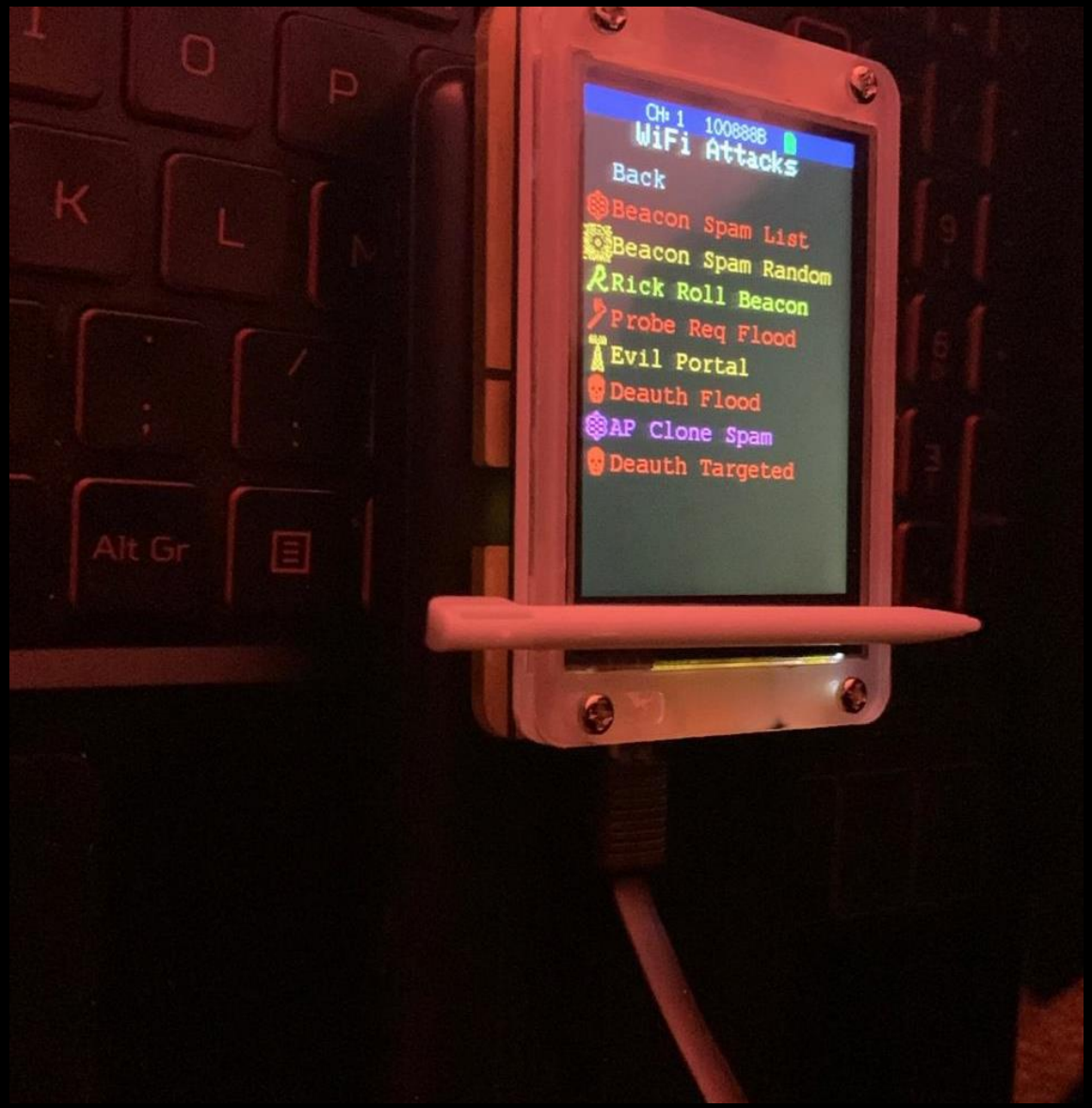


ESP32 MARAUDER

BOUSSETA HATIM

CYBERSECURITY & EMBEDDED SYSTEMS STUDENT . @ENSA-TETOUAN

WHAT IS ESP32 ?

-ESP32 is a low-cost System on Chip (SoC) Microcontroller from Espressif Systems .

-With built-in Wi-Fi and Bluetooth.

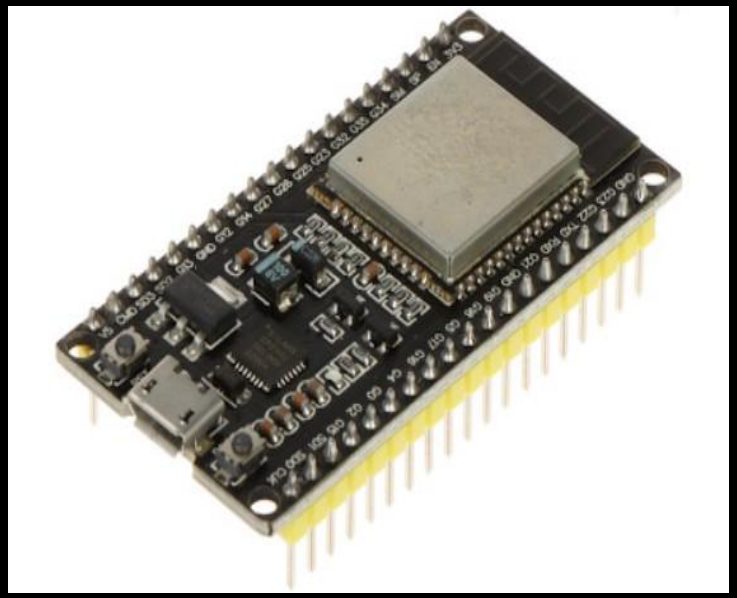
-It features a dual-core processor, offering more power than traditional MCUs like Arduino.

-The ESP32 is perfect for IoT, embedded systems, and cybersecurity projects, with low power consumption and advanced features.

-The ESP32 is like the "brain" of many smart devices you see today (e.g., smart lights, fitness trackers, weather sensors). It’s a tiny, affordable .

-The ESP32 is more than Just an MCU.

-Think of it as a Swiss Army knife for building DIY projects.



ESP32 Security & Development :

Security features :

- **Wi-Fi Security**: Supports WPA/WPA2/WAPI.

- **Hardware Protection** :
  - Secure boot (prevents unauthorized firmware).
  - Flash encryption (keeps code/data safe).
  - Cryptographic acceleration (AES, SHA-2, RSA, ECC).
  - True Random Number Generator (RNG).

- **Development Support** :
  - **Free SDK** for easy programming.
  - Open-source GCC toolchain.
  - Quick firmware updates.

ESP32 Applications + Cybersecurity Projects:

The ESP32 is perfect for **IoT, automation, audio, and security projects.**

Cybersecurity Projects :

- **Network Security Monitor** (detect Wi-Fi intrusions)
- **Secure IoT Gateway** (encrypted data transfer)
- **Encrypted Communication Hub** (VPN/SSL endpoint)
- **Secure Smart Lock System** (biometric + encrypted access)
- **Wi-Fi Penetration Testing Tool** (Bruce , marauder…)

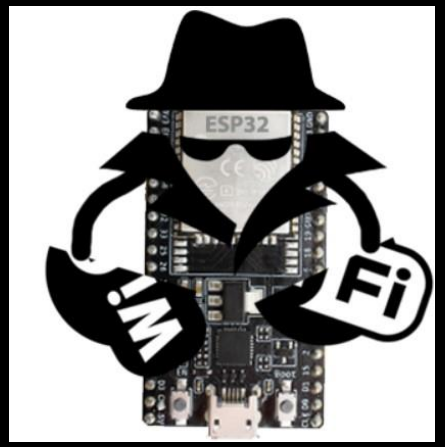
(which is our project today)

Smart Home & Automation

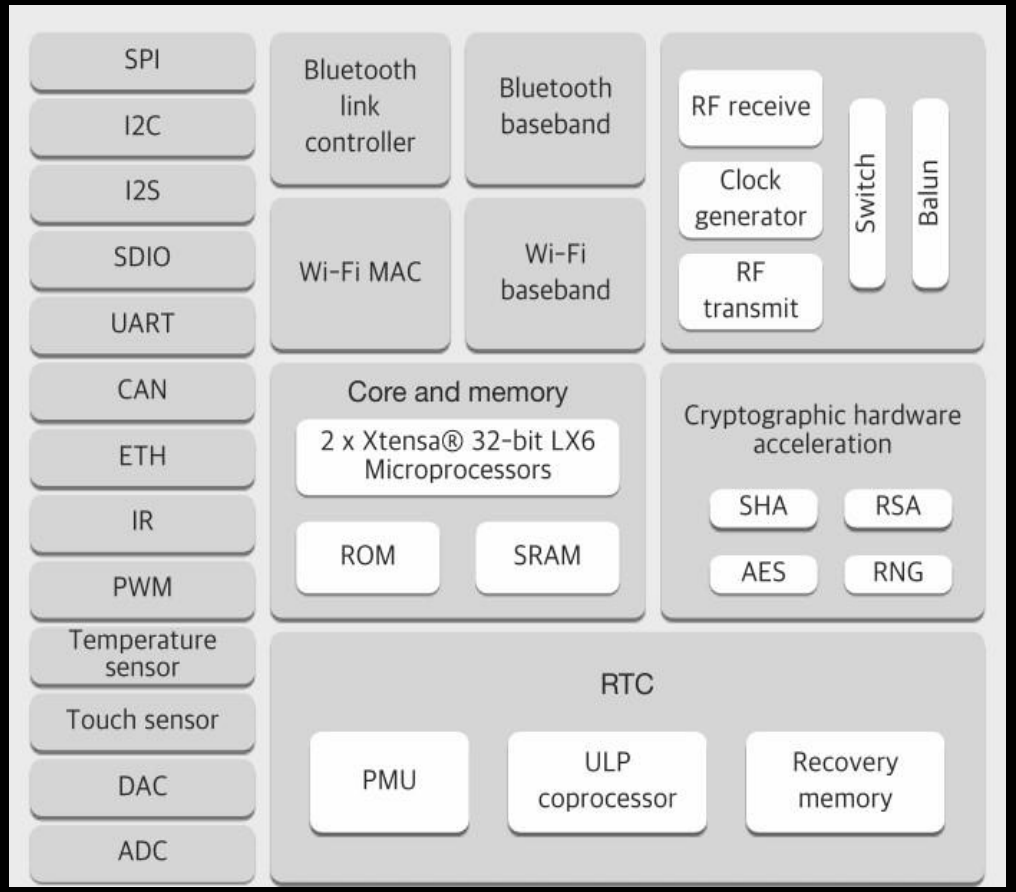
- Smart plugs, home automation, intrusion detection with **secure remote control**

IoT & Sensors

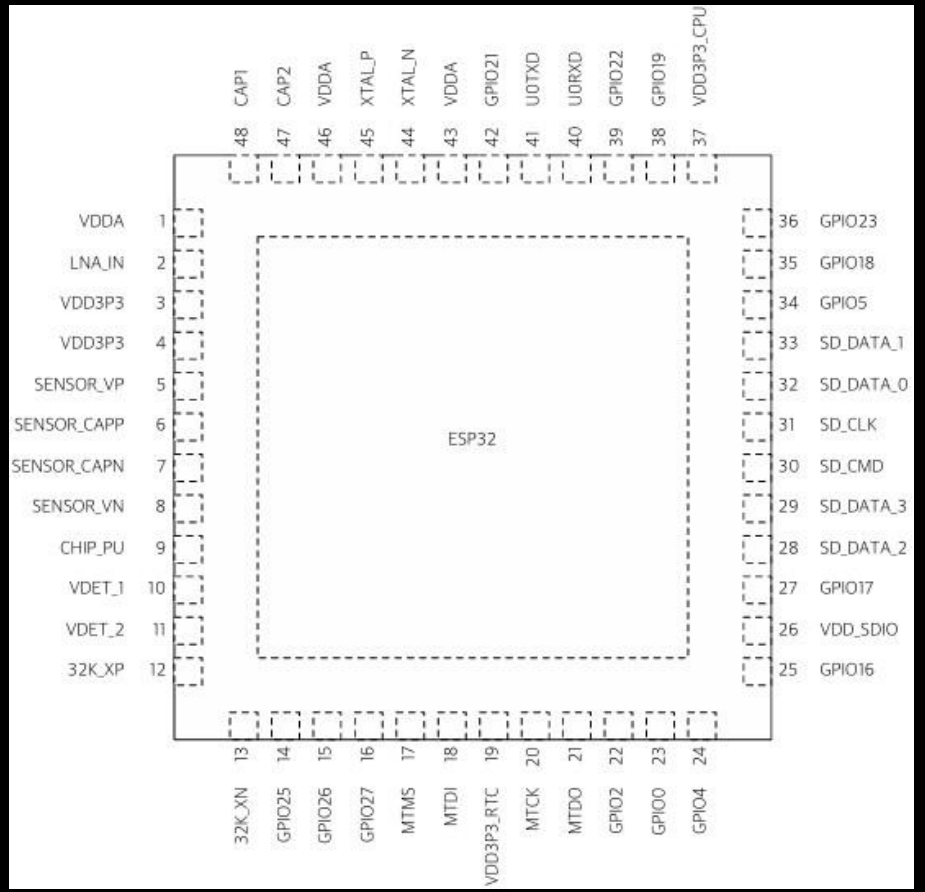
- **Encrypted** wearable health trackers, **tamper-proof** industrial sensors



BLOCK DIAGRAM :



PIN LAYOUT :



ESP32 Series Overview:

ESP32 has multiple series, each catering to different needs . For exemple :

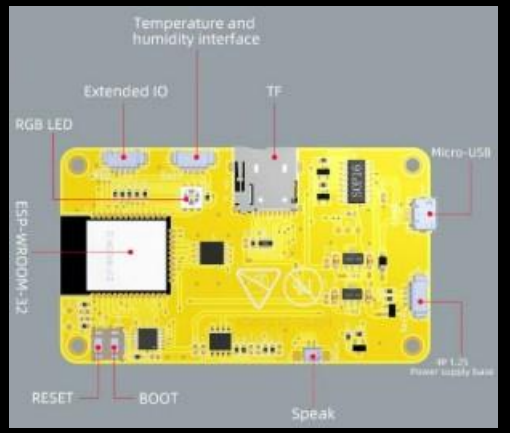
- **ESP32-C3**: Cheapest option with Wi-Fi/BLE.
- **ESP32-S2**: Best for USB support.
- **ESP32-S3**: Ideal for AI/ML projects.
- **ESP32-C6**: Futureproof with Wi-Fi 6.
- **ESP32-WROOM**: Perfect for classic DIY projects.

ESP32 CYD (Cheap Yellow Display):

- Known as the **ESP32 2432S028.**

- S**mall** development module that integrates a **2.4-inch or larger TFT touchscreen display** with an **ESP32 microcontroller**.

- This **all-in-one** module is popular for its **cheap price.**



MARAUDER :

• **Marauder** is a firmware for **ESP32** that turns it into a powerful **Wi-Fi & BLUETOOTH attack , security tool**.

•Commonly used for **penetration testing and cybersecurity research.**

•**ESP32 Marauder** was created by @**JustCallMeKoko**, a cybersecurity researcher and developer.

•[GitHub - justcallmekoko/ESP32Marauder: A suite of WiFi/Bluetooth offensive and defensive tools for the ESP32]

•(https://github.com/justcallmekoko/ESP32Marauder)

Building the ESP32 Marauder:

Minimum Requirements:

- **ESP32-WROOM**
- **TFT Screen**
- Or just a cheap yellow display, **ESP32 CYD. (used in this project)**
- **SD Card**
- **Small Battery** or **Power Bank.**
- **SD card USB adapter .**

Optional:
- **GPS**
- **Case (for protection)**
- **Antenna**

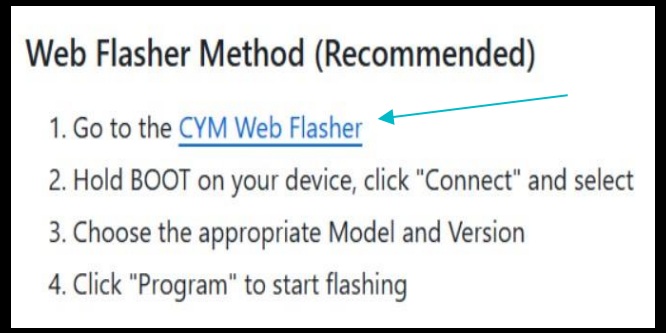
This is the simplest method we'll explore to build the ESP32 Marauder.

STEPS :

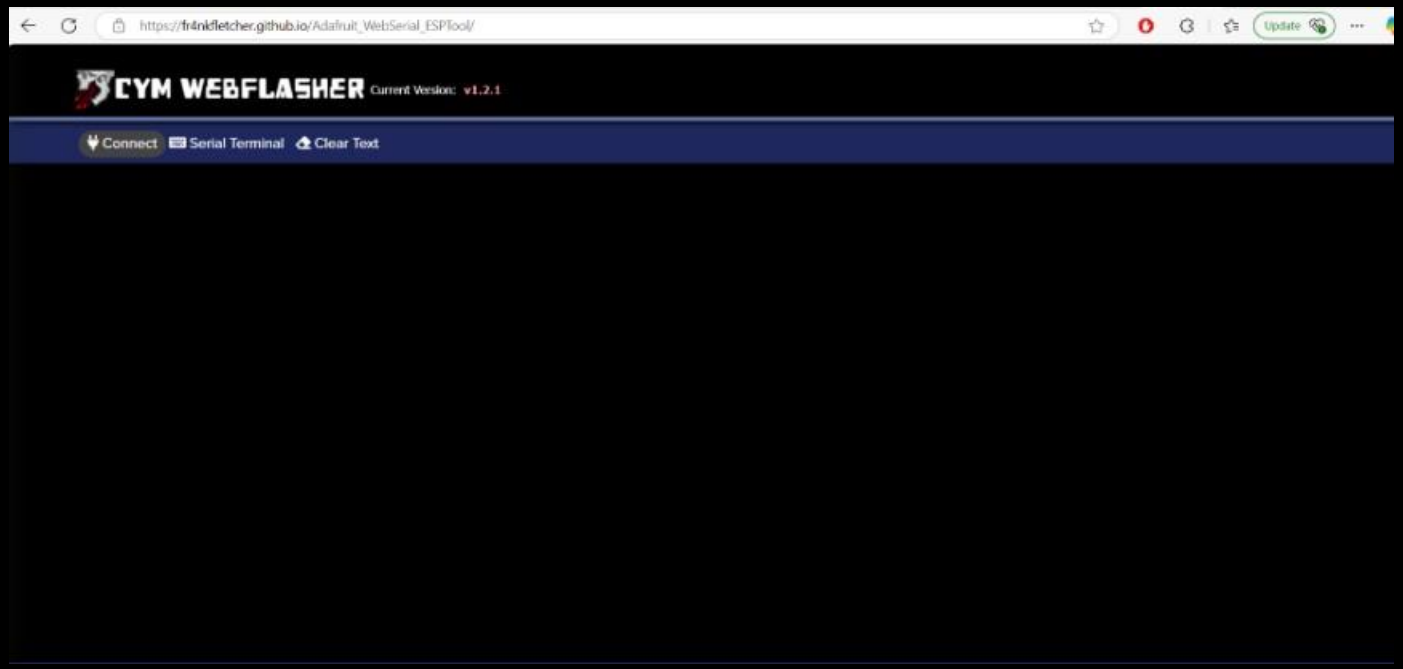
- **Connect the ESP32 CYD** to your computer.

- Go to the following GitHub page:
[GitHub - Fr4nkFletcher/ESP32-Marauder-Cheap-Yellow-Display]

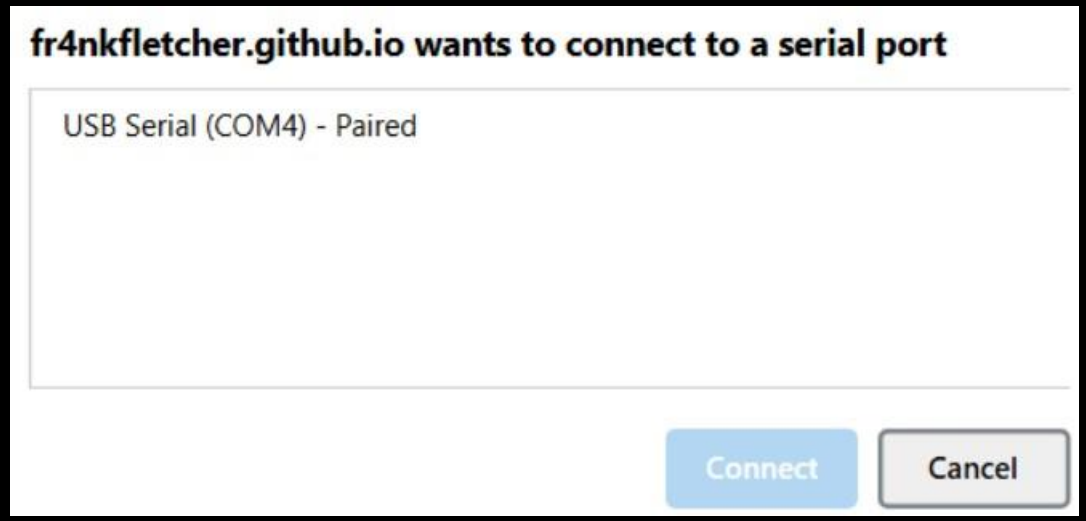
- Go to the CYM Web Flasher .



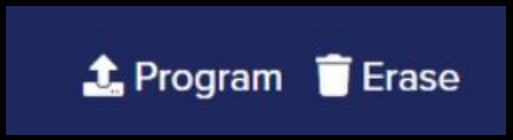
-


https://fr4nkfletcher.github.io/Adafruit_WebSerial_ESPTool/
Update
CYM WEBFLASHER
Current Version: v1.2.1
Connect
Serial Terminal
Clear Text

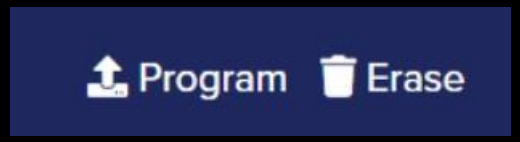
- Connect :


fr4nkfletcher.github.io wants to connect to a serial port
USB Serial (COM4) - Paired
Connect
Cancel

- Click **Erase** to clear the flash memory of the ESP32 before flashing the firmware



- **Choose the right board and version :**

- **Program :** 

- **Unplug** the ESP32 and **plug it back in**.

- **Boom!** It’s working! You should now have the ESP32 Marauder running on your device.

WIFI ATTACKS AND SNIFFERS :

- Wireless_Basics_and_concepts.pdf

- **ESP32 Marauder includes several sniffing capabilities that allow monitoring and analyzing Wi-Fi traffic :**

1. Probe Request Sniff
What it does : Captures probe requests from devices searching for Wi-Fi networks.

2. Beacon Sniff
What it does: Captures beacon frames, packets sent by APs to announce their presence.

3. Deauth Sniff
What it does: Monitors deauthentication packets used to disconnect devices from networks.

4. EAPOL/PMKID Scan
What it does: Captures EAPOL handshakes and PMKID used in WPA/WPA2 authentication.

Using Hashcat or other tools …

5. Packet Monitor
What it does: Monitors all types of Wi-Fi packets (management, control, data frames).
.

6. Detect Pwnagotchi Nearby
What it does: Detects Pwnagotchi devices by their unique Wi-Fi signatures.

7. Scan APs (Access Points)
What it does: Lists all nearby Wi-Fi access points with details (SSID, BSSID, signal strength, encryption type).

8. Raw Capture
What it does: Collects raw 802.11 packets for later analysis with tools like Wireshark.

9. Station Sniff
What it does: Captures data from Wi-Fi stations (clients) like smartphones and laptops.

10. Signal Monitor
What it does: Monitors the signal strength (RSSI) of nearby Wi-Fi devices.

ESP32 Marauder includes several Wi-Fi attack features used for penetration testing and network security assessment :

1. Beacon Spam List
What it does: Sends fake beacon frames using SSIDs from a predefined list.
Effect: Floods nearby devices with fake Wi-Fi networks, creating hundreds of SSIDs at once.
Use case: Confuses users and clutters Wi-Fi scanning lists.

2. Beacon Spam Random
What it does: Generates random SSID names and sends them as fake beacon frames.

3. Rick Roll Beacon
What it does: Spams nearby devices with Wi-Fi SSIDs related to Rick Astley’s song ("Never Gonna Give You Up").
Effect: Fills the network list with RickRoll-related names.
Use case: Fun prank or demonstration of SSID spoofing.

4. Probe Request Flood
What it does: Sends a flood of probe requests, making it look like multiple devices are scanning for networks.
Effect: Overloads APs with fake connection requests, potentially disrupting Wi-Fi operations.
Use case: Tests APs' handling of excessive connection requests.

5. Evil Portal
What it does: Sets up a fake captive portal to trick users into entering credentials.
Effect: Users connect to a fake Wi-Fi network, potentially entering sensitive information.
Use case: Phishing attack simulation for Wi-Fi security testing.
You can create a fake AP and fake login page (html file) , or take a real AP and convert it into a fake one.

6. Deauth Flood
What it does: Sends a massive flood of deauthentication packets to all nearby devices, disconnecting them from Wi-Fi networks.
Effect: Disrupts wireless connections, forcing devices to reconnect repeatedly.

7. AP Clone Spam
What it does: Clones an existing access point and broadcasts multiple fake copies with the same SSID.
Effect: Confuses users, causing them to connect to the wrong AP.

8. Deauth Targeted
What it does: Sends deauthentication packets to a specific device, disconnecting only that device.
Effect: Disconnects a single victim from the Wi-Fi network.

Use case: Stealthy attack for forcing reconnection or capturing handshakes.

Bluetooth Sniffing and attacks :

1. Bluetooth Sniffer
What it does: Scans for nearby Bluetooth devices and collects their MAC addresses, names, and signal strength (RSSI).
Effect: Identifies active Bluetooth devices in the area.

2. Flipper Sniff
What it does: Detects nearby Flipper Zero devices by recognizing their Bluetooth signatures.
Effect: Alerts if a Flipper Zero is active nearby, indicating potential RF hacking or Bluetooth attacks.
Use case: Detects potential security threats from Flipper Zero users in the area.

3. AirTag Sniff
What it does: Scans for Apple AirTags and other Find My network devices by identifying their Bluetooth broadcasts.
Effect: Helps locate hidden AirTags, potentially used for tracking or stalking.
Use case: Privacy protection and detecting AirTag-based tracking attempts.

4. Detect Card Skimmers
What it does: Scans for Bluetooth-based credit card skimmers, often disguised as wireless payment readers.

Effect: Identifies potential fraudulent devices that could be stealing card data.

Attacks :

1. Sour Apple

What it does: Sends spoofed Bluetooth advertisements pretending to be an Apple device (like AirPods or iPhone).
Effect: Tricks nearby devices or apps into believing they are connecting to a legitimate Apple product.

2. SwiftPair Spam

What it does: Sends SwiftPair advertisements used by Windows devices to quickly pair with Bluetooth devices.
Effect: Floods the area with SwiftPair requests, potentially causing annoyance or confusion for nearby Windows devices.
Use case: Can be used to disrupt Bluetooth pairing or perform a DoS attack on Bluetooth connections.

3. Samsung BLE Spam

What it does: Sends Bluetooth Low Energy (BLE) advertisements mimicking Samsung devices.
Effect: Causes Samsung devices to detect false Bluetooth devices in the vicinity.
Use case: Disrupt Samsung devices' Bluetooth discovery or create confusion for users and devices.

4. Google BLE Spam
What it does: Sends Bluetooth Low Energy (BLE) advertisements pretending to be a Google device (e.g., Google Nest, Pixel).
Effect: Causes Google devices to discover fake Bluetooth devices, potentially causing interference or miscommunication.
Use case: Targeting Google devices to disrupt Bluetooth pairing or spoof devices for testing.

5. Flipper BLE Spam
What it does: Mimics a Flipper Zero Bluetooth advertisement and floods the area with fake Flipper devices.
Effect: Disrupts nearby devices that try to connect to a Flipper Zero, possibly confusing users or devices that depend on it.
Use case: Targeted disruption against Flipper Zero users or mimicking their presence for research purposes.

6. BLE Spam All
What it does: Sends Bluetooth Low Energy (BLE) advertisements mimicking multiple devices from different manufacturers (Apple, Google, Samsung, etc.).
Effect: Floods Bluetooth scan lists with advertisements for a wide range of devices.
Use case: Used to create a flooded, confusing Bluetooth environment or conduct DoS attacks by overwhelming devices with multiple fake devices.

7. Spoof AirTag :
What it does: Spoofs an Apple AirTag’s Bluetooth signal, making nearby devices think they are detecting a legitimate AirTag.
Effect: Fools users or devices into believing they have discovered a real AirTag, potentially allowing malicious tracking or unwanted alerts.

Use case: Used for privacy attacks, impersonating AirTags to track users or create confusion with the Find My network.

Please remember, **these techniques should only be used in a legal and ethical context**, such as penetration testing on networks you own or have explicit permission to test. Unauthorized use of these attacks is illegal and can lead to severe consequences.