WIFI-THREAT DETECTOR

Real-time Detection of Deauthentication Attacks in WiFi Networks

GITHUB REPOSITORY LINK – https://github.com/shrey0718/WiFiThreatDetector

DEMO VIDEO YOUTUBE LINK – https://youtu.be/OvL9J5SwkdY?si=_xQpY4sGg88afccb

GOOGLE DRIVE LINK –
https://drive.google.com/drive/folders/1Xk5IH9t-VoUUnBHxLz9kO3RRiTf3hTic?usp=sharing

BY: SHREYA DIXIT

INTRODUCTION

Overview:

- A Python-based tool specifically for Windows that scans nearby WiFi networks.
- Analyzes network security, detects potential threats (e.g., Evil Twin attacks), and presents results interactively.

Purpose:

- To empower security professionals, IT teams, and public WiFi users with actionable insights on wireless network risks.

TOOLS & TECHNOLOGIES

Hardware: WiFi adapter with monitor mode support

Programming Language: Python

Platform: Windows

Libraries Used: Scapy (for packet sniffing)

OUR SOLUTION - WIFI THREAT DETECTOR MAIN FEATURES:

- Automated WiFi Scanning every 120 seconds.
- Threat Analysis & Scoring: Evaluates each network based on encryption and signal strength.
- Historical Logging & Trend Analysis: Uses an SQLite database.
- Interactive Dashboard: Filtering, sorting, and detailed views for each network.
- CSV Export & Advanced Security Check Simulation.

WHAT IS A DEAUTHENTICATION ATTACK?

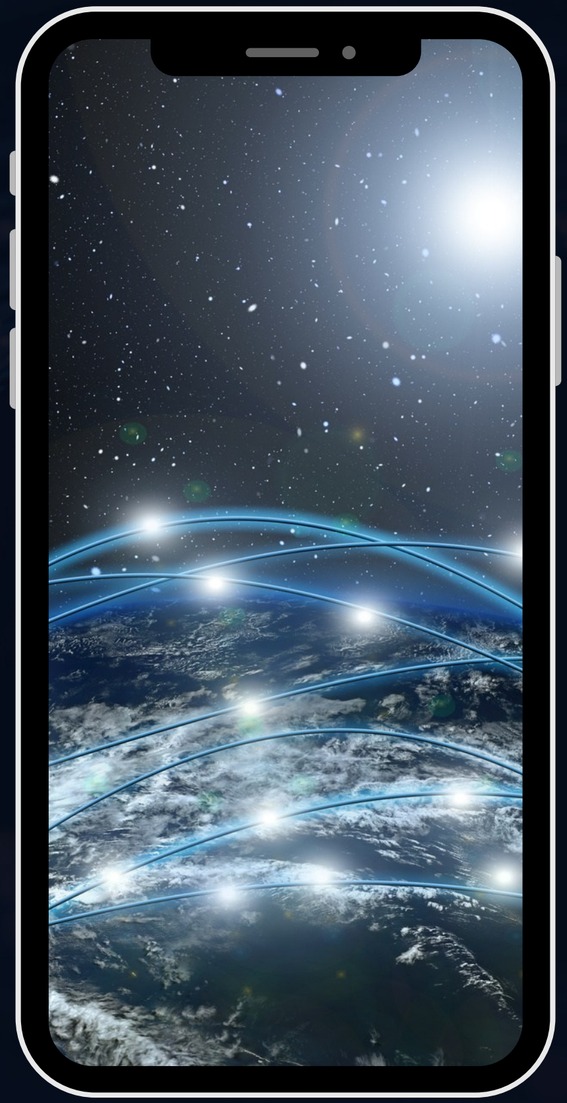
- Exploits 802.11 WiFi management frames.
- Forces a device to disconnect from the access point.
- No authentication is required to send a deauth frame.
- Common in Denial-of-Service (DoS) and Man-in-the-Middle (MITM) attacks.

WHY DETECT DEAUTH ATTACKS?

- Causes repeated disconnections and service disruption.
- Can be used to capture WPA/WPA2 handshake for cracking passwords.
- Often undetected by users and traditional firewalls.
- Early detection helps in securing the network and raising awareness.

OBJECTIVES

- Develop a Python-based tool to detect deauth frames.
- Monitor traffic using WiFi adapter in monitor mode.
- Alert users in real-time upon detecting suspicious activity.
- Display attacker MAC, timestamp, and packet count.



WORKING PRINCIPLE

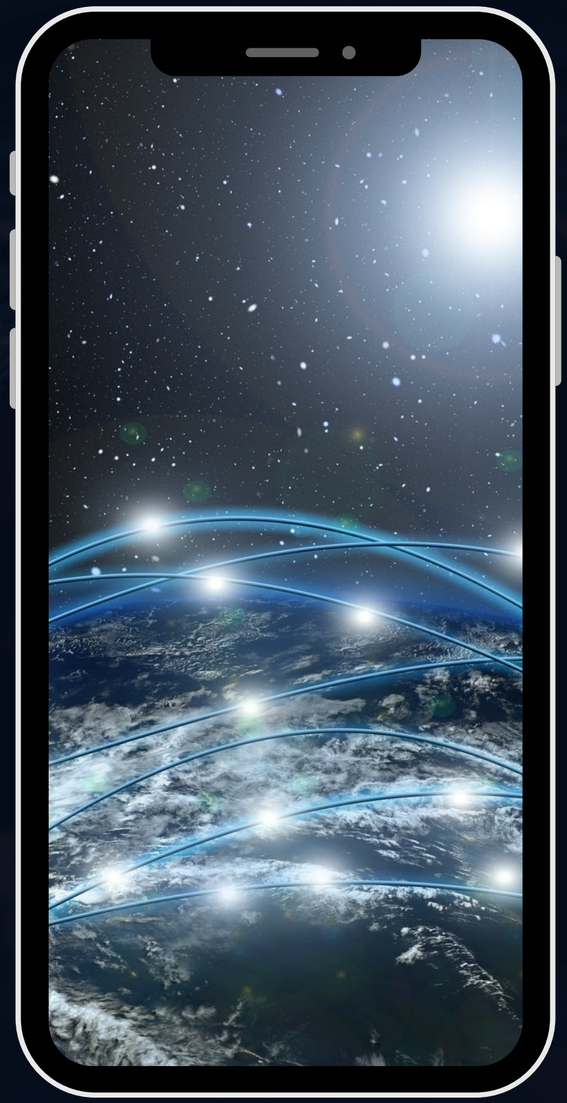
- Put WiFi adapter in monitor mode.
- Sniff network packets on selected channel.
- Identify deauthentication frames: Type 0, Subtype 12.
- Count frequency of packets from each source.
- Trigger alert if packets exceed threshold.

CODE FLOW

- scapy.sniff() listens to packets.
- Packet handler checks for Dot11Deauth frames.
- Deauth count stored in a dictionary by MAC.
- If count > 10/sec → print alert/log attack.
- Optionally display popup or sound alert.

RESULTS

- Tool tested in a controlled lab network and public WiFi.
- Detected deauth frames from known attack tools (e.g., aireplay-ng).
- Real-time alerts with accurate attacker info.
- Minimal false positives in normal traffic.



FUTURE IMPROVEMENTS

- Add prevention mechanism (block MAC / switch channel).
- Web dashboard with logging and analytics.
- Extend to detect other WiFi attacks (e.g., beacon floods, probe spoofing).
- Deploy on Raspberry Pi for portable WiFi defense.

CONCLUSION

- Deauthentication attacks can severely impact WiFi security.
- Our tool helps detect such threats quickly and effectively.
- Provides actionable insights for network administrators and users.
- Future improvements can enhance its utility and scalability.

THANK YOU

BY: SHREYA DIXIT
EMAIL ID : shreyald69@gmail.com
L