A Project Proposal

on

Wi-Fi Network Analyzer and Deauthentication Tool using ESP32 and Kali Linux

Bachelor in Computer Engineering

SUBMITTED TO

Purbanchal University

Biratnagar, Nepal

SUBMITTED BY

Saraswoti Rokaya (Roll No. 23)
Santosh Kumar Shah (Roll No. 22)
Salim Shrestha (Roll No. 18)

Submitted on: July 2025
Fourth Semester Project Proposal

KANTIPUR CITY COLLEGE

Putalisadak, Kathmandu

Project Proposal

1. Title of the Project

Wi-Fi Network Analyzer and Deauthentication Tool using ESP32 and Kali Linux

This project focuses on developing a Wi-Fi Network Analyzer and Deauthentication Tool using the ESP32 microcontroller and Kali Linux.
The analyzer component scans nearby wireless networks, collecting information such as SSIDs, signal strength, and MAC addresses.
The deauthentication tool simulates denial-of-service (DoS) attacks by sending deauth packets to disconnect clients from a network — for ethical testing and educational purposes only. By combining the low-cost, Wi-Fi-enabled ESP32 with Kali Linux's powerful network analysis tools, this project demonstrates common wireless vulnerabilities and raises awareness about network security.
It is intended for academic use in controlled environments to promote hands-on learning in cybersecurity and embedded systems.

2. Group Members

Name	**Roll Number**	**Contact**
Saraswoti Rokaya	23	+977 986-6780843
Santosh Kumar Shah	22	+977 9761774477
Salim Shrestha	18	+977 9705550012

3. Background and Motivation

With the increasing reliance on Wi-Fi networks, it's essential to understand the vulnerabilities they may have. This project aims to demonstrate how wireless networks can be scanned, monitored, and tested for weaknesses using the ESP32 microcontroller and Kali Linux tools. It promotes awareness of cybersecurity and ethical hacking in IoT environments.

4. Problem Statement

Most users assume that Wi-Fi networks are secure by default. However, many networks are vulnerable to simple attacks such as deauthentication or brute-force attempts, which can disrupt service or compromise sensitive data. There is a lack of low-cost, educational tools for demonstrating and understanding these vulnerabilities.

5. Vision

Our vision is to develop an open-source, low-cost Wi-Fi auditing tool that helps students, researchers, and cybersecurity enthusiasts explore wireless vulnerabilities ethically and safely. It should act as a bridge between embedded systems and cybersecurity fundamentals.

6. Objectives

1. To build a low-cost Wi-Fi scanning and attack simulation device using ESP32.
2. To detect nearby Wi-Fi networks and connected clients.
3. To simulate deauthentication attacks (for educational/testing purposes).
4. To integrate the ESP32 output with Kali Linux tools for detailed packet analysis.

7. Scope of the Project

1. Wi-Fi scanning and listing SSIDs, BSSIDs, and signal strengths.
2. Packet sniffing using ESP32 in promiscuous mode.
3. Performing deauthentication (DoS) attacks in a test environment.
4. Visualizing and analyzing data using Kali Linux tools like Wireshark.

8. Required Hardware and Software

Hardware:

1. ESP32 Development Board
2. USB Cable
3. Optional OLED Display
4. PC/Laptop with Wi-Fi card (for Kali Linux)

Software:

1. Arduino IDE (ESP32 libraries)
2. Kali Linux (Wireshark, Aircrack-ng, etc.)
3. Python (for data handling/visualization)
4. Wi-Fi network for testing

9. Methodology

1. Set up and program the ESP32 using Arduino IDE.
2. Enable promiscuous mode to capture Wi-Fi packets.
3. Display or log detected devices and APs.
4. Enable deauthentication mode (send deauth frames).
5. Send logs/data to Kali Linux via serial or Wi-Fi.
6. Analyze data using Wireshark or custom Python scripts.

10. Expected Outcomes

1. A working prototype of a Wi-Fi scanner and tester using ESP32.
2. A basic tool for teaching Wi-Fi vulnerabilities and ethical hacking.
3. Logs and visualizations of scanned networks and test attacks.
4. Awareness of wireless network security.

11. Benefits

1. Increases cybersecurity awareness among students.
2. Promotes hands-on learning with embedded systems and wireless protocols.
3. Encourages responsible and ethical hacking practices.
4. Can be adapted for network monitoring or forensic tools.

12. Deliverables

1. Fully functional ESP32-based Wi-Fi scanner and deauther.
2. Serial or wireless communication with Kali Linux.
3. Documentation with user manual and test cases.
4. Presentation/report explaining system design, security insights, and future improvements.

13. Cost/Budget

Item	**Quantity**	**Approx. Cost (NPR)**
ESP32 Dev Board	1	1,200
USB Cable	1	200
OLED Display (Optional)	1	800
Breadboard & Wires	1 set	300
Miscellaneous	-	500
Total		**3,000 – 3,500**

Kali Linux will be run on existing personal laptops/VMs, so no additional cost is included.

14. Timeline

Week	**Task**
1–2	Research & Hardware setup
3–4	ESP32 programming (scanning)
5–6	Implement deauth (test safely)
7–8	Data forwarding to Kali Linux
9–10	Data analysis & visualization
11–12	Final integration
13–14	Testing & debugging
15	Report & presentation

15. References

1. ESP32 Arduino Documentation
2. Aircrack-ng Suite
3. Wireshark official tutorials
4. Open-source deauth tools for ESP8266 (adapted for ESP32)

16. Prior Work / Related Work by Group Member

Wi-Fi DoS Attack using Kali Linux

One of our group members, **Salim Shrestha**, has already developed and demonstrated a Wi-Fi-based Denial of Service (DoS) attack project using **Kali Linux**, available publicly on GitHub:

GitHub Repository:

WiFi-DOS-Kali by **salimshre** (https://github.com/salimshre/WiFi-DOS-Kali)

Project Summary

This project showcases how Wi-Fi DoS attacks can be executed using **Aircrack-ng tools** within Kali Linux. It covers both practical execution and theory, with a strong emphasis on **ethical usage** and **educational awareness**.

Key Functionalities Demonstrated

1. Monitor mode setup using airmon-ng, iwconfig
2. Scanning Wi-Fi networks via airodump-ng
3. Targeted **deauthentication attacks** using aireplay-ng
4. **Brute-force WPA/WPA2 cracking** with aircrack-ng
5. Demonstration of potential countermeasures

Tools Used

1. Operating System: Kali Linux
2. **Tool Suite**: Aircrack-ng (airodump-ng, aireplay-ng, aircrack-ng)
3. **Hardware**: USB Wi-Fi adapter with monitor mode + packet injection
4. **Permission:** Sudo / root access

Why This Is Relevant

This prior work strengthens our current ESP32 + Kali Linux proposal by showing:

1. A deep understanding of **Wi-Fi vulnerabilities**
2. Hands-on experience with industry-standard tools
3. A strong ethical and educational approach to cybersecurity

By integrating ESP32 in our new project, we aim to demonstrate similar attack scenarios **on embedded microcontrollers** and compare them with **desktop-grade tools** like Kali Linux, further enhancing our research.