Lorenzo Comi

Wireless and Mobile Network Project

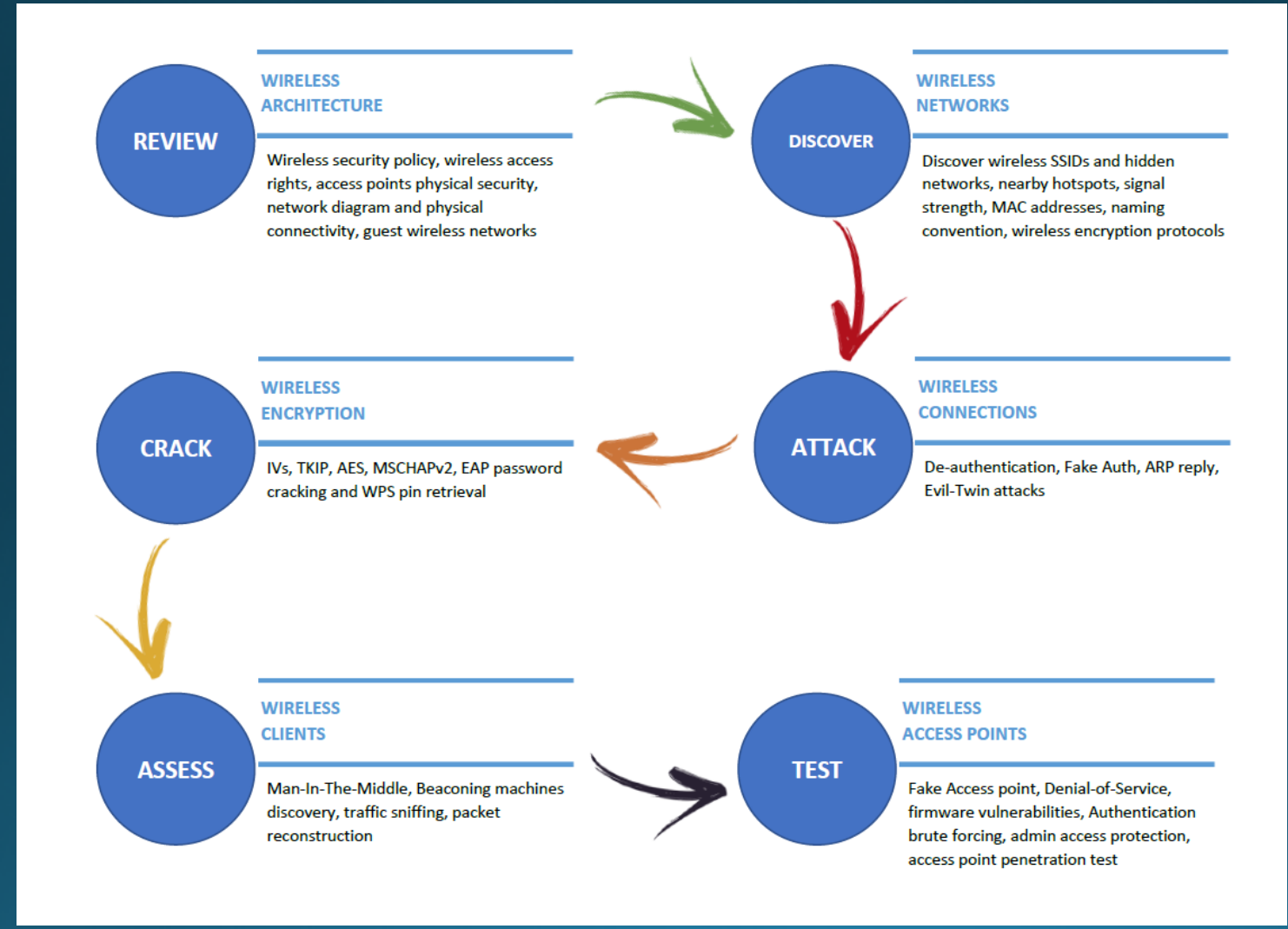
Wireless Mayhem

Why… Because I'm a pentester

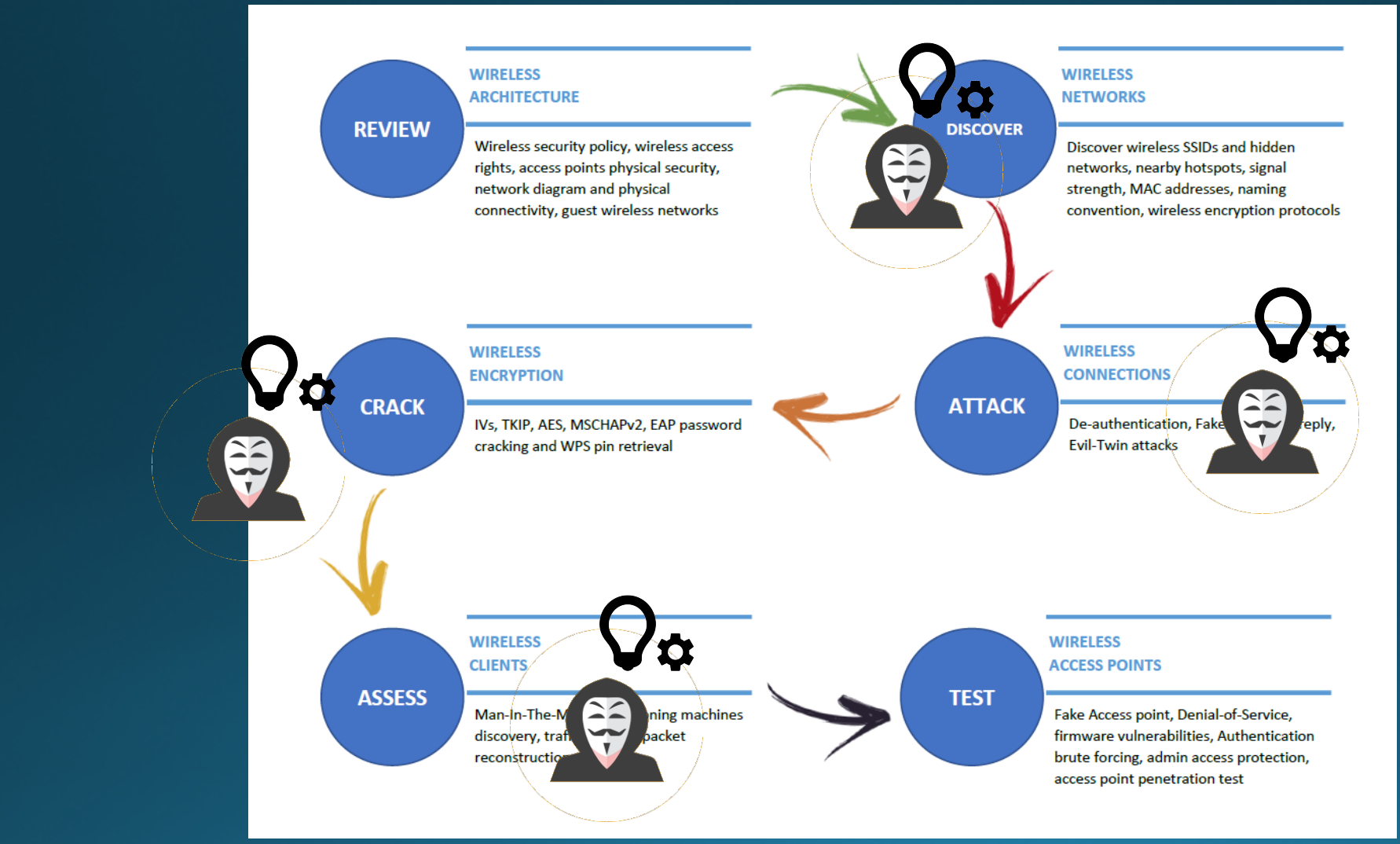
A **pentester** always want to automate all the boring stuff of his job…

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

Wireless Assessment Workflow



Wireless Assessment Workflow



How… With Wireless Mayehm

A Python Framework:

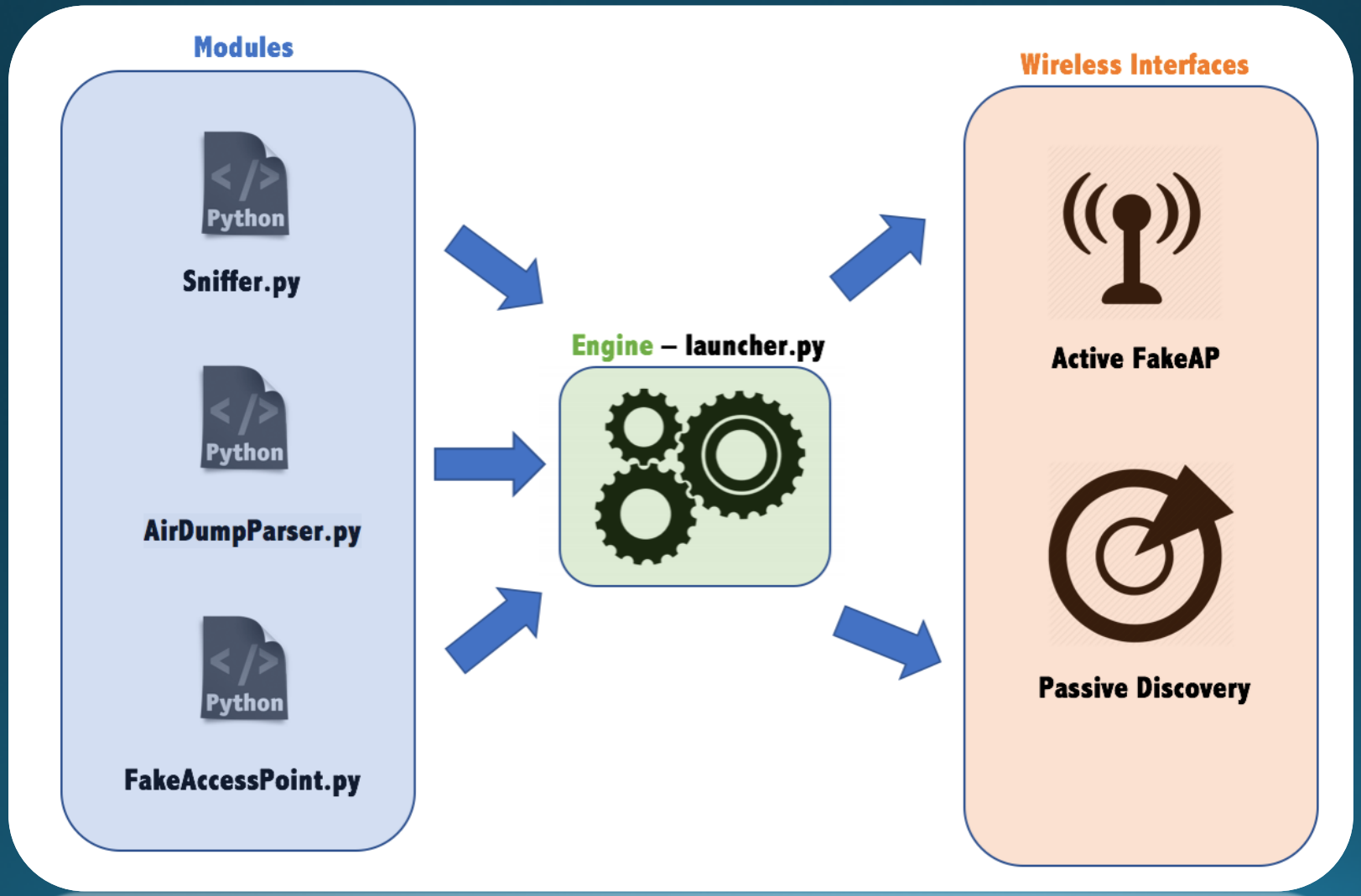
- **Modular**: every feature is a module!
- **Portable**: thanks to python!
- **Expansible & Customizable:** no limit for the expansion of this tool, develop a new module is very simple!

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 passwords hashes** by creating a fake access point that simulate an enterprise network ones.

Architecture



Demo Airodump

1. Put your wireless interface in monitor mode;

   ```
   $ sudo airmon-ng start wlan0
   ```

2. Launch the program with root privileges;

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

3. Digit “5” in order to choose the airodump module;
4. Digit the name of monitor mode interface and choose a filename for the output;
5. Start intercepting.

Demo Airodump

WIRELESS MAYEHM

Demo Airodump


```
CH 12 ][ Elapsed: 6 s ][ 2017-06-02 12:35

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

A4:2B:8C:1C:FA:A5  -67       15       42    0   1  54e. WPA2 CCMP   PSK  ComComWIFI
64:59:F8:BE:F5:DA  -79        3        0    0   4  54e  OPN              Vodafone-WiFi
64:59:F8:BE:F5:D8  -80        4        0    0   4  54e  WPA2 CCMP   PSK  Vodafone-34195397

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

A4:2B:8C:1C:FA:A5  10:1C:0C:6A:75:AE   -1    2e- 0      0        2
A4:2B:8C:1C:FA:A5  00:23:12:0F:81:A0  -25    0 -24e     0        2
A4:2B:8C:1C:FA:A5  CC:FA:00:B5:77:4F  -48    0 - 1      6        2
A4:2B:8C:1C:FA:A5  A0:8D:16:61:A7:EA  -55   48e-54e     1       42
```

Demo Airodump

WIRELESS MAYEHM

```
[INFO] Stop Dumping
[INFO] Analyzing results file: testing-01.csv

[INFO] Access Point Found:
=======================================
Name: Vodafone-34195397
Channel: 4
MAC: 64:59:F8:BE:F5:D8
Encryption: WPA2
Power: -79

=======================================
Name: Vodafone-WiFi
Channel: 4
MAC: 64:59:F8:BE:F5:DA
Encryption: OPN
Power: -79

=======================================
Name: ComComWIFI
Channel: 1
MAC: A4:2B:8C:1C:FA:A5
Encryption: WPA2 WPA
Power: -66

[INFO] Clients Found:
=======================================
Client MAC: A0:8D:16:61:A7:EA
Access Point MAC: A4:2B:8C:1C:FA:A5
Power: -58

=======================================
Client MAC: CC:FA:00:B5:77:4F
Access Point MAC: A4:2B:8C:1C:FA:A5
Power: -45

=======================================
Client MAC: 00:23:12:0F:81:A0
Access Point MAC: A4:2B:8C:1C:FA:A5
Power: -26

=======================================
Client MAC: 10:1C:0C:6A:75:AE
Access Point MAC: A4:2B:8C:1C:FA:A5
Power: -1
```

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