| Cybersecurity |
| --- |
| Flipper Zero Wifi Password Cracking Project |

Javier Urena || QuantumLeap

Presents:

**Flipping Scary!**

## Table of Contents

Disclaimer3

Project I[ntroduction](#_2et92p0) 4

IoT Devices Used Explained in Depth5

IoT Devices Used Explained in Depth [6](#_3rdcrjn)

Further [Possibilities of this Exploitation](#_26in1rg) 7

How to Address and Prevent De-authentication Attacks8

## 

## 

## 

## 

## 

## 

## Disclaimer



## 

**This project was done for educational purposes only, keep in mind that I created a subnet to launch the attack against, doing this kind of activity against networks you do not own without permission is considered illegal.**

# 

## 

## Project Introduction

The end goal of this project is to

Utilize a Flipper zero with ESP32 Marauder board to analyze and capture Wi-Fi network traffic packages through a de-authorization attack, convert the pcaps collected into a hash that I will then proceed to crack using Hashcat executing a dictionary attack.

The following IoT devices and tools will be used to accomplish the goal.

* Flipper Zero
* ESP 32 Marauder Wifi board
* Kali Linux
* Wireshark
* https://hashcat.net/cap2hashcat/
* Hashcat
* Rockyo.txt

Summary of how the devices and technologies will accomplish this goal.

With the Flipper Zero, I will start by scanning nearby access points to determine the network I’m targeting, after I establish the network, then I will proceed to **snif*f****(the process of monitoring and capturing data packets that pass through a network)* with the option of **PMKID***(Pairwise Master Key Identifier)*and proceeding with an **Active-Forced Deauth** attack which disconnects the devices connected to the targeted network**. (It is important to mention that this process only works on 2.4GHz networks ).**

While the de-authentication attack is actively running the flipper will collect **EAPOL***(Extensible Authentication Protocol over LAN)* **data**, which essentially translates to the **4-way handshakes** needed to decrypt the password. (This portion alone can take 5-10 minutes)

I will then proceed to import the **pcaps** collected from the attack to my Kali box and open them on **Wireshark** and search for **wlan.ssid ==”Flipping Scary!” || eapol**(Flipping Scary! is the name of the targeted AP) which Iwill ensure that the **EAPOL 4-way handshake** was effectively captured, then proceed to convert the pcap into a hash using <https://hashcat.net/cap2hashcat/> .

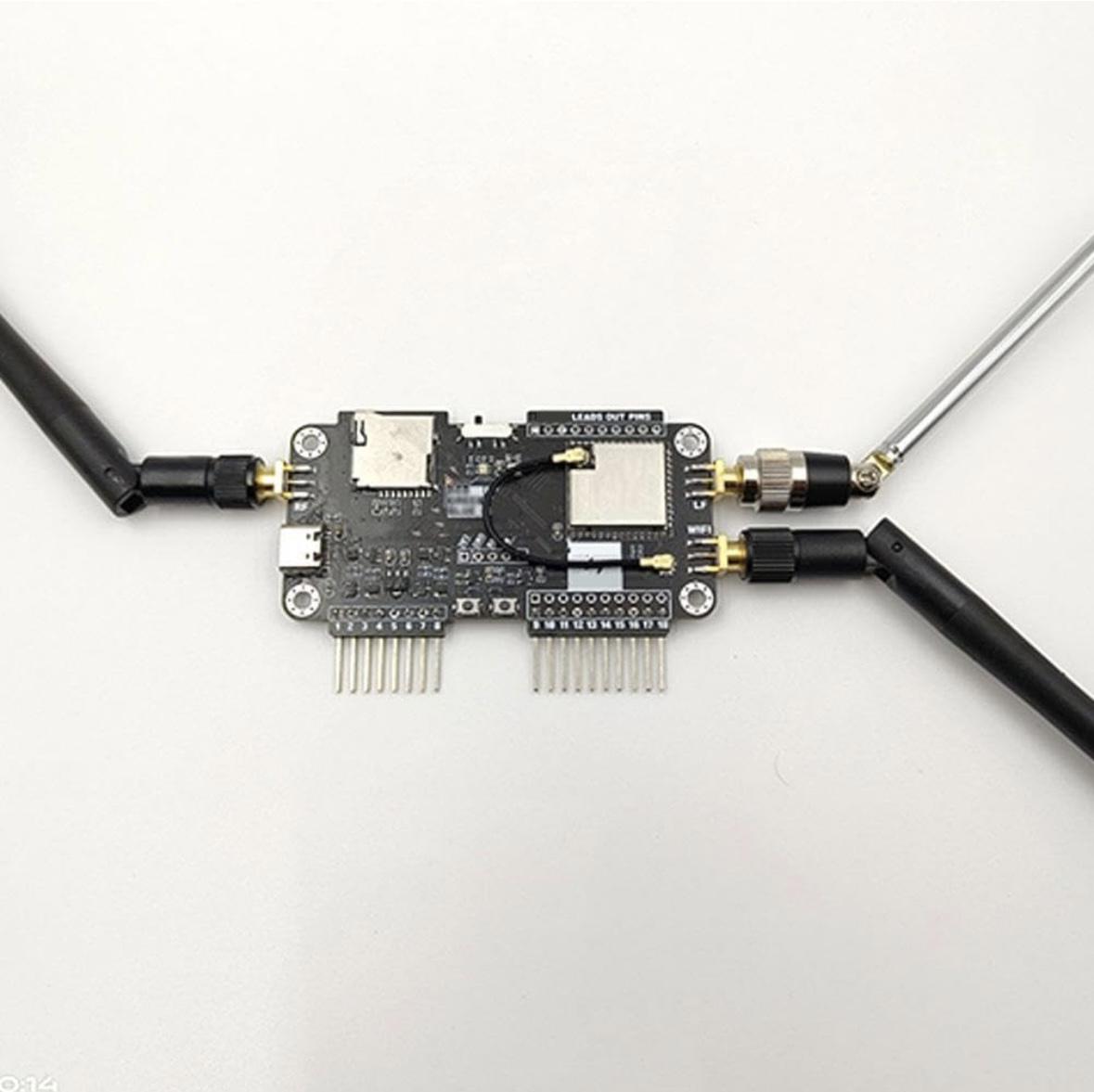
The last step of the project will be executed in the terminal where I will use **Hashcat** in conjunction with the **rockyou.txt** wordlist to crack the password launching a dictionary attack that should give me access to the targeted network.

## IoT Devices Used Explained in Depth

**The Flipper Zero** is a portable multi-tool designed for interacting with digital systems like access controls and radio protocols. Its playful design lets users capture and transmit wireless codes, read and emulate RFID cards, and sniff data from devices like Logitech keyboards. Being open-source, it can be customized for various functionalities.

****

In contrast, the **ESP32 Marauder** **board** is a WiFi and Bluetooth analysis tool that enables frame capture, device enumeration, and frame transmission. It is a compact alternative to larger traffic capture tools, facilitating data collection for analysis.



**When paired with the ESP32 Marauder board, the Flipper Zero** can enhance its capabilities in several ways:

* **WiFi and Bluetooth Analysis**: The ESP32 Marauder can capture WiFi and Bluetooth traffic, allowing the Flipper Zero to analyze and manipulate data packets.
* **Device Enumeration**: It can identify nearby devices, providing insights into connected networks and services.
* **Packet Injection**: The combination allows for sending custom packets, enabling users to test network security and perform penetration testing.
* **Data Collection**: Users can gather data from various wireless protocols for post-operation analysis.
* **Extended Range**: The ESP32 Marauder can increase the effective range for wireless interactions compared to the Flipper Zero alone.

Overall, this combination is useful for security research, penetration testing, and exploring wireless communication.

****

## Further Possibilities of this Exploitation

## 

While I only cracked the password of a Wifi network, this can be seen as the first step for many other more severe exploits that you can fall victim to if someone can access your Wi-Fi network without you knowing, especially if your security measures are weak.

Here are some higher risks associated with unauthorized access:

* **Data Interception** Attackers can intercept sensitive information transmitted over your network, such as passwords, personal messages, and financial data.
* **Bandwidth Theft**Unauthorized users can consume your bandwidth, leading to slower internet speeds and potential overage charges from your ISP.
* **Malware Distribution**An attacker could use your network to distribute malware to connected devices, potentially compromising them.
* **Network Attacks**Unauthorized users can launch attacks against other devices on your network or external targets, using your connection as a base.
* **Privacy Breach**Attackers can monitor your online activities, potentially gathering personal information for malicious purposes.
* **Access to Connected Devices**If your network is not well secured, attackers might gain access to connected devices like cameras or smart home systems, leading to privacy violations.

## How to Address And Prevent De-authentication Attacks

To protect your Wi-Fi network from de-authentication attacks and packet sniffing, you can implement several security measures such as:

* **Use WPA3 Encryption:** Upgrade your Wi-Fi security to WPA3 if supported. It offers better protection against attacks compared to WPA2.
* **Strong Passwords:** Use complex, unique passwords for your Wi-Fi network. Avoid common phrases and ensure your password is 12-16 characters long.
* **Disable WPS:** Wi-Fi Protected Setup (WPS) can be vulnerable to attacks. Disable this feature on your router.
* **Regular Firmware Updates:** Keep your router’s firmware up to date to protect against known vulnerabilities.
* **MAC Address Filtering:** Enable MAC address filtering to restrict which devices can connect to your network. While not foolproof, it adds an extra layer of security.
* **Network Segmentation:** Create separate networks for different device types (guests, IoT devices) to limit potential exposure.
* **Disable SSID Broadcasting:** Consider hiding your SSID to make your network less visible to casual users. This doesn’t stop determined attackers but can reduce visibility.
* **Use a VPN:** Utilize a Virtual Private Network (VPN) to encrypt your internet traffic for added security, especially on public networks.
* **Intrusion Detection/Prevention Systems:** Deploy IDS/IPS solutions to monitor suspicious activities and respond to threats.
* **Limit Signal Range:**  Adjust your router settings to limit the Wi-Fi signal range to just your property, reducing the risk of external attacks.
* **Disable Remote Management:** Turn off remote management features unless necessary to prevent unauthorized access.
* **Monitor Network Traffic:**  Regularly check for unauthorized devices or unusual traffic patterns on your network.

Implementing these measures will significantly enhance the security of your Wi-Fi network against de-authentication attacks and packet sniffing.

## 