wifiDisco Documentation

Overview

`wifiDisco.py` is a Python script that utilizes the Scapy module to perform various wireless security features, including sniffing for Wi-Fi networks and performing Deauthentication (Deauth) attacks on specific clients connected to a detected network.

Prerequisites

- **Python 3.x**: Ensure you have Python 3.x installed.
- **Scapy**: Install Scapy using `pip install scapy`.
- **Root Privileges**: The script requires root privileges to execute.

Usage

To use the script, you need to specify the network interface you want to use for sniffing and packet injection.

```
sudo python wifiDisco.py -i <interface>
```

Replace `<interface>` with your wireless network interface name (e.g., `wlan0`).

Command-line Arguments

- `-i`, `--interface`: The network interface to use for sniffing and packet injection. This argument is required.

Example

```
sudo python wifiDisco.py -i wlan0
```

Script Workflow

1. **Initialization**:
   - The script starts by parsing command-line arguments to get the network interface.
   - It sets up the Scapy configuration to use the specified interface.
   - A dictionary `networks` is initialized to store detected networks.
2. **Channel Hopping**:
   - The script starts a separate process (`channel_hop`) to continuously change the wireless channel of the interface to discover networks on different channels.
3. **Sniffing for Networks**:
   - The script uses Scapy's `sniff` function to capture Wi-Fi Beacon and Probe Response frames, extracting information about available networks.
   - Detected networks are displayed in a table format showing the channel, ESSID, and BSSID.

4. **Stopping the Sniffing**:
    - The script listens for a `CTRL+C` signal to stop sniffing and channel hopping.
5. **Deauthentication Attack**:
    - After stopping the sniffing process, the user is prompted to enter the BSSID of the target network for the Deauth attack.
    - The user can also specify the MAC address of a specific client to target (default is to target all clients).
    - The user can specify the number of Deauth packets to send (default is continuous).
6. **Performing the Deauth Attack**:
    - The script sends Deauth packets to disconnect the specified client (or all clients) from the target BSSID.

Functions

1. **channel_hopper(interface)**:
    - Continuously changes the wireless channel of the specified interface to discover networks on different channels.
2. **stop_channel_hop(signal, frame)**:
    - Signal handler to stop the channel hopping process.
3. **add_network(pkt, known_networks)**:
    - Extracts network information from captured packets and adds it to the known networks dictionary.
4. **keep_sniffing(pkt)**:
    - Returns a boolean to control the sniffing process based on the global `stop_sniffing` flag.
5. **perform_deauth(bssid, client, count)**:
    - Sends Deauth packets to disconnect the specified client (or all clients) from the target BSSID.

Example Output

```
text
Copy code
Press CTRL+C to stop sniffing...
=============================================================================
=======================
Channel ESSID                          BSSID
=============================================================================
=======================
6      MyNetwork                       00:14:22:01:23:45
11     AnotherNetwork                  00:25:9c:cf:1c:ac
```

User Interaction

After stopping the sniffing process, you will be prompted to enter the BSSID of the network you want to target and the client MAC address (if any). You can also specify the number of Deauth packets to send.

```
Enter a BSSID to perform a deauth attack (q to quit): 00:14:22:01:23:45
Changing wlan0 to channel 6
Enter a client MAC address (Default: FF:FF:FF:FF:FF:FF):
Enter the number of deauth packets (Default: -1 [constant]):
Sending Deauth to FF:FF:FF:FF:FF:FF from 00:14:22:01:23:45
Press CTRL+C to quit
```

Important Notes

- **Ethical Use**: Use this script responsibly and only on networks you own or have explicit permission to test.
- **Legal Considerations**: Unauthorized use of this script can be illegal and is considered malicious activity. Ensure you comply with local laws and regulations.

This documentation should help you understand and use the `wifiDisco.py` script effectively.