**evil twin**

**Introduction:**

**Our project represent an evil twin attack. twin attack is a hack attack in which a hacker sets up a fake Wi-Fi network that looks like a legitimate access point to steal victims’ sensitive details.**

## Requirements:

1. **For this attack you will need 2 Wireless USB Adapter (one of them with monitor mode option) , one for monitor and second one to master.**
2. **Linux OP**
3. [**Kali Linux 2019**](https://rootsh3ll.com/rwsps-installing-and-configuring-kali-linux-ch1pt2/)**(Attacker)**
4. **Airmon-ng, airodump-ng, airbase-ng, and aireplay-ng**
5. **DNSmasq**
6. **Iptables**
7. **Apache, mysql**
8. **python wifi==0.3.8 (for the defense tool)**

## Installing the environment:

**Install *dnsmasq*-**

apt-get update

apt-get install dnsmasq -y

**set the adapter to be in monitor mode:**

ifconfig wlan0 up

airmon-ng start wlan0

note: wlan0 be wlan1, wlan2.. its depend on which adapter you want to put on monitor mode

## defense tool

our suggested to protection against the evil twin attack is a tool that check every few second if there is another access point with the same name(ssid), if so the user will get a warning message with the risk level to be under that evil twin attack- high risk if the second ap is a open ap(without password) and low risk if it a close ap.