Semester Project Report

# Wi-Fi Jammer: Understanding Wireless Network Vulnerabilities

**Project Team**

Ahmad Hassan 21F-9095

Ismail Daniyal 21F-9345

Samiullah 21F-9200

Saad Athar 21F-9227

Ahmad Sheikh



Department of Computer Science

National University of Computer and Emerging Science

## 1. Project Overview

**Wi-Fi Jammer** is a project aimed at simulating a deauthentication attack on a wireless network in a controlled environment. This program, written in Python using the **Scapy** library, disrupts the connectivity of all devices connected to a targeted access point by sending continuous deauthentication packets. The project serves as a practical demonstration of wireless network vulnerabilities, enabling cybersecurity professionals to better understand and defend against these threats.

## 2. Purpose

The primary purpose of the **Wi-Fi Jammer** project is to:

1. Analyze Network Weaknesses: Identify vulnerabilities in Wi-Fi networks susceptible to de-authentication attacks.
2. Educate and Train: Provide a hands-on learning experience for ethical hackers and IT professionals in wireless security testing.
3. Enhance Defense Mechanisms: Test real-world countermeasures like WPA3 and wireless intrusion detection systems (WIDS).
4. Raise Awareness: Highlight the importance of implementing robust wireless security measures to protect against network disruption.

## 3. Applications in the Real World

The **Wi-Fi Jammer** project has several practical applications in cybersecurity and network testing:

1. Penetration Testing:
   * Test corporate or personal wireless networks to assess their resistance to deauthentication-based attacks.
   * Validate the effectiveness of security protocols like WPA2 and WPA3.
2. Educational Training:
   * Train ethical hackers, cybersecurity students, and IT professionals in identifying and mitigating wireless network vulnerabilities.
3. Incident Response:
   * Understand how attackers exploit de-authentication to disrupt networks and prepare response strategies to counter such attacks.
4. Wireless Infrastructure Auditing:
   * Evaluate the robustness of wireless networks in sensitive environments such as hospitals, airports, and corporate offices.
5. Developing Defensive Solutions:
   * Create and test countermeasures, such as enabling **Management Frame Protection (MFP)** in enterprise wireless networks.

## 4. Requirements

### Hardware Requirements

1. A Wi-Fi adapter that supports:
   * **Monitor mode**
   * **Packet injection**

**We use ALFA Wifi Adapter W136**

1. A Linux-based system (e.g., Kali Linux).

### Software Requirements

1. Python 3 installed on the system.
2. Scapy Python library for crafting and sending network packets.
3. Aircrack-ng suite for network monitoring and analysis.

### Additional Tools

* Wireless monitoring tools: iwconfig, airmon-ng, airodump-ng.

### Test Network

* An isolated, authorized Wi-Fi network for ethical testing.

## 5. Installation and Setup

### Installing Required Tools

1. Update the system and install Scapy:
2. sudo apt update
3. sudo apt install python3-scapy

### Prepare Monitor Mode

1. Identify the Wi-Fi interface:
2. iwconfig
3. Enable monitor mode:
4. sudo airmon-ng start wlan0

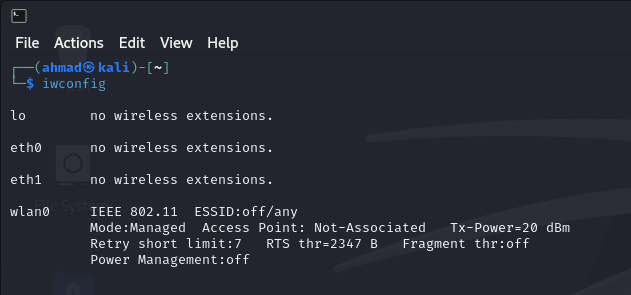
### Capture Target Information

1. Use airodump-ng to list available networks and find the target:
2. airodump-ng wlan0mon
3. Lock onto the target access point:
4. airodump-ng -c <channel> --bssid <BSSID> -w capture wlan0mon

## 6. Steps to Run the Wi-Fi Jammer

1. Prepare the Environment:
   * Ensure the Wi-Fi adapter is in monitor mode.
   * Identify the BSSID of the target access point and its channel.
2. Run the Python Script:
   * Save the following Python code as wifi\_jammer.py:

## 7.Screenshots



A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated 

## 8. Conclusion

The **Wi-Fi Jammer** project is a practical and educational tool for understanding wireless network vulnerabilities and defenses. By simulating a deauthentication attack, it demonstrates the ease with which attackers can disrupt Wi-Fi connections and highlights the importance of implementing robust security measures.

**Recommendations for Defense:**

1. **Enable WPA3**: Use protocols with built-in protections like Management Frame Protection (MFP).
2. **Deploy WIDS**: Detect and alert administrators about deauthentication attacks.
3. **Segment Networks**: Use VLANs to isolate critical systems from easily targeted Wi-Fi networks.

With knowledge gained from this project, cybersecurity professionals can design more secure and resilient wireless networks.