Winner of HackUMass VII Best Security Hack!

AWSY (Are We Secure Yet?)

AWSY collects and mines data from BSSIDs to reveal what we have forgotten about WiFi security.

Overview

AWSY aims to reveal the insecurity of public space. It uses captured BSSIDs and multiple APIs to effectively mine potentially personal information. It is written in Python with supporting modules in Golang.

How it works

There are four main queries made in AWSY:

1. WiGLE.net/GoogleAPI can determine the **latitude and longitude** from a given BSSID.
2. GoogleAPI can use the latitude and longitude data to determine the **address** of the coordinates.
3. ZillowAPI can use the **address** to determine whether or not the property is a household.
4. EkataAPI can use the **address** to mine the **names, historical addresses, phone numbers, associated people, and more about the residents.**

Usage

First the WiFi card must be put into monitor mode. (The RTL8812AU chipset is most commonly used for these purposes.)

```
ip a
```

Find your WiFi cards interface

```
airmon-ng start [interface]
```

This will put the card in monitor mode, it requires sudo permissions.

```
airodump-ng -w data --output-format csv [monitor mode interface]
```

This will start the capture process, note that it will store it in a csv format. Sudo permissions are required.

```
python AWSY.py <bssid>
```

Note that the bssid is given in the form `AAAAAAAAAA` without any colons. It is not case sensitive.

Requirements

Linux software - `aircrack-ng`

Python packages - `pyzillow` - `pandas` - `geopy` - `pygle`

API keys

1. Locator.py

- `Zillow`
- `Google`

2. PyGLE configuration file

- `WiGLE`

3. ReverseAddressLookup.py

- `Ekata`