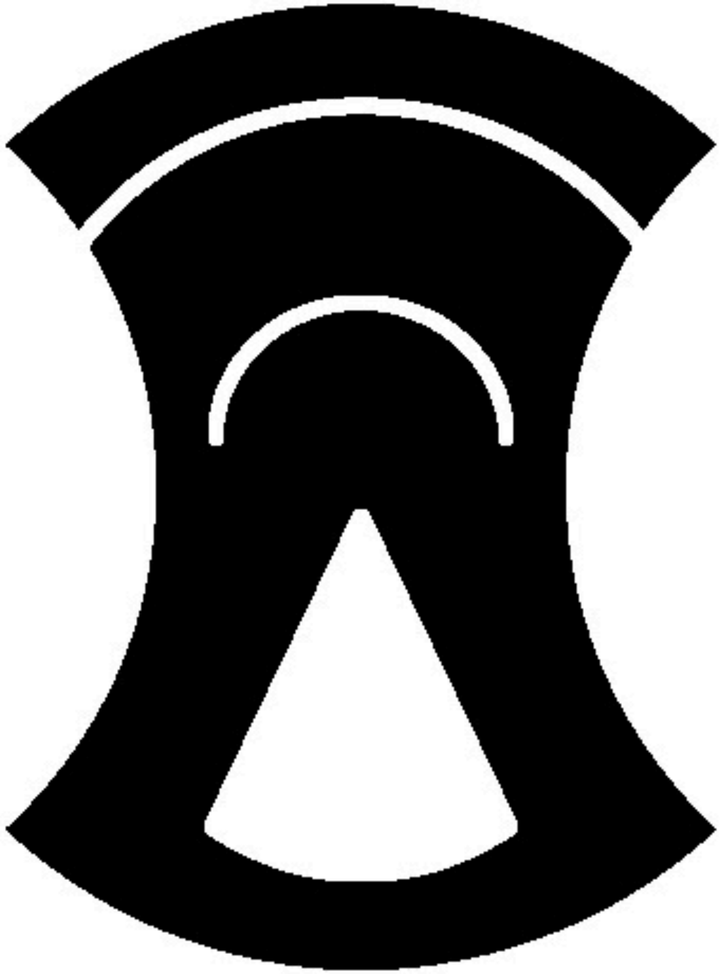
Discovery with Kismet

Guillaume Ross

SECURITY RESEARCHER & PRODUCT MANAGER

@gepeto42 caffeinesecurity.com



Kismet

Creator: Dragon (Mike Kershaw)

Kismet is a wireless network and device detector, sniffer, wardriving tool, and WIDS (wireless intrusion detection) framework.

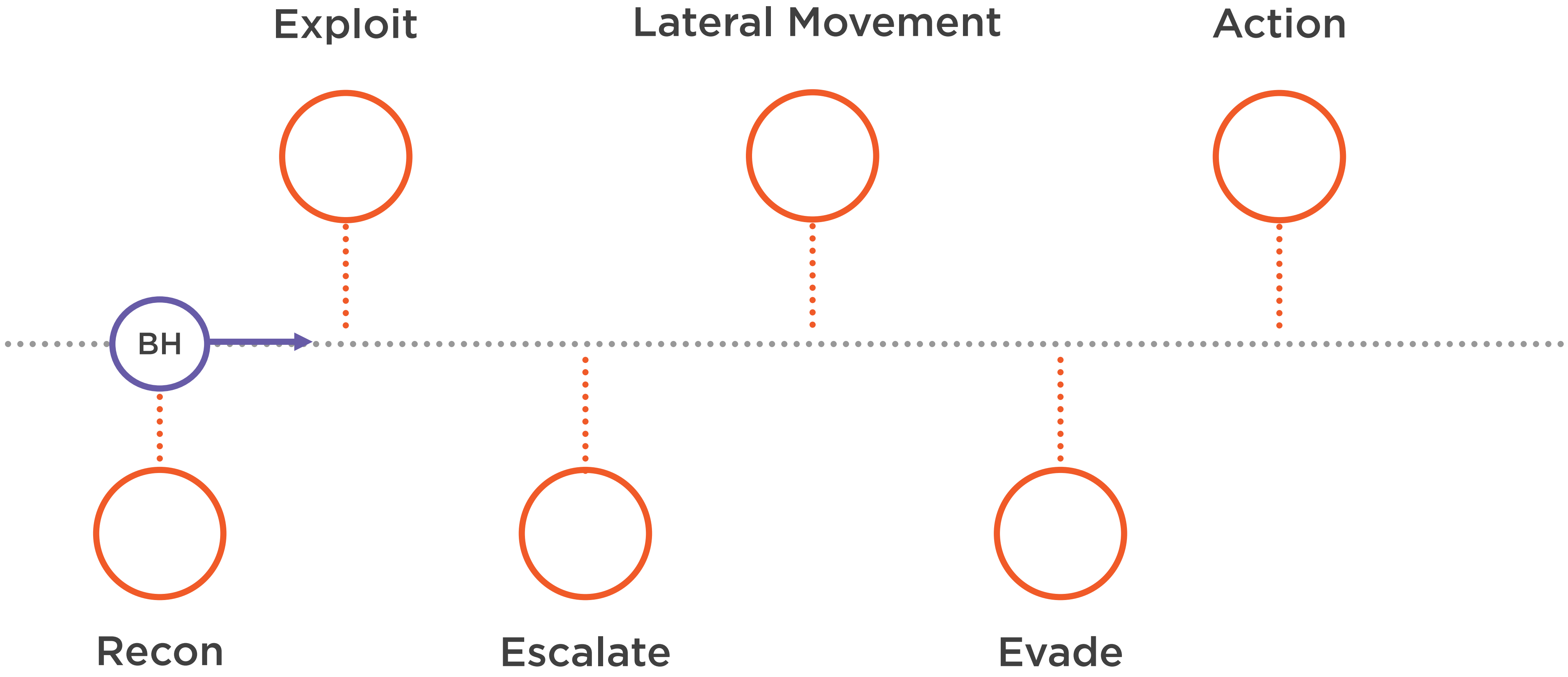
Kismet is a wireless network and device detection tool that allows you to gather information from network names to lists of clients, data being transmitted, and much more.

Available at

https://www.kismetwireless.net/

Not only is it one of the first and best Wi-Fi security tools to be made, it is still actively maintained, and has expanded to support other types of networks.

Kill Chain

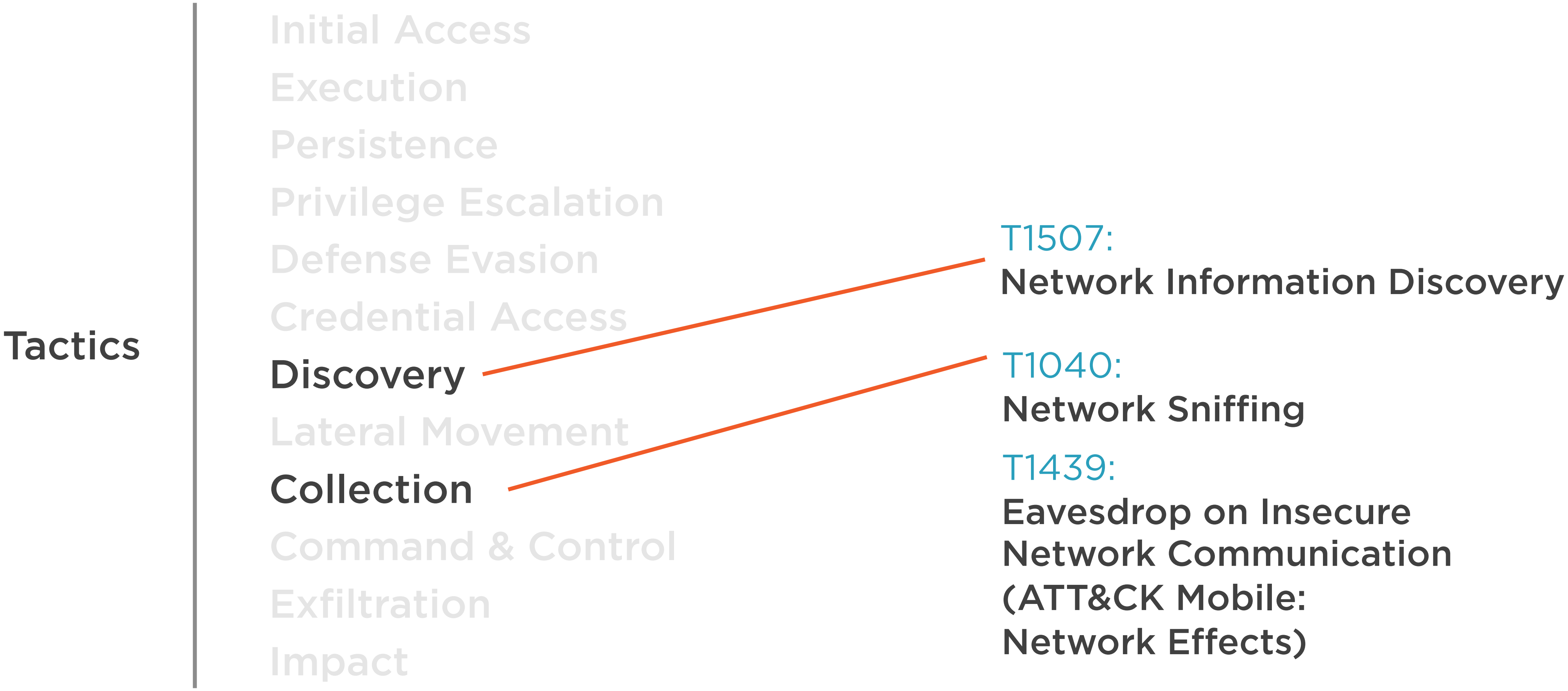


MITRE ATT&CK

Tactics

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

MITRE ATT&CK



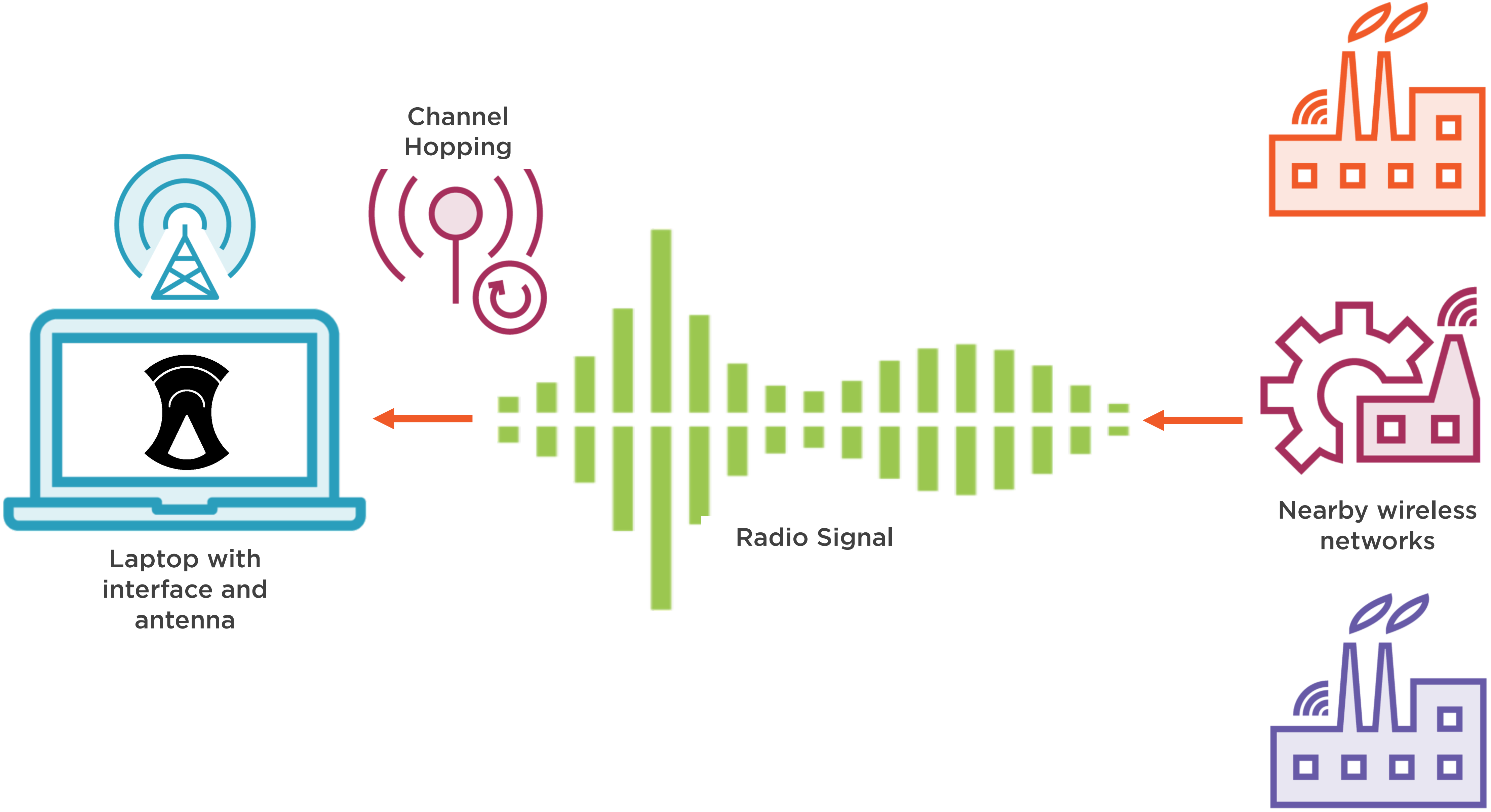
Tactics

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

T1507:
Network Information Discovery

T1040:
Network Sniffing

T1439:
Eavesdrop on Insecure Network Communication (ATT&CK Mobile: Network Effects)


Channel Hopping
Laptop with interface and antenna
Radio Signal
Nearby wireless networks

Prerequisites

Mac / *Win** / Linux Supported

Kali Linux VM suggested for demo

A Wi-Fi adapter compatible with Kismet

Be around some Wi-Fi networks!

Demo Place Holder

1. Installation Tips and Tricks

2. First use instructions & common usage syntax

3. Use of main features on live targets or in live environment

More Information

Capabilities

Remote Packet Capture

https://www.kismetwireless.net/docs/readme/datasources_remote_capture/

GPS Support

https://www.kismetwireless.net/docs/readme/gps/

Related Information

https://www.krackattacks.com

- Attacking WPA2 Networks

Guillaume’s Wireless Security Channel

- Other Pluralsight courses
- Various links
- Updated more frequently