter compatibility:

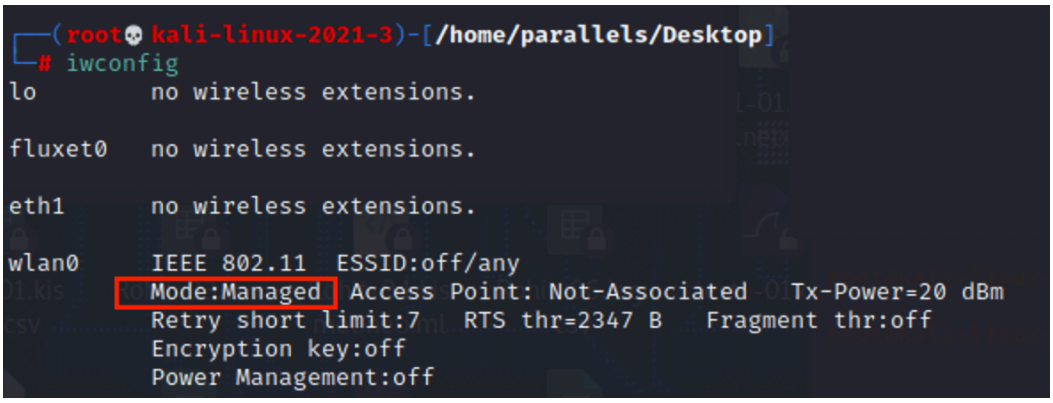
- First, issue the command sudo su to get root privileges.

```
sudo su
```



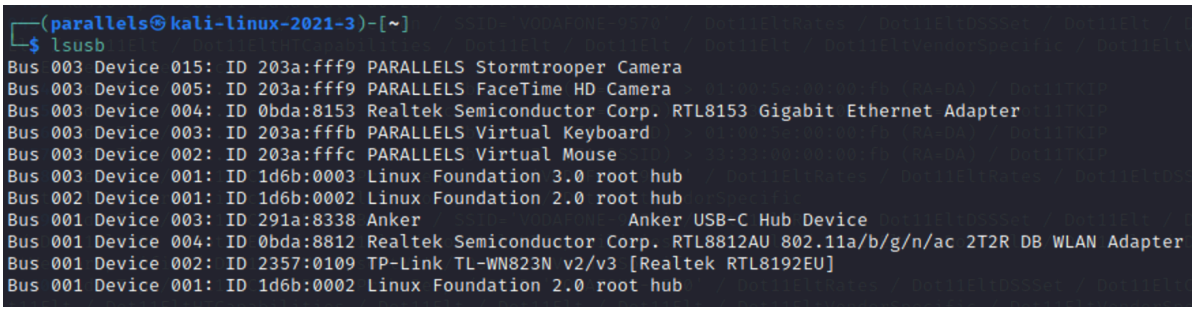
- To check the compatibility of the wireless adapters, we must first check whether they are detected in Kali Linux. To check the same, we must first issue the command.

  ```
  iwconfig
  ```



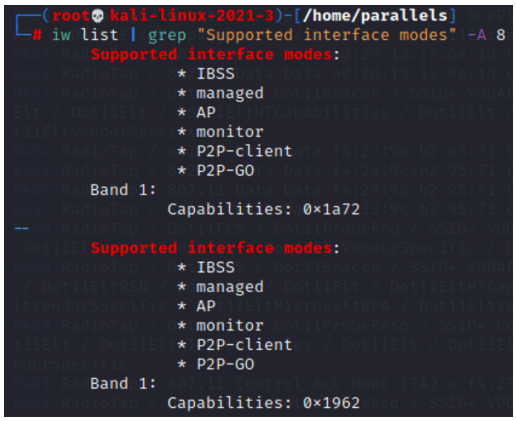
- If the adapter is not detected in iwconfig, we can check whether it is connected and detected by Kali Linux by issuing the command.

  ```
  lsusb
  ```



- We can then check the various modes supported by the adapter by running the following command,

  ```
  iw list | grep "Supported interface modes" -A 8
  ```



- To create an Evil-Twin access point, the Monitor and AP mode must be supported by the adapters.

- If all modes are not supported, or the adapter is not detected, then the adapter is either incompatible or is not running the appropriate driver.

3.2 Preparing the Adapters:

TP-Link TL-WN8223N:

- The adapter is detected by default in Kali Linux, and the default driver supports Monitor and Managed modes.
- With the default driver, the adapter cannot create an Access Point. To fix this, the driver must be updated to rtl8192eu-linux-driver.
- To update the adapter's driver, issue the following commands,

1. Install the required tools.

```
sudo apt-get install git linux-headers-generic build-essential dkms
```

2. Clone the repository rtl8192eu-linux-driver from Github.

git clone https://github.com/Mange/rtl8192eu-linux-driver

3. Change the current directory to the cloned directory

```
cd rtl8192eu-linux-driver
```

4. Update the Makefile by changing the following values (Note: the system used is an M1 MacBook Pro which is ARM-based).

```
...
CONFIG_PLATFORM_I386_PC = n
...
CONFIG_PLATFORM_ARM_AARCH64 = y
```

5. To add the cloned driver to DKMS, issue the following command.

```
sudo dkms add .
```

6. The next step is to build and install the driver with the following command.

```
sudo dkms install rtl8192eu/1.0
```

7. We must blacklist the default driver to run the new one.

```
echo "blacklist rtl8xxxu" | sudo tee /etc/modprobe.d/rtl8xxxu.conf
```

8. We also must force the adapter to boot with the new driver.

```
echo -e "8192eu\n\nloop" | sudo tee /etc/modules
```

9. To avoid any plugin issues with any of the distributions, run the following command

```
echo "options 8192eu rtw_power_mgnt=0 rtw_enusbss=0" | sudo tee /etc/modprobe.d/8192eu.conf
```

10. Update the changes implemented

```
sudo update-grub; sudo update-initramfs -u
```

11. Reboot to load the implemented changes.

```
systemctl reboot -i
```

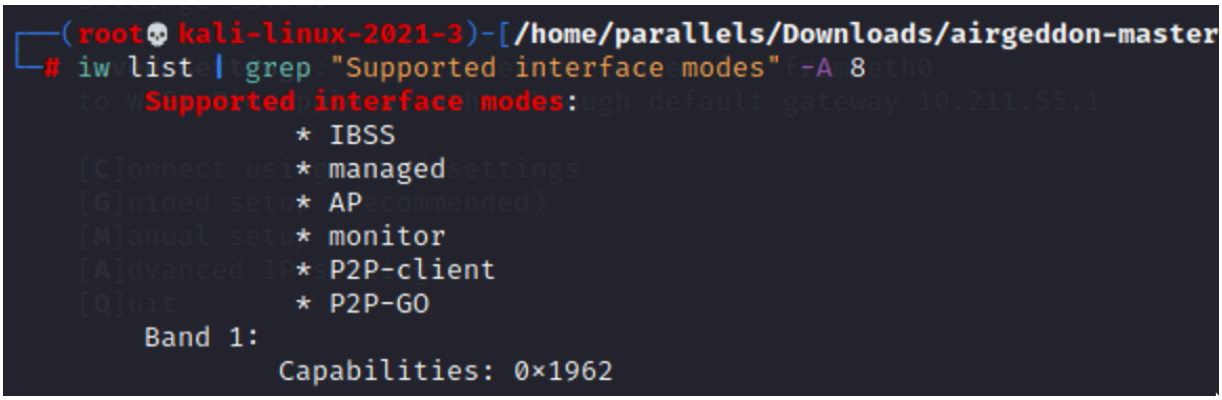
12. To check whether the kernel has loaded the correct module.

```
sudo lshw -c network
```

13. To revert and uninstall the new driver, use the following command.

```
sudo dkms uninstall rtl8192eu/1.0
```

- After the driver is installed, the device will also be able to create an AP, whereas, with the default driver, the adapter can only retrieve the WPA handshake.



Alfa -AWUS036ACH adapter:

- The Alfa adapter does not get detected by Kali Linux by default. (Note: this is the case if the adapter is a dual band).

```
┌──(kali㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.


┌──(kali㉿kali)-[~]
└─$ lsusb
Bus 002 Device 002: ID 0bda:8812 Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac 2T2R DB WLAN Adapter
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 004: ID 0e0f:0008 VMware, Inc. Virtual Bluetooth Adapter
Bus 001 Device 003: ID 0e0f:0002 VMware, Inc. Virtual USB Hub
Bus 001 Device 002: ID 0e0f:0003 VMware, Inc. Virtual Mouse
Bus 001 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
```

- However, it is being detected by Kali Linux under the lsusb command.
- To fix this, the adapter's driver must be updated to rtl8812au.
- Follow the following commands to update the driver.

```
sudo apt update
sudo apt upgrade -y
sudo apt dist-upgrade -y
sudo reboot now
sudo apt update
sudo apt install realtek-rtl88xxau-dkms
sudo apt install dkms
git clone https://github.com/aircrack-ng/rtl8812au
cd rtl8812au/
make
sudo make install
lsusb
iwconfig
```

```
wlan1     unassociated  ESSID:""  Nickname:"<WIFI@REALTEK>"
          Mode:Managed  Frequency=2.412 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

- After Flashing the adapter, all modes are available and can be used with tools.

```
Supported interface modes:
          * IBSS
          * managed
          * AP
          * monitor
          * P2P-client
          * P2P-GO
```

Note: If it does not show in iwconfig, disconnect the adapter, reconnect it, and then it will show.

Hak5 Pineapple Tetra:

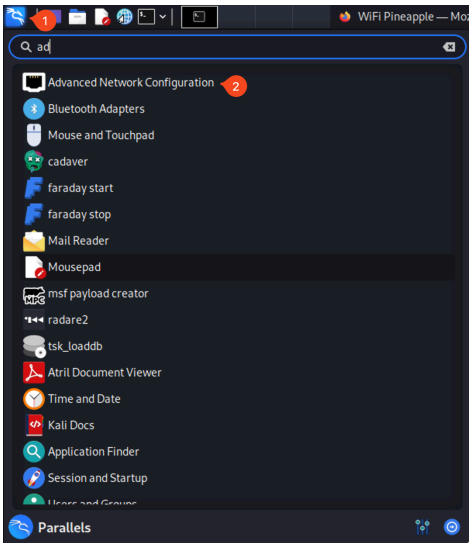
Steps for initial setup of Wi-Fi Pineapple Tetra:

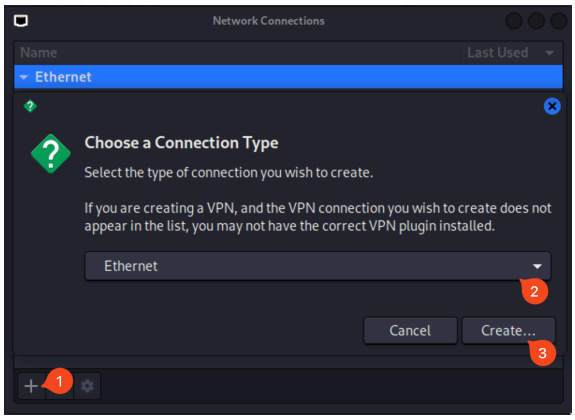
- Connect the Y-USB cable from the laptop to the ETH port of the Pineapple Tetra.
- At the initial boot of the adapter, the orange status led can be seen, followed by the blue led. The blue led will remain constantly on, indicating the device is booted.
- From the terminal issue, the following command is to see the adapter's status.

  `$ifconfig`

```
eth4: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet6 fe80::49f8:a1b7:41ce:b633  prefixlen 64  scopeid 0x20<link>
      ether 00:13:37:a6:c0:0a  txqueuelen 1000  (Ethernet)
      RX packets 0  bytes 0 (0.0 B)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 33  bytes 4579 (4.4 KiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- If the adapter does not show an IP address, manually add the ethernet adapter from the Kali Advance Network Setting option. Click on the '+' button from the bottom left corner, select ethernet, and then click on create.





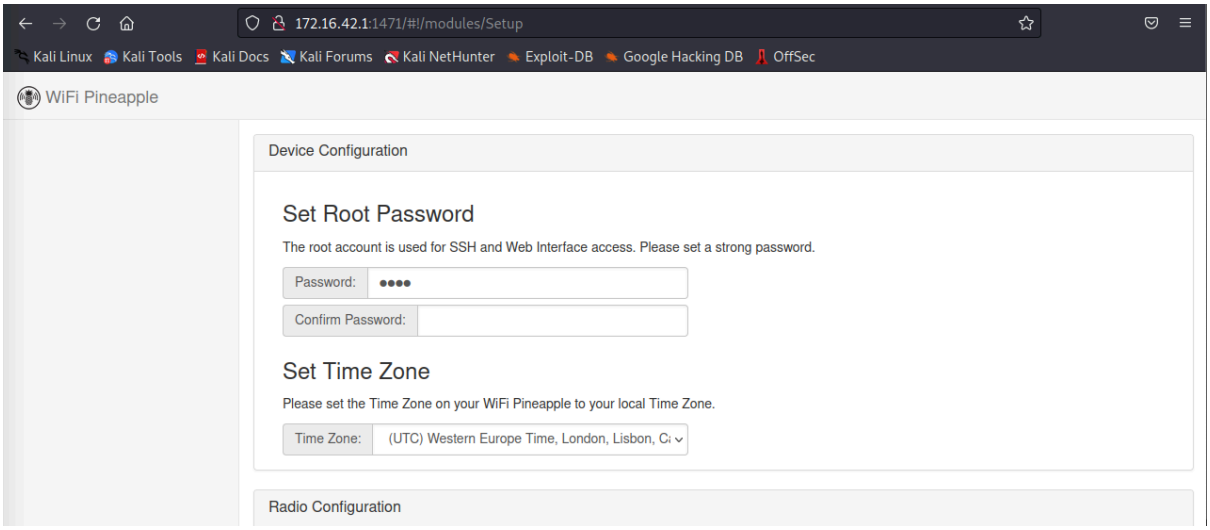
- Test again with the ifconfig command to see the IP address. The default IP address range of the Pineapple Tetra is 172.16.42.x/24.

```
┌──(parallels㉿kali-linux-2021-3)-[~]
└─$ ifconfig eth4
eth4: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 172.16.42.194  netmask 255.255.255.0  broadcast 172.16.42.255
      inet6 fe80::49f8:a1b7:41ce:b633  prefixlen 64  scopeid 0x20<link>
      ether 00:13:37:a6:c0:0a  txqueuelen 1000  (Ethernet)
      RX packets 3983  bytes 2168787 (2.0 MiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 3351  bytes 1032178 (1007.9 KiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- Once the IP address is seen for the ethernet adapter, open the web browser.
- In the URL section, open http://172.16.42.1:1471 to access the GUI of the adapter. The default **username** is **root**, and the **password** is **change_on_install** for the initial setup.

- If you cannot log in, you can reset the adapter to its default settings by pressing the reset button and holding it for about 10 seconds.

- After the device reboots, wait until the status led shows a constant blue light.
- Try logging into the GUI of the Pineapple Tetra, and you will be prompted to complete the initial setup.
- Set a new device password and other fields.

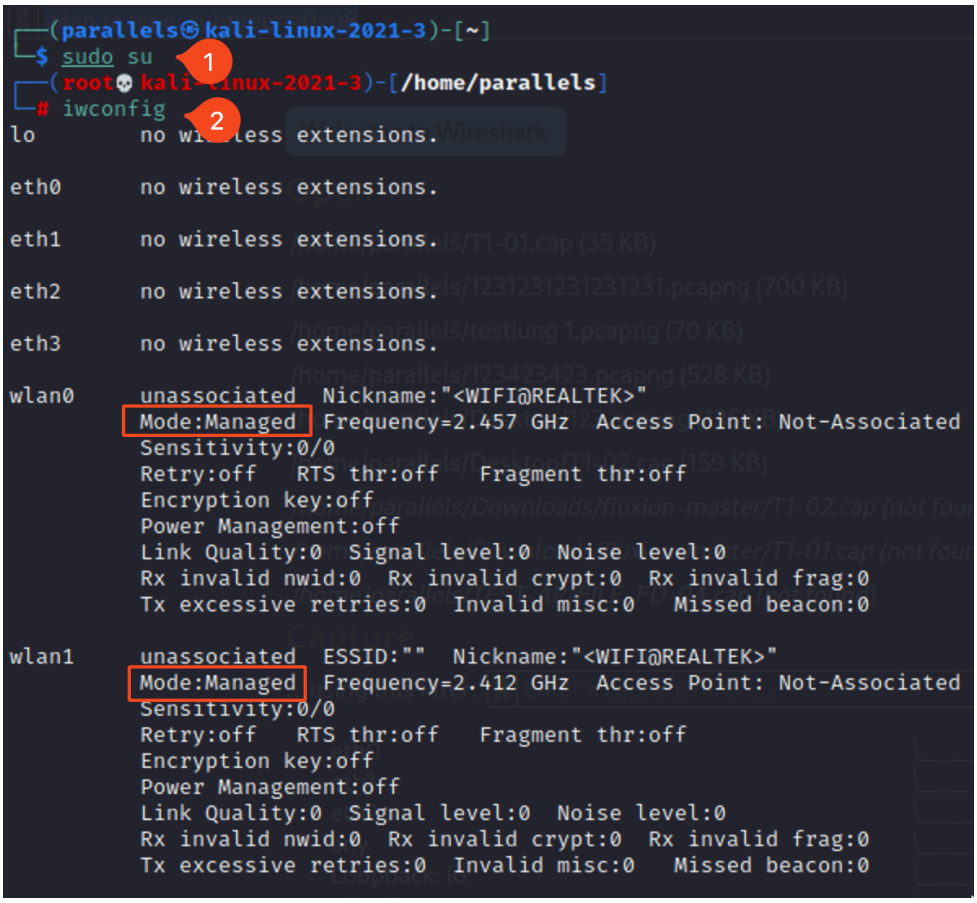


3.3 Preparing the wireless interfaces:

- Open terminal and run the command,
  `sudo su (to get into root environment)`

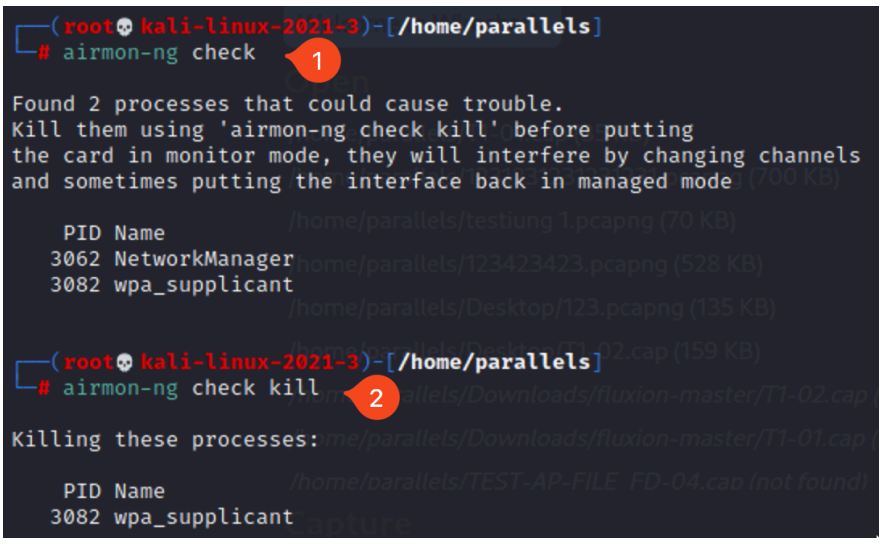
- Then run the following command,
  `iwconfig(to check the mode of wireless interface)`

- The wireless interface is initially in managed mode, as seen in the below screenshot.



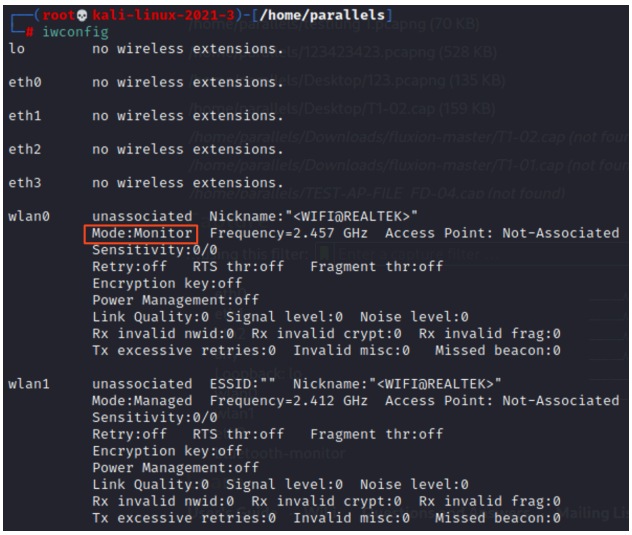
- Then run the following command to check and kill any processes that might interfere with the aircrack-ng suite.
- The following command is used to confirm that the interface mode is changed,

```
airmon-ng check
airmon-ng check kill
```



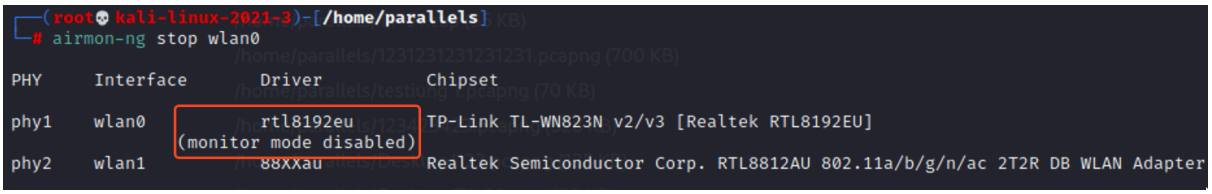
- The command iwconfig can be used to check the wireless mode as well,

  ```
  Iwconfig
  ```



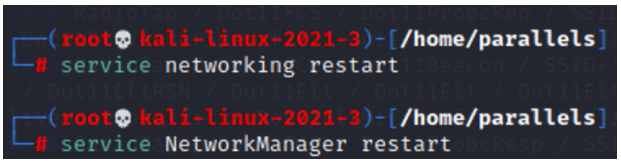
- To revert the mode to managed mode for the interface.

  ```
  airmon-ng stop wlan0
  ```



- To restart the stopped services.

  ```
  service networking restart
  service NetworkManager restart
  ```



3.4 Installing and Running the Tools:

Airgeddon:

- We first need to clone the repository airgeddon from GitHub to install the tool.

  ```
  git clone --depth 1 https://github.com/v1s1t0r1sh3r3/airgeddon.git
  ```

- First, issue the command sudo su to get root privileges.

  ```
  sudo su
  ```

- Change the current directory to the cloned directory.

  ```
  cd /airgeddon-master
  ```

- Run airgeddon.

  ```
  ./airgeddon.sh
  ```

Fluxion:

- We need to clone the repository fluxion from GitHub to install the tool.

  ```
  git clone --depth 1 https://github.com/v1s1t0r1sh3r3/airgeddon.git
  ```

- First, issue the command sudo su to get root privileges.

  ```
  sudo su
  ```

- Change the current directory to the cloned directory.

  ```
  cd /fluxion-master
  ```

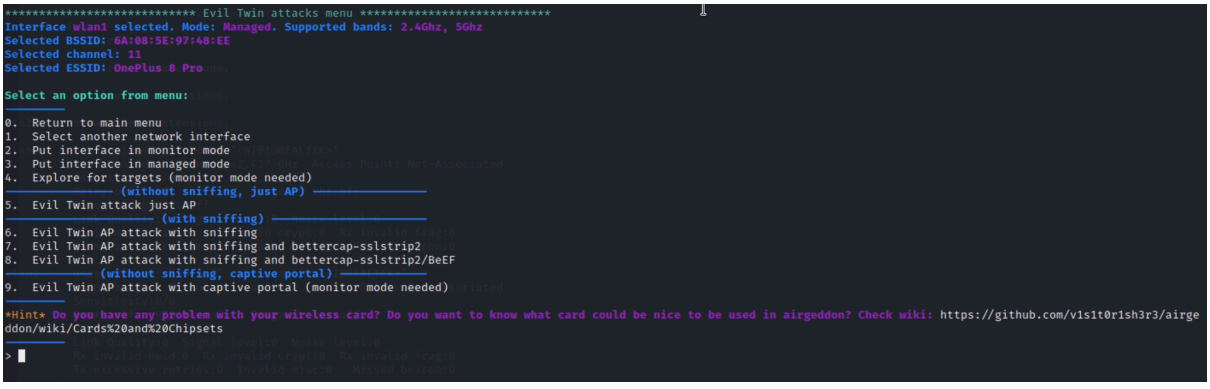
- Run fluxion.

  ```
  ./ fluxion.sh
  ```

Running the wireless auditing tools:

Airgeddon:

Choose the options from the menu as selected in the screenshots to run the tool.



```
File  Actions  Edit  View  Help
************************ airgeddon v11.10 main menu *************************
Interface wlan1 selected. Mode: Managed. Supported bands: 2.4Ghz, 5Ghz

Select an option from menu:

0.  Exit script
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode

4.  DoS attacks menu
5.  Handshake/PMKID tools menu
6.  Offline WPA/WPA2 decrypt menu
7.  Evil Twin attacks menu
8.  WPS attacks menu
9.  WEP attacks menu
10. Enterprise attacks menu

11. About & Credits / Sponsorship mentions
12. Options and language menu

*Hint* Select a wifi card to work in order to be able to do more actions than with an ethernet interface

> 2
Setting your interface in monitor mode...

Monitor mode now is set on wlan1
Press [Enter] key to continue...
```

```
************************ airgeddon v11.10 main menu *************************
Interface wlan1 selected. Mode: Monitor. Supported bands: 2.4Ghz, 5Ghz

Select an option from menu:

0.  Exit script
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode

4.  DoS attacks menu
5.  Handshake/PMKID tools menu
6.  Offline WPA/WPA2 decrypt menu
7.  Evil Twin attacks menu
8.  WPS attacks menu
9.  WEP attacks menu
10. Enterprise attacks menu

11. About & Credits / 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, did you know that yo
e airgeddon window? In this way you don't have to type the path manually

>
```

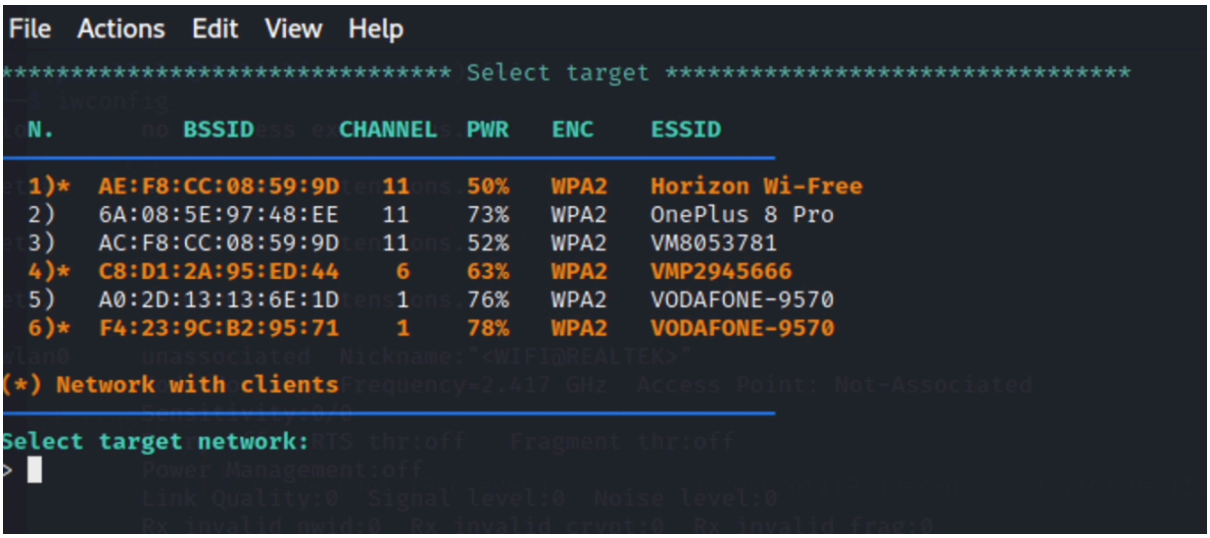
```
************************** Evil Twin attacks menu ***************************
Interface wlan1 selected. Mode: Monitor. Supported bands: 2.4Ghz, 5Ghz
Selected BSSID: 6A:08:5E:97:48:EE
Selected channel: 11
Selected ESSID: OnePlus 8 Pro

Select an option from menu:

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

*Hint* On Evil Twin attack with BeEF integrated, in addition to obtaining keys using sniffing techniques, you can try to control the client's
 vectors. The success of these will depend on many factors such as the kind of client's browser and its version

>
```

```
************************** Evil Twin attacks menu **************************
Interface wlan1 selected. Mode: Monitor. Supported bands: 2.4Ghz, 5Ghz
Selected BSSID: 6A:08:5E:97:48:EE
Selected channel: 11
Selected ESSID: OnePlus 8 Pro

Select an option from menu:

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

*Hint* On Evil Twin attack with BeEF integrated, in addition to obtaining keys using sniffing techniques, you can try to control the client's browser launching numerous attack
 vectors. The success of these will depend on many factors such as the kind of client's browser and its version

> 9

The interface wlan1 you have already selected is not supporting VIF (Virtual Interface). This attack needs it to virtually unfold itself to create the fake access point while
also performing denial of service (DoS). Do you want to continue? If yes, the denial of service will not work being an important part of the attack and making it probably inef
fective [y/N]
> y

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 wlan1 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 ...
```

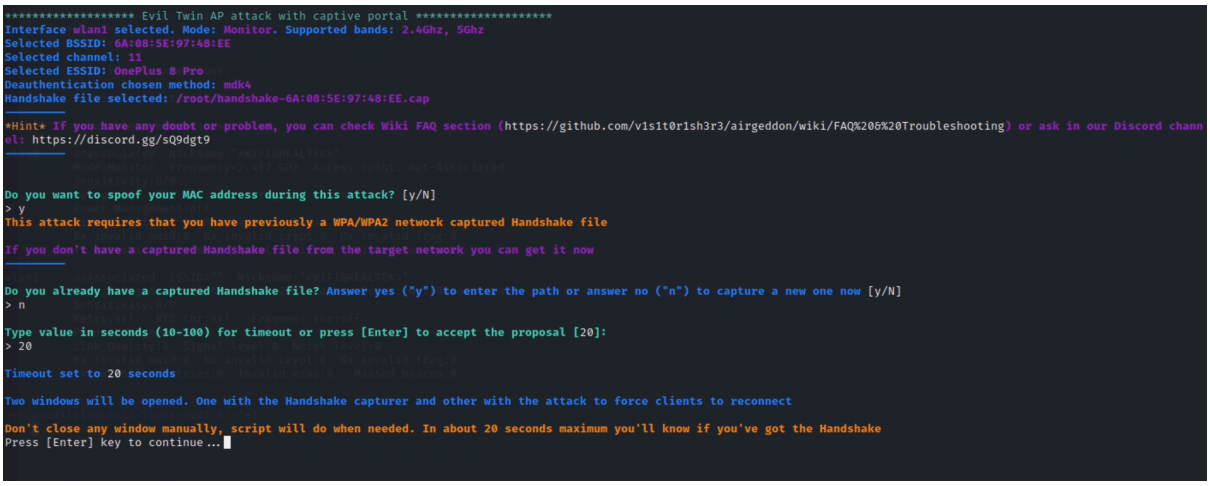
```
root@kali-linux-2021-3: /home/parallels/Downloads
File  Actions  Edit  View  Help
```

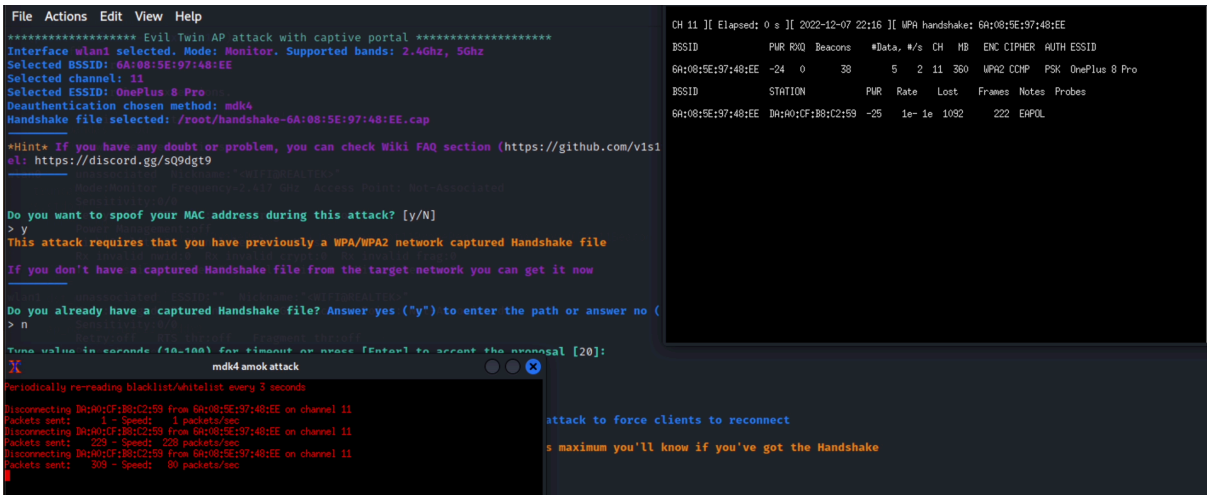

```
************************** Evil Twin attacks menu **************************
Interface wlan1 selected. Mode: Monitor. Supported bands: 2.4Ghz, 5Ghz
Selected BSSID: 6A:08:5E:97:48:EE
Selected channel: 11
Selected ESSID: OnePlus 8 Pro

Select an option from menu:

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

*Hint* On Evil Twin attack with BeEF integrated, in addition to obtaining keys using sniffing tech
 vectors. The success of these will depend on many factors such as the kind of client's browser and its version

> 9

The interface wlan1 you have already selected is not supporting VIF (Virtual Interface). This attack needs it to virtually unfold itself to create the fake access point wh
also performing denial of service (DoS). Do you want to continue? If yes, the denial of service will not work being an important part of the attack and making it probably
fective [y/N]
> y

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 wlan1 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" offer
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
 those that also offering WPA2

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

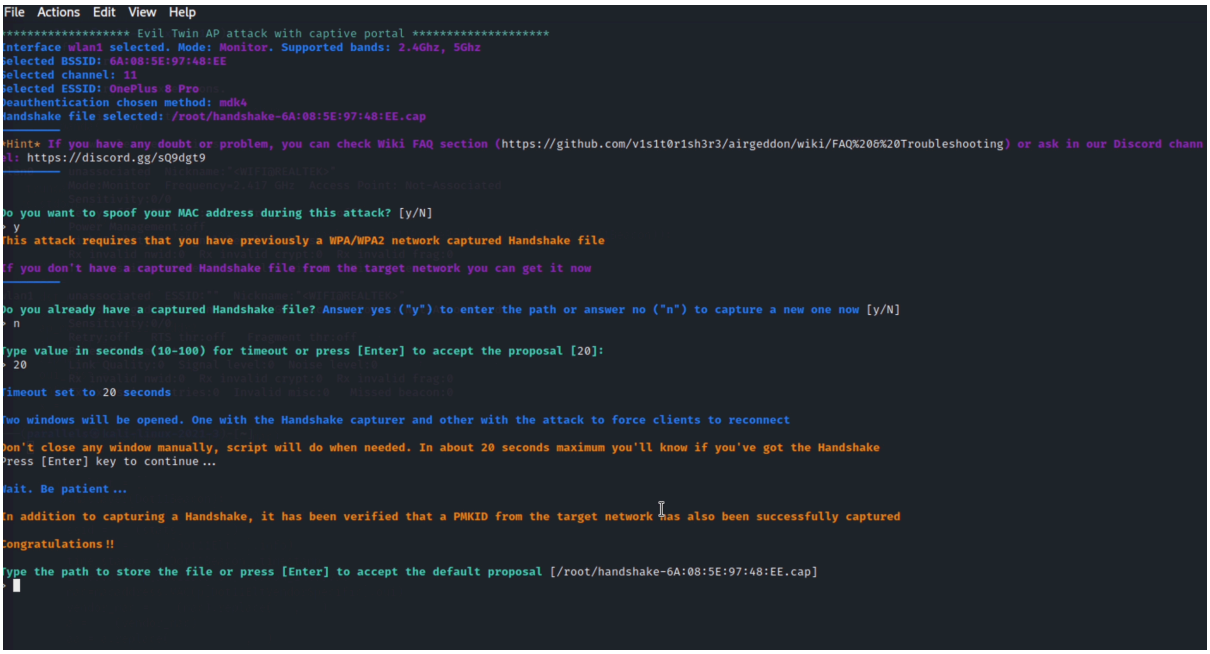

```
Exploring for targets

CH  9 ][ Elapsed: 0 s ][ 2022-12-07 22:16

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

C8:D1:2A:95:ED:44  -38        5        4    1   6  130   WPA2 CCMP   PSK  VMP2945666
A0:2D:13:13:6E:1D  -24        9        3    0   1  130   WPA2 CCMP   PSK  VODAFONE-9570
F4:23:9C:B2:95:71  -22        7        1    0   1  195   WPA2 CCMP   PSK  VODAFONE-9570
6A:08:5E:97:48:EE  -23        8        0    0  11  360   WPA2 CCMP   PSK  OnePlus 8 Pro
AE:F8:CC:08:59:9D  -49        3        0    0  11  195   WPA2 CCMP   MGT  Horizon Wi-Free

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

C8:D1:2A:95:ED:44  A2:37:51:59:78:3E   -1    1e- 0      0        2
F4:23:9C:B2:95:71  E6:4F:C9:3C:73:45  -17   24e- 1e     0        3
```

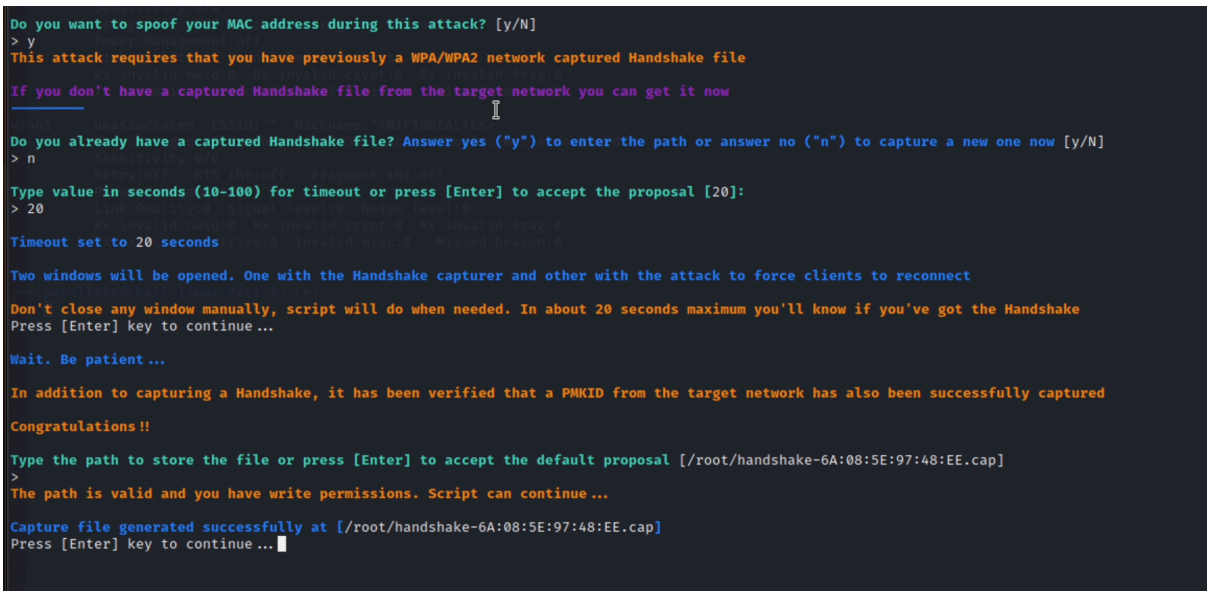

File Actions Edit View Help
Select target
N. BSSID CHANNEL PWR ENC ESSID
1)* AE:F8:CC:08:59:9D 11 50% WPA2 Horizon Wi-Free
2) 6A:08:5E:97:48:EE 11 73% WPA2 OnePlus 8 Pro
3) AC:F8:CC:08:59:9D 11 52% WPA2 VM8053781
4)* C8:D1:2A:95:ED:44 6 63% WPA2 VMP2945666
5) A0:2D:13:13:6E:1D 1 76% WPA2 VODAFONE-9570
6)* F4:23:9C:B2:95:71 1 78% WPA2 VODAFONE-9570
(*) Network with clients
Select target network:
>


Evil Twin deauth
Interface wlan1 selected. Mode: Monitor. Supported bands: 2.4Ghz, 5Ghz
Selected BSSID: 6A:08:5E:97:48:EE
Selected channel: 11
Selected ESSID: OnePlus 8 Pro
Handshake file selected: /root/handshake-6A:08:5E:97:48:EE.cap
Select an option from menu:
0. Return to Evil Twin attacks menu
1. Deauth / disassoc amok mdk4 attack
2. Deauth aireplay attack
3. WIDS / WIPS / WDS Confusion attack
Hint 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
> 1
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 launch again the attack if target AP change its channel countering "channel hopping" [y/N]
>


Evil Twin AP attack with captive portal
Interface wlan1 selected. Mode: Monitor. Supported bands: 2.4Ghz, 5Ghz
Selected BSSID: 6A:08:5E:97:48:EE
Selected channel: 11
Selected ESSID: OnePlus 8 Pro
Deauthentication chosen method: mdk4
Handshake file selected: /root/handshake-6A:08:5E:97:48:EE.cap
Hint If you have any doubt or problem, you can check Wiki FAQ section (https://github.com/v1s1t0r1sh3r3/airgeddon/wiki/FAQ%206%20Troubleshooting) or ask in our Discord channel: https://discord.gg/sQ9dgt9
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...

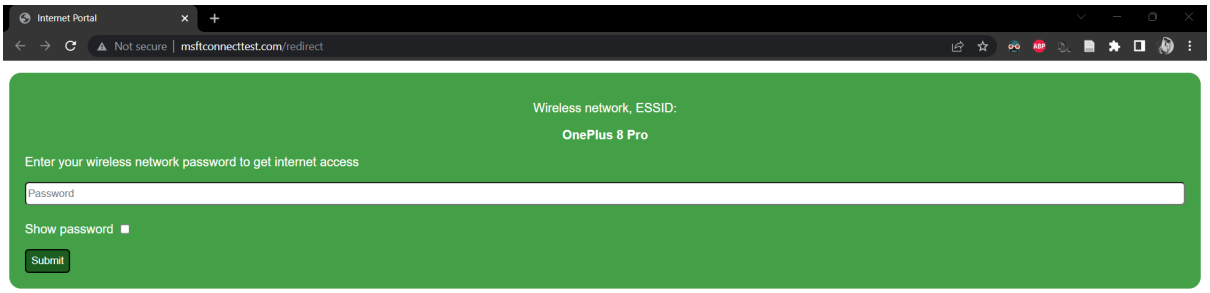

File Actions Edit View Help
****************** Evil Twin AP attack with captive portal ******************
Interface wlan1 selected. Mode: Monitor. Supported bands: 2.4Ghz, 5Ghz
Selected BSSID: 6A:08:5E:97:48:EE
Selected channel: 11
Selected ESSID: OnePlus 8 Pro
Deauthentication chosen method: mdk4
Handshake file selected: /root/handshake-6A:08:5E:97:48:EE.cap
Hint If you have any doubt or problem, you can check Wiki FAQ section (https://github.com/v1s1
el: https://discord.gg/sQ9dgt9
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
Type value in seconds (10-100) for timeout or press [Enter] to accept the proposal [20]:
mdk4 amok attack
Periodically re-reading blacklist/whitelist every 3 seconds
Disconnecting BA:A0:CF:B8:C2:59 from 6A:08:5E:97:48:EE on channel 11
Packets sent: 1 - Speed: 1 packets/sec
Disconnecting BA:A0:CF:B8:C2:59 from 6A:08:5E:97:48:EE on channel 11
Packets sent: 229 - Speed: 228 packets/sec
Disconnecting BA:A0:CF:B8:C2:59 from 6A:08:5E:97:48:EE on channel 11
Packets sent: 309 - Speed: 80 packets/sec
attack to force clients to reconnect
s maximum you'll know if you've got the Handshake
CH 11][Elapsed: 0 s][2022-12-07 22:16][WPA handshake: 6A:08:5E:97:48:EE
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
6A:08:5E:97:48:EE -24 0 38 5 2 11 360 WPA2 CCMP PSK OnePlus 8 Pro
BSSID STATION PWR Rate Lost Frames Notes Probes
6A:08:5E:97:48:EE BA:A0:CF:B8:C2:59 -25 1e- 1e 1092 222 EAPOL

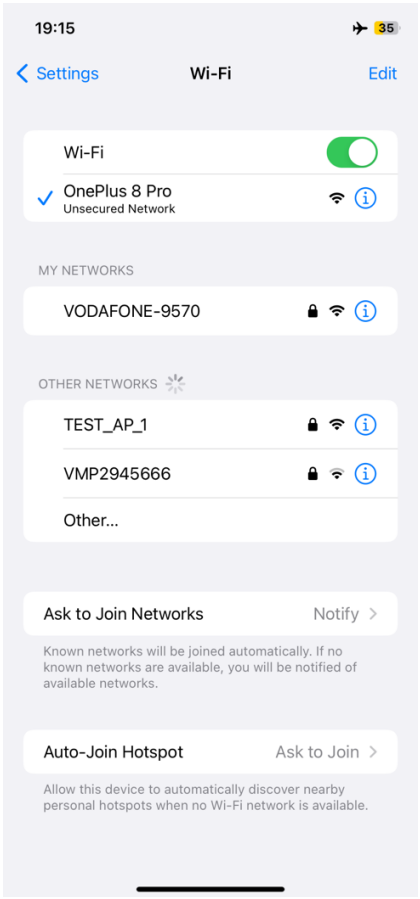

File Actions Edit View Help
****************** Evil Twin AP attack with captive portal ******************
Interface wlan1 selected. Mode: Monitor. Supported bands: 2.4Ghz, 5Ghz
Selected BSSID: 6A:08:5E:97:48:EE
Selected channel: 11
Selected ESSID: OnePlus 8 Pro
Deauthentication chosen method: mdk4
Handshake file selected: /root/handshake-6A:08:5E:97:48:EE.cap
Hint If you have any doubt or problem, you can check Wiki FAQ section (https://github.com/v1s1t0r1sh3r3/airgeddon/wiki/FAQ%206%20Troubleshooting) or ask in our Discord chann
el: https://discord.gg/sQ9dgt9
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...
Wait. Be patient...
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-6A:08:5E:97:48:EE.cap]

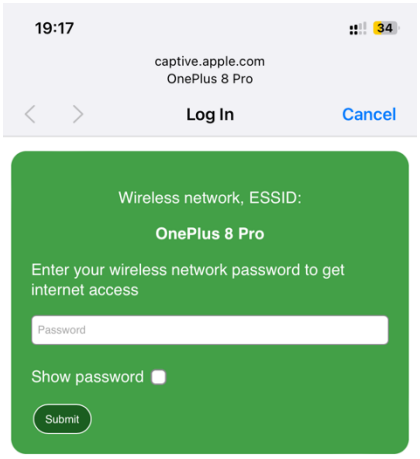

Do you want to spoof your MAC address during this attack? [y/N]
> y
This attack requires that you have previously a WPA/WPA2 network captured Handshake file
If you don't have a captured Handshake file from the target network you can get it now
Do you already have a captured Handshake file? Answer yes ("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...
Wait. Be patient...
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-6A:08:5E:97:48:EE.cap]
>
The path is valid and you have write permissions. Script can continue...
Capture file generated successfully at [/root/handshake-6A:08:5E:97:48:EE.cap]
Press [Enter] key to continue...

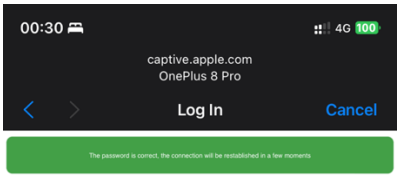
```
Type the path to store the file or press [Enter] to accept the default proposal [/root/handshake-6A:08:5E:97:48:EE.cap]
>
The path is valid and you have write permissions. Script can continue...

Capture file generated successfully at [/root/handshake-6A:08:5E:97:48:EE.cap]
Press [Enter] key to continue...

BSSID set to 6A:08:5E:97:48:EE

Channel set to 11

ESSID set to OnePlus 8 Pro

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 defa
ult proposal [/root/evil_twin_captive_portal_password-OnePlus 8 Pro.txt]
```

```
File  Actions  Edit  View  Help
****************** Evil Twin AP attack with captive portal ******************
Interface wlan1 selected. Mode: Monitor. Supported bands: 2.4Ghz, 5Ghz
Selected BSSID: 6A:08:5E:97:48:EE
Selected channel: 11
Selected ESSID: OnePlus 8 Pro
Deauthentication chosen method: mdk4
Handshake file selected: /root/handshake-6A:08:5E:97:48:EE.cap

Choose the language in which network clients will see the captive portal:

0.  Return to Evil Twin attacks menu
1.  English
2.  Spanish
3.  French
4.  Catalan
5.  Portuguese
6.  Russian
7.  Greek
8.  Italian
9.  Polish
10. German
11. Turkish
12. Arabic

*Hint* To perform an Evil Twin attack you'll need to be very close to the target AP or have a very powerful wifi antenna. Your signal must reach clients equally strong or more
 than the legitimate AP

>
```



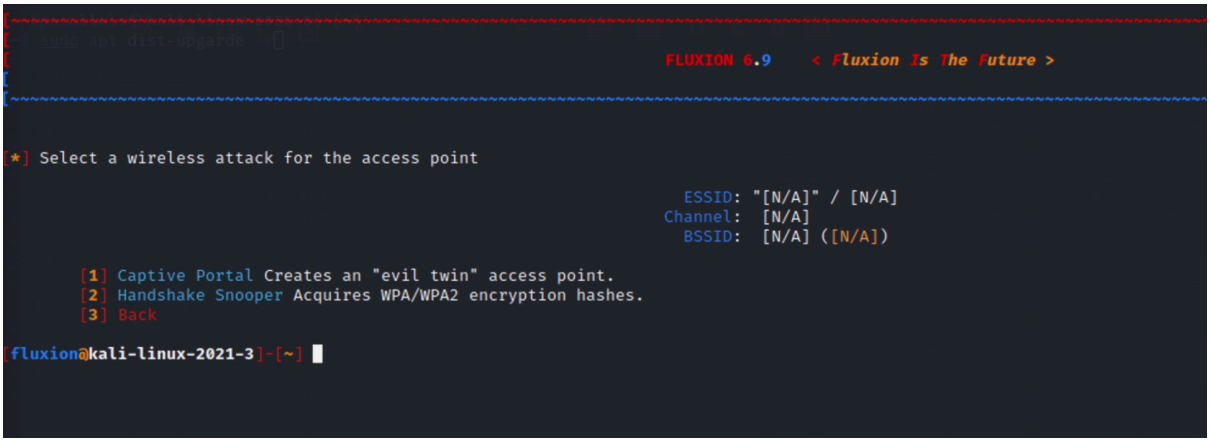

19:15
35
Settings
Wi-Fi
Edit
Wi-Fi
OnePlus 8 Pro
Unsecured Network
MY NETWORKS
VODAFONE-9570
OTHER NETWORKS
TEST_AP_1
VMP2945666
Other...
Ask to Join Networks
Notify
Known networks will be joined automatically. If no known networks are available, you will be notified of available networks.
Auto-Join Hotspot
Ask to Join
Allow this device to automatically discover nearby personal hotspots when no Wi-Fi network is available.

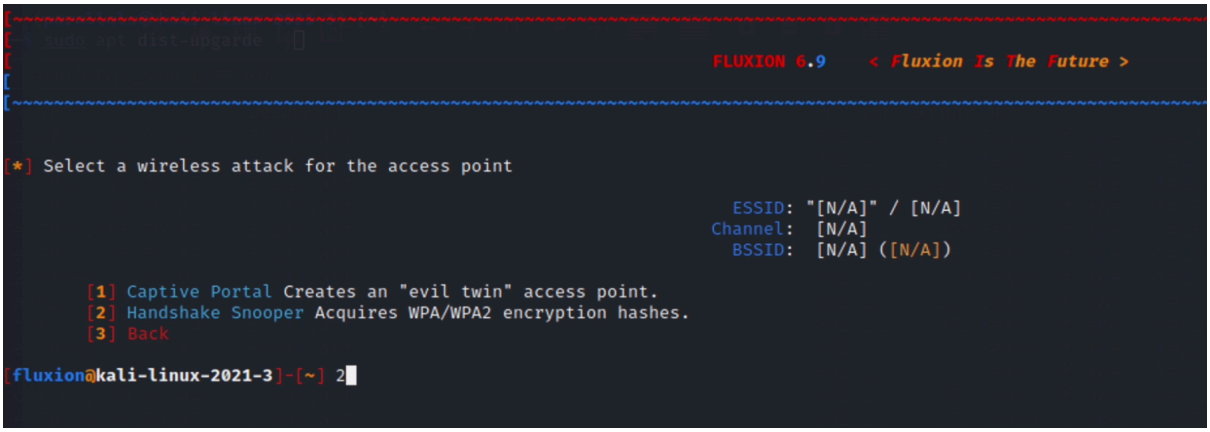

19:17
34
captive.apple.com
OnePlus 8 Pro
Log In
Cancel
Wireless network, ESSID:
OnePlus 8 Pro
Enter your wireless network password to get internet access
Password
Show password
Submit

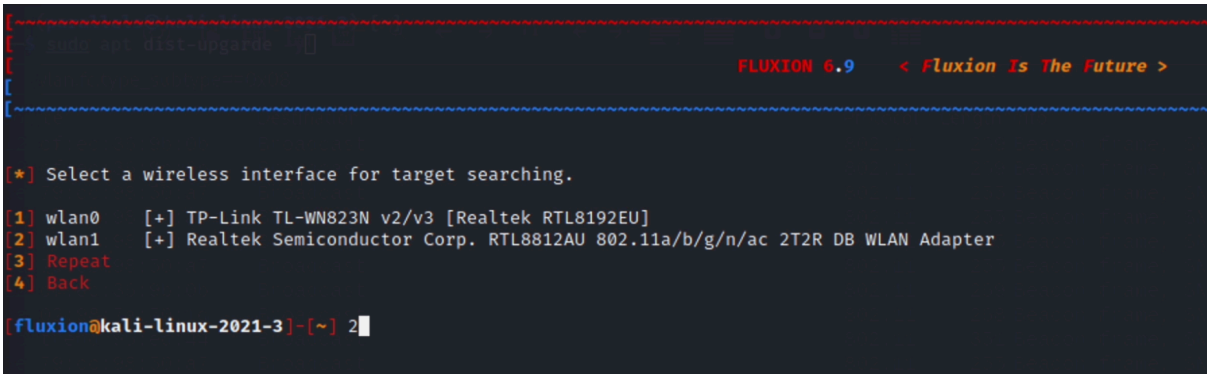

00:30
4G
100
captive.apple.com
OnePlus 8 Pro
Log In
Cancel
The password is correct, the connection will be restablished in a few moments

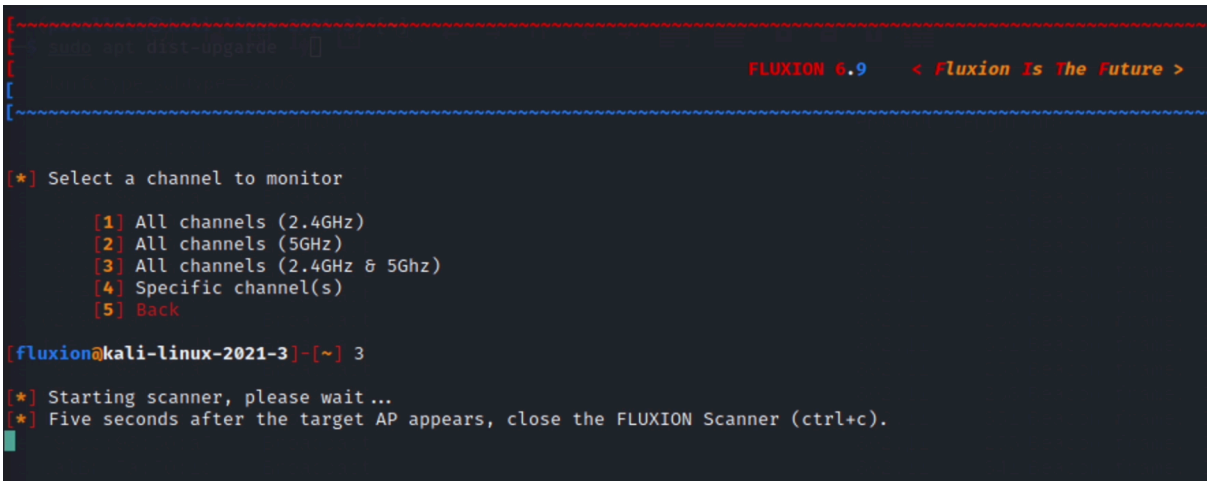
Fluxion:

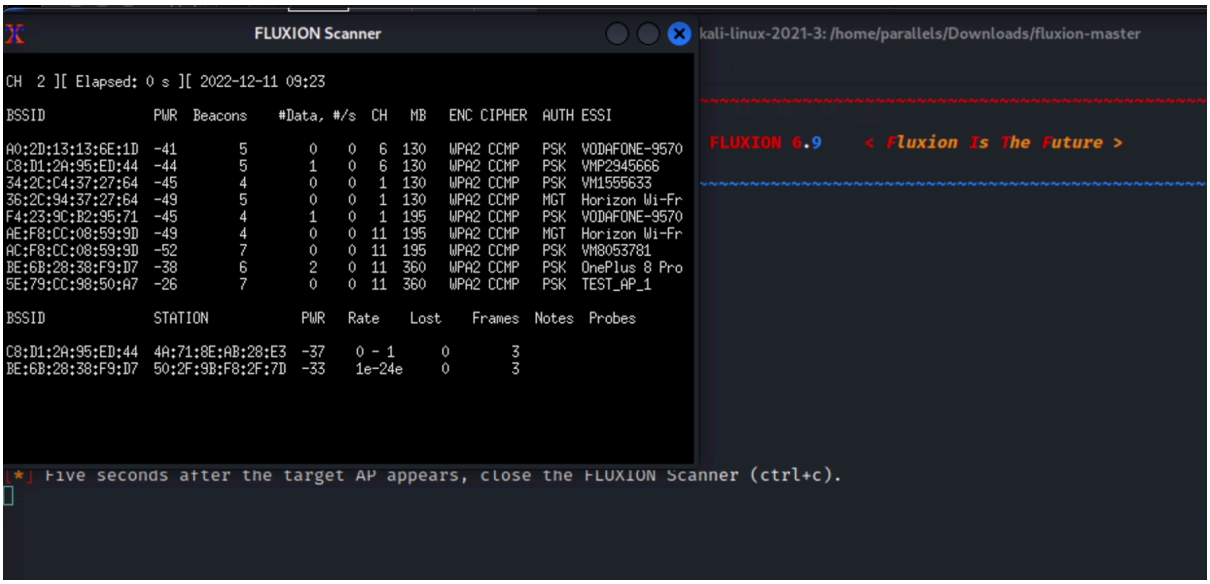
Choose the options from the menu as selected in the screenshots to run the tool.

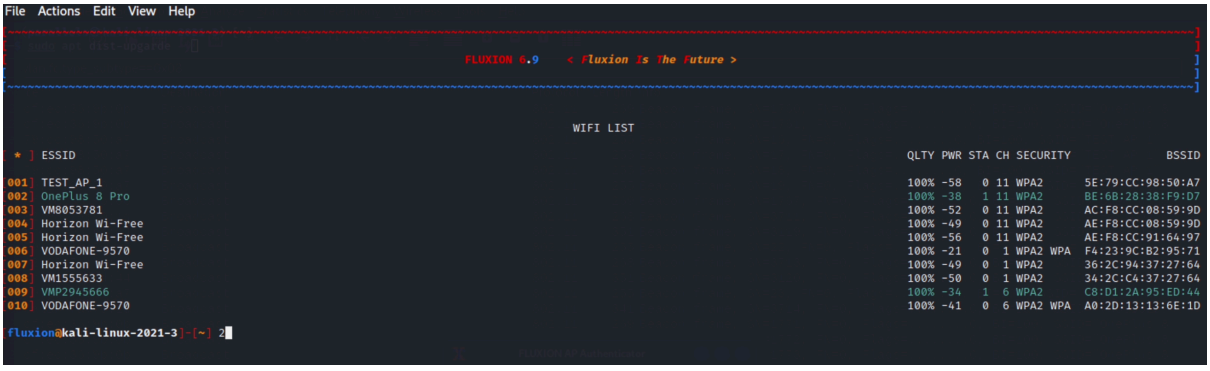


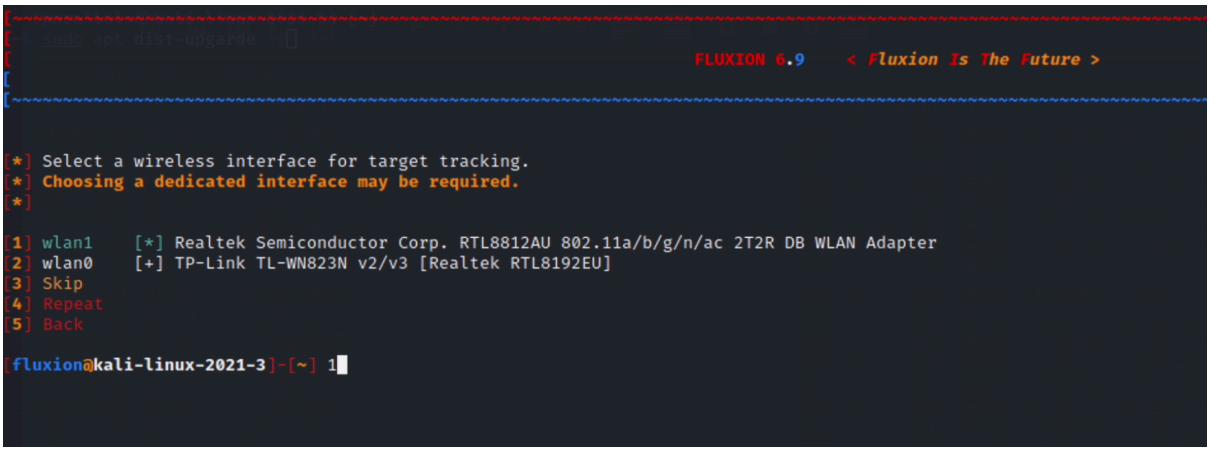


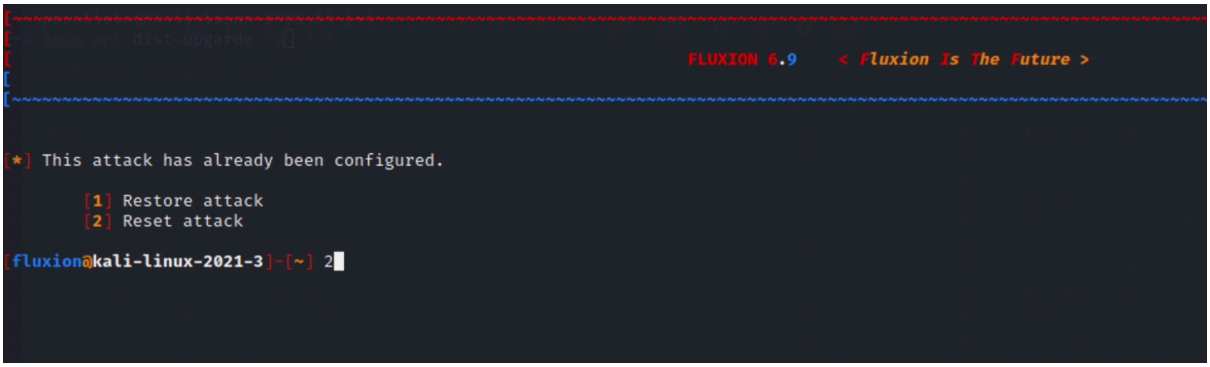



FLUXION 6.9 < Fluxion Is The Future >
[*] Select a channel to monitor
[1] All channels (2.4GHz)
[2] All channels (5GHz)
[3] All channels (2.4GHz & 5Ghz)
[4] Specific channel(s)
[5] Back
[fluxion@kali-linux-2021-3]-[~] 3
[*] Starting scanner, please wait...
[*] Five seconds after the target AP appears, close the FLUXION Scanner (ctrl+c).

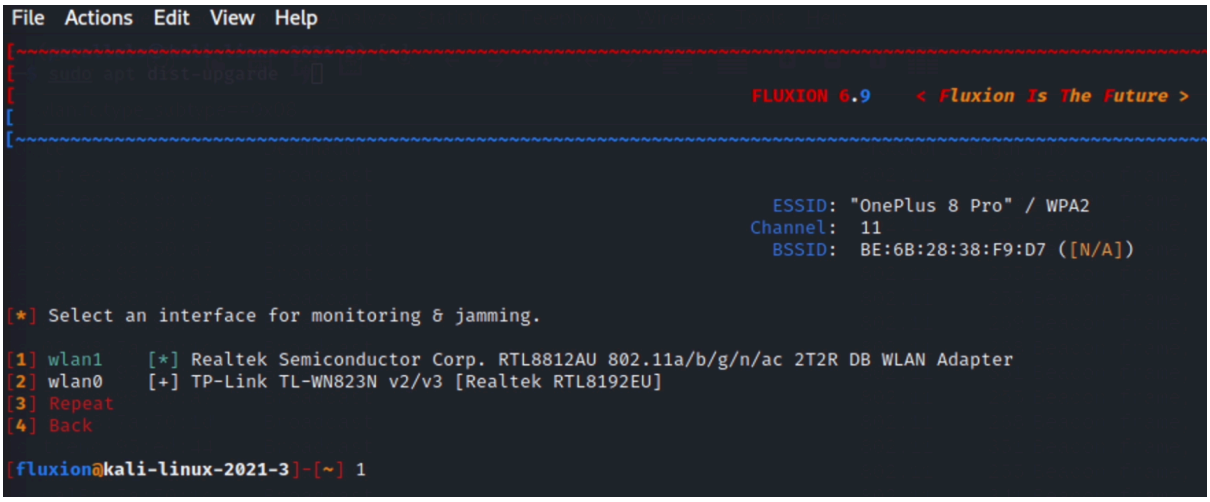

FLUXION Scanner
kali-linux-2021-3: /home/parallels/Downloads/fluxion-master
CH 2][Elapsed: 0 s][2022-12-11 09:23
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSI
A0:2D:13:13:6E:1D -41 5 0 0 6 130 WPA2 CCMP PSK VODAFONE-9570
C8:D1:2A:95:ED:44 -44 5 1 0 6 130 WPA2 CCMP PSK VMP2945666
34:2C:C4:37:27:64 -45 4 0 0 1 130 WPA2 CCMP PSK VM1555633
36:2C:94:37:27:64 -49 5 0 0 1 130 WPA2 CCMP MGT Horizon Wi-Fr
F4:23:9C:B2:95:71 -45 4 1 0 1 195 WPA2 CCMP PSK VODAFONE-9570
AE:F8:CC:08:59:9D -49 4 0 0 11 195 WPA2 CCMP MGT Horizon Wi-Fr
AC:F8:CC:08:59:9D -52 7 0 0 11 195 WPA2 CCMP PSK VM8053781
BE:6B:28:38:F9:D7 -38 6 2 0 11 360 WPA2 CCMP PSK OnePlus 8 Pro
5E:79:CC:98:50:A7 -26 7 0 0 11 360 WPA2 CCMP PSK TEST_AP_1
BSSID STATION PWR Rate Lost Frames Notes Probes
C8:D1:2A:95:ED:44 4A:71:8E:AB:28:E3 -37 0 - 1 0 3
BE:6B:28:38:F9:D7 50:2F:9B:F8:2F:7D -33 1e-24e 0 3
FLUXION 6.9 < Fluxion Is The Future >
[*] Five seconds after the target AP appears, close the FLUXION Scanner (ctrl+c).

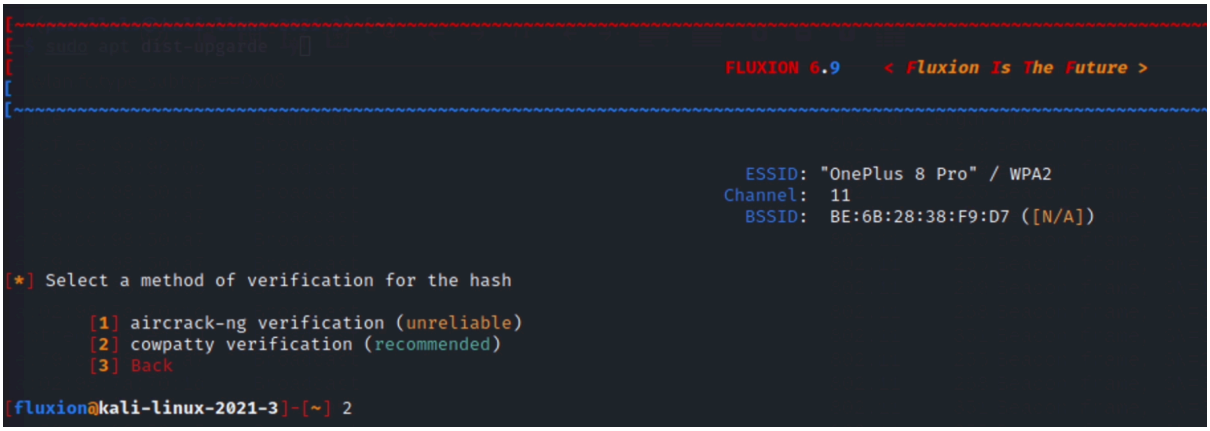

File Actions Edit View Help
FLUXION 6.9 < Fluxion Is The Future >
WIFI LIST
[*] ESSID QLTY PWR STA CH SECURITY BSSID
001] TEST_AP_1 100% -58 0 11 WPA2 5E:79:CC:98:50:A7
002] OnePlus 8 Pro 100% -38 1 11 WPA2 BE:6B:28:38:F9:D7
003] VM8053781 100% -52 0 11 WPA2 AC:F8:CC:08:59:9D
004] Horizon Wi-Free 100% -49 0 11 WPA2 AE:F8:CC:08:59:9D
005] Horizon Wi-Free 100% -56 0 11 WPA2 AE:F8:CC:91:64:97
006] VODAFONE-9570 100% -21 0 1 WPA2 WPA F4:23:9C:B2:95:71
007] Horizon Wi-Free 100% -49 0 1 WPA2 36:2C:94:37:27:64
008] VM1555633 100% -50 0 1 WPA2 34:2C:C4:37:27:64
009] VMP2945666 100% -34 1 6 WPA2 C8:D1:2A:95:ED:44
010] VODAFONE-9570 100% -41 0 6 WPA2 WPA A0:2D:13:13:6E:1D
fluxion@kali-linux-2021-3]-[~] 2


FLUXION 6.9 < Fluxion Is The Future >
[*] Select a wireless interface for target tracking.
[*] Choosing a dedicated interface may be required.
[*]
[1] wlan1 [*] Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac 2T2R DB WLAN Adapter
[2] wlan0 [+] TP-Link TL-WN823N v2/v3 [Realtek RTL8192EU]
[3] Skip
[4] Repeat
[5] Back
[fluxion@kali-linux-2021-3]-[~] 1


FLUXION 6.9 < Fluxion Is The Future >
[*] This attack has already been configured.
[1] Restore attack
[2] Reset attack
[fluxion@kali-linux-2021-3]-[~] 2

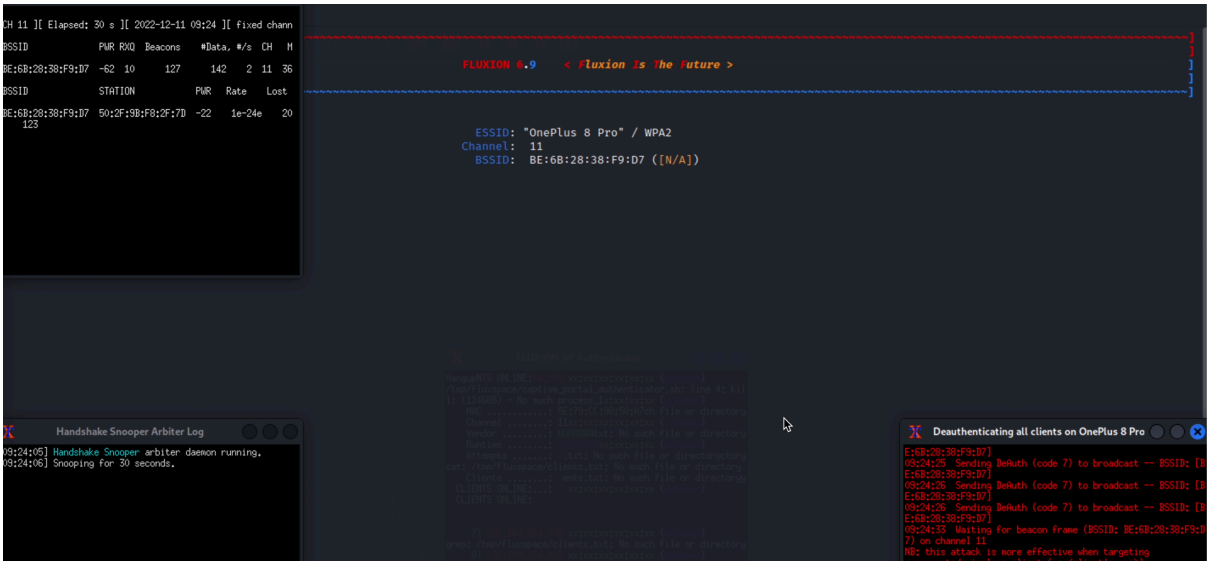

FLUXION 6.9 < Fluxion Is The Future >
ESSID: "OnePlus 8 Pro" / WPA2
Channel: 11
BSSID: BE:6B:28:38:F9:D7 ([N/A])
[*] Select a method of handshake retrieval
[1] Monitor (passive)
[2] aireplay-ng deauthentication (aggressive)
[3] mdk4 deauthentication (aggressive)
[4] Back
[fluxion@kali-linux-2021-3]-[~] 2

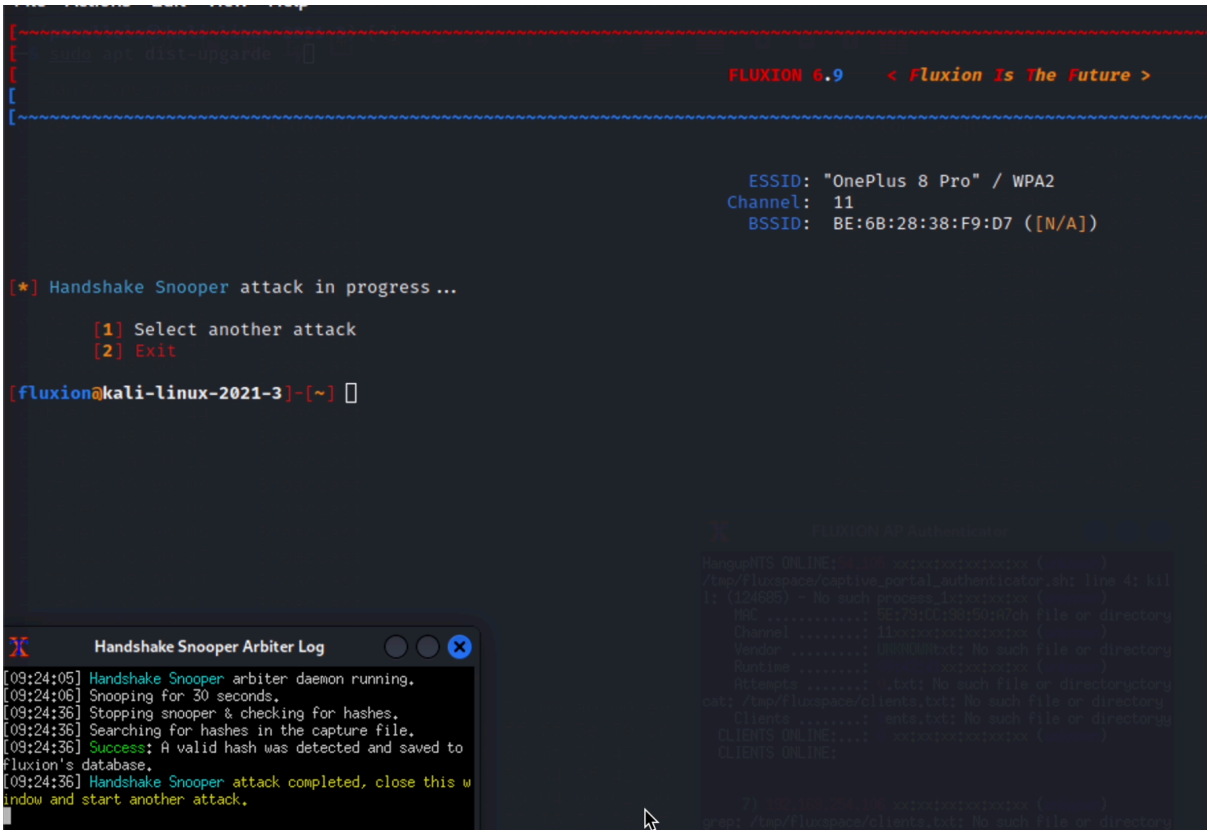

File Actions Edit View Help
FLUXION 6.9 < Fluxion Is The Future >
ESSID: "OnePlus 8 Pro" / WPA2
Channel: 11
BSSID: BE:6B:28:38:F9:D7 ([N/A])
[*] Select an interface for monitoring & jamming.
[1] wlan1 [*] Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac 2T2R DB WLAN Adapter
[2] wlan0 [+] TP-Link TL-WN823N v2/v3 [Realtek RTL8192EU]
[3] Repeat
[4] Back
[fluxion@kali-linux-2021-3]-[~] 1


FLUXION 6.9 < Fluxion Is The Future >
ESSID: "OnePlus 8 Pro" / WPA2
Channel: 11
BSSID: BE:6B:28:38:F9:D7 ([N/A])
[*] Select a method of verification for the hash
[1] aircrack-ng verification (unreliable)
[2] cowpatty verification (recommended)
[3] Back
[fluxion@kali-linux-2021-3]-[~] 2

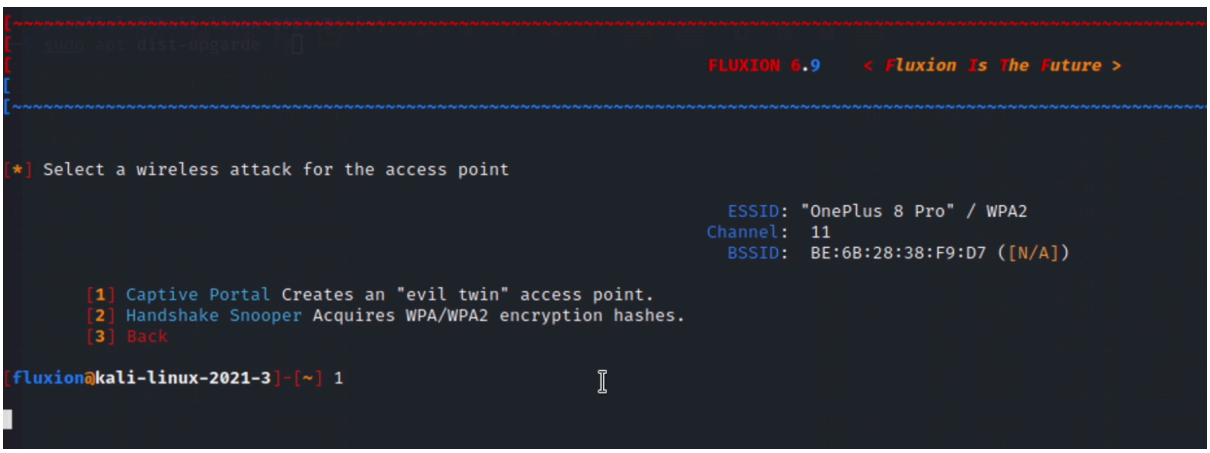

FLUXION 6.9 < Fluxion Is The Future >
ESSID: "OnePlus 8 Pro" / WPA2
Channel: 11
BSSID: BE:6B:28:38:F9:D7 ([N/A])
[*] How often should the verifier check for a handshake?
[1] Every 30 seconds (recommended).
[2] Every 60 seconds.
[3] Every 90 seconds.
[4] Back
[fluxion@kali-linux-2021-3]-[~] 1

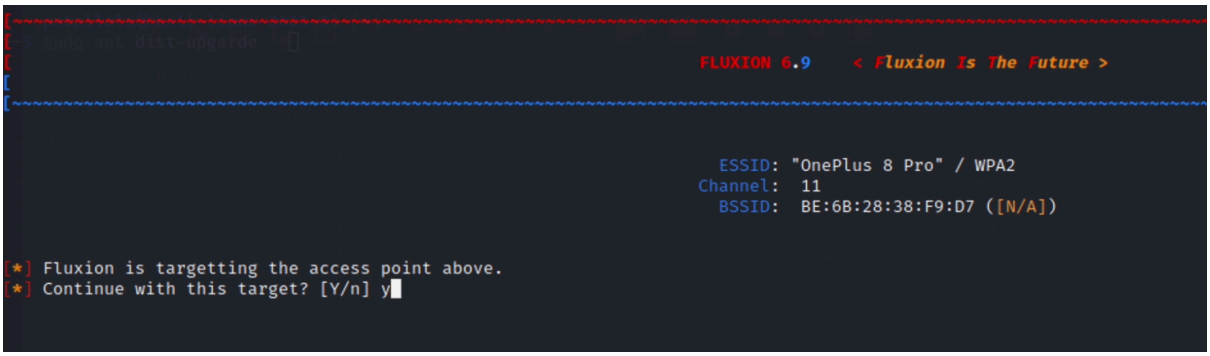

FLUXION 6.9 < Fluxion Is The Future >
ESSID: "OnePlus 8 Pro" / WPA2
Channel: 11
BSSID: BE:6B:28:38:F9:D7 ([N/A])
*] How should verification occur?
[1] Asynchronously (fast systems only).
[2] Synchronously (recommended).
[3] Back
fluxion@kali-linux-2021-3]-[~] 2

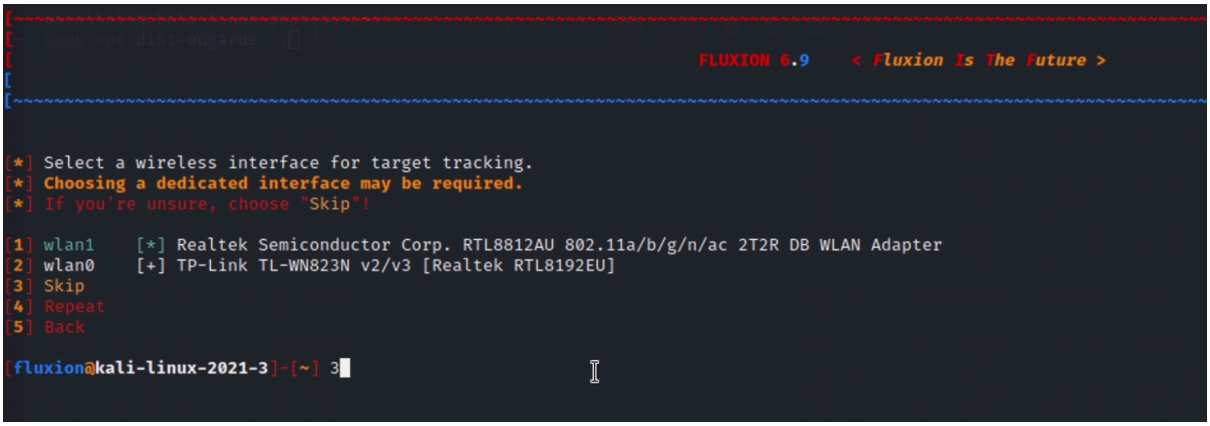

CH 11][Elapsed: 30 s][2022-12-11 09:24][fixed chann
BSSID PWR RXQ Beacons #Data, #/s CH M
BE:6B:28:38:F9:D7 -62 10 127 142 2 11 36
BSSID STATION PWR Rate Lost
BE:6B:28:38:F9:D7 50:2F:9B:F8:2F:7D -22 1e-24e 20
123
FLUXION 6.9 < Fluxion Is The Future >
ESSID: "OnePlus 8 Pro" / WPA2
Channel: 11
BSSID: BE:6B:28:38:F9:D7 ([N/A])
Handshake Snooper Arbiter Log
09:24:05] Handshake Snooper arbiter daemon running.
09:24:06] Snooping for 30 seconds.
Deauthenticating all clients on OnePlus 8 Pro
E:6B:28:38:F9:D7]
09:24:25 Sending DeAuth (code 7) to broadcast -- BSSID: [B
E:6B:28:38:F9:D7]
09:24:26 Sending DeAuth (code 7) to broadcast -- BSSID: [B
E:6B:28:38:F9:D7]
09:24:26 Sending DeAuth (code 7) to broadcast -- BSSID: [B
E:6B:28:38:F9:D7]
09:24:33 Waiting for beacon frame (BSSID: BE:6B:28:38:F9:D
7) on channel 11
NB: this attack is more effective when targeting

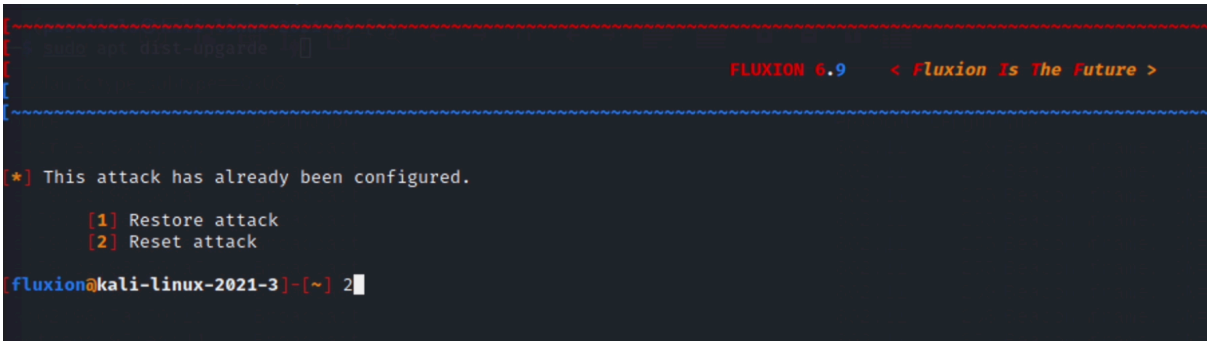

FLUXION 6.9 < Fluxion Is The Future >
ESSID: "OnePlus 8 Pro" / WPA2
Channel: 11
BSSID: BE:6B:28:38:F9:D7 ([N/A])
[*] Handshake Snooper attack in progress ...
[1] Select another attack
[2] Exit
[fluxion@kali-linux-2021-3]-[~]
Handshake Snooper Arbiter Log
[09:24:05] Handshake Snooper arbiter daemon running.
[09:24:06] Snooping for 30 seconds.
[09:24:36] Stopping snooper & checking for hashes.
[09:24:36] Searching for hashes in the capture file.
[09:24:36] Success: A valid hash was detected and saved to fluxion's database.
[09:24:36] Handshake Snooper attack completed, close this window and start another attack.

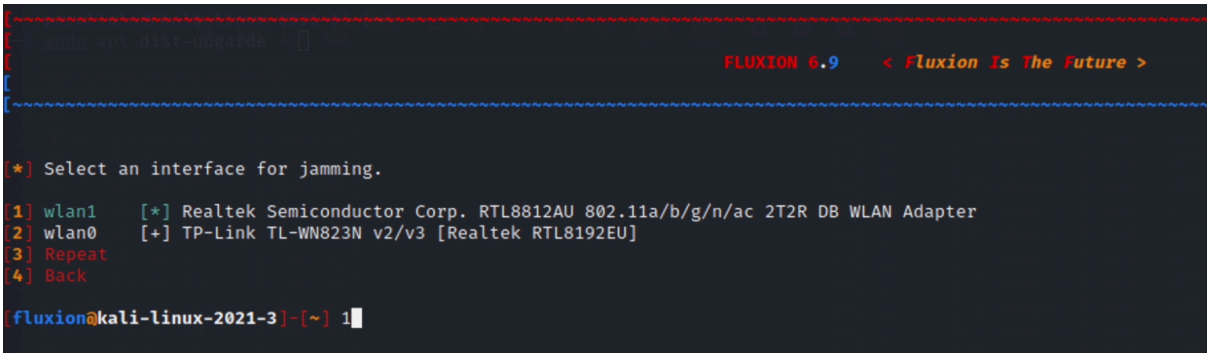

File Actions Edit View Help
FLUXION 6.9 < Fluxion Is The Future >
ESSID: "OnePlus 8 Pro" / WPA2
Channel: 11
BSSID: BE:6B:28:38:F9:D7 ([N/A])
[*] Handshake Snooper attack in progress ...
[1] Select another attack
[2] Exit
[fluxion@kali-linux-2021-3]-[~] 1

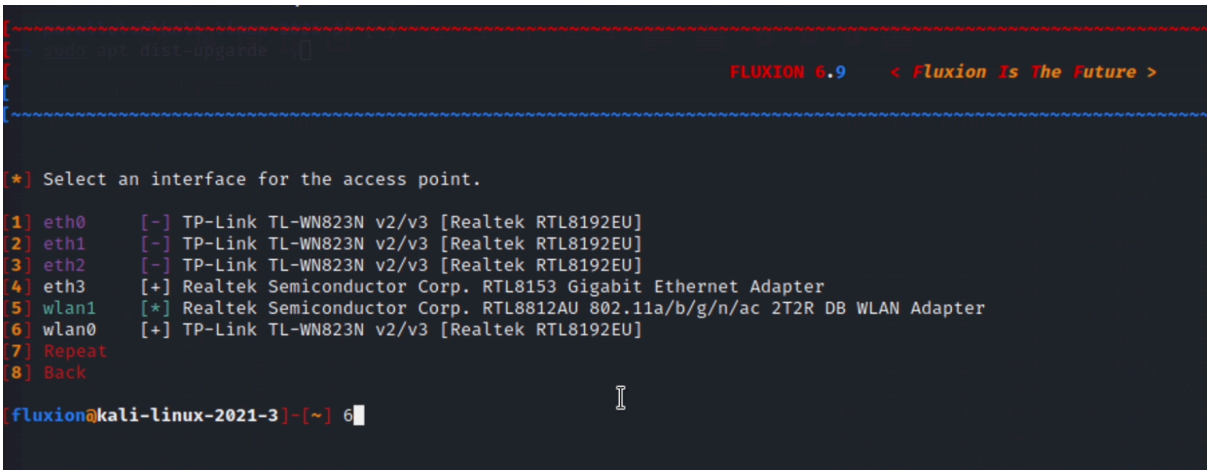

FLUXION 6.9 < Fluxion Is The Future >
[*] Select a wireless attack for the access point
ESSID: "OnePlus 8 Pro" / WPA2
Channel: 11
BSSID: BE:6B:28:38:F9:D7 ([N/A])
[1] Captive Portal Creates an "evil twin" access point.
[2] Handshake Snooper Acquires WPA/WPA2 encryption hashes.
[3] Back
[fluxion@kali-linux-2021-3]-[~] 1

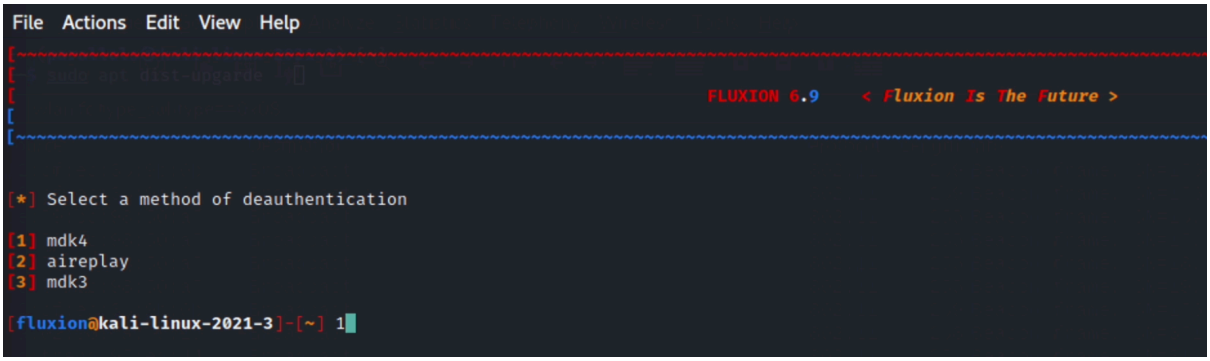

FLUXION 6.9 < Fluxion Is The Future >
ESSID: "OnePlus 8 Pro" / WPA2
Channel: 11
BSSID: BE:6B:28:38:F9:D7 ([N/A])
[*] Fluxion is targetting the access point above.
[*] Continue with this target? [Y/n] y


FLUXION 6.9 < Fluxion Is The Future >
[*] Select a wireless interface for target tracking.
[*] Choosing a dedicated interface may be required.
[*] If you're unsure, choose "Skip"!
[1] wlan1 [*] Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac 2T2R DB WLAN Adapter
[2] wlan0 [+] TP-Link TL-WN823N v2/v3 [Realtek RTL8192EU]
[3] Skip
[4] Repeat
[5] Back
[fluxion@kali-linux-2021-3]-[~] 3

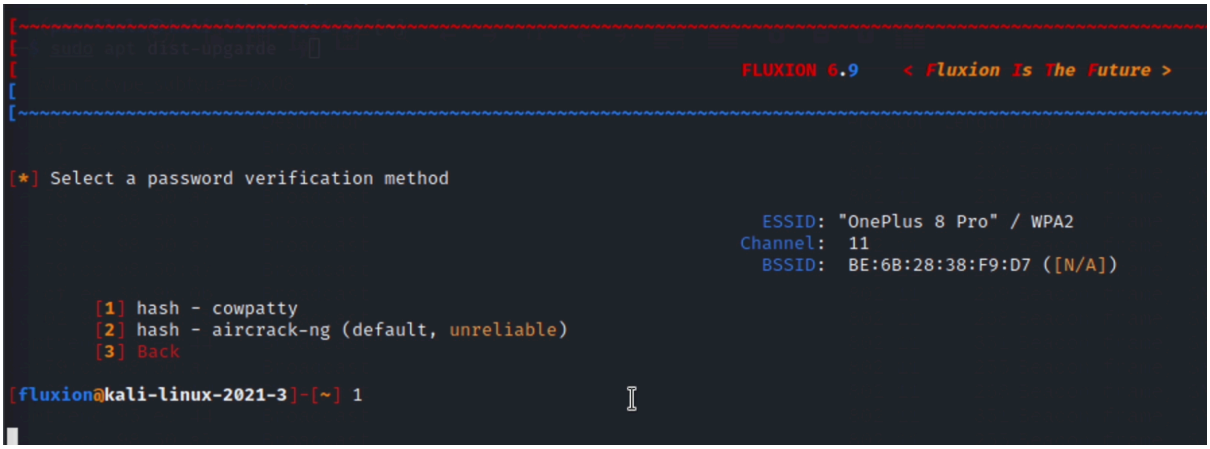

FLUXION 6.9 < Fluxion Is The Future >
[*] This attack has already been configured.
[1] Restore attack
[2] Reset attack
[fluxion@kali-linux-2021-3]-[~] 2


FLUXION 6.9 < Fluxion Is The Future >
[*] Select an interface for jamming.
[1] wlan1 [*] Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac 2T2R DB WLAN Adapter
[2] wlan0 [+] TP-Link TL-WN823N v2/v3 [Realtek RTL8192EU]
[3] Repeat
[4] Back
[fluxion@kali-linux-2021-3]-[~] 1

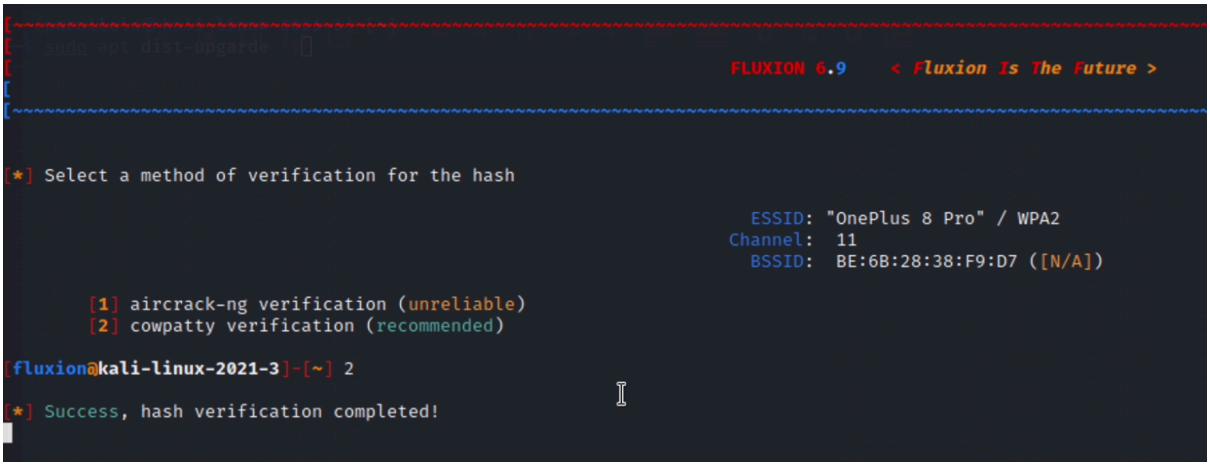

FLUXION 6.9 < Fluxion Is The Future >
[*] Select an interface for the access point.
[1] eth0 [-] TP-Link TL-WN823N v2/v3 [Realtek RTL8192EU]
[2] eth1 [-] TP-Link TL-WN823N v2/v3 [Realtek RTL8192EU]
[3] eth2 [-] TP-Link TL-WN823N v2/v3 [Realtek RTL8192EU]
[4] eth3 [+] Realtek Semiconductor Corp. RTL8153 Gigabit Ethernet Adapter
[5] wlan1 [*] Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac 2T2R DB WLAN Adapter
[6] wlan0 [+] TP-Link TL-WN823N v2/v3 [Realtek RTL8192EU]
[7] Repeat
[8] Back
[fluxion@kali-linux-2021-3]-[~] 6

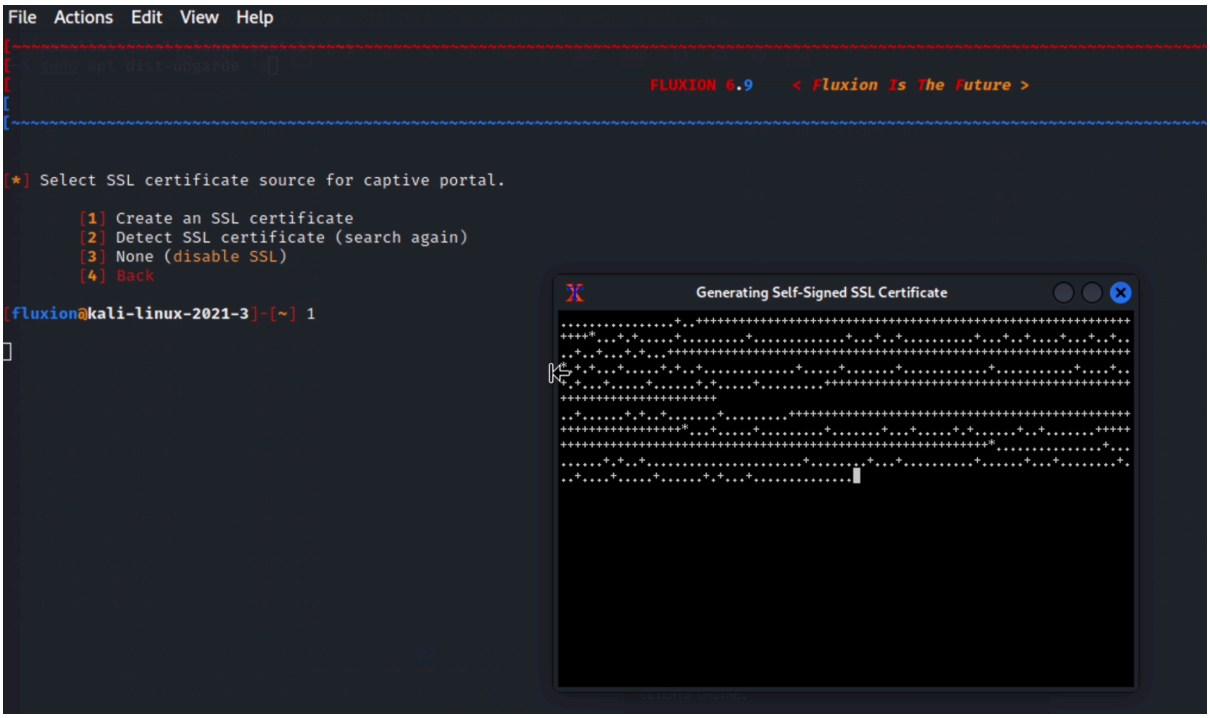

File Actions Edit View Help
FLUXION 6.9 < Fluxion Is The Future >
[*] Select a method of deauthentication
[1] mdk4
[2] aireplay
[3] mdk3
[fluxion@kali-linux-2021-3]-[~] 1

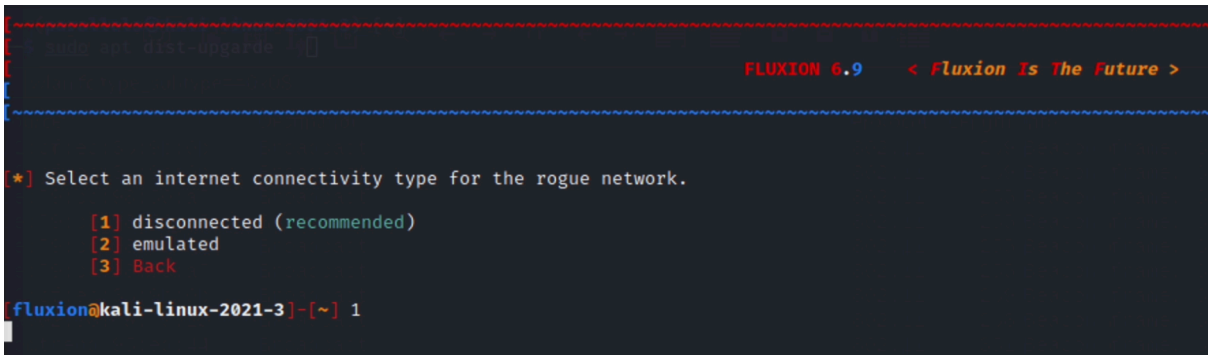

FLUXION 6.9 < Fluxion Is The Future >
[*] Select an access point service
ESSID: "OnePlus 8 Pro" / WPA2
Channel: 11
BSSID: BE:6B:28:38:F9:D7 ([N/A])
[1] Rogue AP - hostapd (recommended)
[2] Rogue AP - airbase-ng (slow)
[3] Back
[fluxion@kali-linux-2021-3]-[~] 1

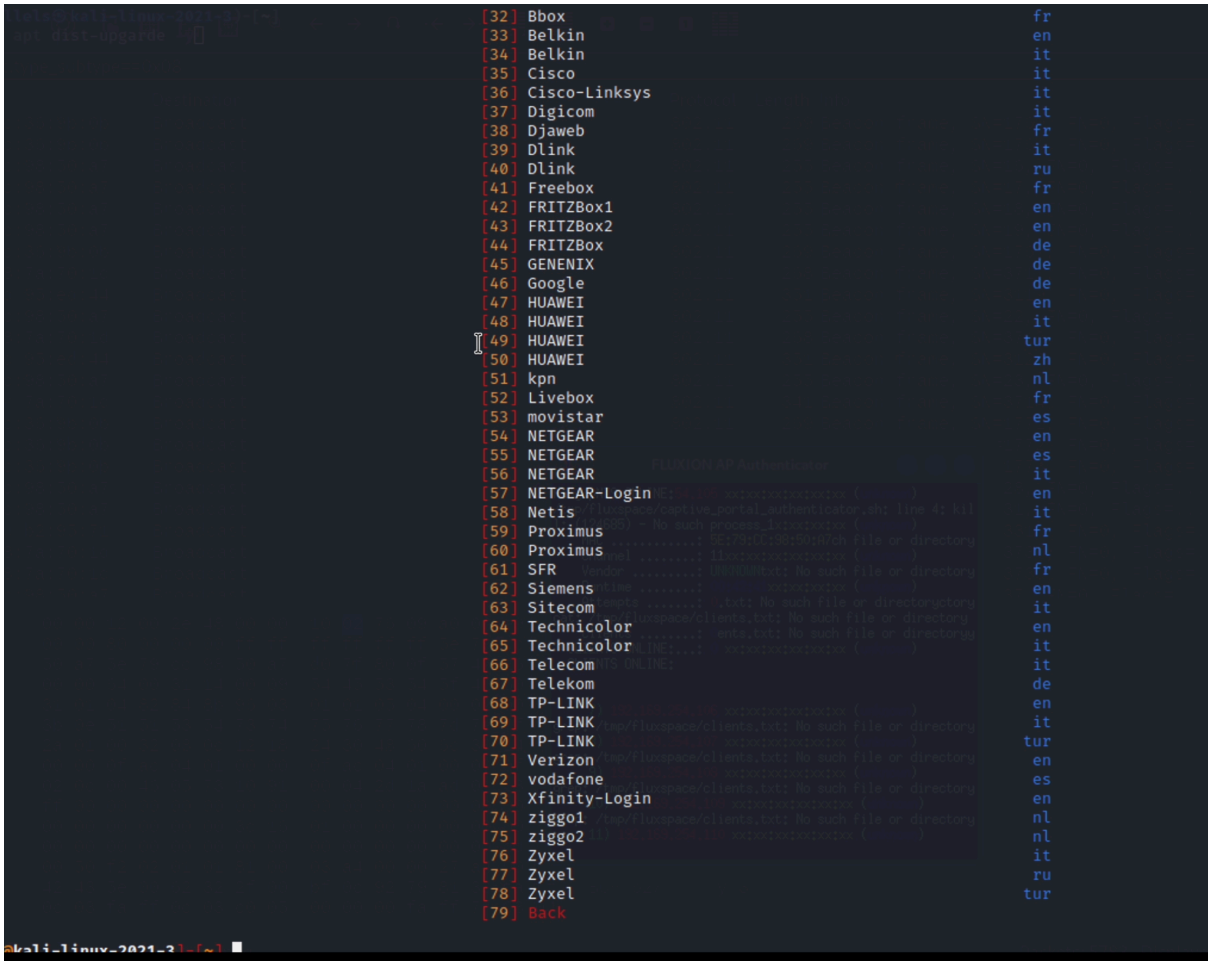

FLUXION 6.9 < Fluxion Is The Future >
[*] Select a password verification method
ESSID: "OnePlus 8 Pro" / WPA2
Channel: 11
BSSID: BE:6B:28:38:F9:D7 ([N/A])
[1] hash - cowpatty
[2] hash - aircrack-ng (default, unreliable)
[3] Back
[fluxion@kali-linux-2021-3]-[~] 1

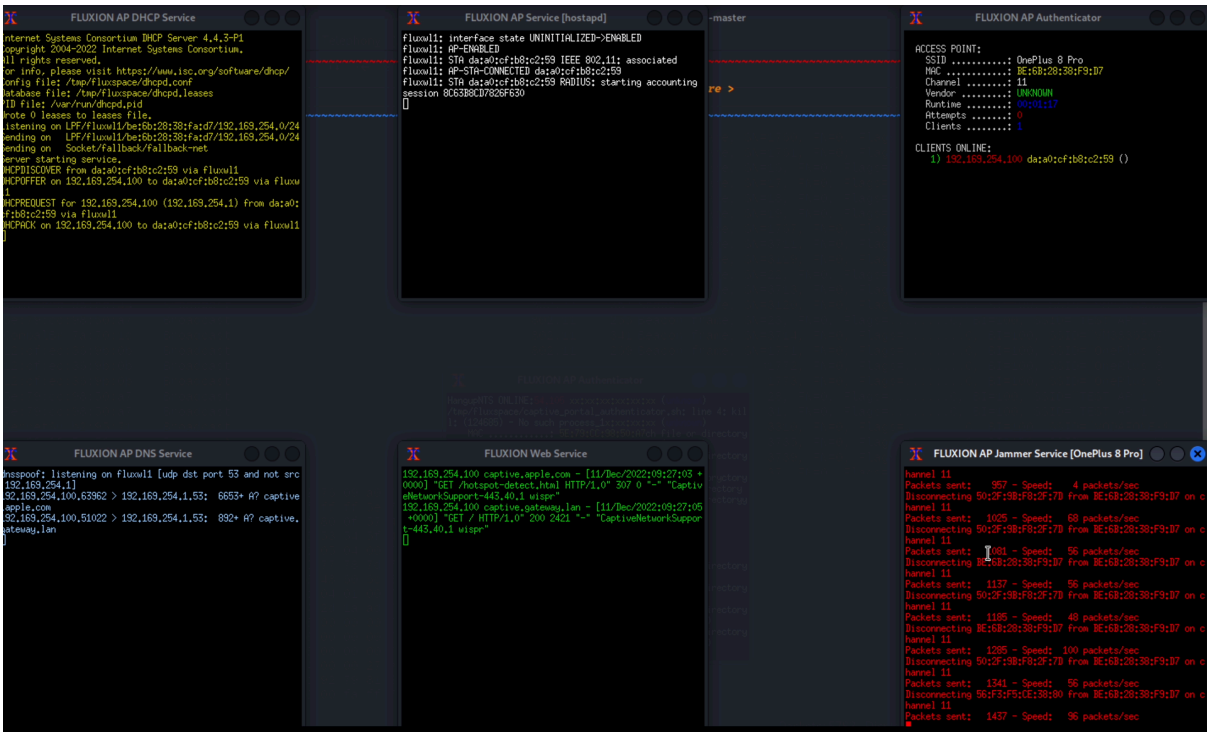

FLUXION 6.9 < Fluxion Is The Future >
[*] A hash for the target AP was found.
[*] Do you want to use this file?
[1] Use hash found
[2] Specify path to hash
[3] Rescan handshake directory
[4] Back
fluxion@kali-linux-2021-3 ~ 1

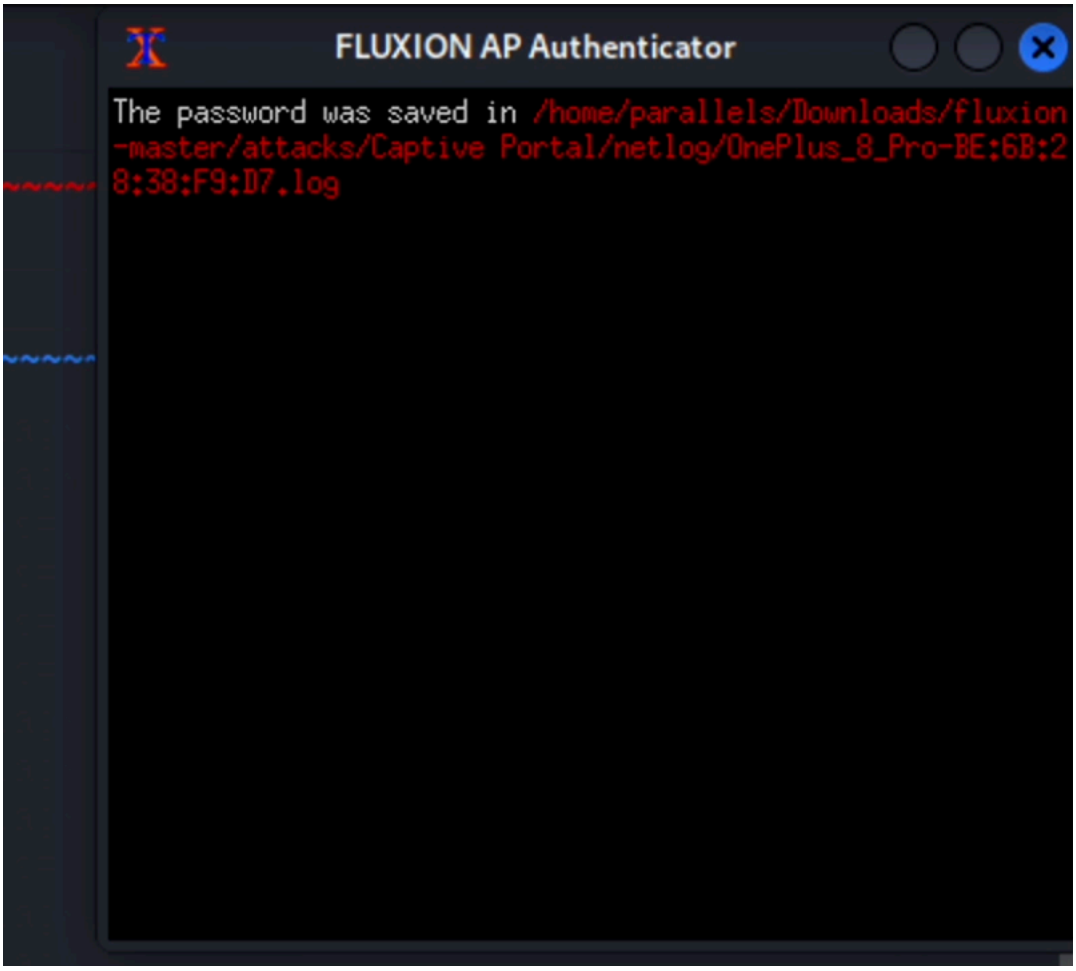

FLUXION 6.9 < Fluxion Is The Future >
[*] Select a method of verification for the hash
ESSID: "OnePlus 8 Pro" / WPA2
Channel: 11
BSSID: BE:6B:28:38:F9:D7 ([N/A])
[1] aircrack-ng verification (unreliable)
[2] cowpatty verification (recommended)
fluxion@kali-linux-2021-3 ~ 2
[*] Success, hash verification completed!

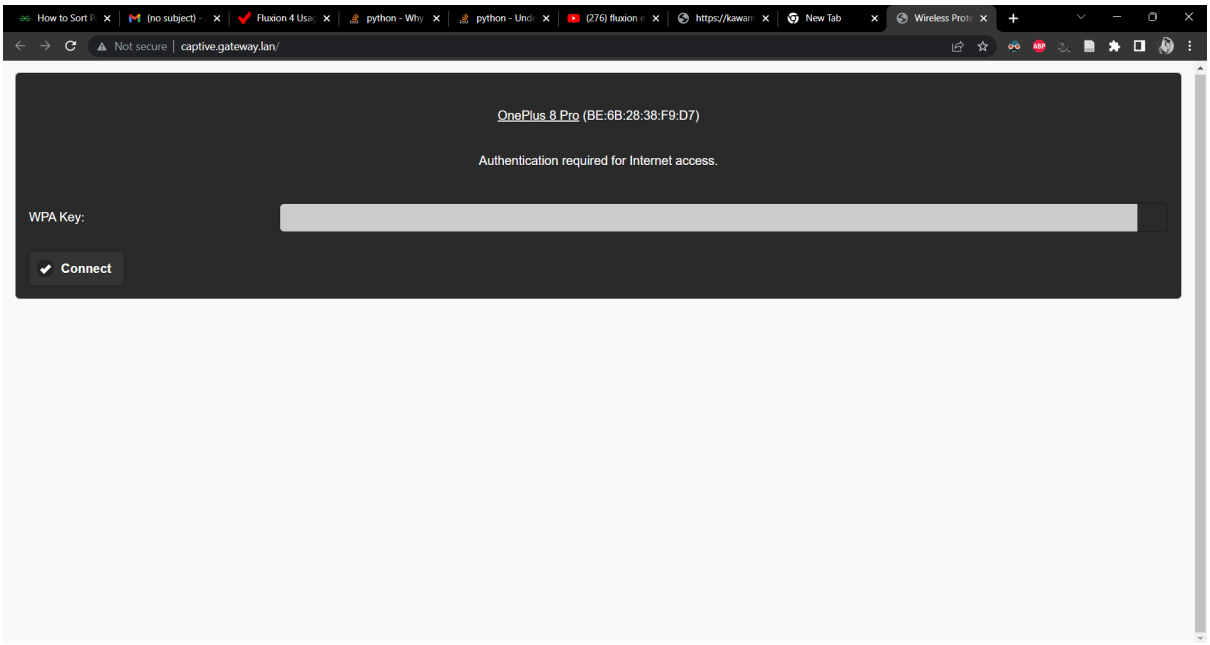

File Actions Edit View Help
FLUXION 6.9 < Fluxion Is The Future >
[*] Select SSL certificate source for captive portal.
[1] Create an SSL certificate
[2] Detect SSL certificate (search again)
[3] None (disable SSL)
[4] Back
fluxion@kali-linux-2021-3 ~ 1
Generating Self-Signed SSL Certificate

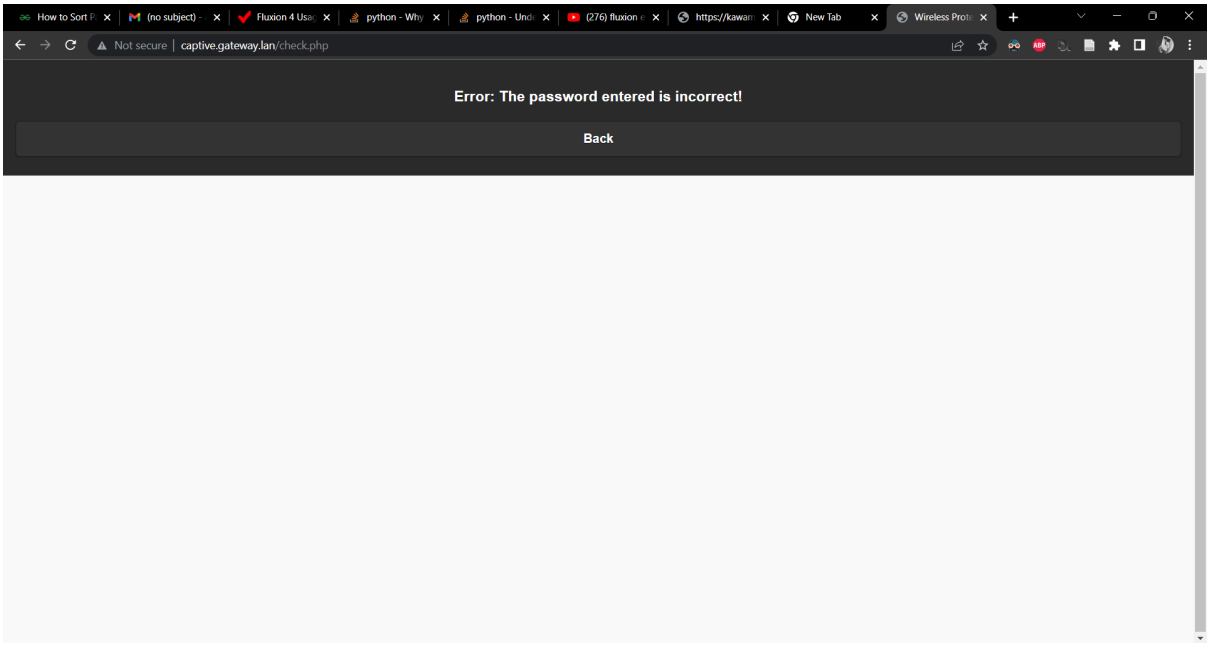

FLUXION 6.9 < Fluxion Is The Future >
[*] Select an internet connectivity type for the rogue network.
[1] disconnected (recommended)
[2] emulated
[3] Back
fluxion@kali-linux-2021-3]-[~] 1

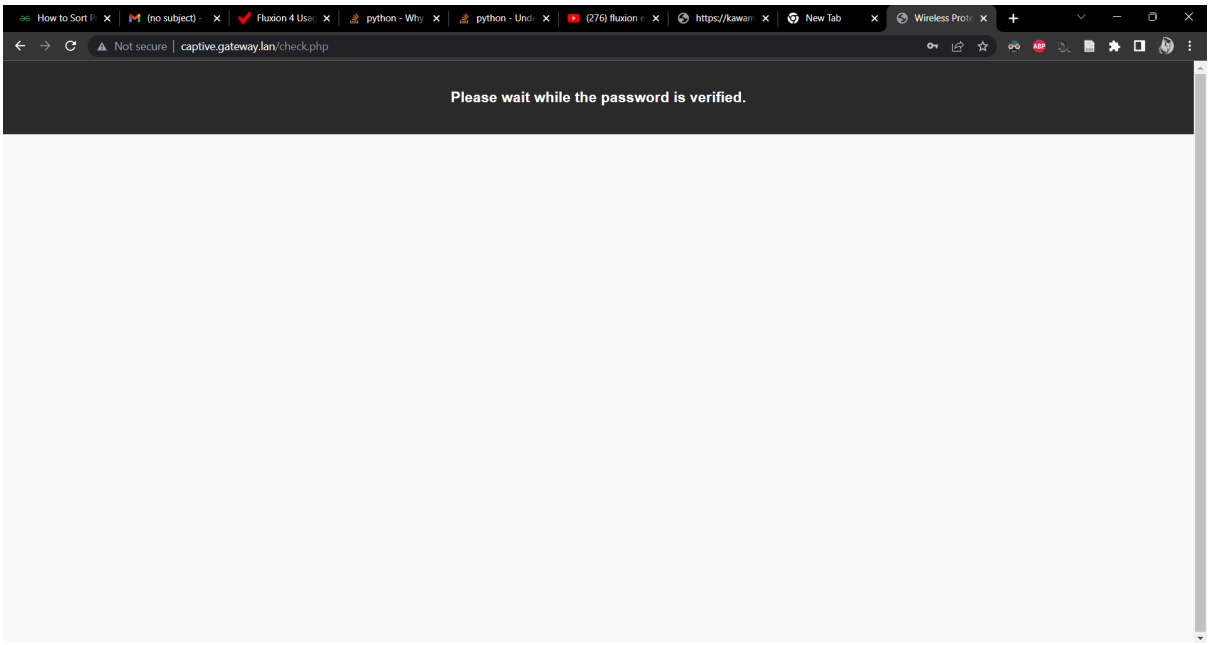

[32] Bbox fr
[33] Belkin en
[34] Belkin it
[35] Cisco it
[36] Cisco-Linksys it
[37] Digicom it
[38] Djaweb fr
[39] Dlink it
[40] Dlink ru
[41] Freebox fr
[42] FRITZBox1 en
[43] FRITZBox2 en
[44] FRITZBox de
[45] GENENIX de
[46] Google de
[47] HUAWEI en
[48] HUAWEI it
[49] HUAWEI tur
[50] HUAWEI zh
[51] kpn nl
[52] Livebox fr
[53] movistar es
[54] NETGEAR en
[55] NETGEAR es
[56] NETGEAR it
[57] NETGEAR-Login en
[58] Netis it
[59] Proximus fr
[60] Proximus nl
[61] SFR fr
[62] Siemens en
[63] Sitecom it
[64] Technicolor en
[65] Technicolor it
[66] Telecom it
[67] Telekom de
[68] TP-LINK en
[69] TP-LINK it
[70] TP-LINK tur
[71] Verizon en
[72] vodafone es
[73] Xfinity-Login en
[74] ziggo1 nl
[75] ziggo2 nl
[76] Zyxel it
[77] Zyxel ru
[78] Zyxel tur
[79] Back

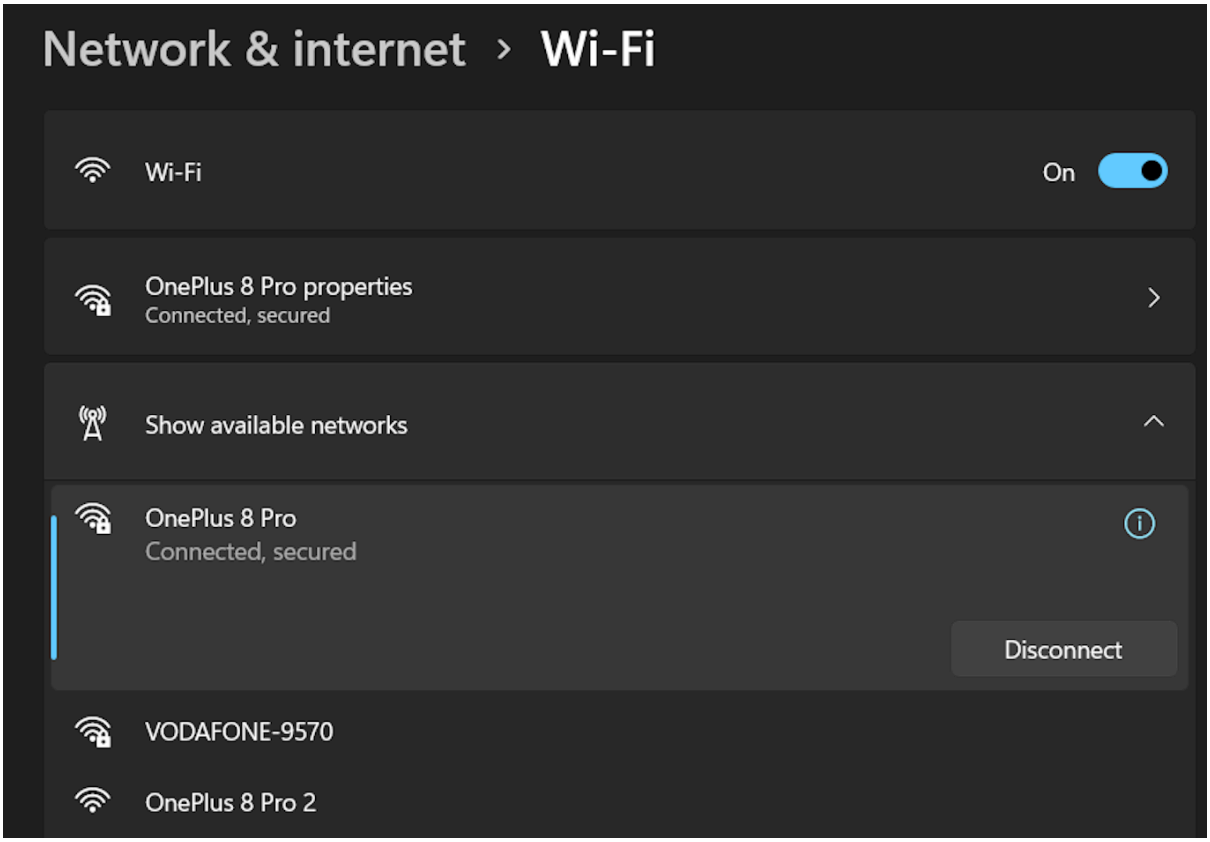

FLUXION AP DHCP Service
FLUXION AP Service [hostapd]
FLUXION AP Authenticator
FLUXION AP DNS Service
FLUXION Web Service
FLUXION AP Jammer Service [OnePlus 8 Pro]

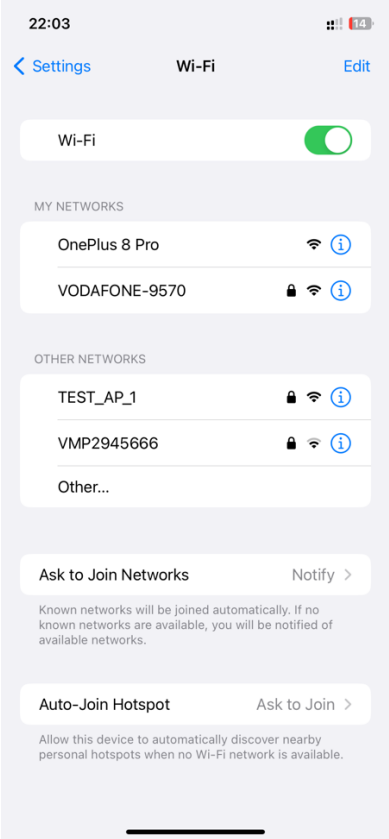

FLUXION AP Authenticator
The password was saved in /home/parallels/Downloads/fluxion-master/attacks/Captive Portal/netlog/OnePlus_8_Pro-BE:6B:28:38:F9:D7.log

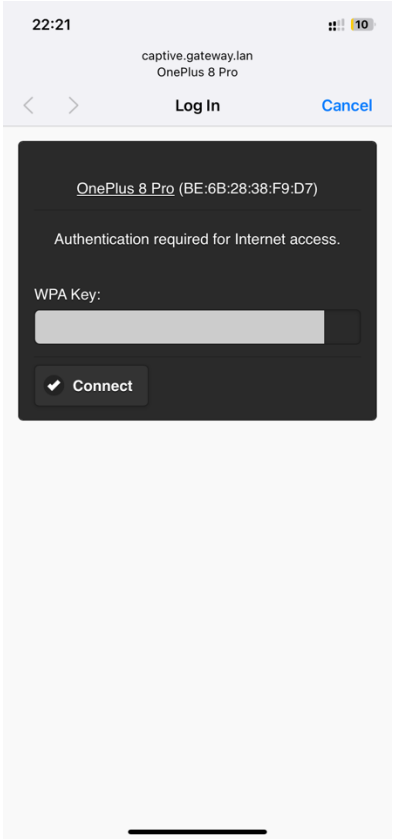

Not secure | captive.gateway.lan/
OnePlus 8 Pro (BE:6B:28:38:F9:D7)
Authentication required for Internet access.
WPA Key:
Connect

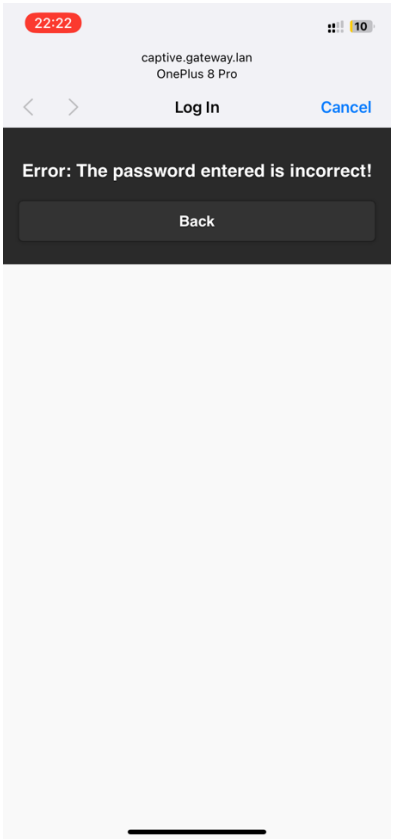

Not secure | captive.gateway.lan/check.php
Error: The password entered is incorrect!
Back

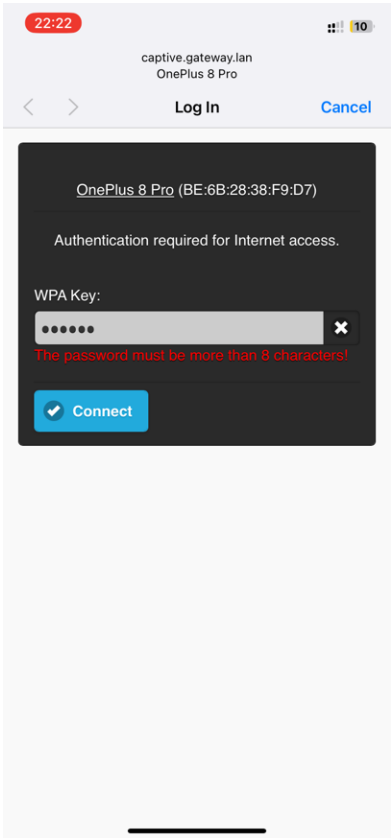

Not secure | captive.gateway.lan/check.php
Please wait while the password is verified.


Network & internet › Wi-Fi
Wi-Fi
On
OnePlus 8 Pro properties
Connected, secured
Show available networks
OnePlus 8 Pro
Connected, secured
Disconnect
VODAFONE-9570
OnePlus 8 Pro 2


22:03
Settings
Wi-Fi
Edit
Wi-Fi
MY NETWORKS
OnePlus 8 Pro
VODAFONE-9570
OTHER NETWORKS
TEST_AP_1
VMP2945666
Other...
Ask to Join Networks
Notify
Known networks will be joined automatically. If no known networks are available, you will be notified of available networks.
Auto-Join Hotspot
Ask to Join
Allow this device to automatically discover nearby personal hotspots when no Wi-Fi network is available.

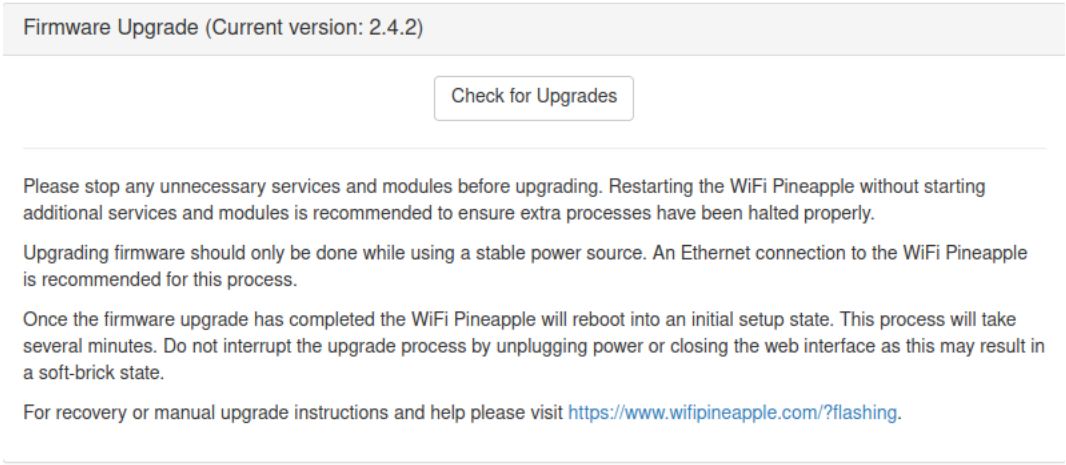

22:21
captive.gateway.lan
OnePlus 8 Pro
Log In
Cancel
OnePlus 8 Pro (BE:6B:28:38:F9:D7)
Authentication required for Internet access.
WPA Key:
Connect

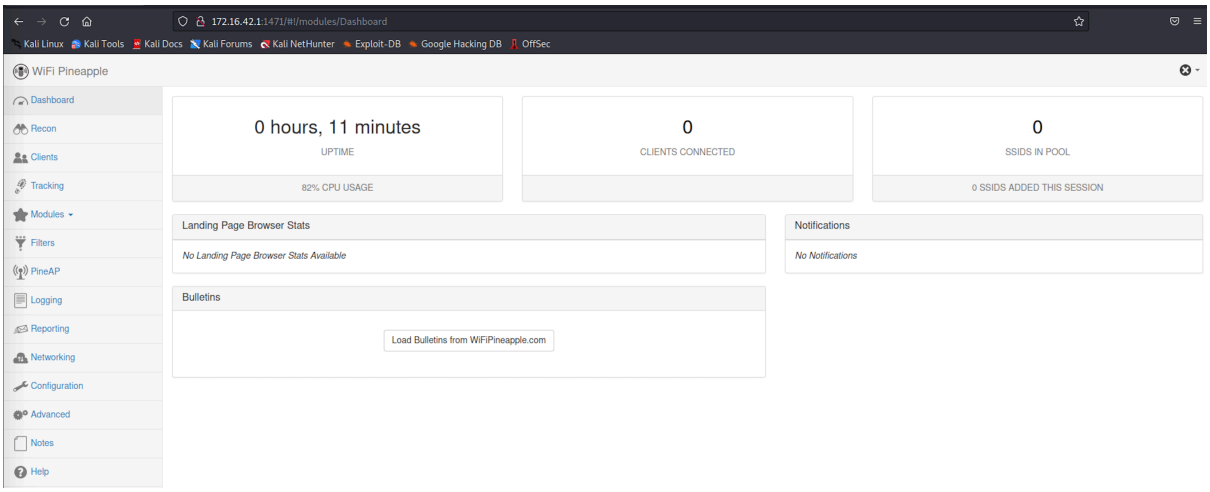

22:22
captive.gateway.lan
OnePlus 8 Pro
Log In
Cancel
Error: The password entered is incorrect!
Back

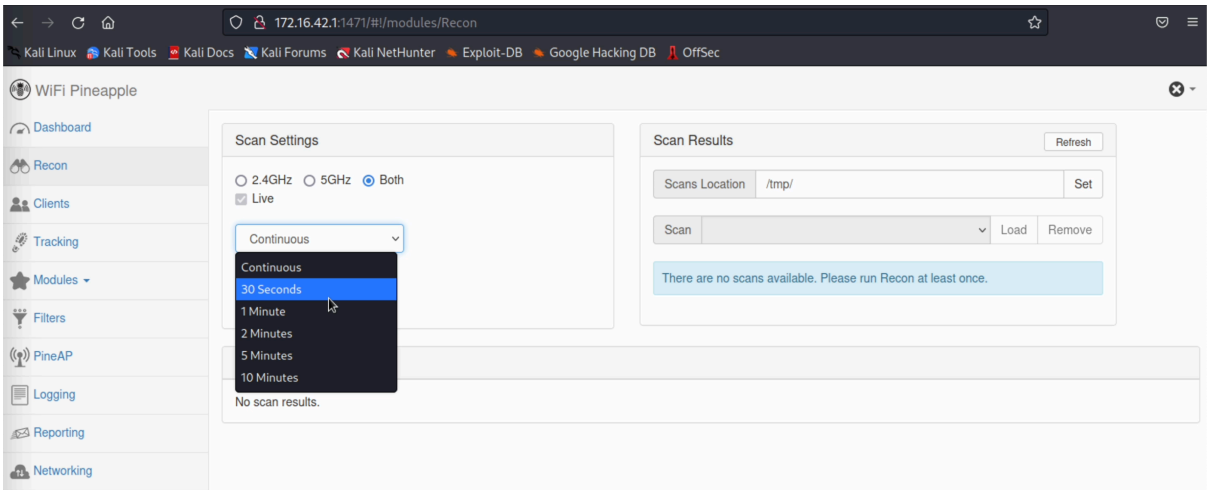

22:22
captive.gateway.lan
OnePlus 8 Pro
Log In
Cancel
OnePlus 8 Pro (BE:6B:28:38:F9:D7)
Authentication required for Internet access.
WPA Key:
The password must be more than 8 characters!
Connect

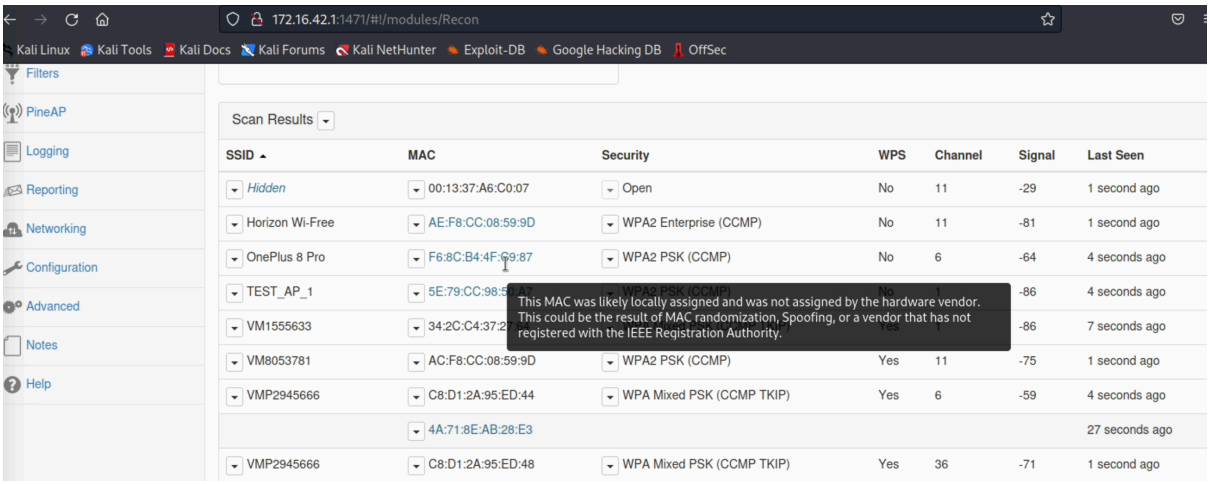
PineAp:

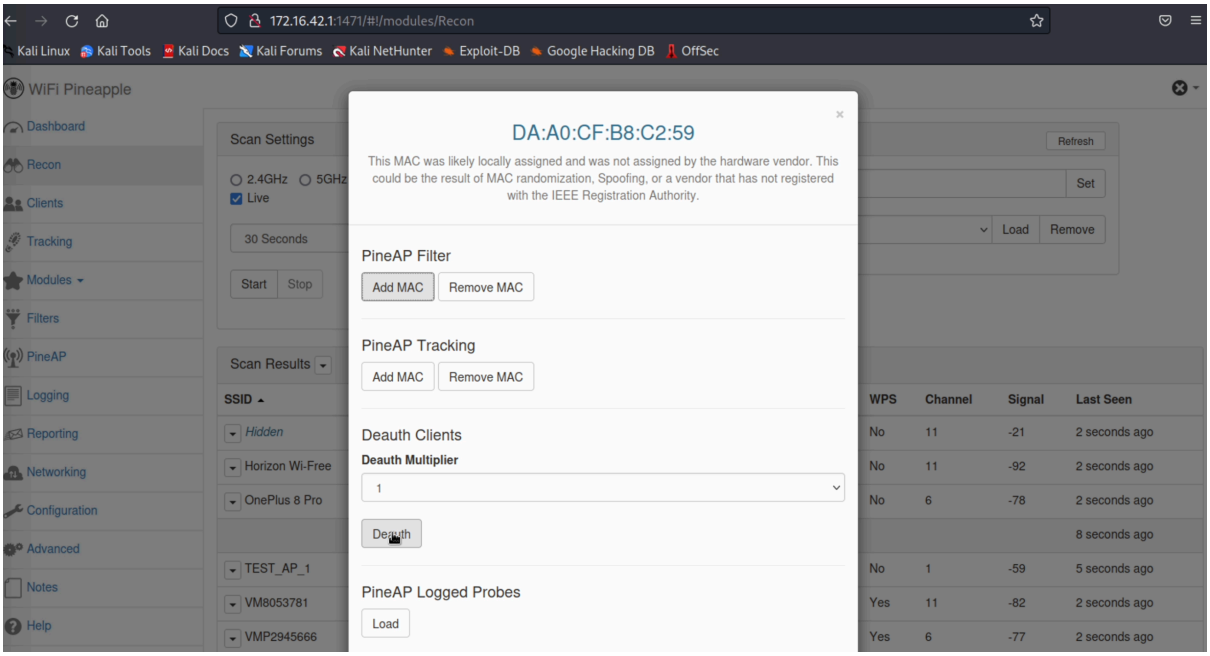
Choose the options from the menu as selected in the screenshots to run the tool.

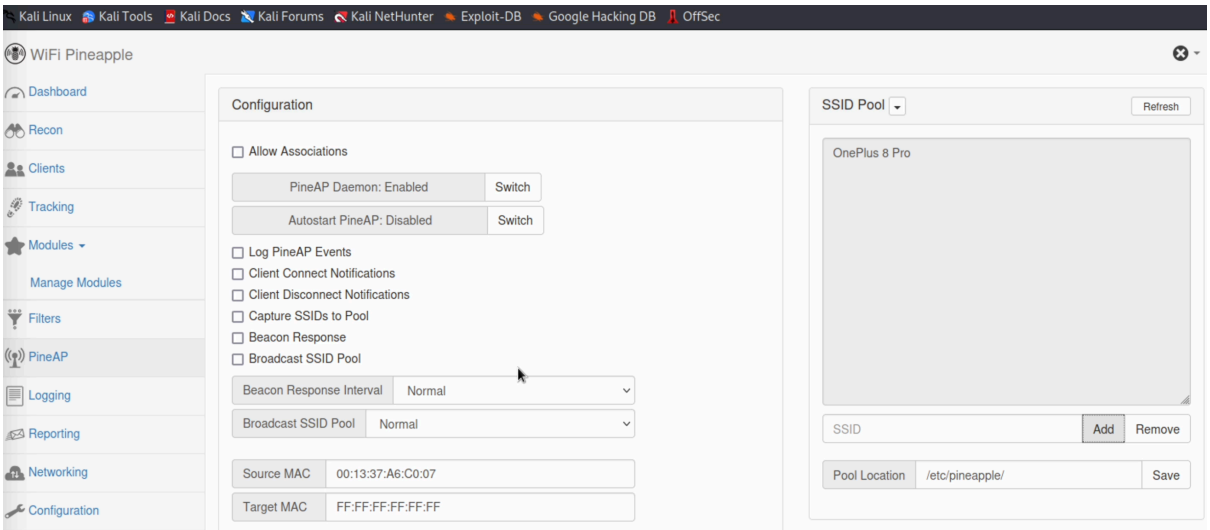


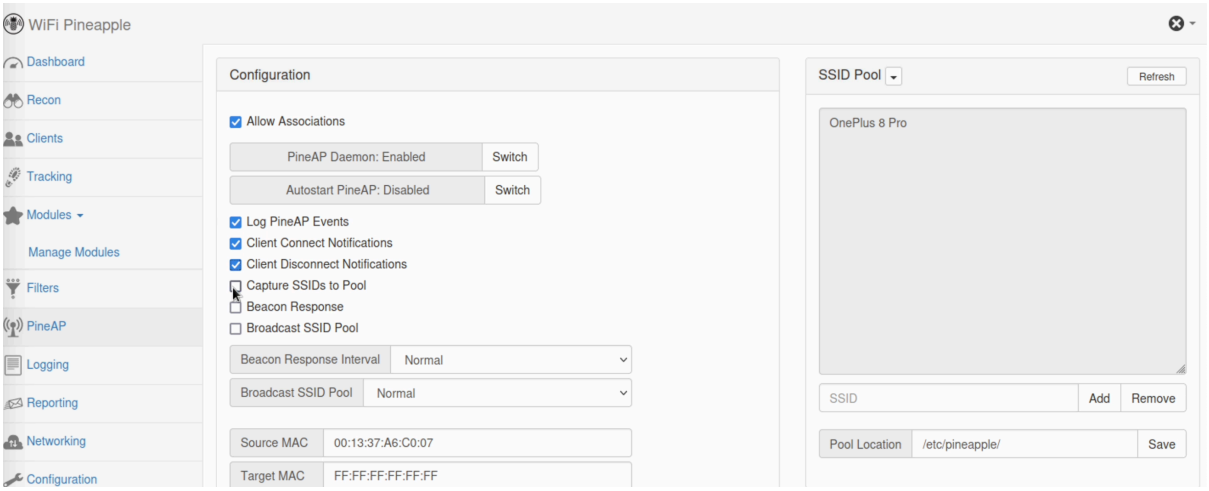


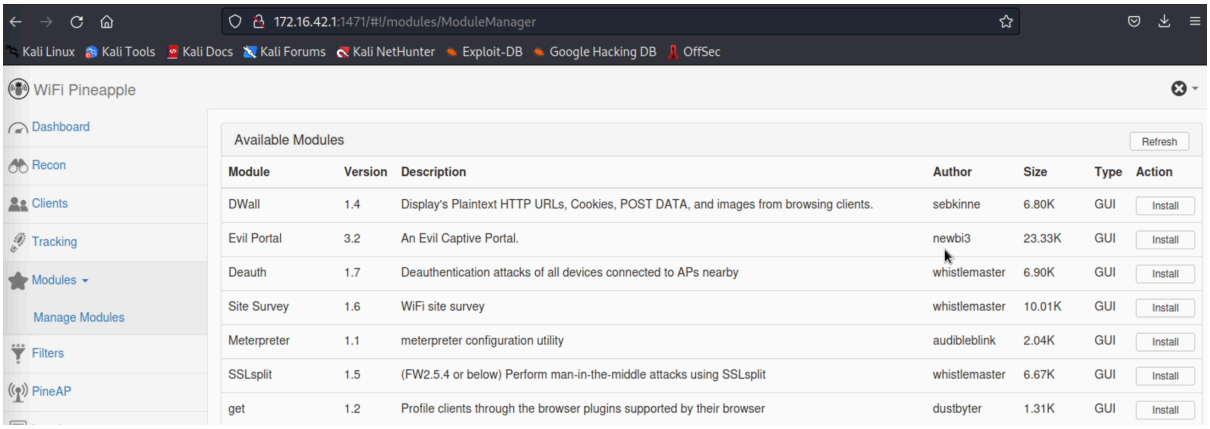


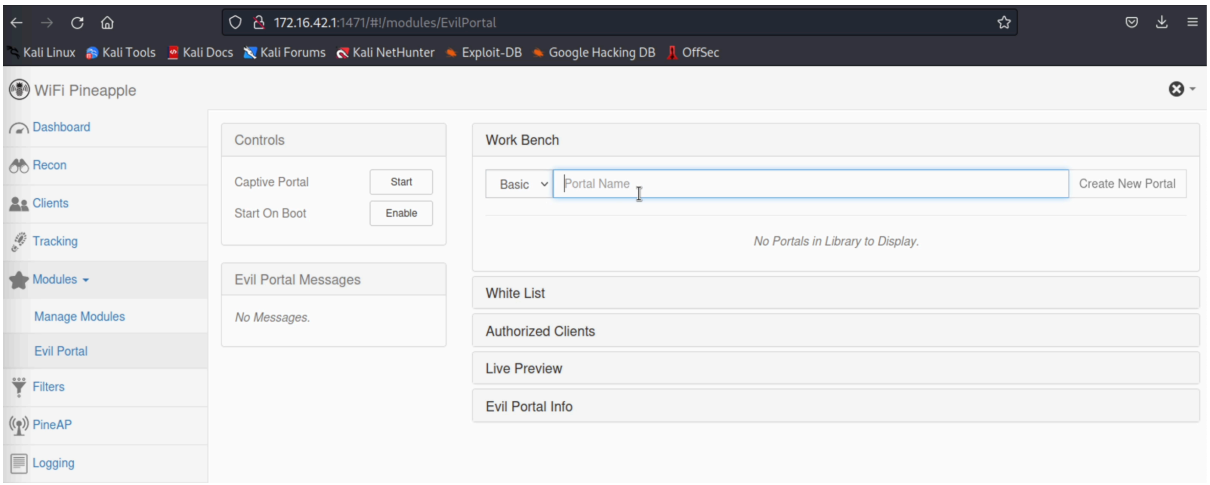

172.16.42.1:1471/#!/modules/Recon
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Filters
PineAP
Logging
Reporting
Networking
Configuration
Advanced
Notes
Help
Scan Results
SSID MAC Security WPS Channel Signal Last Seen
Hidden 00:13:37:A6:C0:07 Open No 11 -29 1 second ago
Horizon Wi-Free AE:F8:CC:08:59:9D WPA2 Enterprise (CCMP) No 11 -81 1 second ago
OnePlus 8 Pro F6:8C:B4:4F:69:87 WPA2 PSK (CCMP) No 6 -64 4 seconds ago
TEST_AP_1 5E:79:CC:98:5 -86 4 seconds ago
VM1555633 34:2C:C4:37:2 -86 7 seconds ago
This MAC was likely locally assigned and was not assigned by the hardware vendor. This could be the result of MAC randomization, Spoofing, or a vendor that has not registered with the IEEE Registration Authority.
VM8053781 AC:F8:CC:08:59:9D WPA2 PSK (CCMP) Yes 11 -75 1 second ago
VMP2945666 C8:D1:2A:95:ED:44 WPA Mixed PSK (CCMP TKIP) Yes 6 -59 4 seconds ago
4A:71:8E:AB:28:E3 27 seconds ago
VMP2945666 C8:D1:2A:95:ED:48 WPA Mixed PSK (CCMP TKIP) Yes 36 -71 1 second ago

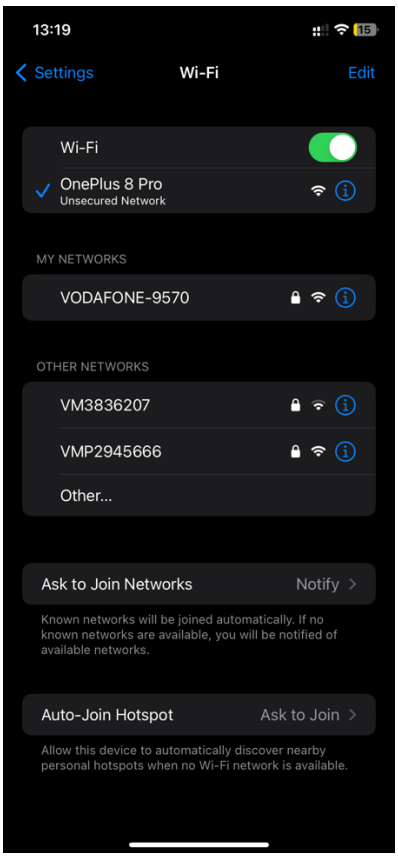

172.16.42.1:1471/#!/modules/Recon
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
WiFi Pineapple
Dashboard
Recon
Clients
Tracking
Modules
Filters
PineAP
Logging
Reporting
Networking
Configuration
Advanced
Notes
Help
Scan Settings
2.4GHz 5GHz
Live
30 Seconds
Start Stop
Scan Results
SSID
Hidden
Horizon Wi-Free
OnePlus 8 Pro
TEST_AP_1
VM8053781
VMP2945666
DA:A0:CF:B8:C2:59
This MAC was likely locally assigned and was not assigned by the hardware vendor. This could be the result of MAC randomization, Spoofing, or a vendor that has not registered with the IEEE Registration Authority.
PineAP Filter
Add MAC Remove MAC
PineAP Tracking
Add MAC Remove MAC
Deauth Clients
Deauth Multiplier
1
Deauth
PineAP Logged Probes
Load
Refresh
Set
Load Remove
WPS Channel Signal Last Seen
No 11 -21 2 seconds ago
No 11 -92 2 seconds ago
No 6 -78 2 seconds ago
8 seconds ago
No 1 -59 5 seconds ago
Yes 11 -82 2 seconds ago
Yes 6 -77 2 seconds ago

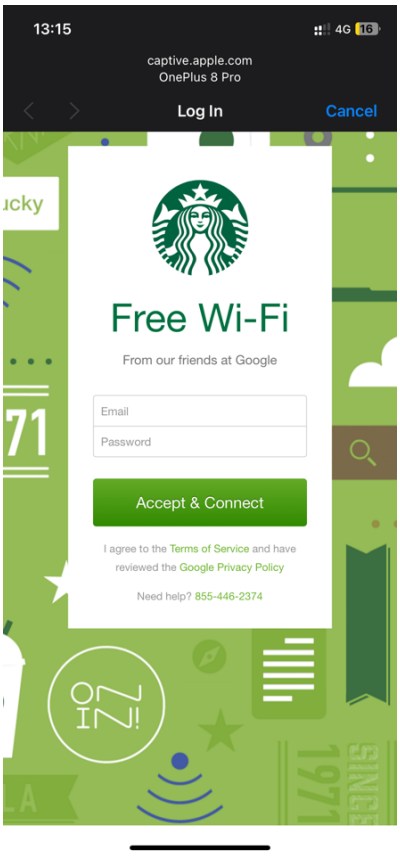

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
WiFi Pineapple
Dashboard
Recon
Clients
Tracking
Modules
Manage Modules
Filters
PineAP
Logging
Reporting
Networking
Configuration
Configuration
Allow Associations
PineAP Daemon: Enabled Switch
Autostart PineAP: Disabled Switch
Log PineAP Events
Client Connect Notifications
Client Disconnect Notifications
Capture SSIDs to Pool
Beacon Response
Broadcast SSID Pool
Beacon Response Interval Normal
Broadcast SSID Pool Normal
Source MAC 00:13:37:A6:C0:07
Target MAC FF:FF:FF:FF:FF:FF
SSID Pool
Refresh
OnePlus 8 Pro
SSID Add Remove
Pool Location /etc/pineapple/ Save


WiFi Pineapple
Dashboard
Recon
Clients
Tracking
Modules
Manage Modules
Filters
PineAP
Logging
Reporting
Networking
Configuration
Configuration
Allow Associations
PineAP Daemon: Enabled
Switch
Autostart PineAP: Disabled
Switch
Log PineAP Events
Client Connect Notifications
Client Disconnect Notifications
Capture SSIDs to Pool
Beacon Response
Broadcast SSID Pool
Beacon Response Interval
Normal
Broadcast SSID Pool
Normal
Source MAC
00:13:37:A6:C0:07
Target MAC
FF:FF:FF:FF:FF:FF
SSID Pool
Refresh
OnePlus 8 Pro
SSID
Add
Remove
Pool Location
/etc/pineapple/
Save


172.16.42.1:1471/#!/modules/ModuleManager
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
WiFi Pineapple
Dashboard
Recon
Clients
Tracking
Modules
Manage Modules
Filters
PineAP
Available Modules
Refresh
Module
Version
Description
Author
Size
Type
Action
DWall
1.4
Display's Plaintext HTTP URLs, Cookies, POST DATA, and images from browsing clients.
sebkinne
6.80K
GUI
Install
Evil Portal
3.2
An Evil Captive Portal.
newbi3
23.33K
GUI
Install
Deauth
1.7
Deauthentication attacks of all devices connected to APs nearby
whistlemaster
6.90K
GUI
Install
Site Survey
1.6
WiFi site survey
whistlemaster
10.01K
GUI
Install
Meterpreter
1.1
meterpreter configuration utility
audibleblink
2.04K
GUI
Install
SSLsplit
1.5
(FW2.5.4 or below) Perform man-in-the-middle attacks using SSLsplit
whistlemaster
6.67K
GUI
Install
get
1.2
Profile clients through the browser plugins supported by their browser
dustbyter
1.31K
GUI
Install


172.16.42.1:1471/#!/modules/EvilPortal
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
WiFi Pineapple
Dashboard
Recon
Clients
Tracking
Modules
Manage Modules
Evil Portal
Filters
PineAP
Logging
Controls
Captive Portal
Start
Start On Boot
Enable
Evil Portal Messages
No Messages.
Work Bench
Basic
Portal Name
Create New Portal
No Portals in Library to Display.
White List
Authorized Clients
Live Preview
Evil Portal Info



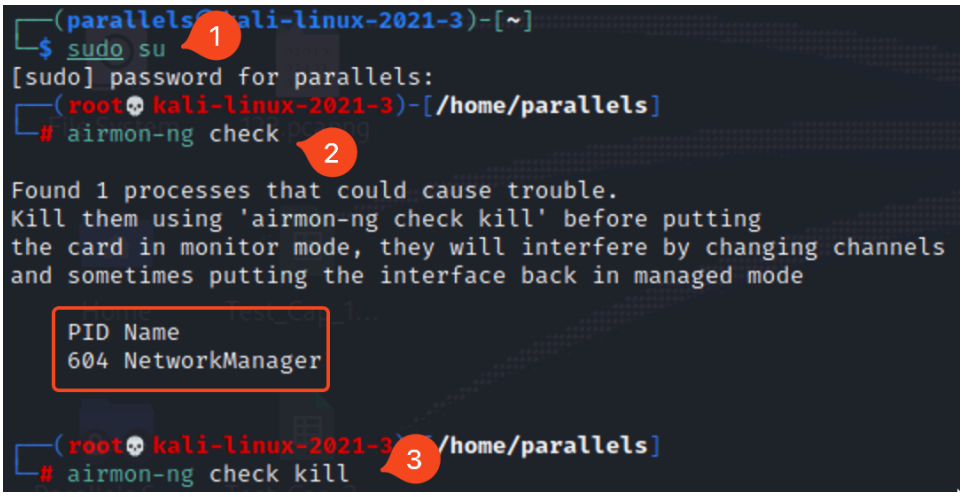


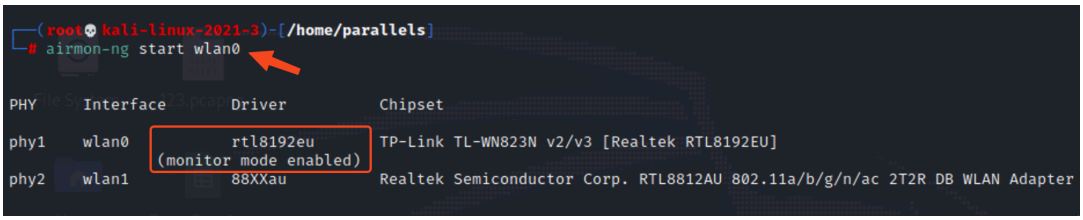
Detection script:

- Install dependencies for the script by installing the packages required by the detection script. The following packages need to be installed.
    1. **Scapy 2.4.5**
       `pip install scapy`
    2. **mac-vendor-lookup 0.1.12**
       `pip install mac-vendor-lookup`
    3. **macaddress 2.0.2**
       `pip install macaddress`
    4. **pandas 1.5.2**
       `pip install pandas`

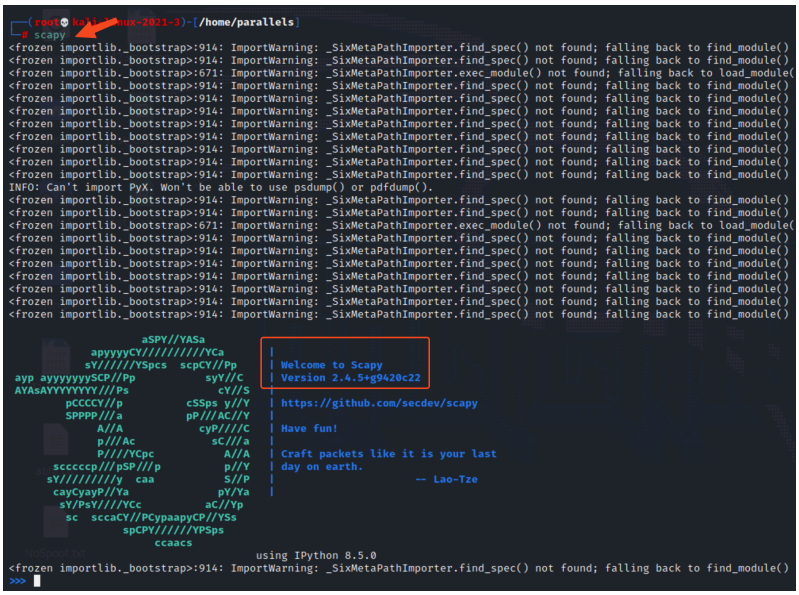
Running scapy manually:

- To run the scapy tool manually, first, open the terminal with root privileges.
- Make sure to change the mode of the wireless interface to monitor mode.
- Also, the processes we must kill the “networking” and the “NetworkManager” processes.





- Then run the command scapy to run the application.



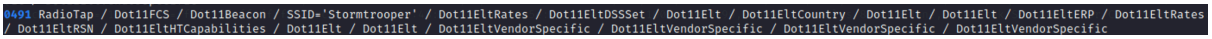
- Run the sniff() function to capture the packets by passing the name of the wireless interface in the iface parameter and an interval for the count parameter and saving the data in the pkts variable.

```
>>> pkts=sniff(iface="wlan0",count=500)
```

- The nsummary() function provides the output of the various packets captured.

```
>>> pkts.nsummary()
```

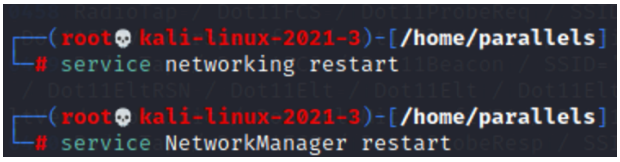
- The individual packet can be saved in the new variable “pkt.”



- We can then display the contents of the individual packet.

- To restart the services killed issue the following commands.

```
service networking restart
service NetworkManager restart
```



To run the Detection script:

- Navigate to the directory where the script is stored.
- Change the wireless interface to be used to monitor mode.
- Run the script by passing the name of the wireless interface and the interval value.
- The script will save the output in a generated .csv file.

Wireshark:

- Install Wireshark.
  ```
  sudo apt-get install Wireshark
  ```

- Open Wireshark and choose the interface to capture the packets.
- To filter out the beacon frames captured, run the following filter.

  ```
  wlan.fc.type_subtype==0x08
  ```

Note: The filter will only show beacon frames since the beacon frames are management frames and have type 0 and subtype 8.