**Introduction to Airgeddon**

Airgeddon is a Linux command line tool. It is commonly used on the Kali Linux Operating system but is compatible with many Linux distributions. It uses a multi-purpose bash script to perform audits and security assessments of wireless networks. Airgeddon has 26 key features, making this tool a must-have for both offensive and defensive security professionals. For this lab, we will be focusing on WEP encryption cracking.

**How to download, install, use Airgeddon**

Airgeddon will have to be install on your Linux machine. It requires some dependencies to work properly but these are pre-installed on Kali Linux. The script will not work if aircrack-ng, iproute2, procps, bash, iw, tmux, gawk, pciutils and xterm are not installed. It is hosted on GitHub, with the easiest installation method being in the command line. Open the terminal and enter *$ git clone --depth 1* [*https://github.com/v1s1t0r1sh3r3/airgeddon.git*](https://github.com/v1s1t0r1sh3r3/airgeddon.git). This method pulls the GitHub repo to your machine and creates a new directory in one step. Navigate to the created directory with $ cd airgeddon. Now run the program with root permissions *$ sudo bash airgeddon.sh*

**Tools needed to perform the attack**

Virtual machine – Kali Linux

Wireless network adapter with a chipset that supports of packet injection and monitor mode.

A vulnerable wireless network using WEP encryption

Airodump-NG

Besside-NG

**Airgeddon Attack**

Open a Kali Linux terminal window and plug in the wireless network adapter. We must locate the name of the adapter by typing $ if config. Locating any wi-fi connections using WEP is next, run command $ airodump-ng wlan1 –encrypt wep. Wlan1 is an example and should be change to the name of the wi-fi adapter. Note the channel number and mac address (BSSID) for the wep encryption. Now startup Besside ng, enter $ besside-ng wlan1 -c (channel number) -b (mac address). Besside-ng then selects the network to be attacked.

Text

Description automatically generated

Text

Description automatically generated

**Attack results**

**D**

**References:**

[**https://github.com/v1s1t0r1sh3r3/airgeddon/wiki**](https://github.com/v1s1t0r1sh3r3/airgeddon/wiki)

[**https://www.kali.org/tools/airgeddon/**](https://www.kali.org/tools/airgeddon/)

**https://kalitut.com/the-easiest-way-to-hack-wifi/**