Lorenzo Comi

Wireless and Mobile Network Project

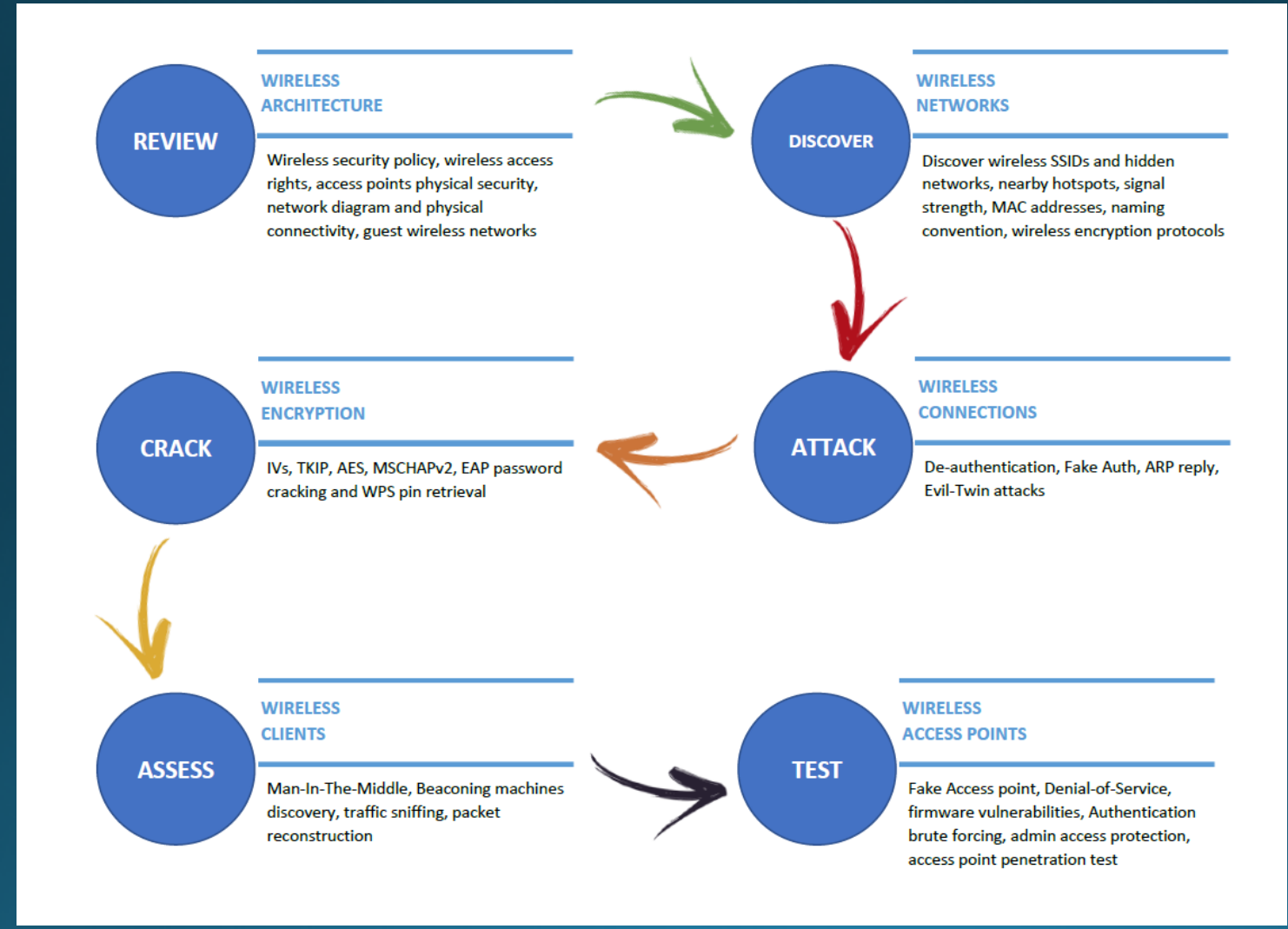
Wireless Mayhem

Why… Because I'm a pentester

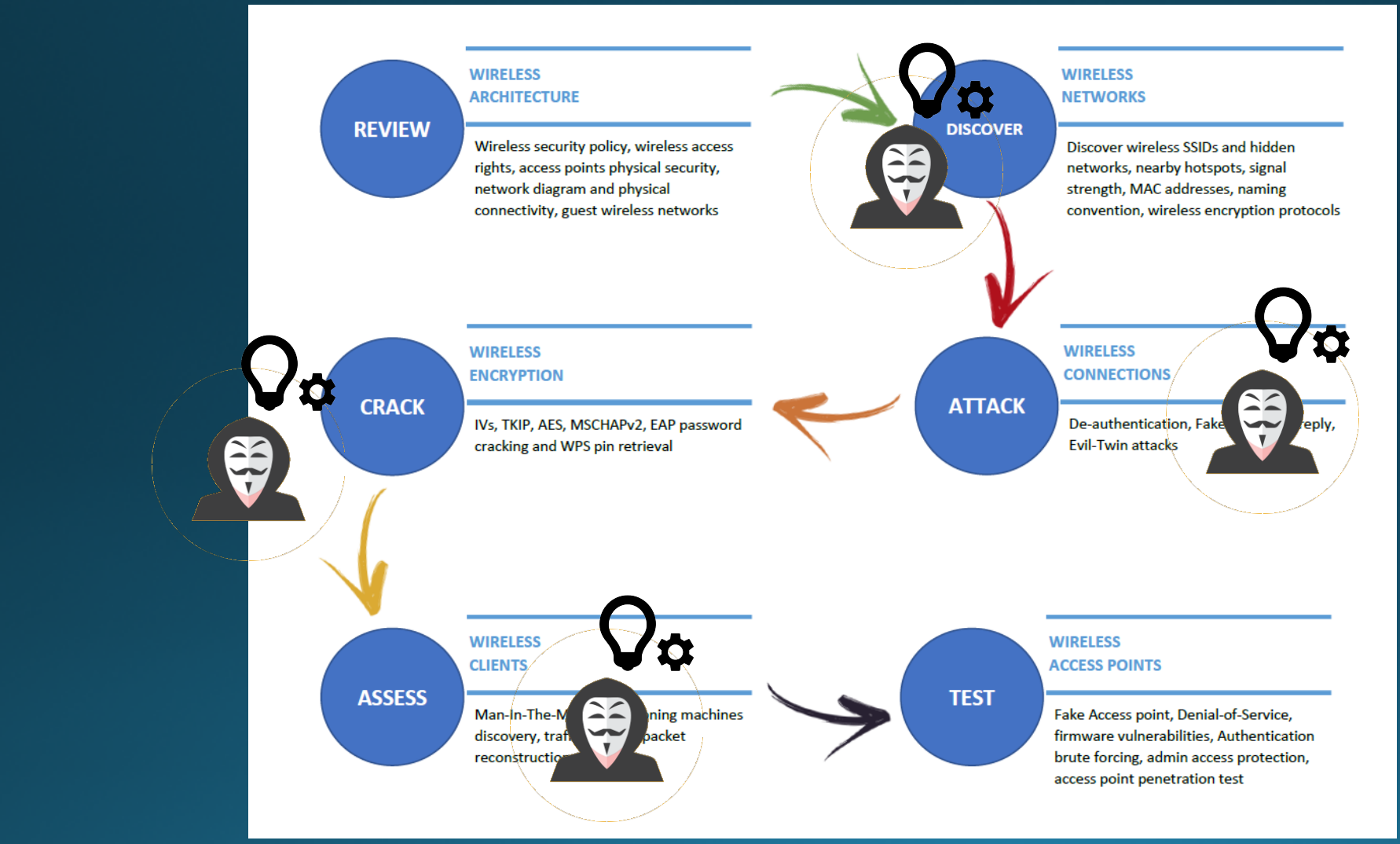
A **pentester** always want to automate all the boring stuff of his job…

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

Wireless Assessment Workflow



Wireless Assessment Workflow



How… With Wireless Mayehm

A Python Framework:

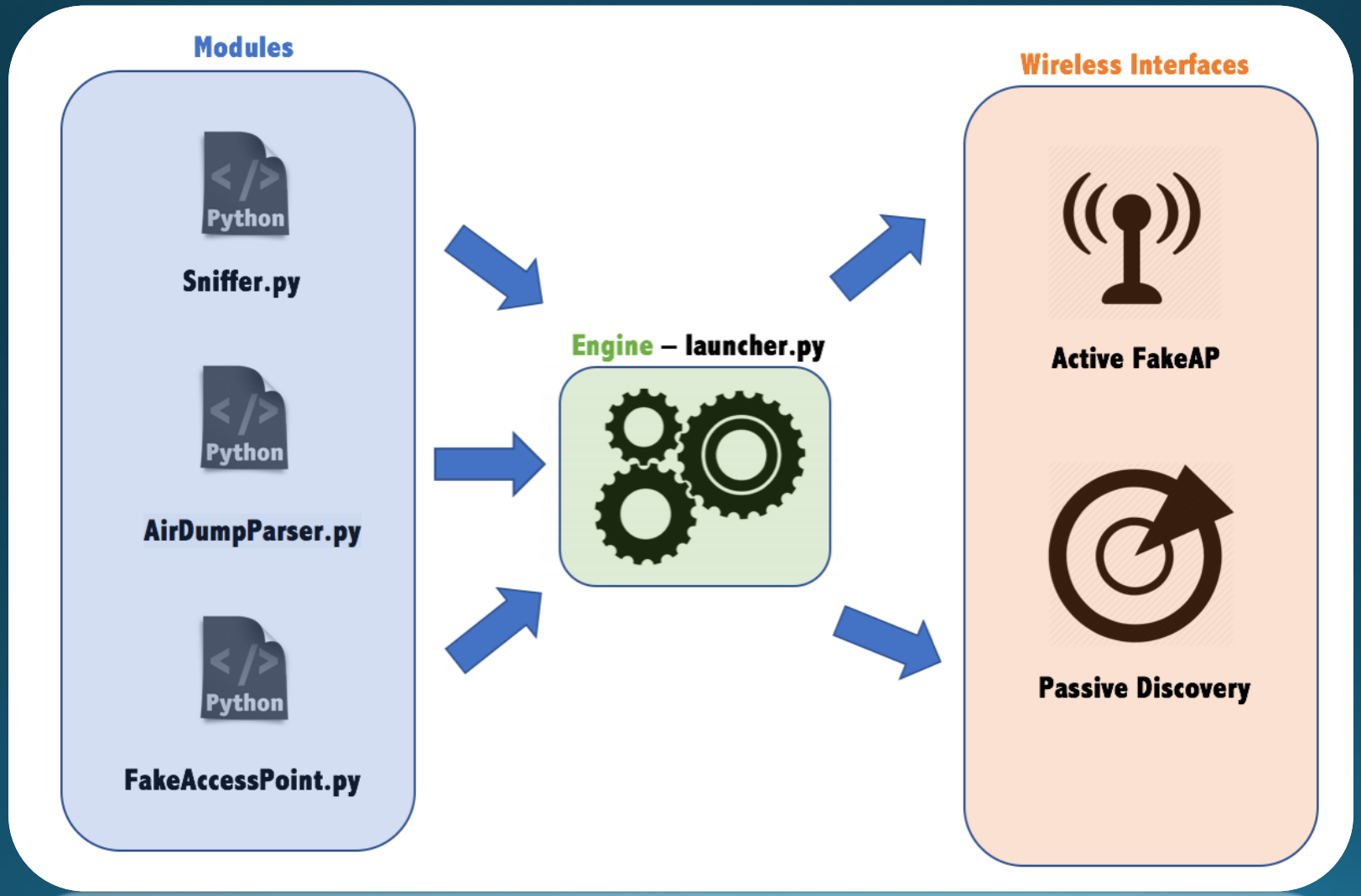
- **Modular**: every feature is a module!
- **Portable**: thanks to python!
- **Expansible & Customizable:** no limit for the expansion of this tool, develop a new module is very simple!

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

1. Put your interface in monitor mode;
2. Launch the program with root privileges;

```
$ sudo python launcher.py
```

3. Digit “1” in order to choose the discovery module;
4. Insert the name of the monitor mode interface;
5. Start intercepting.

Video Demo FTP

WIRELESS MAYEHM

WPA Enterprise

WIRELESS MAYEHM

- WPA/WPA2-Enterprise uses a seperate login ID and password for each person and authenticates them over a RADIUS server.
- An attacker can create a fake access point with the same SSID as the original network and associates a RADIUS server to that access point. Then sends a deauthentication probe or passively waits for clients to connect to fake access point.

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