Documentation for wifiDico.py

Created by Walt D. on 20Jul24

Overview

`wifiDico.py` is a Python script that scans for wireless networks and performs a deauthentication (deauth) attack on a selected network's clients. The script utilizes the Scapy library to handle packet manipulation and the threading library to manage concurrent tasks. The purpose of this tool is for educational purposes and authorized security testing only.

Prerequisites

- **Kali Linux**: The script is designed to run on Kali Linux.
- **Python 3**: Ensure Python 3 is installed.
- **Scapy**: Install Scapy if not already installed:

```
sudo apt-get install python3-scapy
```

Setting Up Monitor Mode with airmon-ng (already installed in Kali Linux)

1. **List wireless interfaces:**

   ```
   sudo airmon-ng
   ```

2. **Stop any conflicting processes:**

   ```
   sudo airmon-ng check kill
   ```

3. **Enable monitor mode on your wireless interface:**

   ```
   sudo airmon-ng start wlan0
   ```
   (replace `wlan0` with your interface name**)**

4. **Verify that the interface is in monitor mode:**

   ```
   iwconfig
   ```

   Your interface should now be something like `wlan0mon`.

Running wifiDico.py

1. **Download and execute the script:**

   ```
   sudo python3 wifiDico.py -i wlan0mon
   ```

2. **Script Interaction:**

- **Initial Network Scanning:** The script will start by scanning for wireless networks for a set duration (default is 2 minutes).

  ```
  Sniffing for 2 minutes...
  ================================================================
  ==================================
  Channel     ESSID                         BSSID
  ================================================================
  ==================================
  1           ExampleNetwork1               AA:BB:CC:DD:EE:FF
  6           ExampleNetwork2               11:22:33:44:55:66
  ...
  ```

- **Select a Network:** After the scanning period, you will be prompted to select a network by entering the corresponding number:

  ```
  Select a network by number to perform a deauth attack (0 to
  quit):
  ```

- **Client Scanning:** Once a network is selected, the script will change the wireless interface to the channel of the selected network and start scanning for clients connected to that network. Detected clients will be printed as they are found:

  ```
  Client XX:XX:XX:XX:XX:XX detected on BSSID AA:BB:CC:DD:EE:FF
  ```

  To stop client scanning, press `Ctrl-C`.

- **Perform Deauth Attack:** If clients are found, you will be asked if you want to perform a continuous deauth attack:

  ```
  Perform continuous deauth attack? (y/n):
  ```

- **Deauth Attack Execution:**
  - If you choose `y`, the deauth attack will continue indefinitely until you press `Ctrl-C`.
  - If you choose `n`, a single round of deauth packets will be sent to the clients.

Detailed Code Walkthrough

The script consists of several key components:

1. **Imports and Setup:**
   - Import necessary libraries.
   - Suppress Scapy runtime warnings.
2. **Global Variables:**
   - `stop_event`: Controls the stopping of the channel hopper and sniffing.
   - `stop_sniffing`: Boolean flag to control sniffing.

3. **Channel Hopper:**
    - A function to randomly hop channels every 5 seconds to discover networks on different channels. Since we're in the us, limited to 1-13. But, adjustable.
4. **Network and Client Addition Functions:**
    - Functions to add discovered networks and clients to dictionaries and print them.
5. **Deauth Attack Function:**
    - A function to send deauthentication packets to clients.
6. **Main Execution:**
    - Argument parsing to get the wireless interface.
    - Initial network scanning for a set duration.
    - User prompt to select a network.
    - Client scanning for the selected network.
    - Prompt for deauth attack and execution.

Example Usage

```
# Enable monitor mode
sudo airmon-ng start wlan0

# Run the script
sudo python3 wifiDico.py -i wlan0mon

# Follow the prompts in the script to select a network and perform the deauth
attack
```

Notes

- **Educational and Authorized Use Only:** This tool is for educational purposes and authorized testing only. Unauthorized use is illegal.
- **Adjust Scanning Time:** You can adjust the initial scanning time by modifying the `dSniffTime` variable in the script.