**Wifi Jammer by Ziyuan Chen – Documentation**

**Principle of Operation**

The WiFi jammer script utilizes a vulnerability of the 802.11 protocol that all connected interfaces, no matter authenticated to a network or not, can disguise themselves as access points/clients and send a specific frame to clients/APs to tell them that the clients have been de-authenticated from the network. Also, it is possible to disguise the attacker as a client and tell the access point that it wants to de-authenticate. By sending these two types of frames repeatedly to all clients connected to a Wi-Fi access point, the script is able to make the access point unusable.

**Programming**

The script is written in Python. The Scapy library is used extensively to intercept wireless packets flying in the air.

**Program Flow**

The script first scans for available wireless interface(s) installed on the host machine. If none is available, the script returns an error.

The script then turns on the monitor mode of the wireless interface. If multiple wireless interfaces exist, the first wireless interface is chosen by default. If the interface does not support monitor mode, the script reports an error. If none of the detected interfaces can be used as wireless monitors, the script exits with an error.

The script then uses the wireless interface to monitor wireless traffic in the range in order to find available access points’ MAC IDs and SSIDs. It also finds the corresponding clients connected to these access points. It then lists all unique SSIDs found and prompts the user to enter the specific network(s) he or she would like to jam.

The script then sends out the de-authentication frames as mentioned before. This process is done repeatedly in an infinite loop, resulting in WiFi jamming in the range of the wireless interface.

**Limitations**

Some functionalities such as turning on the monitor mode on Wi-Fi card relies on Unix commands so the script can only work on a Unix-based operating system.

The script cannot jam networks whose SSIDs are hidden, such as vummiv.

The effectiveness, range, and number of access points that can be jammed depend on the capability of the wireless card.

It requires a very strong wireless card and sufficient scan time to be able to discover all wireless APs/clients within range.

**Problems Encountered and Future Improvements**

Given the current implementation, the script cannot de-authenticate a client that connects to the targeted network(s) after the jamming starts. Because of technical difficulty, multithreading, which can solve this problem, was not implemented.