Illustrating the Wireless Attack Methodology

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

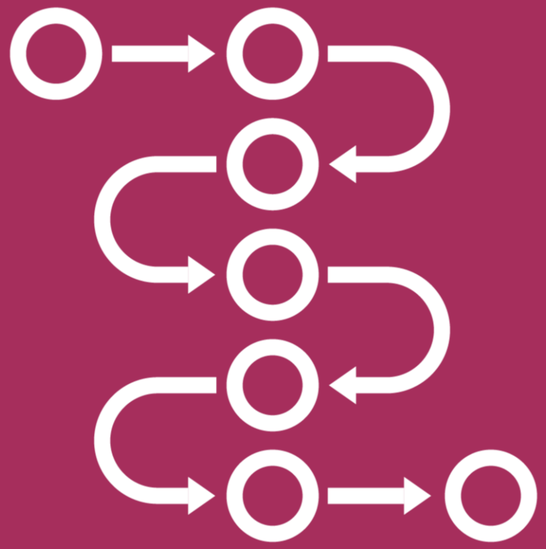
dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

“Methodology gives those with no ideas something to do.”

Mason Cooley

Wi-Fi Discovery

Wi-Fi Discovery



First step

See what's going on

Discovery and footprinting

Understanding the network

Footprinting Methods

Passive Method

Active Method

Applications

inSSIDer	Kismet	WiGLE.net	Chalking
Open source, multi-platform Wi-Fi scanning software	**Network discovery tool to find wireless access points**	**Open platform that collects information on wireless hotspots**	**Visual signs available for all to see**

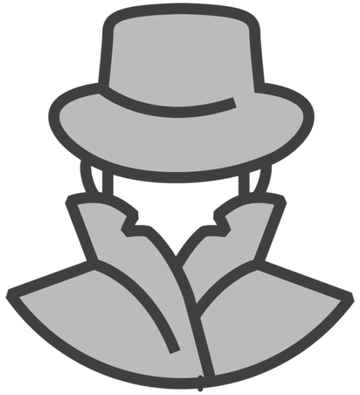
Demo

Finding WPS-enabled AP using Wash

Demo

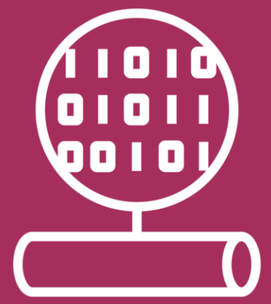
STEP 2: GPS Mapping

Wireless Traffic Analysis



Reconnaissance

SSIDs



Wireless Hacking Tools

- **NetSurveyor and Wi-Fi Scanner**
- **inSSIDer Plus**
- **AirMagnet**
- **Omnipeek**
- **AirSnort**

Choose the right Wi-Fi card

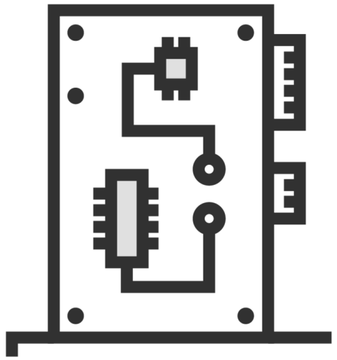
Recognize that the manufacturer of the card may not be the same as the manufacturer of the card's chipset

Identify the right chipset for your needs

Verify the chipset's capabilities

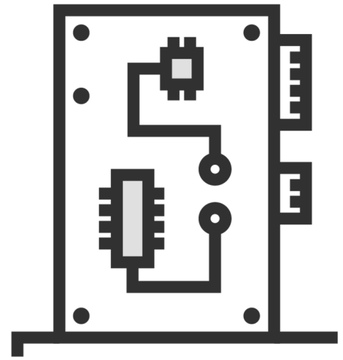
Determine if drivers are available for your chosen chipset

Ensure the card can both listen and inject packets



AirPcap

Sniffs packets and links into Wireshark



Acrylic

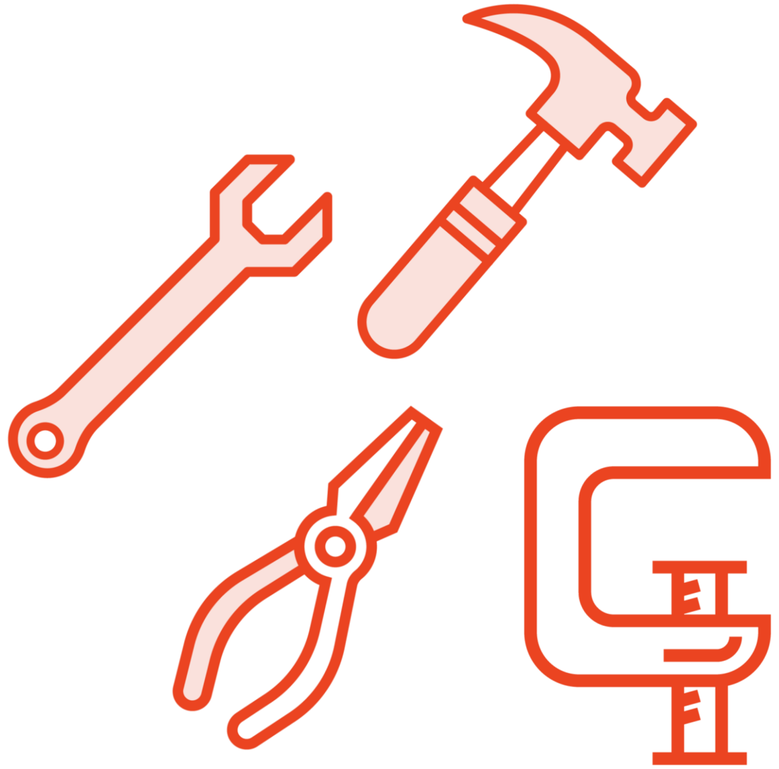
Software that runs on multiple name brand cards

Cain and Abel
Wireshark
Aircrack-ng

Demo

Using your Phone and Wi-Fi Analyzer

Launching an Attack



Aircrack-ng

- **Aircrack-ng**
- **Aireplay-ng**
- **Easside-ng**
- **Airodump-ng**
- **Airmon-ng**

Demo

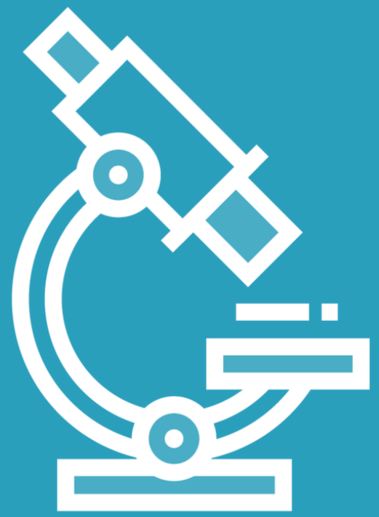
Finding hidden SSIDs with Airodump-ng

The Evil Twin

Evil Twin

A duplicate access point is connected with the same name as a valid access point

After connecting the malicious access point duplicates their information



Undetected

Website accessed

Authentication issues

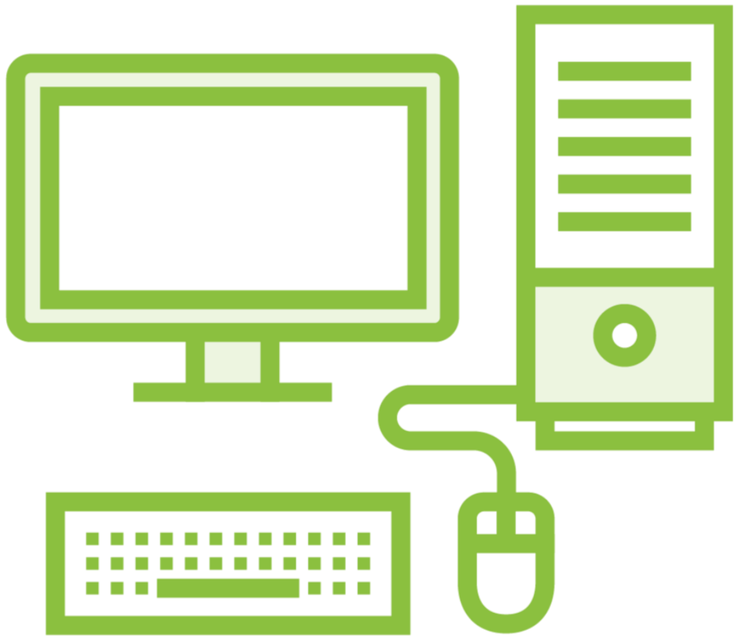
KARMA

Demo

Evil Twin Demo

Wi-Jacking Attack

Wi-Jacking Attack



- Gains control through a wireless connection
- Tricks devices and computers into establishing a false connection with an attacker-controlled computer
- Uses malware and keyloggers to capture information
- Enables hackers to hijack the victim's session

Wi-Jacking Attack

- The attacker must be in close physical proximity to the system
- The target must be connected to an open network
- The target must be using a chromium-based web browser
- The browser must store the admin credentials of the interface
- The target must use a non-encrypted connection to the router interface

Cracking the Encryption

More Cracking Tools

Aircrack-ng

KisMAC

Kali Linux

KillerBee, Blueport, BlueRanger, RedFang, and WiFiHoney

Cain and Abel

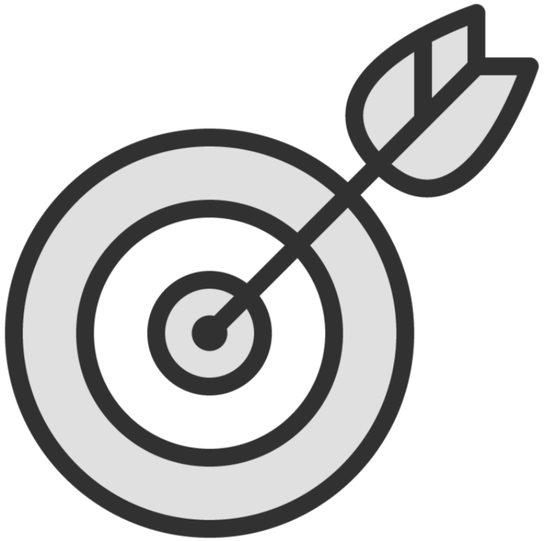
Demo

Cracking WPA with Aircrack-ng

Learning Check

Learning Check

- Passive
- WiGLE.net
- inSSIDer
- AirPcap and Acrylic
- Airodump-ng



Up Next:
Explaining Bluetooth Hacking