## ABSTRACT

The ESP8266 Wi-Fi Deauthentication Project is an open-source initiative that repurposes the ESP8266 microcontroller to perform deauthentication attacks on

802.11 wireless networks. By exploiting the unprotected nature of Wi-Fi management frames, particularly deauthentication frames, the device can send forged packets to disconnect clients from their access points. This functionality is facilitated through a user-friendly web interface hosted directly on the ESP8266, eliminating the need for additional software.

Beyond deauthentication, the firmware also supports beacon flooding and probe request attacks, enabling users to simulate multiple fake networks and mimic client devices searching for networks. These features are accessible via a web interface hosted on the ESP8266, eliminating the need for additional software.

The primary objective of this project is to serve as an educational tool, demonstrating the vulnerabilities inherent in the Wi-Fi protocol and emphasizing the importance of implementing security measures such as Protected Management Frames (PMF). While the project provides a practical demonstration of these vulnerabilities, it is crucial to note that it is intended solely for authorized testing and educational purposes. Unauthorized use on networks without explicit permission is illegal and unethical. Users are encouraged to utilize this tool responsibly to understand network vulnerabilities and advocate for stronger security measures in wireless communications.

**CHAPTER-1**

# INTRODUCTION

Wireless networking has become an integral part of modern communication, yet it is not without its vulnerabilities. One such vulnerability exists within the IEEE 802.11 protocol, where management frames, including deauthentication frames, are transmitted in an unprotected manner. This oversight allows malicious entities to craft and send deauthentication packets, disconnecting devices from their networks. The ESP8266 Wi-Fi Deauthentication Project leverages this vulnerability by programming the ESP8266 microcontroller to send spoofed deauthentication frames, effectively disconnecting devices from their access points. Beyond deauthentication, the firmware also supports beacon flooding and probe request attacks, enabling users to simulate multiple fake networks and mimic client devices searching for networks. These features are accessible via a web interface hosted on the ESP8266, eliminating the need for additional software. The project aims to educate users about Wi-Fi security flaws and underscores the necessity of adopting enhanced security protocols, such as WPA3 and PMF, to safeguard wireless communications. It is essential to emphasize that the use of this tool should be confined to authorized environments for educational and testing purposes only. Unauthorized use on networks without explicit permission is illegal and unethical. Users are encouraged to utilize this tool responsibly to understand network vulnerabilities and advocate for stronger security measures in wireless communications.

## CHAPTER-2

Method

Step-by-Step Procedure to Run ESP8266 DEAUTHENTICATION OF WIFI- NETWORKS:

###### Install Required Tools

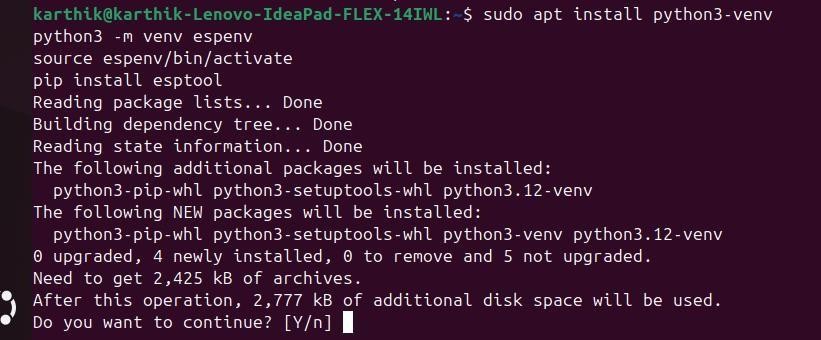
Open a terminal and run:

sudo apt update

sudo apt install python3-pip git unzip pip3 install esptool

For this we need to activate virtual environment

By adding espenv, you are automating the configuration process for the ESP8266/ESP32 environment, so you don’t have to manually set environment variables like PATH, ESPPORT, ESPTOOL, etc., each time you work with the microcontroller. It helps make the development process more seamless.

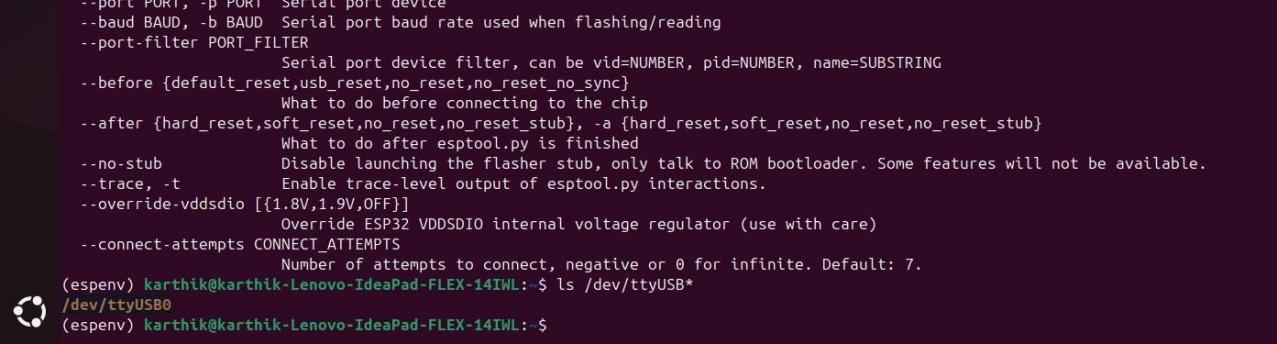


##### Identify USB Port

Plug in your ESP8266 and run:

dmesg | grep tty

Look for something like /dev/ttyUSB0 or /dev/ttyACM0.



Why to identify usb port:

**Serial Communication:** If you’re debugging or interacting with your ESP8266 over serial, you need to identify the correct USB port to establish communication. Using the wrong port could lead to errors or failed connections.

To identify the USB port on your computer, you can typically check the device manager (on Windows) or use ls /dev/tty\* or dmesg | grep tty (on Linux/macOS) to locate the specific port to which the ESP8266 is connected.

If you see permission errors, add yourself to the dialout group: sudo usermod -aG dialout $USER

sudo usermod -aG dialout $USER

Then reboot or re-login.

##### Download Deauther Firmware

Visit: [GitHub](https://github.com/SpacehuhnTech/esp8266_deauther?utm_source=chatgpt.com)

https://github.com/SpacehuhnTech/esp8266\_deauther Download the .bin file for your board, for example: ESP8266\_DEAUTHER-1.6.5-NodeMCU.bin

Save it somewhere like your Downloads folder.

##### Flash the Firmware

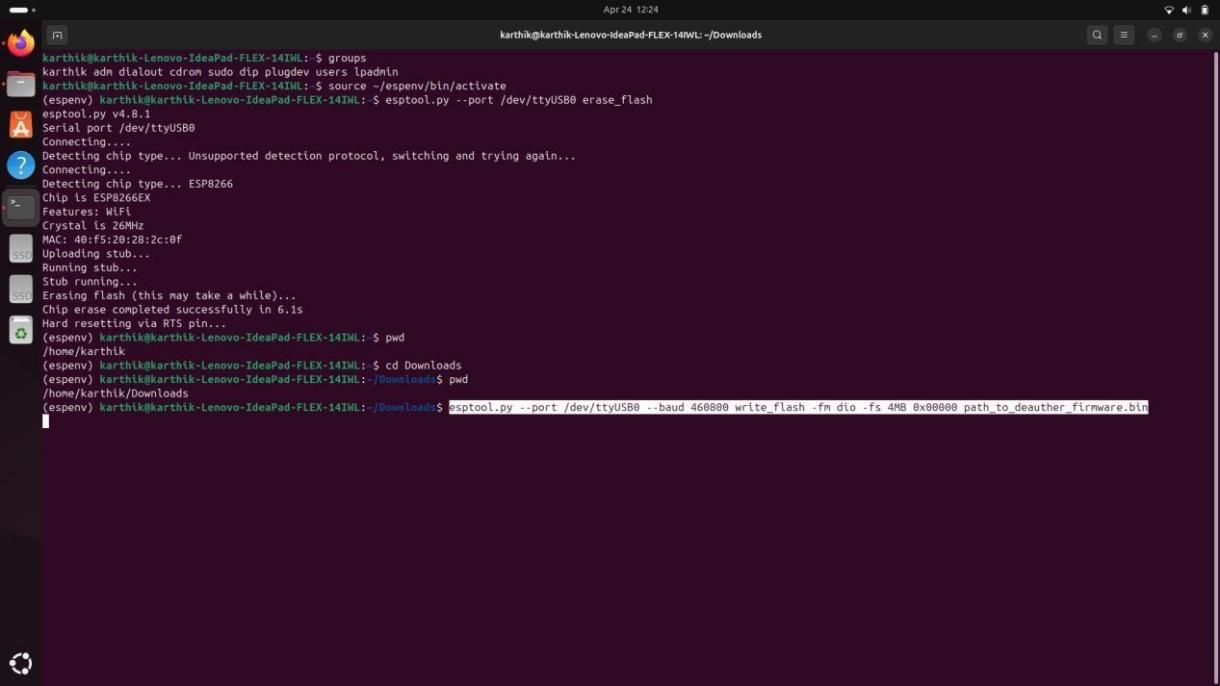
Navigate to the folder with the .bin file:

cd ~/Downloads

Then flash it with esptool.py:

esptool.py --port /dev/ttyUSB0 erase\_flash

esptool.py --port /dev/ttyUSB0 write\_flash -fm dio 0x00000 ESP8266\_DEAUTHER- 1.6.5-NodeMCU.bin



Make sure to replace /dev/ttyUSB0 with your actual device path, and the .bin file name with the one you downloaded.

##### Connect and Use the Deauther

Unplug and replug the ESP8266.

It will create a Wi-Fi access point, usually called pwned or Deauther. Connect to it from another device (phone/laptop).

Open a browser and go to: [http://192.168.4.1](http://192.168.4.1/)

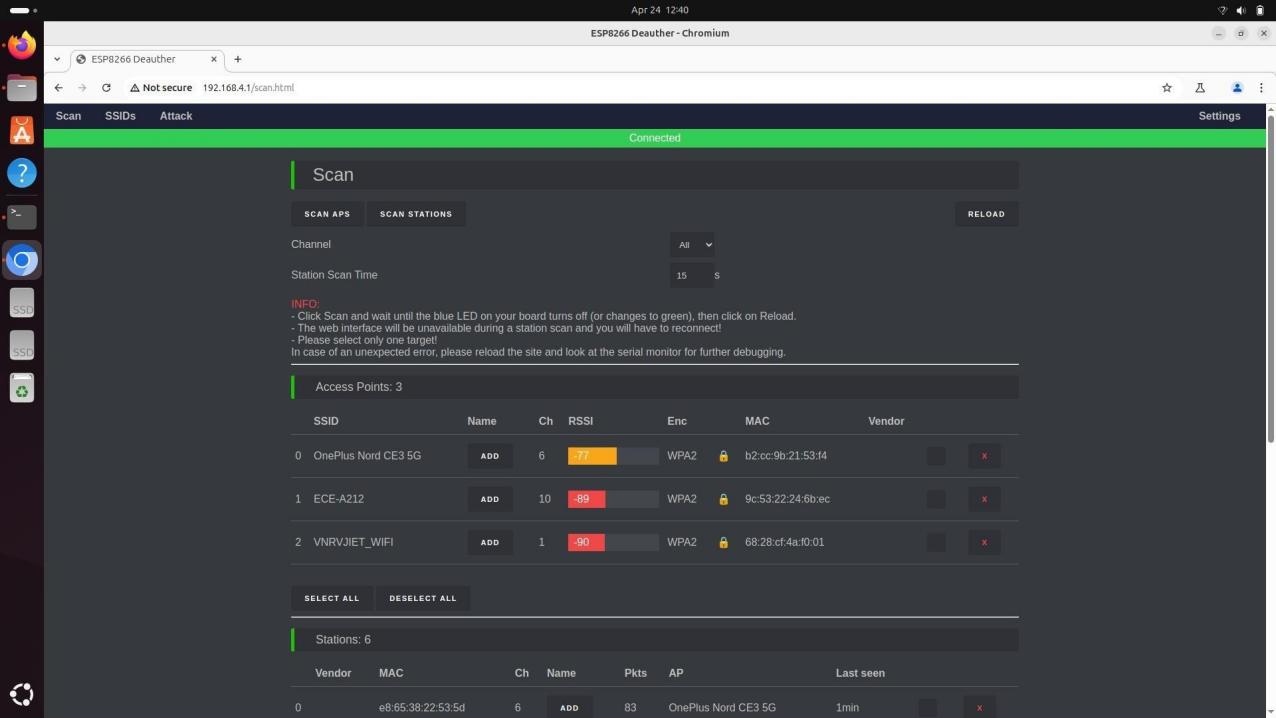
Use the interface to:

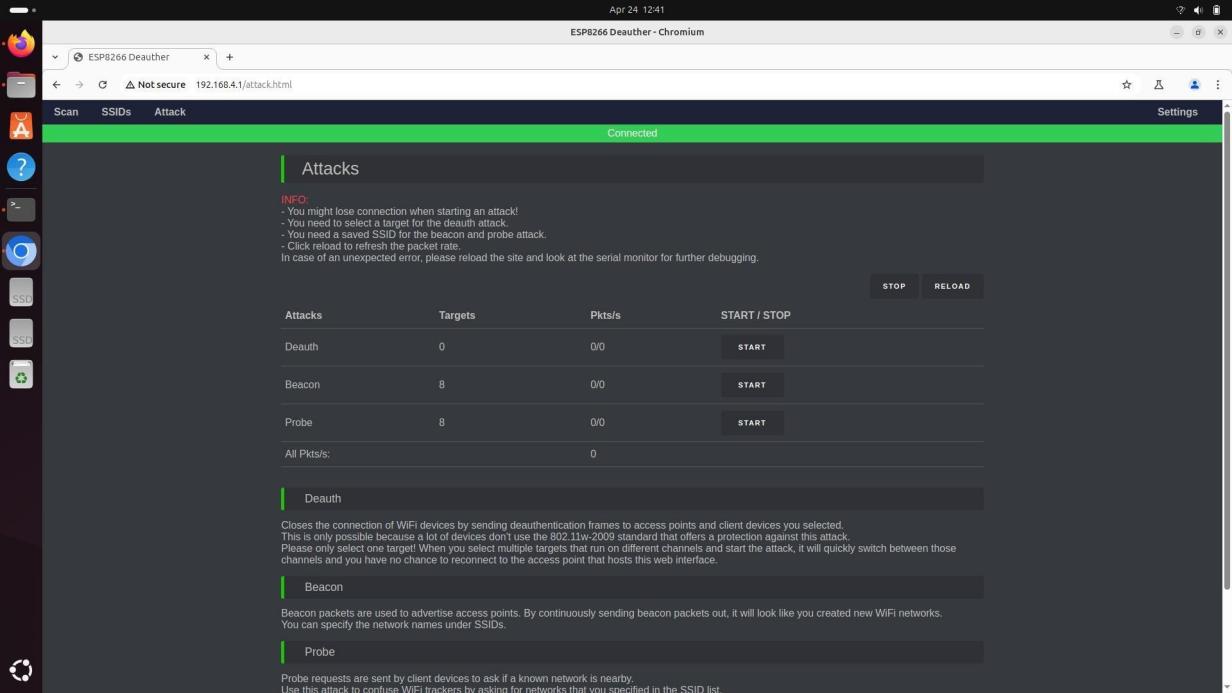
Scan for networks Select a target

Start Deauth, Beacon spam, or Probe attack

**CHAPTER-3**

# TEST CASES/ OUTPUT

****

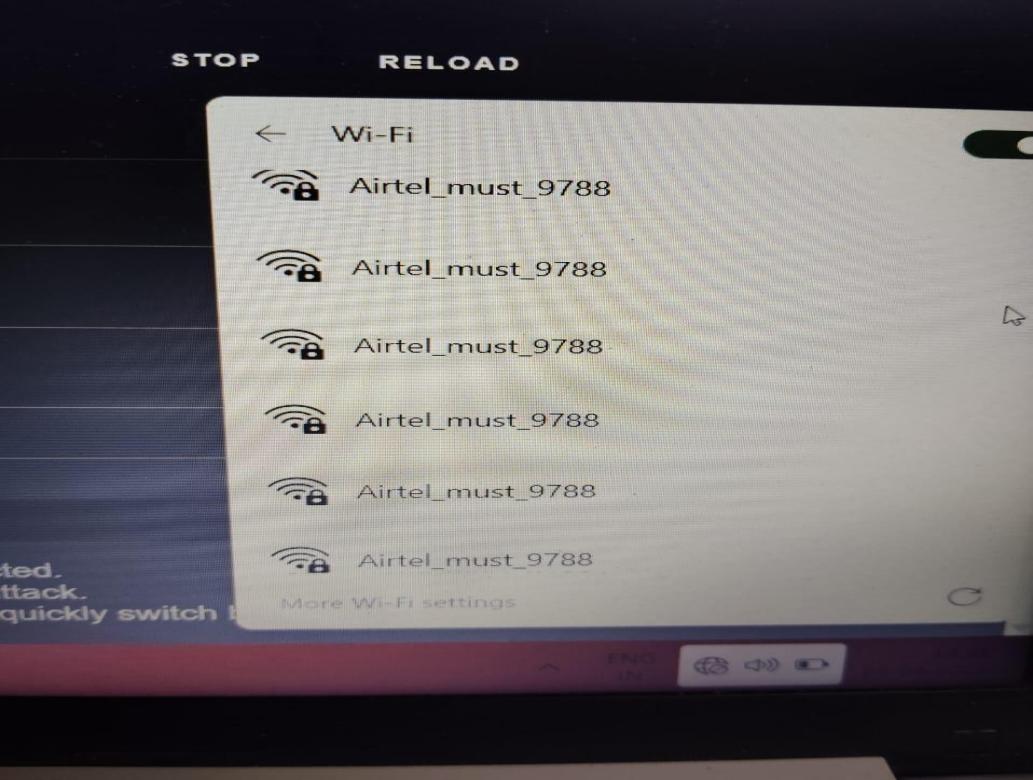
****

**CHAPTER-4**

# RESULTS

**Things we could do:**

## BEACON ATTACK:



A beacon attack on an ESP8266 typically refers to the act of broadcasting fake or malicious Wi-Fi access points (AP;s) in the surrounding environment. This is often done by an attacker to impersonate legitimate access points or trick devices into connecting to a rogue AP. In this context, a beacon frame is a special type of frame used by Wi-Fi access points to announce their presence.

CHAPTER 5

Summary

##### Conclusion of WIFI Deauthentication

###### ESP8266 Wi-Fi Deauthentication Project – Summary

This project demonstrates vulnerabilities in the IEEE 802.11 protocol using the ESP8266 microcontroller to perform Wi-Fi attacks such as deauthentication, beacon flooding, and probe request flooding. These attacks exploit unprotected management frames, causing devices to disconnect, search for fake networks, and increasing overall network traffic—highlighting weaknesses in unsecured Wi-Fi setups.

###### Key Observations:

* Devices were forcibly disconnected from access points.
* Clients attempted to connect to fake or non-existent networks.
* Network performance degraded due to increased scanning and traffic.

###### Mitigation Strategies:

* **Enable PMF (IEEE 802.11w):** Encrypts and authenticates management frames to prevent spoofing.
* **Use WPA3:** Enhances security with stronger encryption and safeguards against offline attacks.
* **Monitor Networks Regularly:** Intrusion detection can help identify and respond to suspicious activity.

**Disclaimer:** This project is for educational use in authorized environments only. Unauthorized deployment is illegal and unethical.