

NETHERCAP

PANDUAN PENGGUNA



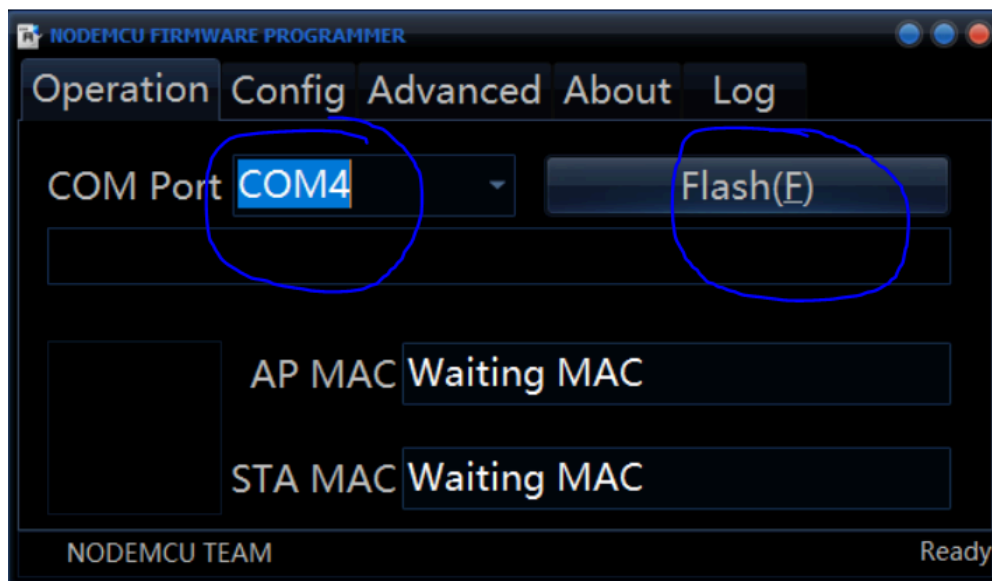
Versi 1.0.0

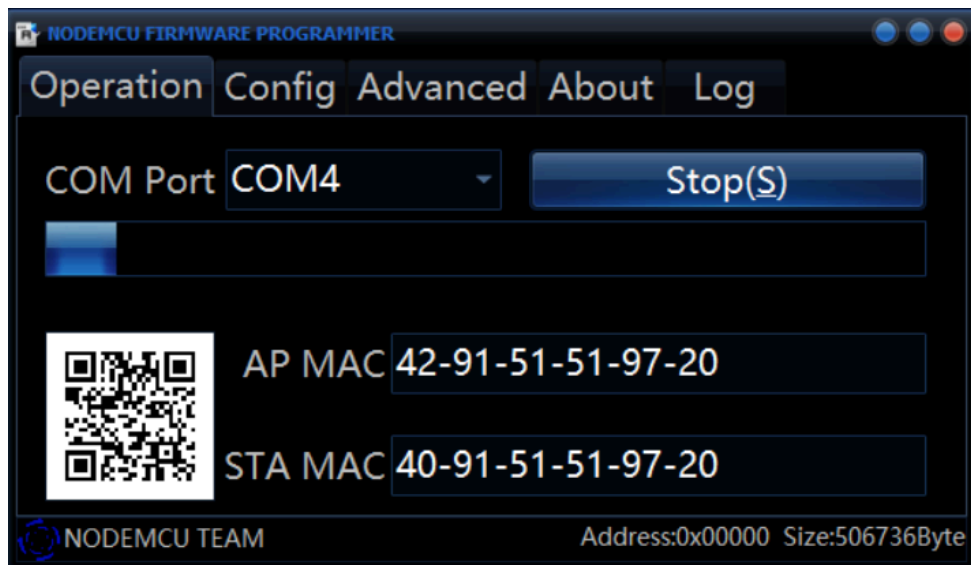
A. CARA MENGINSTALL

1. Buka laman web NETHERCAP pada link <https://github.com/Cancro29/NETHERCAP>.
2. Unduh firmware terbaru. Sesuaikan tipe driver OLED, ukuran OLED, dan ukuran memori pada ESP8266 anda.

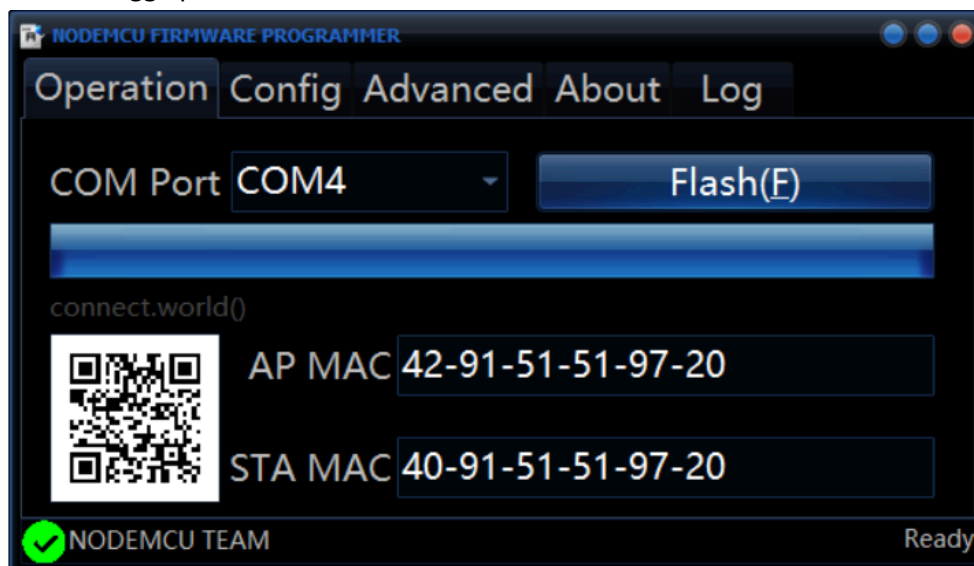
Jika menggunakan PC:

3. Pastikan PC telah terinstall driver CH340 atau CP210X.
CH340:
<https://www.arduino.cc/en/Reference/CH340>
CP210X:
<https://www.silabs.com/developers/usb-to-uart-bridge-vcp-drivers?tab=downloads>
4. Download ESP8266Flasher pada link
<https://github.com/nodemcu/nodemcu-flasher/blob/master/Win64/Release/ESP8266Flasher.exe>
5. Buka tab Config, Pilih firmware dengan mengklik tombol gear dan biarkan offset tersetting di 0x00000. Setelah itu buka tab Operation, Pilih COM Port dan klik Flash





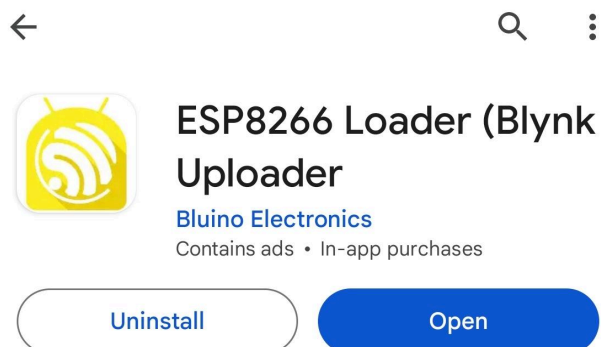
6. Tunggu proses selesai



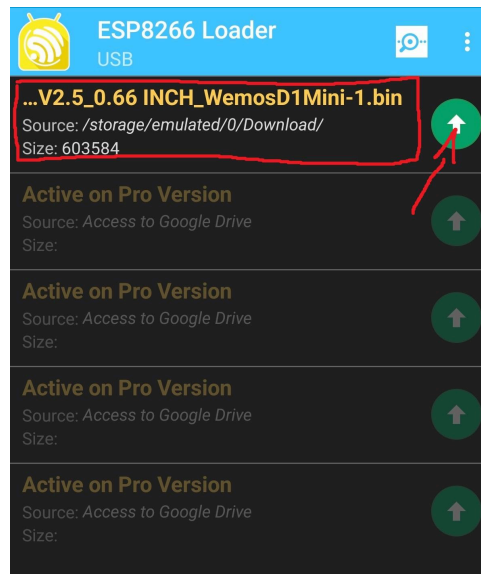
7. NETHERCAP siap digunakan

Jika menggunakan Smartphone:

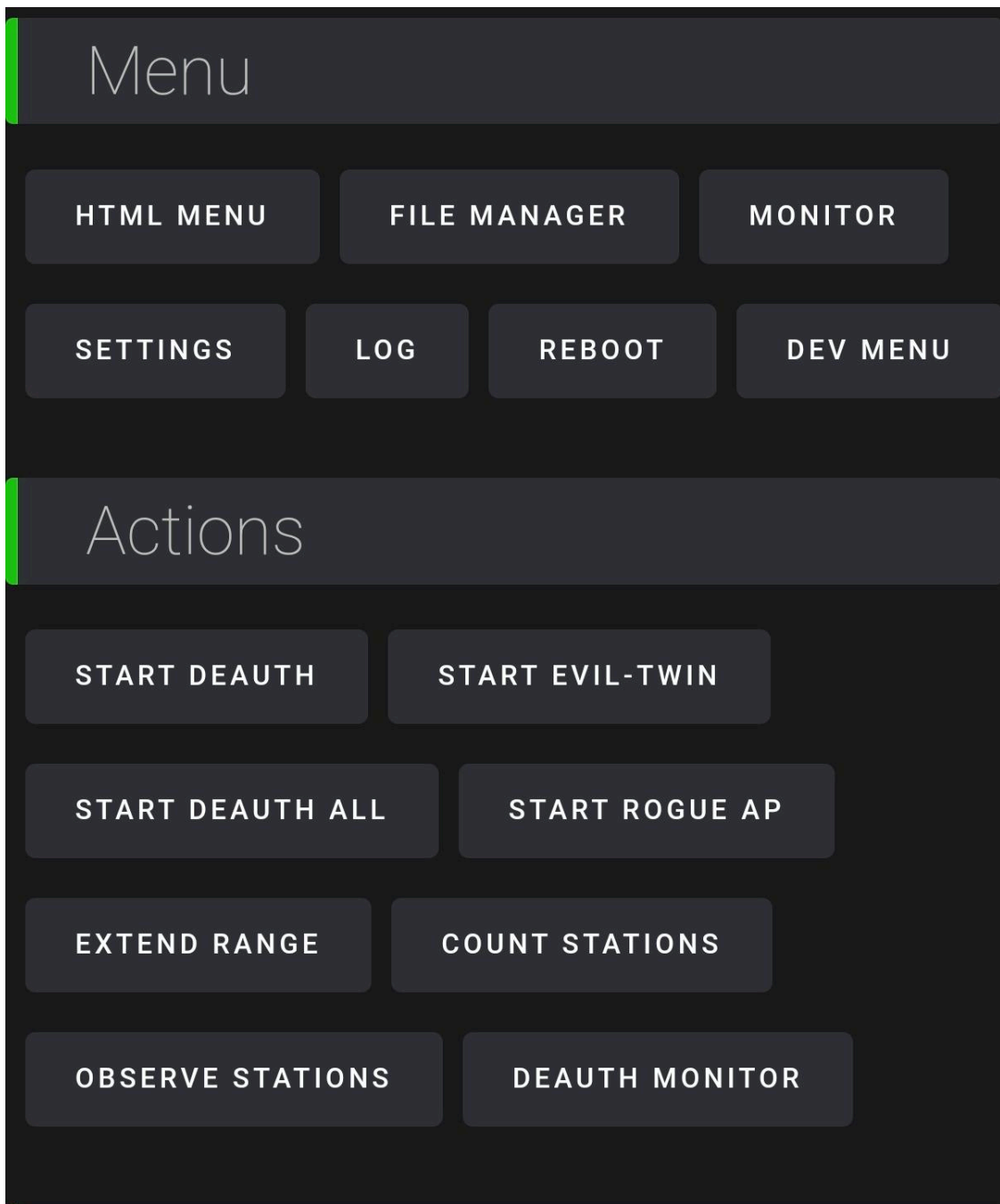
3. Unduh ESP8266 Loader dari Google Play



4. Sambungkan ESP8266 ke Smartphone yang mendukung OTG, pilih firmware dengan tap zona yang ditandai, dan tap tombol flash yang ditunjuk anak panah



B. MENU



1. HTML Menu

NETHERCAP V.2.5

BACK

MONITOR

LANGUAGE EDITOR

Rogue AP

ROGUE1

ROGUE2

ROGUE3

ROGUE4

ROGUE5

Evil-Twin

DEFAULT

ETWIN1

ETWIN2

ETWIN3

ETWIN4

ETWIN5

Preview

Error 509 : Sambungan Wi-Fi gagal.

Masukkan ulang password

Masukkan password Wi-Fi untuk melanjutkan.

Password

Lanjutkan

All rights reserved 2024

Digunakan untuk memilih halaman web dalam format HTML yang nantinya akan digunakan dalam menjalankan serangan Evil-Twin dan Rogue AP. Terdapat 5 slot halaman Rogue AP dan 5 slot halaman Evil-Twin ditambah 1 slot halaman Evil-Twin bawaan. Saat slot dipilih, akan muncul pratinjau atas halaman web yang dimaksud.

Halaman Evil-Twin dan halaman tunggu bawaan dapat dimodifikasi melalui menu “Language Editor”

LANGUAGE EDITOR

BACK

CAPTIVE PAGE

VERIFY PAGE

SAVE LANGUAGE

Error header: This is

Re-enter: how custom language

Re-enter2: works on

Submit button: you can even

Password: NETHERCAP

Additional: see the preview in real-time!

Preview

This is

how custom language

works on

NETHERCAP

you can even

see the preview in real-time!

2. File Manager

FILE MANAGER

BACK REFRESH

Total space : 2072.58 KB, free space : 2031.62 KB

Choose File No file chosen Upload

Rename

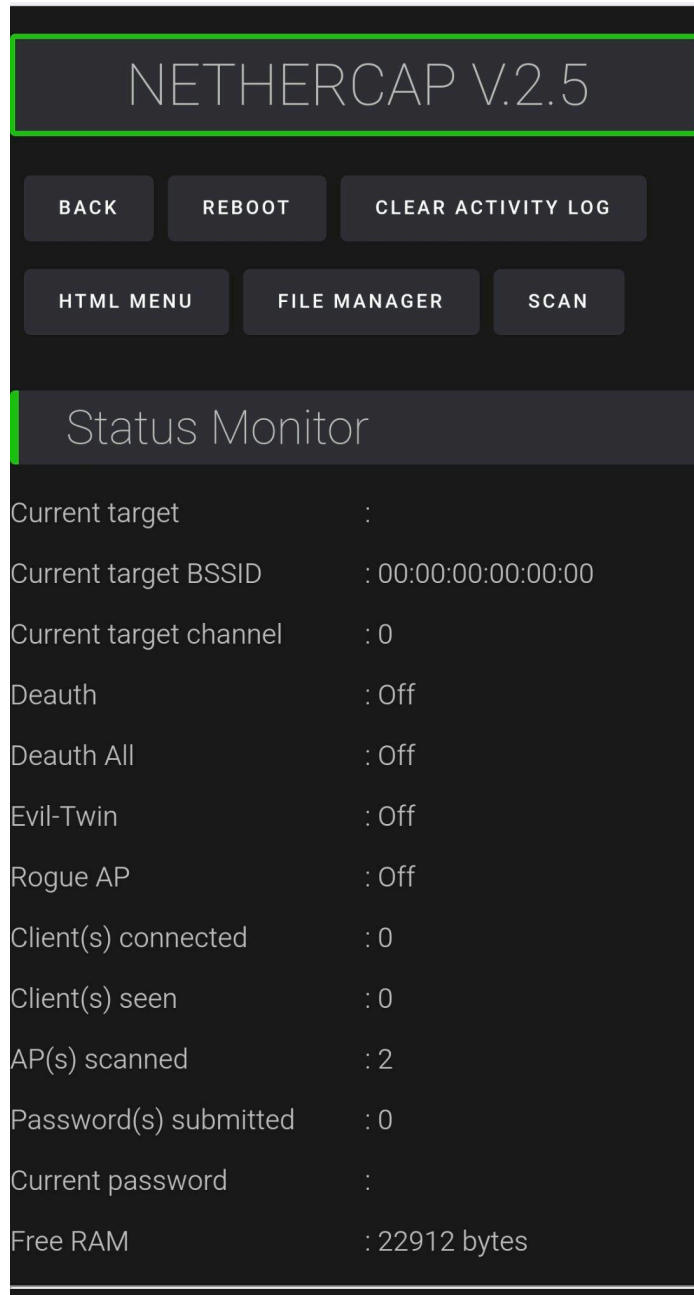
NAME	SIZE	SELECT
config.json	623.00 B	SELECT
customlanguage.json	345.00 B	SELECT
log.txt	126.00 B	SELECT

Digunakan untuk mengelola file yang disimpan dalam *SPI Flash Memory*, Anda dapat mengunggah, menamai ulang, membuka, dan menghapus file. Fitur ini melakukan perlakuan khusus terhadap file berikut:

- *.html : jika file ini dipilih, akan muncul tombol "Assign" yang dapat digunakan untuk memasukkan halaman web ke slot Evil-Twin / Rogue AP.
- *.bin : jika file ini dipilih, akan muncul tombol "Flash" yang dapat digunakan untuk memperbarui firmware atau memasang firmware lainnya. Harap diingat bahwa fitur ini memerlukan ruang kosong minimal sebesar 900 kb.
- jquery-min.js : digunakan untuk mengaktifkan fitur "Text Editor", fitur ini dapat digunakan untuk mengedit file HTML secara langsung dari File Manager.

3. Monitor

Digunakan untuk memantau aktivitas dan keadaan. Terdapat informasi mengenai target dan jejak aktivitas serangan (jika ada).



4. Settings

The image shows a two-column interface for the 'Evil-Twin' settings. The left column contains the main settings menu, and the right column shows the details for the 'Powersave Mode' setting.

SETTINGS

BACK RESET SETTINGS HIDE SSID

MAC: 40:91:51:51:97:C8

Language

Set language for default fake captive page

ENGLISH **INDONESIAN** CUSTOM

LED Blink

Set internal LED on/off (requires restart)

ON OFF

Auto Resume

If set on, it will attempt to continue current attack after power loss

ON OFF

Powersave Mode

Enters deep sleep after 2 hours of inactivity

ON OFF

Display

Set how long the OLED stays on when there's no activity.

Display Sleep (ms): 60000

Rogue AP

Rogue AP SSID: Free Wifi

Access Point

AP SSID: NETHERCAP2

AP Password: deauther

Extender

Extender SSID: NETHERCAP_extend

Extender Password: deauther

Extender Connect Timeout (s): 30

a. Language

Setel bahasa pada halaman Evil-Twin bawaan beserta halaman tunggu. Saat ini mendukung Bahasa Indonesia, Bahasa Inggris, dan bahasa kustom.

b. LED Blink

Hidupkan/matikan lampu LED bawaan. Hasil pengaturan akan efektif setelah dilakukan restart.

c. Auto Resume

Jika aktif, serangan Evil-Twin/Rogue AP secara otomatis berlanjut setelah ESP8266 mati secara tidak sengaja, seperti aliran listrik yang terputus. Sesaat setelah menyala, lampu LED akan berkedip selama 10 detik untuk mengkonfirmasi apakah serangan akan

berlanjut atau tidak. Tekan tombol reset selama periode ini untuk membatalkan serangan.

d. Powersave Mode

Jika aktif, ESP8266 akan mati secara otomatis dalam waktu 2 jam jika tidak ada aktivitas. Fitur ini berguna untuk mencegah konsumsi daya yang berlebihan pada baterai.

e. Display

Setel waktu yang dibutuhkan untuk mematikan layar saat tidak ada aktivitas (dalam satuan waktu milidetik).

f. Rogue AP

Setel nama hotspot yang akan digunakan dalam serangan Rogue AP.

g. Access Point

Setel nama hotspot dan password yang digunakan untuk mengoperasikan NETHERCAP.

h. Extender

Setel nama dan password pada hotspot extender.

5. Log

Digunakan untuk melihat jejak aktivitas. Hal-hal yang direkam dalam menu ini adalah sebagai berikut:

- Password Evil-Twin
- Password Rogue AP
- Hasil pemindaian dari fitur "Observe Station" dan "Count Stations"

6. Reboot

Digunakan untuk memulai ulang ESP8266.

C. Actions

1. Deauth

Memutuskan sambungan hotspot target yang berjumlah 1 atau lebih. Setiap router memiliki tingkat ketahanan terhadap serangan deauth, jadi tidak semua router dapat dilakukan serangan deauth.

2. Evil-Twin

Membuat hotspot baru dengan nama yang sama dengan nama hotspot target. Hotspot tersebut tidak memiliki password dan terpasang Captive Portal. Jika seseorang tersambung dengan hotspot ini, maka akan muncul halaman web palsu yang meminta password hotspot yang asli.

3. Deauth All

Memutuskan sambungan semua hotspot yang terdapat pada tabel Target. Daftar target diperbarui setiap menit.

4. Rogue AP

Membuat hotspot baru dengan Captive Portal yang bertujuan untuk meminta informasi sensitif ke pihak yang terhubung.

5. Extend Range

Menyebarkan ulang sambungan Wi-Fi dengan nama hotspot yang lain dengan bandwidth maksimal 5 mbit/detik.

6. Observe Stations

Melakukan pemindaian secara menyeluruh terhadap hotspot sekitar, dan menghitung berapa banyak pengguna yang terhubung ke masing-masing hotspot.

7. Deauth Monitor

Digunakan untuk memantau paket deauth. Jika jumlah paket deauth yang diterima tidak normal, lampu LED akan berkedip dan layar akan menampilkan teks "Deauth" serta muncul nama hotspot yang terkena serangan deauth tersebut.