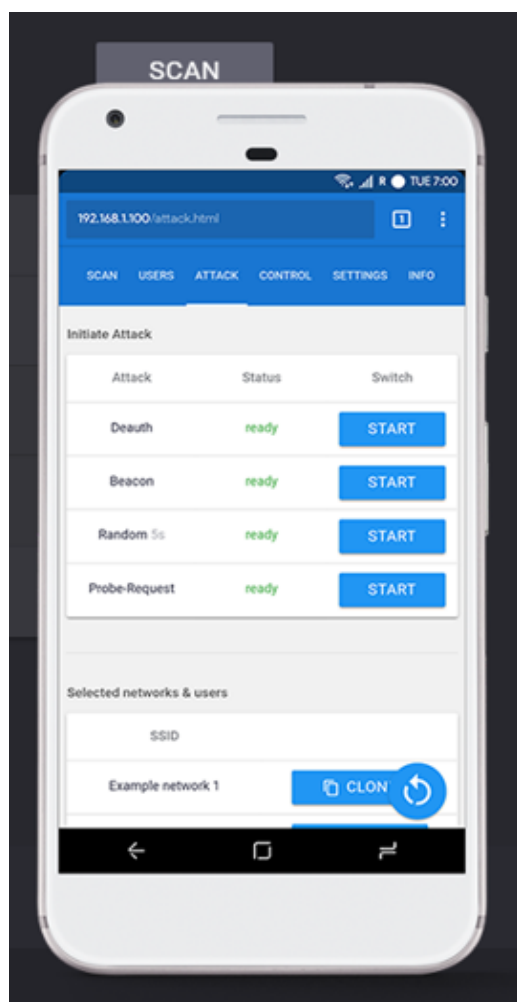




WiFi Deauther RR

WiFi Deauther



Modo de uso

O que é um wifi Deauther? É um dispositivo para teste de desautenticação Wi-Fi, em equipamentos que utilizam o protocolo de comunicação Wpa2, Wpa, cujo qual possuem uma vulnerabilidade antiga.

Um ataque de desautenticação geralmente é confundido com interferência de Wi-Fi (Ataque Jamming, que na grande maioria dos países, assim como no Brasil, é um crime grave, por colocar a sociedade em risco), a confusão acontece pois ambos impedem que os usuários acessem redes Wi-Fi, porém o Wi-Fi Deauther utiliza de vulnerabilidades dos roteadores e afins, **não** impedindo a comunicação de radios, aviões, telefones, comunicação com a polícia etc., com isso o seu uso para testes **em ambiente controlado NÃO** É identificado como **CRIME**.

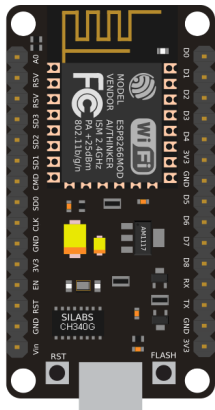
***** ATENÇÃO:** Qualquer teste realizado fora de

um ambiente controlado ou um laboratório pode ser retratado como crime. Então seu uso deve ser apenas para estudos.

Pode ser somado com diversos testes, como engenharia social por exemplo.

Especificações abaixo:

Hardware



NODEMCU driver CH340 com modulo Wi-Fi ESP8266

O Hardware já vem configurado pronto para uso.

Para ser utilizado, você precisará conectá-lo ou em um Power Bank ou diretamente em seu computador.

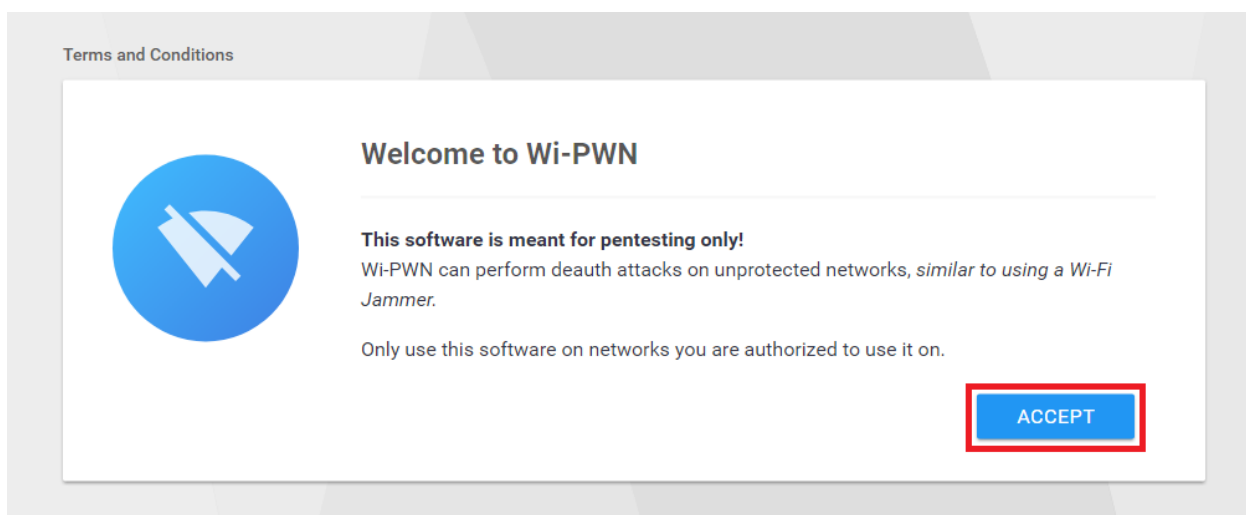
PS: Não conectar em fonte de carregamento de celulares devido a amperagem de carregadores mais modernos serem altas, os tais chamados Super Charger ou os Turbo Charges, carregadores turbos. Eles podem superaquecer o dispositivo causando a deficiência de alguns componentes, e perda do dispositivo, sendo considerado mau uso.

Software

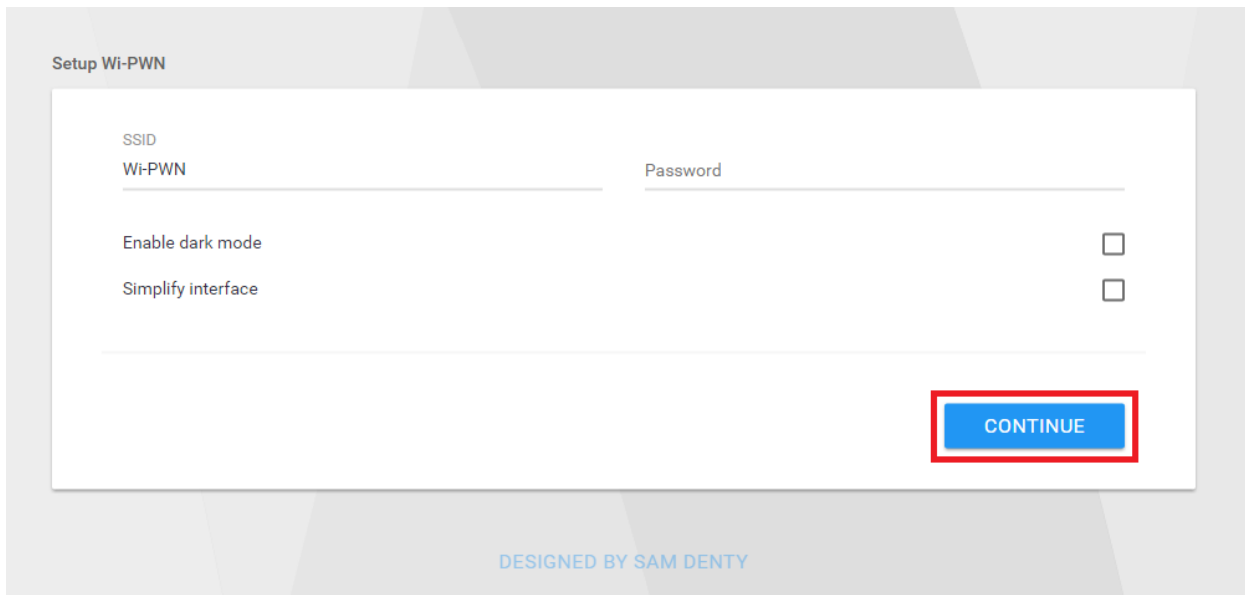
O Software utilizado foi o WiFi-PWN open source que pode ser encontrado na internet onde vc pode reconfigurar seu dispositivo.

Como utilizar

1. Conecte seu ESP8266 a uma fonte de alimentação USB (você pode alimentá-lo com seu telefone usando um cabo OTG)
2. Procure redes Wi-Fi no seu dispositivo e conecte-se Wi-PWN(sem senha por padrão).
3. Uma vez conectado, abra seu navegador e vá para <http://192.168.4.1>
4. Clique em ACCEPT para aceitar os Termos e Condições



5. Especifique um SSID e senha para o Wi-PWN usar e clique em CONTINUE **ATENÇÃO:**
Anote a senha para não esquecer



Setup Wi-PWN

SSID
Wi-PWN

Password

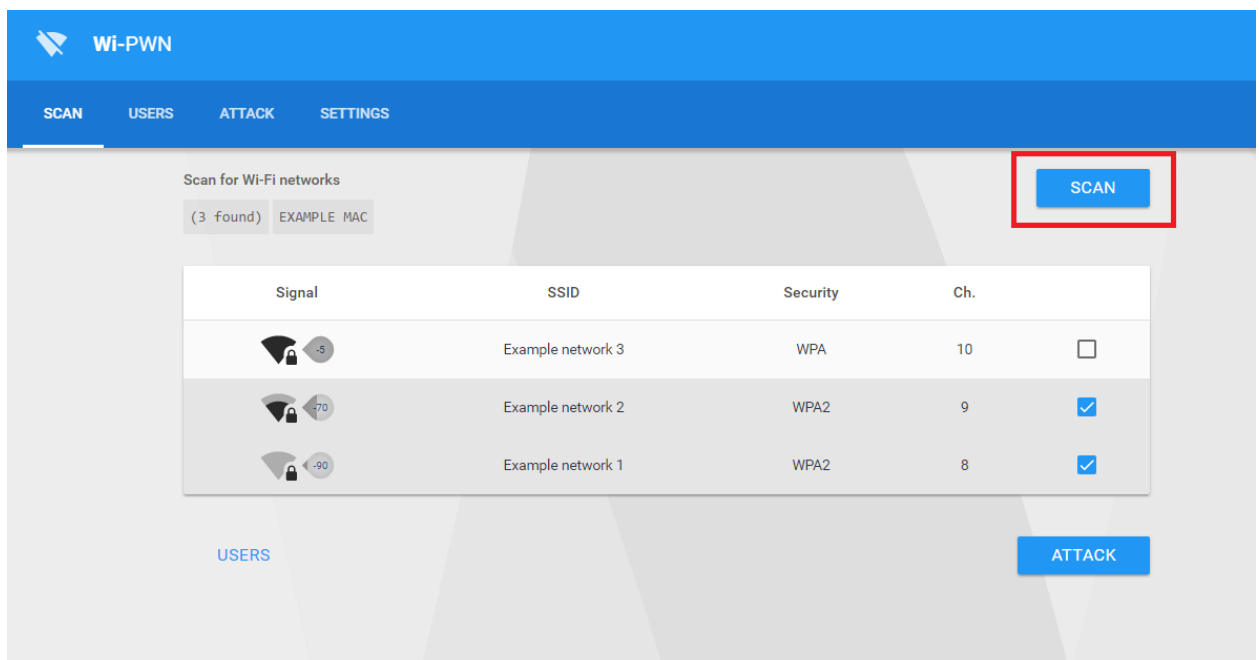
Enable dark mode ☐

Simplify interface ☐

CONTINUE

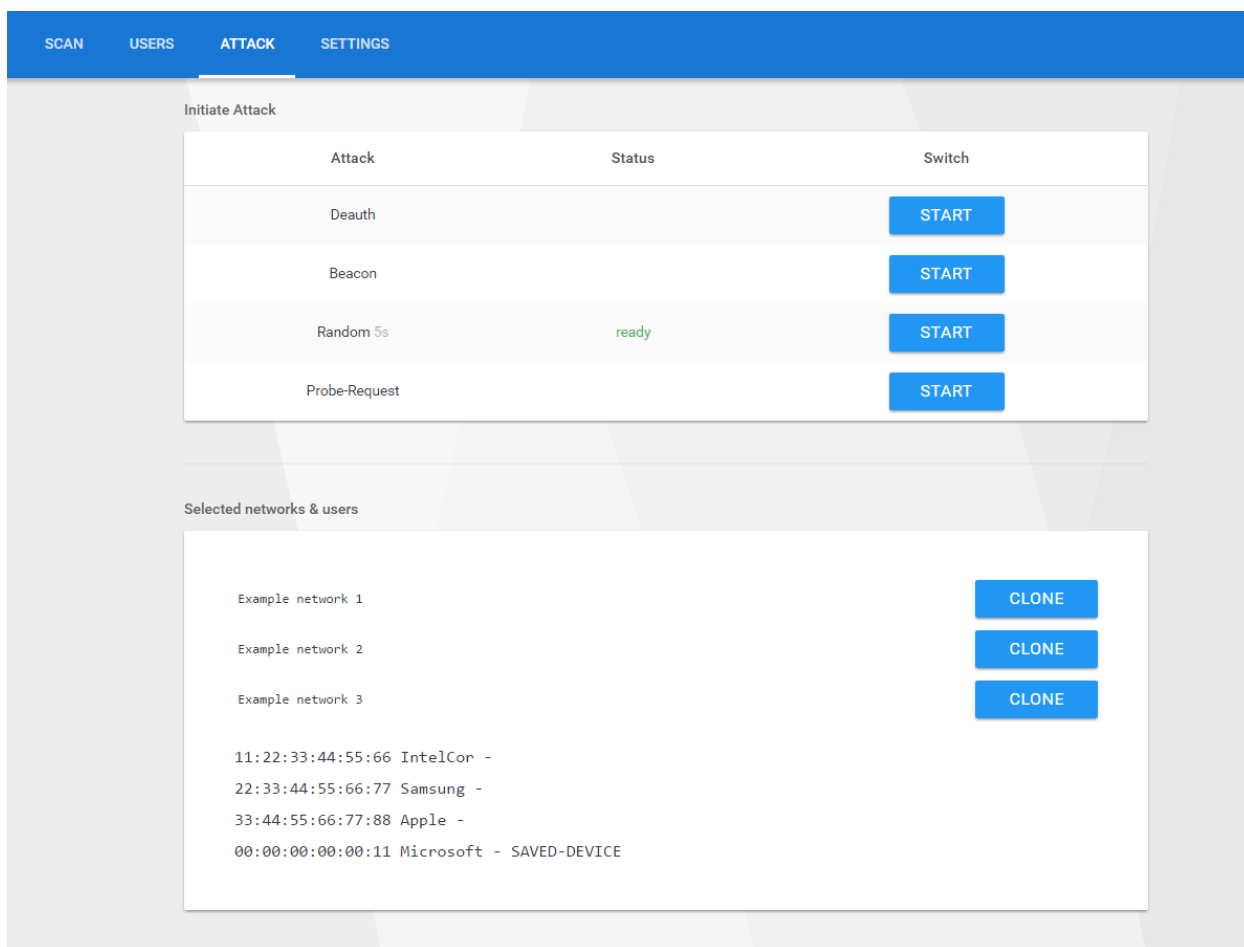
DESIGNED BY SAM DENTY

6. Reconecte-se à nova rede usando o SSID e a senha que você especificou na etapa anterior.
7. Volte para o seu navegador e a página deve recarregar (abra <http://192.168.4.1> novamente se a página não recarregar)
8. Clique no botão Scan para procurar redes Wi-Fi Nota: Talvez seja necessário reconectar-se à rede Wi-Fi.



9. Selecione a(s) rede(s) WiFi em que deseja realizar o ataque. Quando terminar, clique no Attackbotão

10. Selecione o ataque que deseja realizar



Perguntas frequentes

- Só é capaz de se conectar à rede Wi-Fi em alguns dispositivos!?!

R: Isso acontece devido a um conflito de canal. Basta navegar para 192.168.4.1/settings.html em um dispositivo capaz de se conectar à rede Wi-Fi e alterar o número do canal de 1 para qualquer número até 14.

espcomm_sync failed/ espcomm_openao carregar

- A ferramenta de upload ESP não pode se comunicar com o chip.

R: Reconecte o chip usando uma porta USB e um cabo diferentes.

Instale os drivers USB (cp2102 ou ch340).

Certifique-se de que a porta COM correta esteja selecionada.

- Os SSIDs não carregam? (Sem botão de limpar)

R: Tente redefinir a lista SSID visitando 192.168.4.1/clearSSID.json enquanto estiver conectado ao seu ESP.