Evil Twin Attack

- Last resort to gain access to a WPA/WPA2 network.
- Relies on social engineering.

Idea:

1. Start a fake AP with same name as target network.
2. Disconnect a client.
3. Wait for them to connect to the fake AP.
4. Automatically display a page asking for network key.

Advantage – no need for guessing.

Drawbacks:

1. User have to connect to open fake AP.
2. They have to enter their WPA key in a web page.

Evil Twin Attack

Using Fluxion

Fluxion allow us to run Evil Twin attacks automatically, it will automatically do all of the following:

1. Start a fake AP with the same name as the target network.
2. Start a web server with a fake login page.
3. Disconnect all clients from this network.
4. Display this login page once a client connects to the fake AP
5. Check the entered password and make sure its the correct one.

FLUXION