**DEAUTHENTICATION ATTACK DETECTOR**

**DOCUMENTATION**

Ranjith V

14 December 2024

**TABLE OF CONTENTS**

Introduction 2

What is a Deauthentication attack? 2

OS compatibility 3

Installation Guide 3

Usage Guide 4

How It Works 5

Example Output 6

Security Considerations 7

Conclusion 7

INTRODUCTION

My name is Ranjith, as a Computer Science undergraduate with a growing passion for cybersecurity. I have basic knowledge of programming languages, operating systems, networking, and hardware.

In this documentation, I will showcase a **Deauthentication Attack Detector** built using Python. This tool detects deauthentication attacks in wireless networks. It’s a practical project aimed at enhancing network security using the skills I’ve developed.

WHAT IS AN DEAUTHENTICATION ATTACK?

A **Deauthentication attack** is a type of **DoS** attack on Wi-Fi networks where an attacker sends fake deauthentication frames to disconnect devices from the network. By impersonating the access point or a device, the attacker forces disconnections, causing network disruption and potentially enabling other attacks like **Man-in-the-Middle**.

OS COMPATIBILITY

This tool is designed to run exclusively on **Linux-based operating systems**, such as Kali Linux, Ubuntu, and other Debian-based distributions. It relies on tools and commands (e.g., arp, netstat, ip, and ping) that are typically available in Linux environments. While it is possible to adapt the tool for other operating systems like Windows or macOS, it may require significant modifications to handle platform-specific commands and dependencies. I will try to update the same tool for running on Windows OS soon.

INSTALLATION GUIDE

Packages to be Installed:

# Update package list

*sudo apt update*

*sudo apt install python3*

#Check python & pip version

*python3 --version*

*pip3 --version*

# Install pip for Python 3 if not installed

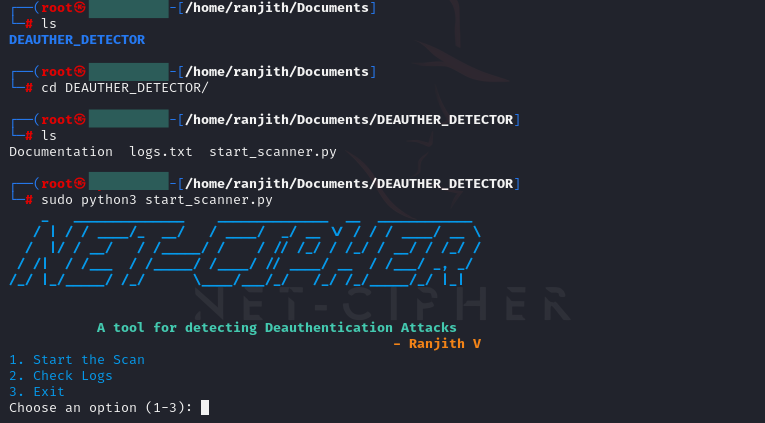
*sudo apt install python3-pip*

# Install required libraries

*pip3 install rich pyfiglet* #if rich is not installing, please use "venv" and install through it.

USAGE GUIDE

* First, navigate to the directory where the tool is located in your Kali Linux terminal.
* Eg: cd “DEAUTHER\_DETECTOR DIRECTORY”
* Check the files using: ls command
* Then, use **python3** to start the tool.
* Run the following command to launch the tool:
* sudo python3 start\_scanner.py



HOW IT WORKS?

The **Deauthentication Attack Detector** works by monitoring the devices connected to a Wi-Fi network. It periodically scans the network for connected devices and compares the current list with the previous one. If a significant number of devices are disconnected within a short period, it detects a potential **Deauthentication attack** and triggers an alert. The tool also provides useful network information, such as interface details and ping status, while logging attack events for further analysis. This helps in identifying and responding to disruptions in network connectivity caused by deauthentication attacks

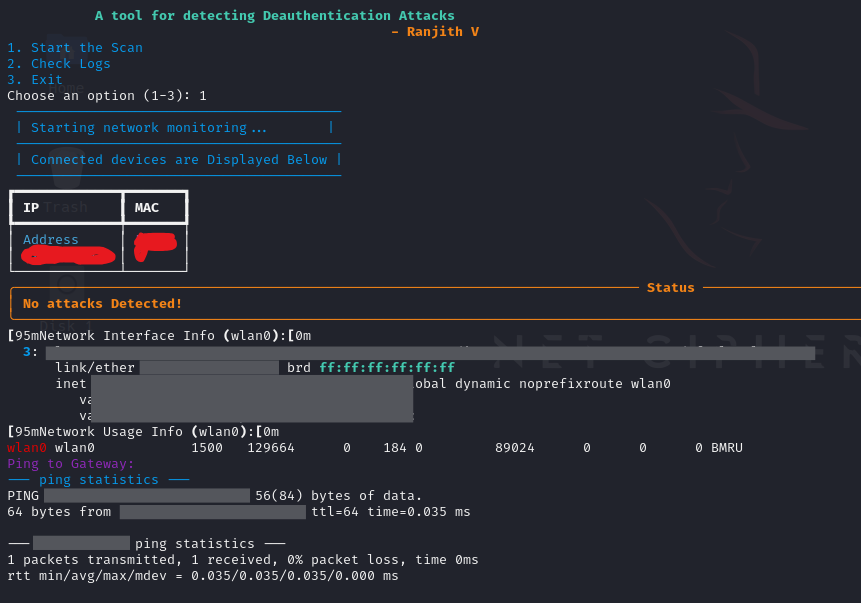
.

Set-Up for Your IP Address

Enter your Gateway IP address in these fields:



EXAMPLE OUTPUT



The example output shows a list of connected devices with their IP and MAC addresses. If a Deauthentication attack is detected, it alerts with "Deauthentication attack detected!" It also displays network interface details and logs attack events for future reference.

SECURITY CONSIDERATIONS

When using the **Deauthentication Attack Detector**, ensure the tool is run on a trusted network to avoid unauthorized monitoring. Always keep the system and dependencies up to date to prevent vulnerabilities. Be aware that running this tool on a network without permission could be considered illegal or unethical. It is important to use it only for educational purposes or on networks you own or have explicit consent to monitor.

### **Disclaimer**

I will not be responsible for any unauthorized or illegal activities conducted using this tool. It is intended solely for educational purposes and should only be used on networks you own or have explicit permission to monitor. Using this tool without proper authorization may violate laws or ethical guidelines. Please ensure you have permission before using it on any network.

CONCLUSION

The **Deauthentication Attack Detector** is a useful tool for monitoring wireless networks and detecting potential deauthentication attacks. By tracking connected devices and identifying unusual disconnections, it helps enhance network security. This project demonstrates the application of Python in cybersecurity and provides a practical solution for network administrators to detect and respond to attacks.