

Tấn công kết hợp Deauthentication và Rogue Access Point

A. Chuẩn bị:

I. Công cụ:

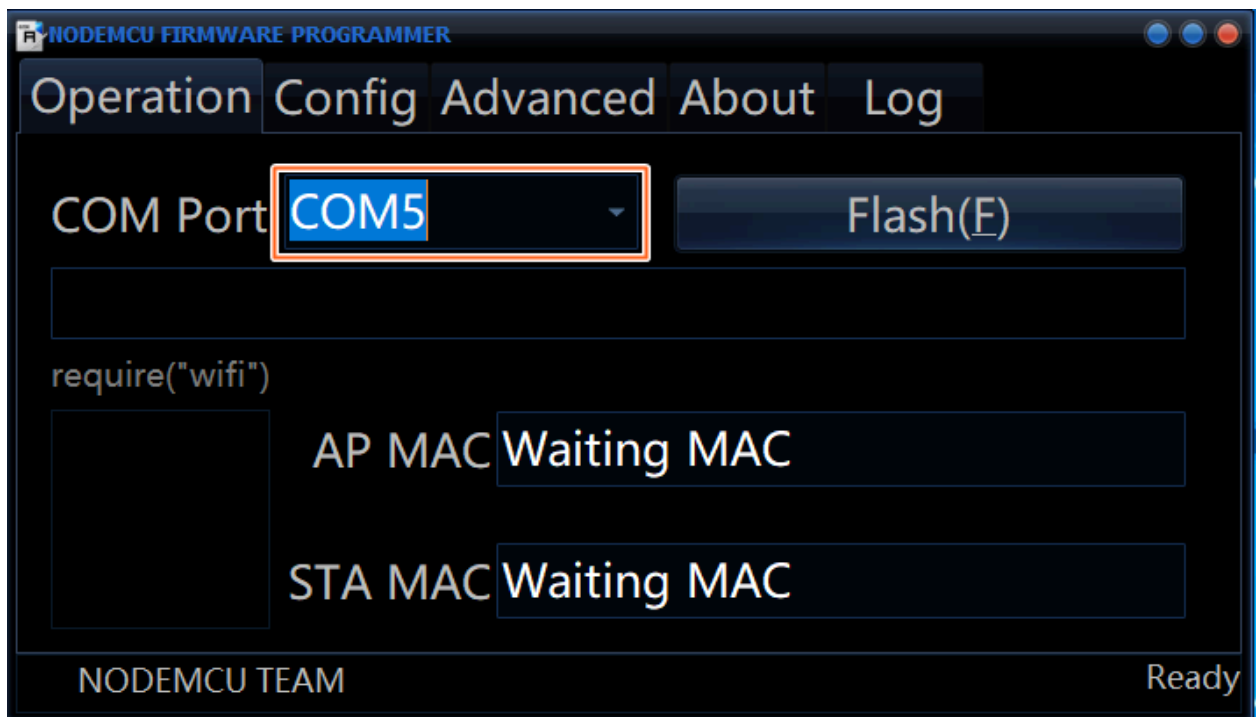
- Airmon-ng
- NodeMCU Flasher : <https://github.com/nodemcu/nodemcu-flasher>
- Captive Portal : <https://github.com/D3vKn1ght/ESP8266-Captive-Portal>
- Code demo: <https://github.com/D3vKn1ght/Wireless-Network-Security>.

II. Triển khai Captive Portal:

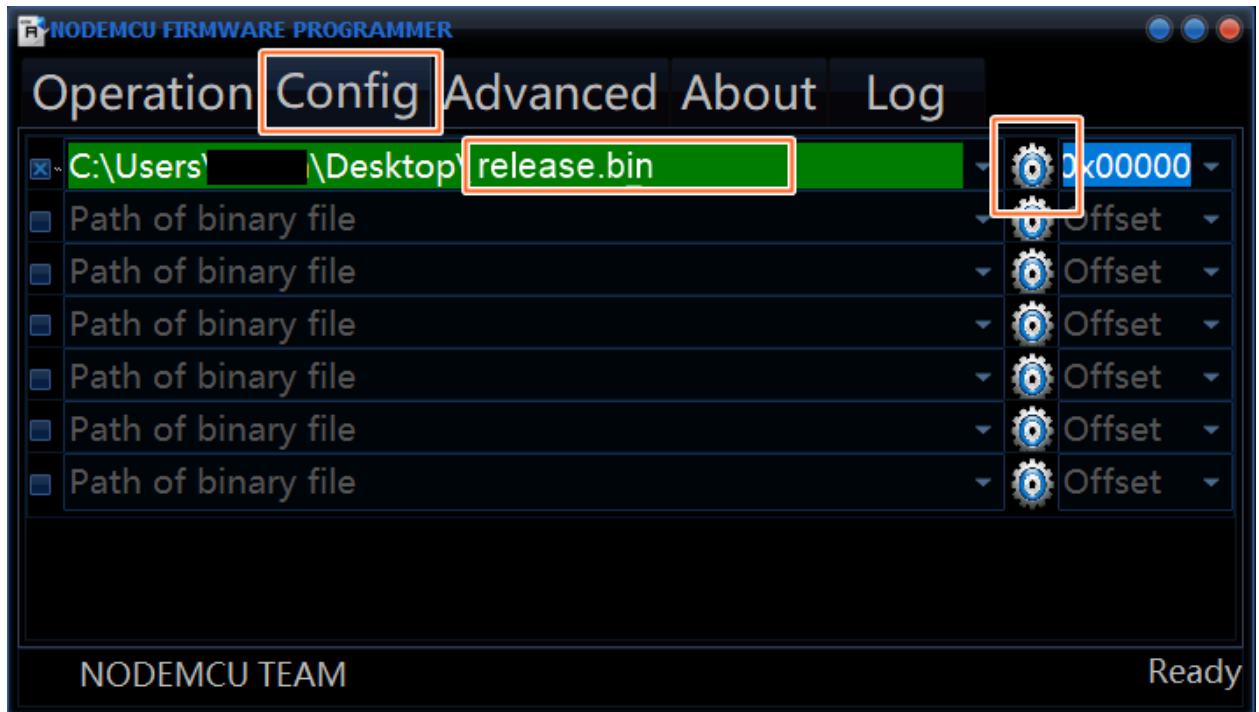
Sau khi tải source code captive portal, tiến hành nạp code vào một ESP8266.

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



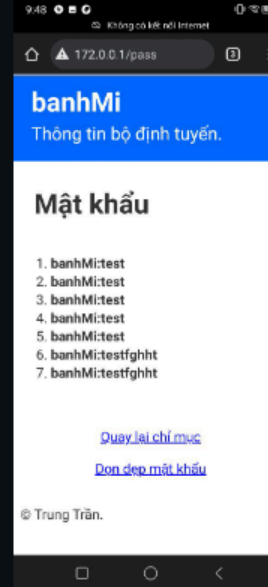

Mở **NodeMCU Flasher** kết nối với port của ESP8266.



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.

172.0.0.1/index	172.0.0.1/post	172.0.0.1/pass	172.0.0.1/ssid
This is the main page. Here the user will write his password and send it.	This is the post page. The user will be redirected here after posting the password.	This is where the attacker can retrieve all the passwords that has been posted.	Here the attacker can change the SSID name of the Access Point on the go.
			

III. Bật monitor mode wifi:

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

```

[New Branch] ~/Network-Security: git:(main) iwconfig
lo                no wireless extensions.

enp7s0            no wireless extensions.

docker0           no wireless extensions.

vmnet1            no wireless extensions.

vmnet8            no wireless extensions.

wlp0s20f3         IEEE 802.11  ESSID:"PTNATT301_5G"
                  Mode:Managed  Frequency:5.745 GHz  Access Point: 28:6C:07:66:E0:3F
                  Bit Rate=650 Mb/s   Tx-Power=22 dBm
                  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
phy0     wlp0s20f3      iwlwifi     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:

I. 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.



172.0.0.1/ssid



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:

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.



Wi-Fi



Bật



Mạng đã được kết nối



banhMi

Đăng nhập vào mạng

Mạng có sẵn



banhMi

Đã lưu



..



Access Point 01



BUFFALO-E18B48

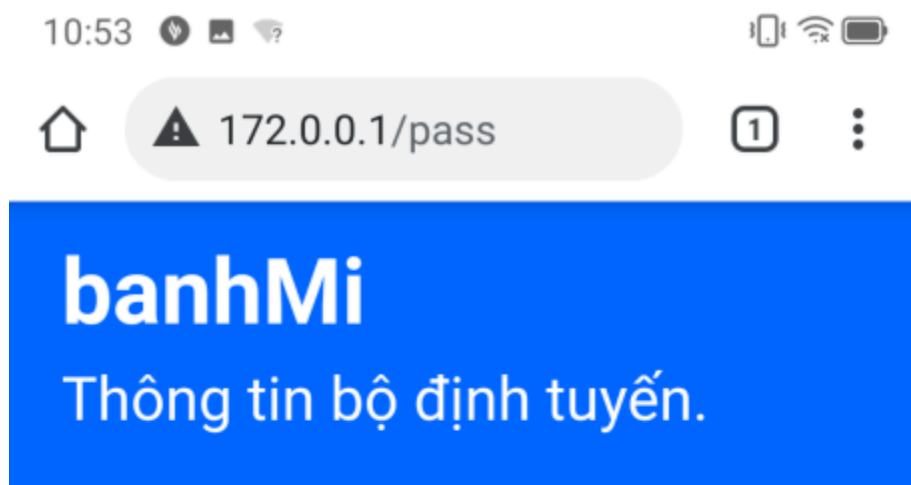


HONEYPOT



Khongbiet

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



Mật khẩu

1. **banhMi:12345678**





[Quay lại chỉ mục](#)

[Dọn dẹp mật khẩu](#)

© Trung Trần.

2. Tấn công deauthentication:

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

Name	Size	Modified	
 detect	3 items	T5	☆
 deauthen.py	1,1 kB	Yesterday	☆
 fakeaccesspoint.py	800 bytes	Yesterday	☆
 showwificlient.py	1,5 kB	Yesterday	☆

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.

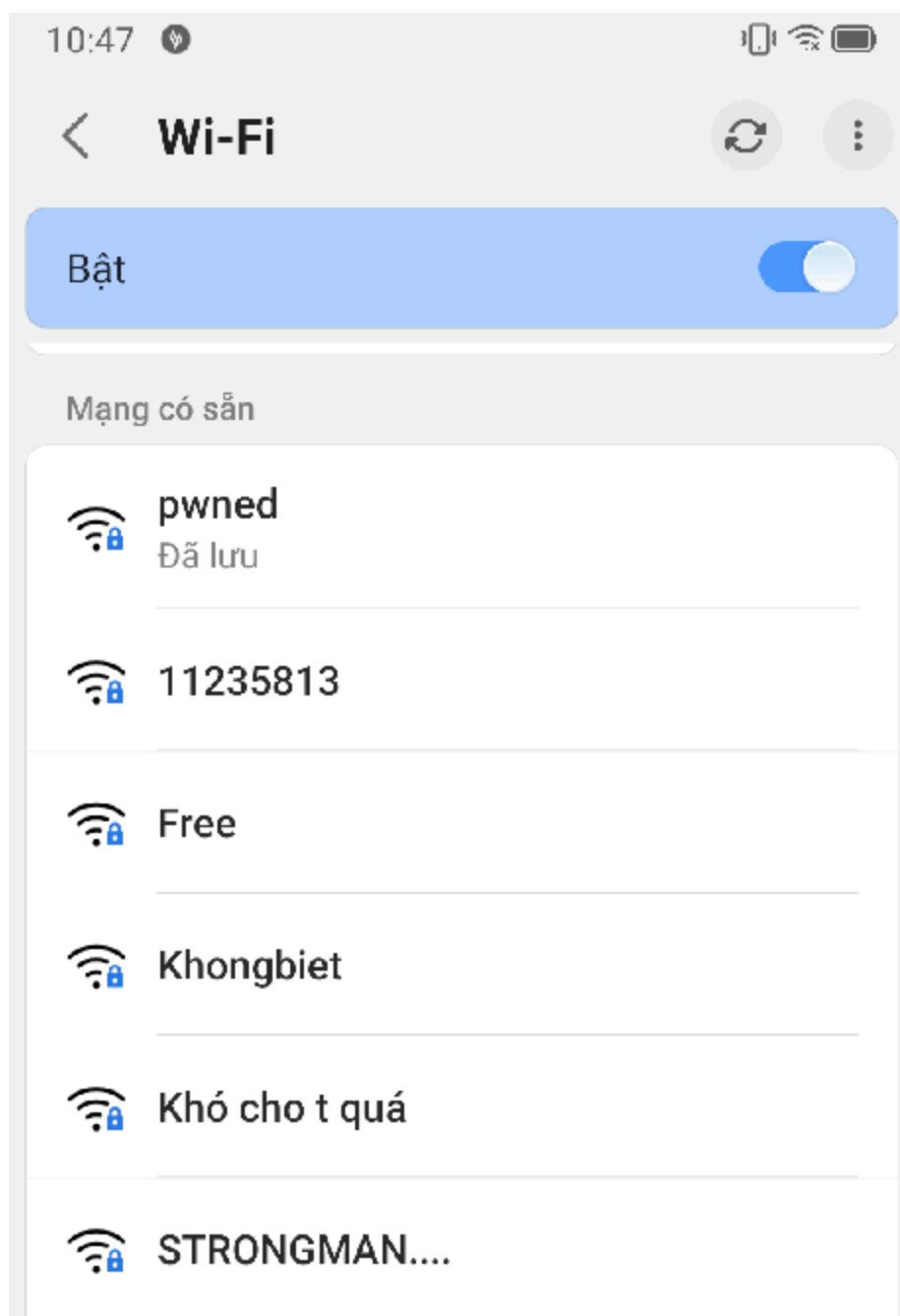
Tiến hành nhập interface mà ta thấy ở bước chuẩn bị, ở đây là wlp0s20f3mon.

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

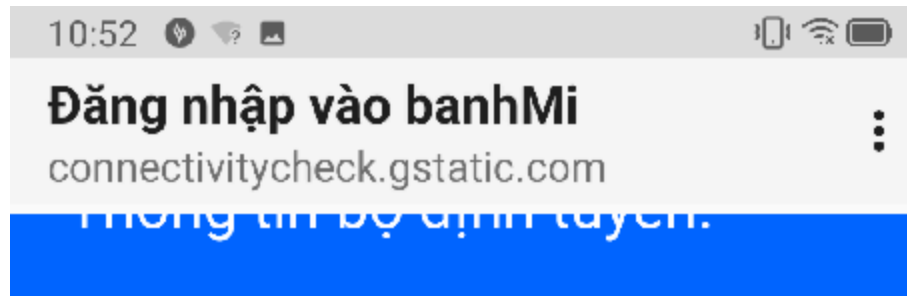
Ta có địa chỉ BSSID là **E8:48:B8:EF:5A:7C**, MAC kết nối tới điểm truy cập SSID banhMi là **00:D2:79:B3:D4:D4**:

[illegible][illegible][illegible]

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.



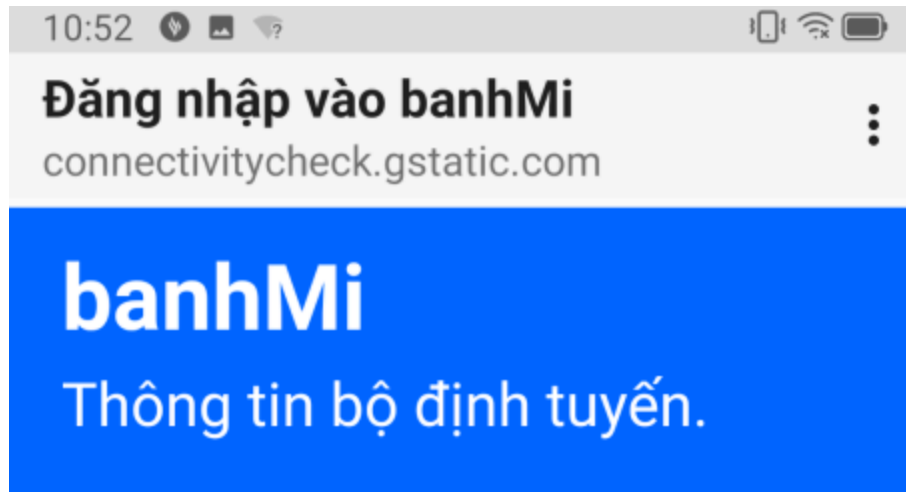
Cập nhật

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: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 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:ff, SSID: Unknown SSID
Deauth detected from 7e:05:55:c8:55:1b to ff:ff:ff:ff:ff:ff, SSID: 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
```