

Initial Access with Aircrack-ng



Ricardo Reimao
CYBER SECURITY CONSULTANT







Founder: Thomas d'Otreppe de Bouvette



A complete suite of tools to assess WiFi network security. Used for monitoring, attacking, testing, and cracking wireless networks.





Open source tool for WiFi security assessments

The most used tool by wireless penetration testers

Available on Kali Linux, Parrot Linux or on Github

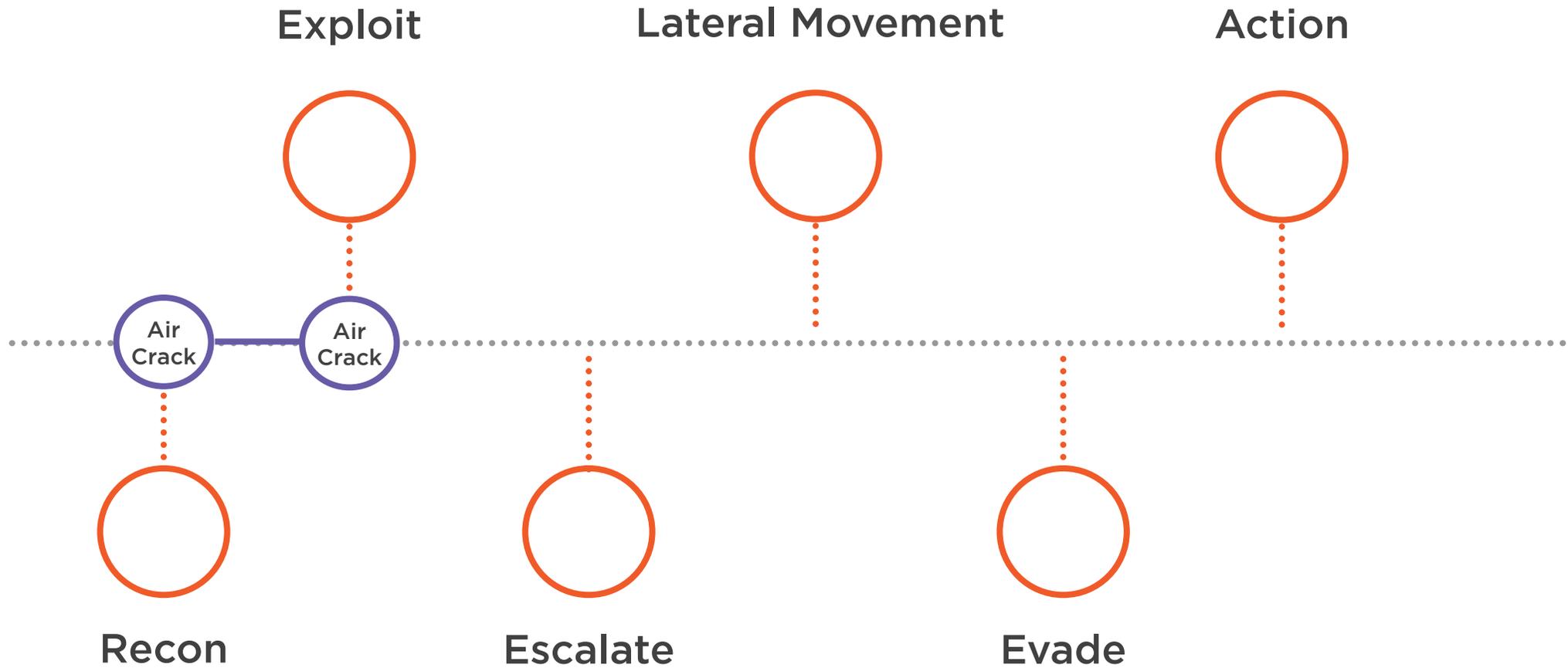
<https://github.com/aircrack-ng/aircrack-ng>

Is able to attack WPE networks as well as WPA and WPA2

Can give you initial access to a company network



Kill Chain



MITRE ATT&CK

Tactics

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command & Control
Exfiltration
Impact



MITRE ATT&CK

Tactics

Initial Access

T1465:

WiFi Access Points

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

T1110:

Brute Force (WPA2)

Discovery

Lateral Movement

Collection

Command & Control

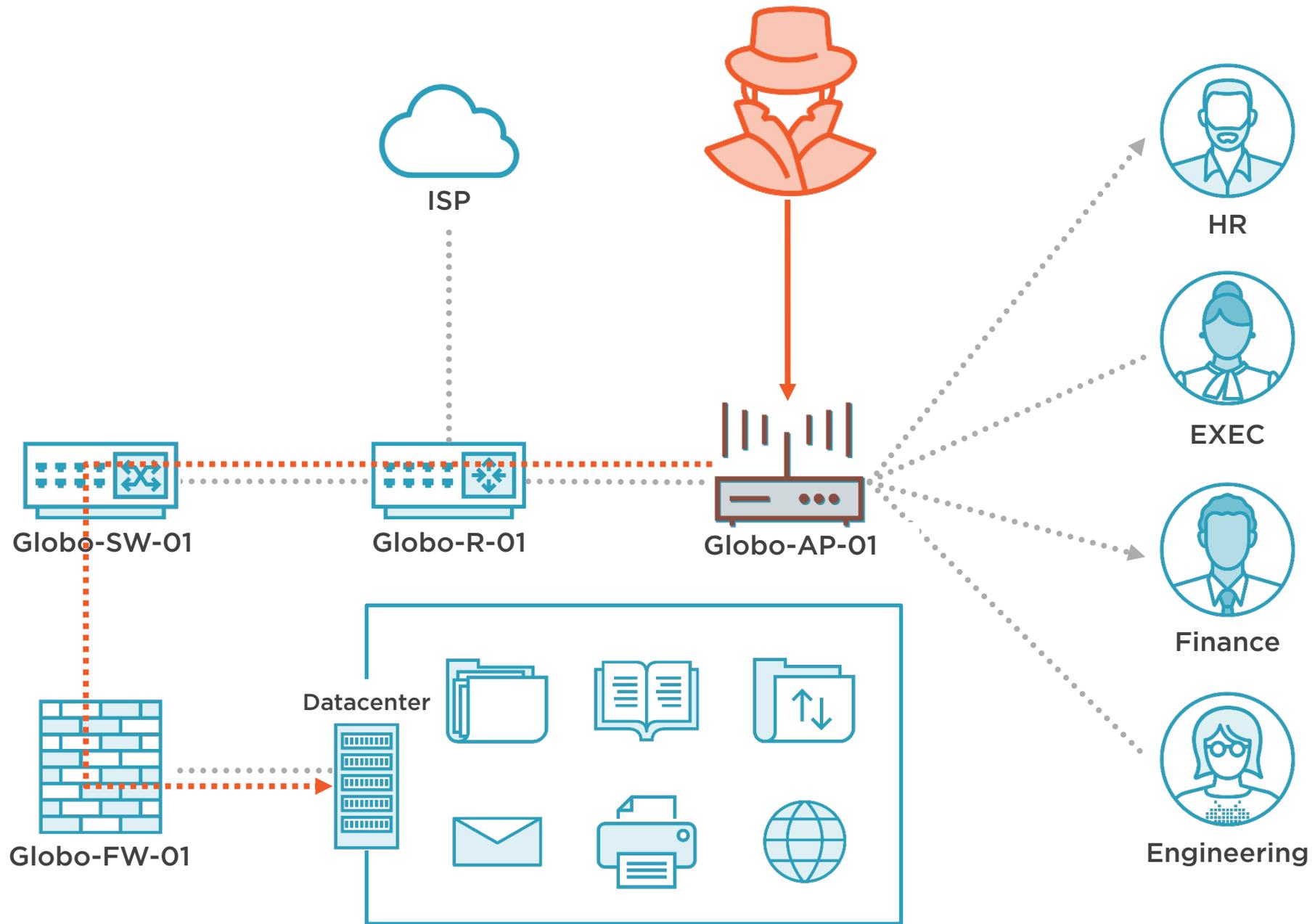
Exfiltration

Impact

T1464:

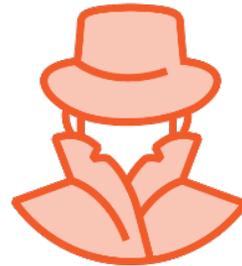
Denial of Service





Staying Legal

Hacking into WiFi networks without authorization is **ILLEGAL** in most of the countries



Letter of engagement, detailing dates and scope of what will be executed

Formal document, signed by the client, authorizing the types of attack you may perform

Always consult the client before any attack that may impact the network



Prerequisites



Kali Linux

Version: 2020.1 or superior

Up to date:

```
$ apt-get update
```

```
$ apt-get upgrade
```



WiFi Network Card

Must support "Monitor Mode"

Suggested models:

- TP-LINK: TL-WN722N

- Alfa: AWUS036NH

