Lorenzo Comi

Wireless and Mobile Network Project

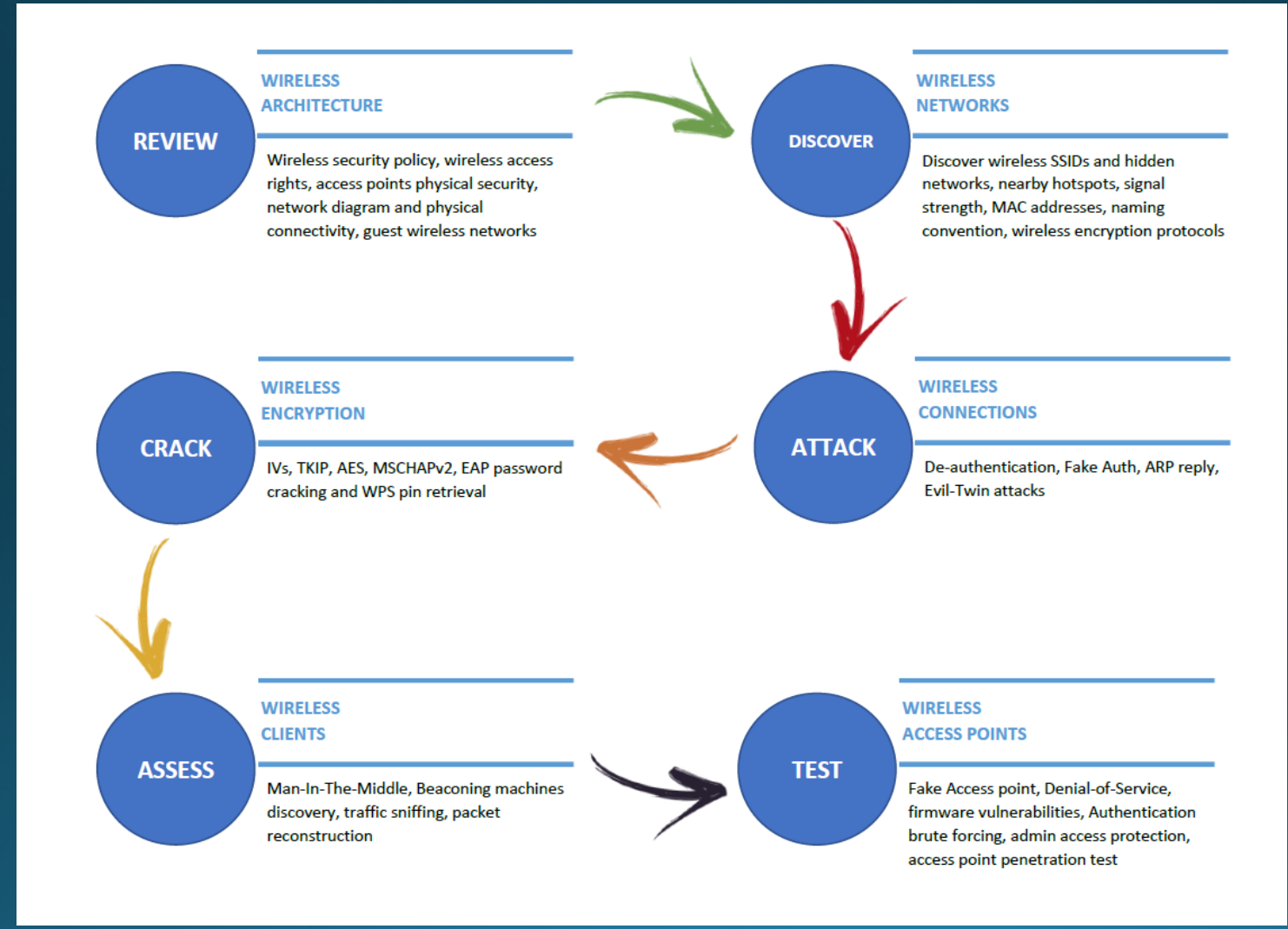
# Wireless Mayhem

# Why… Because I'm a pentester

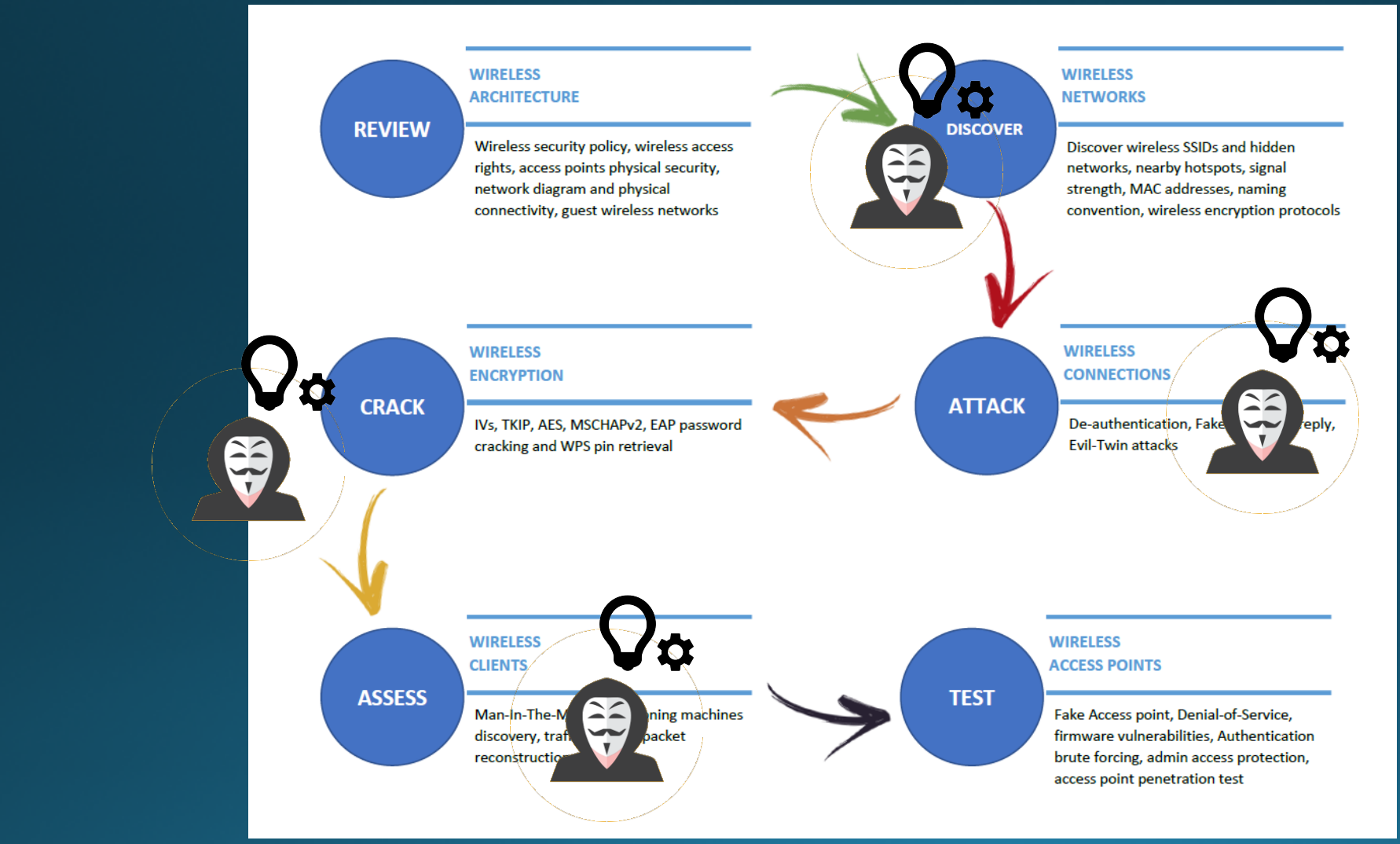
A **pentester** always want to automate all the boring stuff of his job…

Let's try to automate also a **wifi assessment** process!

# Wireless Assessment Workflow



# Wireless Assessment Workflow



# How… With Wireless Mayehm

A Python Framework:

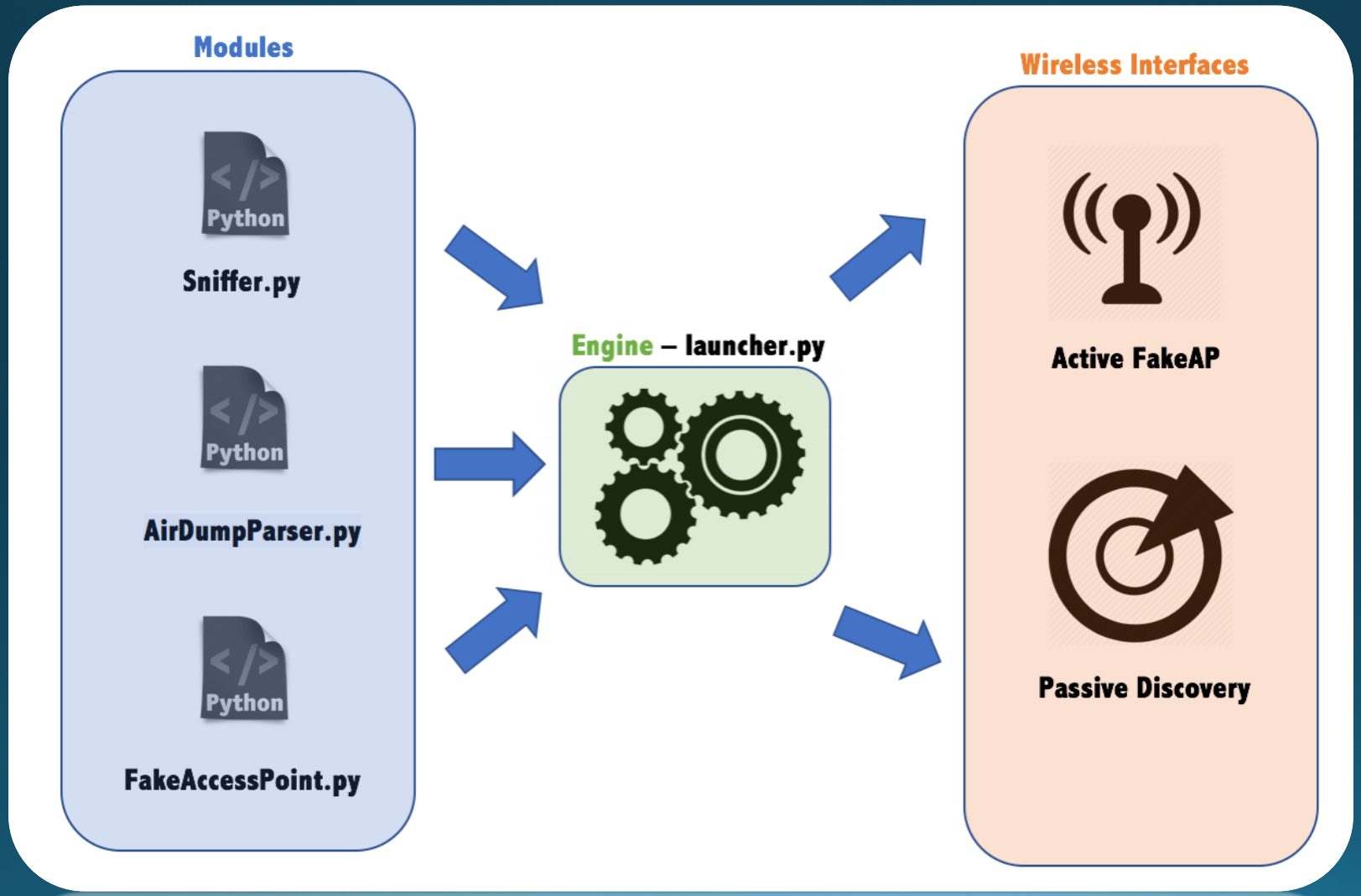
- **Modular**: every feature is a module!
- **Portable**: thanks to python!
- **Expansible & Customizable:** no limit for the expansion of this tool, develop a new module is very simple!

# What it can do


**Main Features**

- **Discover** all the wireless signal around you and prompt a human readable output.
- **Sniff wireless traffic** and intercept sensible data (such as credentials or mail account).
- **Capture password's hashes** by creating a fake access point that simulate an enterprise network ones.

# Architecture



# Demo Discovery


- Put your interface in monitor mode
- Launch the program with sudo privileges
- `$ sudo python laucher.py`
- Digit "1" in order to choose the discovery module
- Insert the name of the monitor mode interface

# Video Demo FTP

WIRELESS MAYEHM

# Video Demo Fake AP

WIRELESS MAYEHM

# Cost Evaluation & Info

WIRELESS MAYEHM

- Source code: IT IS FREE!
  - https://github.com/comix/WirelessMayhem
- TP-link TL-WN722N or an any Wi-Fi antenna with Atheros chipset
  - About 10€ on Amazon

# Future Development


- More modules = More Features
  - Protocol Fuzzing (DoS)
  - Client attack
- Make the code more portable (now works only on linux-based pc)
- Multi-processing and threads management optimization
- Prettify the CLI / develop a GUI

WIRELESS MAYEHM

Lorenzo Comi

Wireless and Mobile Network Project

# ThankYou